DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO EN NUBE PARA LOS SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA KAISE DE TEMPEL PERÚ

INFORME DE ORIGINALIDAD

14%	13%	2%	5%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	Submitted to Universidad Nacional Tecnologica De Lima Sur Trabajo del estudiante	1%
2	dspace.espoch.edu.ec Fuente de Internet	1%
3	repositorio.untels.edu.pe Fuente de Internet	1%
4	www.coursehero.com Fuente de Internet	1%
5	hdl.handle.net Fuente de Internet	<1%
6	learn.microsoft.com Fuente de Internet	<1%
7	repositorio.unprg.edu.pe Fuente de Internet	<1%
8	upc.aws.openrepository.com Fuente de Internet	<1%

UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJOS DE INVESTIGACIÓN EN EL REPOSITORIO INSTITUCIONAL DE LA UNTELS

(Art. 45º de la ley Nº 30220 – Ley)

Autorización de la propiedad intelectual del autor para la publicación de tesis en el Repositorio Institucional de la Universidad Nacional Tecnológica de Lima Sur (https://repositorio.untels.edu.pe), de conformidad con el Decreto Legislativo N° 822, sobre la Ley de los Derechos de Autor, Ley N° 30035 del Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso Abierto, Art. 10º del Rgto. Nacional de Trabajos de Investigación para optar grados académicos y títulos profesionales en las universidades – RENATI Res. N° 084-2022-SUNEDU/CD, publicado en El Peruano el 16 de agosto de 2022; y la RCO N° 061-2023-UNTELS del 01 marzo 2023.

TIPO DE TRABAJO DE INVESTIGACIÓN

1). TESIS ( ) 2). TRABAJO DE SUFICIENCIA PROFESIONAL (x)

DATOS PERSONALES

Apellidos y Nombres:	ZUÑIGA HUAMANI, ANTHONY ADOLFO
D.N.I.:	76530297
Otro Documento:	
Nacionalidad:	PERUANA
Teléfono:	966713315
e-mail:	2013100640@untels.edu.pe

DATOS ACADÉMICOS

Pregrado

Facultad:	FACULTAD DE INGENIERÍA Y GESTIÓN
Programa Académico:	TRABAJO DE SUFICIENCIA PROFESIONAL
Título Profesional otorgado:	INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

Postgrado

Universidad de Procedencia:	
País:	
Grado Académico otorgado:	

Datos de trabajo de investigación

Título:	"DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO EN NUBE PARA LOS SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA KAISE DE TEMPEL PERÚ"
Fecha de Sustentación:	14 DE DICIEMBRE DEL 2024
Calificación:	APROBADO POR UNANIMIDAD
Año de Publicación:	2025

UNTELS | UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

AUTORIZACIÓN DE PUBLICACIÓN EN VERSIÓN ELECTRÓNICA

A través de la presente, autorizo la publicación del texto completo de la tesis, en el Repositorio Institucional de la UNTELS especificando los siguientes términos:

Marcar con una X su elección.

1) Usted otorga una licencia especial para publicación de obras en el REPOSITORIO INSTITUCIONAL DE LA UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR.

Si autorizo X No autorizo _____

2) Usted autoriza para que la obra sea puesta a disposición del público conservando los derechos de autor y para ello se elige el siguiente tipo de acceso.

Derechos de autor		
TIPO DE ACCESO	ATRIBUCIONES DE ACCESO	ELECCIÓN
ACCESO ABIERTO 12.1(*)	**info:eu-repo/semantics/openAccess** (Para documentos en acceso abierto)	(X)

3) Si usted dispone de una **PATENTE** puede elegir el tipo de **ACCESO RESTRINGIDO** como derecho de autor y en el marco de confiabilidad dispuesto por los numerales 5.2 y 6.7 de la directiva Nº 004-2016-CONCYTEC DEGC que regula el Repositorio Nacional Digital de CONCYTEC (Se colgará únicamente datos del autor y el resumen del trabajo de investigación).

Derechos de autor		
TIPO DE ACCESO	ATRIBUCIONES DE ACCESO	ELECCIÓN
ACCESO RESTRINGIDO	**info:eu-repo/semantics/restrictedAccess** (Para documentos restringidos)	( )
	info:eu-repo/semantics/embargoedAccess (Para documentos con períodos de embargo. Se debe especificar las fechas de embargo)	( )
	info:eu-repo/semantics/closedAccess (para documentos confidenciales)	( )

(*) http://renati.sunedu.gob.pe

UNTELS | UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

Rellene la siguiente información si su trabajo de investigación es de acceso restringido:

Atribuciones de acceso restringido:

Motivos de la elección del acceso restringido:

ZUÑIGA HUAMANI ANTHONY ADOLFO

APELLIDOS Y NOMBRES

76530297

DNI

Firma y huella:

Lima, 17 de enero del 2025

UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA Y GESTIÓN
ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

“DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO EN NUBE PARA LOS SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA KAISE DE TEMPEL PERÚ”

TRABAJO DE SUFICIENCIA PROFESIONAL
Para optar el Título Profesional de

INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

PRESENTADO POR EL BACHILLER

ZUÑIGA HUAMANI, ANTHONY ADOLFO
ORCID: 0000-0002-0020-210X

ASESOR
CONTRERAS COSSIO, JORGE LUIS
ORCID: 0000-0001-7801-5833

Villa El Salvador
2024

UNIVERSIDAD NACIONAL
TECNOLÓGICA DE LIMA SUR

ACTA DE SUSTENTACIÓN DE TRABAJO DE SUFICIENCIA PROFESIONAL PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

En Villa El Salvador, siendo las 14:00 horas del día 14 de diciembre del año 2024, reunidos en las instalaciones de la UNTELS, los miembros del Jurado Evaluador, integrado por:

PRESIDENTE: **Mg. Fredy Campos Aguado** ORCID N° 0000-0003-3419-925X Colegiatura N°173769

SECRETARIO: **Mg. Edgard Oporto Díaz** ORCID N° 0000-0003-4019-1860 Colegiatura N° 106881

VOCAL : **Mg. Max Fredi Quispe Aguilar** ORCID N° 0000-0002-4199-0974 Colegiatura N°138642

Nombrados por Resolución de Decanato N° 232-2024, de fecha 12 de diciembre 2024, quienes dan inicio a la Sesión Pública de Sustentación del Trabajo de Suficiencia Profesional.

Acto seguido, el aspirante al Título Profesional de **Ingeniero Electrónico y Telecomunicaciones**
Don (ña): **ANTHONY ADOLFO ZUÑIGA HUAMANI** identificado(a) con D.N.I. N° 76530297; procedió con la Sustentación del Trabajo de Suficiencia Profesional Titulado: **DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO EN NUBE PARA LOS SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA KAISE DE TEMPEL PERÚ**

Autorizado mediante Resolución de Decanato N° 237-2024, de fecha 12 de diciembre de 2024, de conformidad con las disposiciones del Reglamento General para el Otorgamiento de Grado Académico y Título Profesional vigente, sustentó y absolvió las interrogantes que le formularon los señores miembros del Jurado Evaluador.
Concluida la Sustentación se procedió a la evaluación y calificación correspondiente, de acuerdo al **Art. 57°** del Reglamento General para optar el Título Profesional.

CALIFICACIÓN		CONDICIÓN	EQUIVALENCIA
NÚMERO	LETRAS		
16	Dieciseis	Aprobado por unanimidad	Bueno

Siendo las 14:30 del día 14 de diciembre del 2024, se dio por concluido el acto de sustentación, firmando el jurado evaluador el Acta de Sustentación y con firma del sustentante en señal de conformidad.

Mg. Fredy Campos Aguado
PRESIDENTE

Mg. Edgard Oporto Díaz
SECRETARIO

Mg. Max Fredi Quispe Aguilar
VOCAL

ANTHONY ADOLFO ZUÑIGA HUAMANI
SUSTENTANTE

Nota: Artículo 50°. - Para el inicio y desarrollo de la sustentación se requiere la presencia física y permanente de los integrantes del jurado. De faltar algún miembro del jurado, la sustentación procederá con los dos integrantes presentes.
En caso de ausencia del presidente del jurado, ésta será asumida por el jurado de mayor categoría y antigüedad. En caso de ausencia de dos (02) integrantes del jurado, se suspenderá el acto de sustentación, pudiendo reprogramarse dentro de los cinco (05) días hábiles siguientes, sin perjuicio de aplicar el artículo 62° del presente Reglamento.

DEDICATORIA

A mis queridos padres,

Por su amor incondicional, por ser mi guía en cada etapa de mi vida y por inculcarme los valores que han sido fundamentales para alcanzar mis metas.

Por su esfuerzo constante y sacrificios, que me han inspirado a perseverar y dar lo mejor de mí en cada momento.

Este logro es el reflejo de todo lo que me han enseñado y un pequeño tributo a su dedicación y apoyo inquebrantable.

AGRADECIMIENTOS

Agradezco primero a Dios y a mis padres por esta meta que no habría sido posible con el amor y dedicación que me dieron. Valoro mucho las lecciones de vida y el cariño que siempre me han brindado, a mis amigos por su apoyo incondicional y su presencia en los momentos más importantes de mi vida. Mi gratitud hacia todos ellos.

ÍNDICE

LISTADO DE FIGURAS

LISTADO DE TABLAS

RESUMEN

El trabajo consistió en el diseño e implementación de un sistema de monitoreo en la nube para los Sistemas de Alimentación Ininterrumpida (UPS, por sus siglas en ingles Uninterruptible Power Supply) de la marca Kaise, fabricados y distribuidos por Tempel Perú, con el objetivo de mejorar la gestión operativa, mantenimientos, prolongar su vida útil y optimizar la aplicación de garantías. Antes de este proyecto, cada vez que un cliente presentaba una alerta o reporte de falla, el equipo técnico de Tempel debía brindar soporte remoto donde guiaban al cliente para resolver el problema a través de posibilidades de videollamada o accediendo directamente a los sistemas. En muchos casos, era necesario realizar un diagnóstico en las instalaciones del cliente, lo que generaba tiempos de respuesta prolongados y altos gastos operativos. La dependencia de tales acciones también aumentaba el riesgo de que los equipos no estuvieran disponibles por períodos prolongados, comprometiendo así la operatividad del cliente. Esta situación evidencio la necesidad de un sistema que permitiera monitorear los UPS de manera remota y en tiempo real, facilitando la toma de decisiones del equipo de soporte técnico.

El sistema de monitoreo fue diseñado e implementado utilizando la plataforma Zabbix, permitiendo la supervisión remota de múltiples UPS Kaise mediante una interfaz centralizada. La comunicación entre los UPS y la nube se realizó a través del protocolo SNMP (Simple Network Management Protocol), lo que garantizó una transmisión eficiente y segura de datos en tiempo real. El monitoreo incluyó variables críticas como tensión, corriente, temperatura y tiempo de operación, con alertas en tiempo real y acceso a informes históricos. Esto facilitó un mejor seguimiento de los mantenimientos realizados y permitió la revisión del historial del equipo en caso de fallas, ayudando a evaluar la aplicación de garantías.

Los resultados alcanzados tras la implementación del sistema de monitoreo mostraron una reducción del 80% en los tiempos de inactividad y una optimización significativa en la planificación de mantenimientos preventivos, lo que permitió prolongar la vida útil de los equipos en un 43%, entre otras mejoras. A futuro, se contempla la integración de análisis predictivo para anticiparse a posibles fallas y continuar mejorando la eficiencia operativa.

INTRODUCCIÓN

En los últimos años, se proyectó que el mercado de soluciones de monitoreo en la nube experimentaría un crecimiento significativo, alcanzando los 24,5 mil millones de dólares para 2025 (MarketsandMarkets, 2024). El monitoreo en la nube en el sector energético surgió como una herramienta clave para mejorar la eficiencia y la sostenibilidad. Entre los beneficios que ofrecía la nube, destacaban la eficiencia, flexibilidad, impulso a la innovación y control de costos. La adopción de estrategias en la nube mostró una tasa de crecimiento anual compuesto del 21,9% hasta 2025 (IDC, 2022). El sector energético comenzó a apostar por la transición digital, integrando los servicios en la nube como parte del cambio necesario en los paradigmas de producción, distribución y consumo energéticos, impulsados por la sostenibilidad. Una de las principales ventajas asociadas a esta transición fue la reducción de costos, ya que al migrar la infraestructura de servidores a la nube se eliminaban gastos relacionados con la compra y mantenimiento del hardware (Rodero, 2023).

En Perú, la calidad del servicio eléctrico presentó desafíos significativos, especialmente en relación con la continuidad del suministro. En 2021, el 45,3% de los hogares con acceso a energía eléctrica mediante red pública a nivel nacional experimentaron cortes o interrupciones, un aumento de 9,2 puntos porcentuales respecto a 2020 (Instituto Nacional de Estadística e Informática, 2022). Estas interrupciones impactaron negativamente a diversas industrias, afectando su productividad y generando costos adicionales por la necesidad de recurrir a sistemas de respaldo, como generadores o sistemas de alimentación ininterrumpida (UPS, por sus siglas en ingles Uninterruptible Power Supply). Para mitigar este problema, el gobierno impulsó iniciativas para mejorar la infraestructura de transmisión y distribución, además de promover el uso de energías renovables para estabilizar la red y reducir las interrupciones (Ministerio de Energía y Minas, 2015).

Kaise, la marca propia de Tempel Group, se consolidó como un referente en el sector de soluciones de respaldo energético en Perú, ganando posición en el mercado de UPS. En los últimos años, la empresa experimentó un crecimiento sostenido en la fabricación y comercialización de estos equipos. El éxito de la

marca se debió, en gran parte, a la calidad de sus productos y su capacidad para satisfacer las necesidades de diversas industrias, desde pequeñas empresas hasta grandes infraestructuras críticas que requerían un respaldo energético confiable para evitar interrupciones en sus operaciones (Kaise, 2020). Además, el crecimiento de la demanda de UPS en Perú fue impulsado por la necesidad creciente de asegurar la continuidad operativa en un contexto de inestabilidad energética (Lezama, 2024).

En un entorno donde la continuidad operativa siempre ha sido vital, Tempel Group, reafirmando su compromiso con la innovación y la satisfacción de sus clientes, desarrolló un sistema de monitoreo en la nube para los UPS Kaise, utilizando el código abierto de Zabbix. La implementación de software libre, como Zabbix y Nagios, no solo redujo gastos, sino que también permitió identificar problemas y prevenir futuros inconvenientes antes de que afectaran a los usuarios finales (Nagios, 2023; Zabbix, 2023). Esta solución ofreció un valor agregado frente a la competencia, permitiendo a los usuarios supervisar el estado de sus equipos en tiempo real y con ello, se acató con lo recomendado por la norma ANSI/TIA-942, que exigía disponer de un sistema centralizado de UPS, reforzando la posición de liderazgo de Tempel Group en el mercado (ANSI, 2005).

El presente trabajo incluyó los siguientes capítulos: en el capítulo I se desarrolló una descripción del contexto de la empresa, se elaboró la delimitación del proyecto y se definieron los objetivos del trabajo. En el capítulo II, se precisaron los antecedentes nacionales e internacionales utilizados como base para este trabajo y se describieron las bases teóricas del documento. Finalmente, en el capítulo III se realizó el desarrollo del trabajo profesional, en el cual se mencionó la implementación del proyecto y los resultados obtenidos.

CAPÍTULO I. ASPECTOS GENERALES

1.1. Contexto

Tempel Group es una empresa internacional fundada en 1978, que se especializa en soluciones tecnológicas en cuatro áreas principales: Energía, Ingeniería, Consumo y Servicios. A lo largo de su trayectoria, ha ampliado su presencia en países de habla hispano-portuguesa, estableciéndose como un actor clave en los sectores industrial y comercial. Con su sede en Perú, ubicada en Av. Dionisio Derteano 184, San Isidro - Lima, la empresa ha tenido una participación destacada en importantes eventos nacionales, como EXPO SOLAR 2024, donde por tercer año consecutivo ha mostrado sus innovaciones y consolidado su liderazgo en el sector energético (Tempel Group, 2024a).

La misión de Tempel Group es ofrecer un valor agregado a clientes, proveedores, empleados y accionistas, basando su trabajo en la excelencia y la innovación, lo que le otorga una ventaja competitiva en el entorno global (Tempel Group, 2024b).

La visión de la empresa está enfocada en la creación de un mundo más sostenible y saludable, promoviendo soluciones tecnológicas en áreas como Smart Energy, Eficiencia Energética y Smart Engineering. Su estrategia empresarial está alineada con el compromiso hacia la sostenibilidad y la reducción del impacto ambiental, impulsando tecnologías que aumenten la eficiencia operativa mientras minimizan el daño ecológico (Tempel Group, 2024c).

En el ámbito de productos, Tempel Group ha desarrollado su marca Kaise, que ofrece portafolio grande de baterías y sistemas UPS, dirigidos a sectores industriales y mineros. Además, la empresa se especializa en ofrecer diferentes soluciones para el sector eléctrico industrial, cubriendo áreas como almacenamiento de energía, energías renovables, calidad de energía, iluminación LED, confinamiento para Data Center, Sistemas de Refrigeración, etc. Con un equipo técnico altamente cualificado, compuesto en un 35% por ingenieros especializados, Tempel Group destaca por su capacidad de llevar a cabo proyectos energéticos innovadores, manteniendo un firme compromiso con el servicio, la calidad y el avance tecnológico (Tempel Group, 2024d).

1.2. Delimitación del Proyecto temporal y espacial del trabajo

1.2.1. Delimitación Temporal

El desarrollo del proyecto se llevó a cabo desde julio hasta agosto de 2024. Durante julio, se realizó la primera fase, que consistió en la implementación del servidor en la nube. La segunda fase, llevada a cabo en agosto, se centró en la realización de pruebas, lo que permitió el lanzamiento de la versión final del sistema para los clientes.

1.2.2. Delimitación Espacial

El proyecto se ejecutó en las oficinas y laboratorio de Tempel Group, ubicados en la Avenida Dionisio Derteano 184, San Isidro, Lima, Perú. En estas instalaciones se llevaron a cabo la integración de tecnologías y el desarrollo de pruebas necesarias para garantizar el correcto funcionamiento del sistema en nube.

1.3. Objetivos

1.3.1. Objetivo General

Diseñar e implementar un sistema de monitoreo en nube para los Sistemas de Alimentación Ininterrumpida Kaise de Tempel Perú.

1.3.2. Objetivos Específicos

- Diseñar un sistema que permita monitorear los UPS Kaise de Tempel Perú en tiempo real.
- Implementar un sistema que permita monitorear los UPS Kaise de Tempel Perú en tiempo real.
- Validar la funcionalidad del sistema de monitoreo en tiempo real de los UPS Kaise de Tempel Perú.

CAPÍTULO II. MARCO TEÓRICO

2.1. Antecedentes

2.1.1. Antecedentes Nacionales

Bernuy y Villarreal (2023) desarrollaron un sistema de alarmas de monitoreo ambiental para centros de datos utilizando la plataforma Zabbix, y siguiendo normativas reconocidas, como ANSI/TIA-942B, que establece pautas para la infraestructura de telecomunicaciones en centros de datos y normas de la Sociedad Americana de Ingenieros de Calefacción, Refrigeración y Aire Acondicionado para el control ambiental (ASHRAE). Este sistema integró sensores para monitorear temperatura, humedad, vibración y presencia de agua, con el fin de asegurar la integridad de equipos críticos, incluidos servidores y switches. Los resultados validaron la eficacia del sistema, mostrando un tiempo promedio de respuesta ante alertas de 2 segundos, lo cual demostró una rápida detección de condiciones anómalas. Asimismo, el sistema alcanzó una precisión del 95% al 100% en el monitoreo de condiciones ambientales, mejorando significativamente el control del entorno. La implementación incluyó sensores inteligentes y alertas personalizadas en un panel de control (dashboard) y exploró la tolerancia a fallos para garantizar la continuidad operativa. Esta solución optimizó la seguridad y eficiencia del centro de datos, contribuyendo a la robustez de la infraestructura tecnológica de WOW PERÚ.

Enciso (2020) llevó a cabo el estudio Diseño e Implementación de un Sistema de Monitoreo del Centro de Datos para la Red del INICTEL-UNI utilizando Software Libre, enfocado en la implementación de un sistema de monitoreo basado en Zabbix para mejorar la gestión y supervisión de la infraestructura tecnológica del Instituto Nacional de Investigación y Capacitación de Telecomunicaciones de la Universidad Nacional de Ingeniería (INICTEL-UNI). La problemática radicaba en la dependencia de desplazamientos físicos del personal técnico para atender incidencias, tales como fallas de conectividad y problemas con los equipos de red y los Sistemas de Alimentación Ininterrumpida (UPS). Como solución, se implementó un sistema de monitoreo unificado y centralizado, que permitió

identificar, prevenir y controlar fallas en tiempo real, optimizando la respuesta y resolución de incidencias. Los resultados indicaron una detección de incidencias un 80% más rápida, con una disponibilidad de red del 93%. Además, el 49% de los problemas se resolvieron en menos de 10 minutos, y la satisfacción de los usuarios de la red alcanzó un 90%.

Quispe (2019) en su estudio “Implementación de un prototipo de monitoreo de dispositivos de comunicación y usuarios finales utilizando el protocolo SNMP basada en software libre para una empresa e-Commerce” cuyo objetivo era monitorear en tiempo real los dispositivos de comunicación, como routers, switches y puntos de acceso, además de dispositivos de usuario final, incluyendo laptops, computadoras e impresoras, empleando el Protocolo Simple de Administración de Red (SNMP) y software libre. Dirigido a una empresa de comercio electrónico, este prototipo buscó mejorar la productividad de la empresa. Permitía a los especialistas en redes controlar dispositivos mediante alertas y reportes de eventos ante fallos o anomalías en su funcionamiento. Para ello, el prototipo supervisaba la actividad de la red mediante sondeos que verificaban periódicamente el estado de los nodos de la red, usando el Protocolo de Mensajes de Control de Internet (ICMP) y SNMP. Los eventos detectados se presentaban mediante informes gráficos, facilitando la toma de decisiones para garantizar la continuidad del negocio. Implementado en GNU/Linux, la solución redujo costos, fomentó el aprendizaje de un nuevo sistema operativo y personalizó el monitoreo, mejorando el rendimiento de la empresa.

2.1.2. Antecedentes Internacionales

Manrique et al. (2021), desarrollaron el estudio Herramientas de Código Abierto para el Monitoreo de Redes LAN con el objetivo de analizar y comparar diversas herramientas de código abierto para el monitoreo de redes de área local (LAN), identificando aquellas con mejores parámetros de alerta para garantizar la operatividad de la infraestructura de red. La problemática principal consistía en la necesidad de un sistema eficiente que detectara fallos y gestionara recursos de manera adecuada en redes de telecomunicaciones, empleando el Protocolo Simple de Administración de Red (SNMP) como medio de comunicación entre los equipos

y el sistema de monitoreo. Tras evaluar cinco herramientas en un entorno virtual, los autores implementaron y compararon el rendimiento de estas herramientas. Los resultados mostraron que Nagios y Zabbix eran las únicas que cumplían con el modelo Fault, Configuration, Accounting, Performance, Security (FCAPS), lo que incluía capacidades de gestión en fallos, recolección de datos, configuración y mantenimiento. En comparación, ICINGA mostró deficiencias debido a su desarrollo en progreso, mientras que OpenNMS y Cacti presentaron limitaciones en rendimiento y seguridad, respectivamente. La investigación concluyó que Nagios y Zabbix eran las soluciones más efectivas para el monitoreo de redes LAN, gracias a su gestión integral y fiabilidad en el procesamiento de datos.

Toapanta Carvajal, (2023) en su trabajo “Implementación de un Sistema Integral de Monitoreo en Tiempo Real en la Red Core con SNMPv3 Utilizando el Software Zabbix”, para la Empresa Maxxnet la problemática de falta de control sobre el acceso a la red y los riesgos de suplantación de identidad y modificaciones no autorizadas de mensajes. Para resolver esta situación, propuso la implementación de SNMPv3, un protocolo que permite un manejo seguro de la información mediante autenticación y encriptación, garantizando un control de acceso restringido. Además, se utilizó Zabbix, un sistema de monitoreo de redes de código abierto compatible con múltiples dispositivos y versiones de SNMP, para establecer canales de comunicación seguros. La implementación se realizó a través de una interfaz web amigable, que permitía a los administradores verificar el estado de los equipos y monitorear el consumo de ancho de banda. Los resultados del diseño de monitoreo propuesto fueron significativos, proporcionando información crítica sobre tiempos de actividad (uptime), tiempos de inactividad (downtime) y consumo de ancho de banda, lo cual facilitó diagnósticos precisos y un mantenimiento preventivo eficaz, cumpliendo con el objetivo de mejorar la seguridad de la infraestructura de Maxxnet.

Castro (2020) en su estudio “Implementación en la nube de un sistema de monitoreo de eventos de fallas para infraestructura de redes y de seguridad informática utilizando la integración de zabbix, grafana y zammad” cuyo objetivo principal era desarrollar un sistema integrado de monitoreo y gestión de infraestructura de redes y seguridad informática en la nube, que ofrezca resultados

personalizados y permita la escalación proactiva de tickets de servicio ante cambios de estado en los sistemas. Para lograrlo, se implementaron Zabbix, Grafana y Zammad en contenedores Docker dentro de una máquina virtual en Google Cloud con CentOS 7, optimizando costos al utilizar recursos mínimos. La metodología incluyó la configuración de múltiples elementos, como servidores Linux y un firewall Sophos, y la creación de dashboards personalizados en Grafana para visualizar datos en tiempo real. Los resultados mostraron una reducción del 90% en el tiempo de respuesta a incidentes y un aumento del 85% en la disponibilidad de servicios. Además, se automatizó la generación de tickets en un 100% de los eventos críticos, evidenciando la eficacia de la integración de estas herramientas de código abierto para mejorar la gestión de incidencias y, en consecuencia, incrementar la satisfacción del usuario final.

2.2. Bases teóricas

2.2.1. Administrador de Dispositivos

La administración de dispositivos concede a las instituciones conservar y administrar dispositivos, implicando los equipos físicos, las máquinas virtuales, los dispositivos móviles y los dispositivos IoT. La administración de dispositivos es un componente esencial de la táctica de seguridad de cualquier institución. Asiste a respaldar que los dispositivos sean seguros, actualizados y compatibles con las directivas de la organización, con el propósito de preservar la red corporativa y los datos contra el acceso no acreditado. A medida que las organizaciones admiten empleados remotos e híbridos, es más fundamental contar con una estrategia de administración de dispositivos consolidada. Las organizaciones deben proteger y proteger sus recursos y datos en cualquier dispositivo (MandiOhlinger, 2023).

2.2.2. Protocolo Simple de Administración de Red o SNMP

SNMP (Simple Network Management Protocol) es un protocolo estándar de comunicación utilizado para gestionar y monitorear dispositivos en redes IP. Permite a los administradores de red supervisar el estado de los dispositivos, como

routers, switches, servidores y otros equipos, a través de una red. SNMP facilita la recopilación de información sobre el rendimiento de la red, la detección de problemas y la gestión de configuraciones (Misra, 2004).

Componentes Principales de SNMP

A. Agentes SNMP: Son programas que se ejecutan en los dispositivos de red. Se encargan de recopilar y enviar información sobre el estado y el rendimiento del dispositivo a un sistema de gestión.

B. Gestores SNMP: Son aplicaciones que ejecutan el software de gestión de red. Reciben y procesan la información enviada por los agentes y pueden enviar comandos a estos para realizar acciones específicas.

C. Base de datos MIB (Management Information Base): Es una colección de definiciones de objetos que se pueden gestionar mediante SNMP. Cada objeto en la MIB tiene un identificador único y contiene información sobre el estado y la configuración de los dispositivos (Misra, 2004).

Funcionamiento de SNMP

En la Figura 1 se detalla el flujo de administración de datos del protocolo SNMP.

A. **Recopilación de Datos**: Los agentes recopilan información sobre el estado y el rendimiento del dispositivo y la almacenan en la MIB.

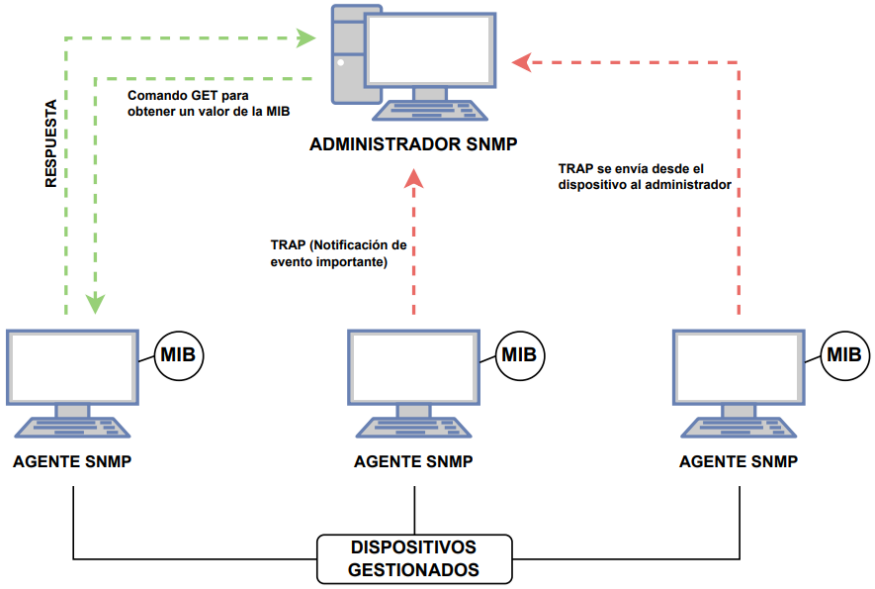
B. **Consulta de Datos**: El gestor envía solicitudes a los agentes para obtener información específica sobre los dispositivos, utilizando comandos como GET, GETNEXT y GETBULK.

C. **Notificaciones (Traps)**: Los agentes pueden enviar notificaciones al gestor de eventos o cambios importantes en el estado del dispositivo, sin necesidad de que el gestor lo solicite.

D. **Configuración Remota:** Los gestores pueden enviar comandos a los agentes para cambiar configuraciones o reiniciar dispositivos utilizando el comando SET (Misra, 2004)**.**

Figura 1

Diagrama de comunicación SNMP



Nota. El diagrama ilustra cómo el Administrador SNMP interactúa con los dispositivos gestionados a través de los Agentes SNMP, utilizando comandos para monitorear la red y recibir alertas sobre eventos significativos.

Versiones de SNMP

- **SNMPv1**: La primera versión, que proporciona funciones básicas de gestión. No incluye características de seguridad avanzadas.

- **SNMPv2c**: Introduce mejoras en el rendimiento y la capacidad de monitoreo, pero mantiene el mismo nivel de seguridad que SNMPv1.

- **SNMPv3**: La versión más reciente, que agrega características de seguridad, como autenticación y encriptación, para proteger la información transmitida (Bibbs & Matt, 2006).

2.2.3. Base de Información de Gestión o MIB

Es una colección estructurada de información organizada jerárquicamente que permite gestionar dispositivos en redes de telecomunicaciones. Utilizada junto con el protocolo SNMP (Simple Network Management Protocol), las MIBs contienen variables definidas en los dispositivos gestionados (como routers, switches y servidores), las cuales son monitoreadas y controladas por administradores de red. Los SNMP Managers interactúan con estas MIBs mediante comandos como get o set para recuperar o modificar valores en los dispositivos, lo que es esencial para sistemas de monitoreo como Zabbix, Nagios y PRTG. Las MIBs están estructuradas siguiendo las reglas de la Structure of Management Information (SMI), que establece cómo nombrar objetos, definir tipos y codificar sus valores, proporcionando métricas y alertas para el monitoreo efectivo (Stallings, 2014).

2.2.4. Identificador de Objeto o OID

Es un identificador único utilizado en la gestión de redes SNMP para referirse a un objeto específico dentro de una Management Information Base (MIB). Cada OID está compuesto por una secuencia numérica jerárquica que representa una ruta dentro de la estructura de la MIB, permitiendo a los administradores de red acceder, monitorear y modificar parámetros de los dispositivos gestionados. Los OIDs se utilizan en comandos SNMP, como get o set, para identificar variables específicas en los dispositivos y obtener información como estado del sistema, rendimiento o alertas. Los sistemas de monitoreo de red, como Zabbix, Nagios y PRTG, dependen de los OIDs para realizar consultas y generar métricas que permitan la supervisión eficiente de la red (Stallings, 2014).

2.2.5. Seguridad en Redes

La seguridad en redes se describe al grupo de políticas, prácticas y tecnologías destinadas a resguardar la integridad, confidencialidad y disponibilidad de la información transmitida y almacenada en una red. Esto comprende prever accesos no acreditados, ataques malignos y pérdida de datos.

Elementos clave de la seguridad en redes:

- Confidencialidad: Garantizar que la información solo sea alcanzable para personas acreditadas.
- Integridad: Asegurar que los datos no sean alterados durante su transmisión.
- Disponibilidad: Mantener los recursos de la red accesibles para los usuarios legítimos.

El uso de redes privadas virtuales (VPN) y protocolos de cifrado, como IPsec, son herramientas fundamentales para implementar una red segura (Soriano, 2014).

2.2.6. VPN

Una red privada virtual (VPN, por sus siglas en inglés) es una tecnología que le permite crear una conexión segura y encriptada entre dos puntos de una red pública como Internet. Su función principal es respaldar la privacidad, seguridad y anonimato en las comunicaciones y simular que los dispositivos conectados están en la misma red privada, aunque estén separados físicamente (Rodero, 2023).

2.2.7. Tipos de VPN

Los tipos de VPN son diferentes a los proveedores de VPN. Mientras que los tipos de VPN se refieren a su función y aplicación, como si fueran diferentes modelos de autos (utilitario, todoterreno, etc.), los proveedores de VPN son como las marcas de autos, como Surfshark o Nord Security.

No existe una clasificación universalmente aceptada de los tipos de VPN, pero en términos generales, se pueden clasificar de la siguiente manera:

- **VPN de acceso remoto**: Permite que un usuario se conecte de manera segura a una red desde un lugar remoto, comúnmente utilizado en empresas para que los empleados accedan a su red desde fuera de la oficina. Funciona instalando

un cliente VPN en el dispositivo del usuario, que cifra los datos entre el dispositivo y el servidor VPN.

- **VPN de sitio a sitio**: Conecta dos o más redes privadas de manera segura, típicamente utilizada por empresas para enlazar diferentes sucursales o ubicaciones. Este tipo de VPN usa routers que funcionan como servidores y clientes para crear una red privada entre las oficinas.
- **VPN personales**: Son configuradas por el usuario para acceder de manera segura a su red doméstica, como para acceder a una impresora en casa desde un lugar distante. También incluye servicios comerciales destinados a usuarios individuales, como los de Surfshark.
- **VPN móviles**: Permiten la conexión segura desde teléfonos móviles, lo que resulta útil especialmente en viajes o cuando se utilizan redes wifi públicas no seguras. Las VPN móviles suelen tener aplicaciones específicas para sistemas operativos como Android o iOS.
- **VPN en la nube**: Son utilizadas para acceder de forma segura a servicios y recursos basados en la nube. A diferencia de las VPN tradicionales, las VPN en la nube no dependen de ubicaciones físicas y pueden ser rápidamente desplegadas y accesibles globalmente.
- **VPN doble**: Una función de seguridad que enruta el tráfico a través de dos servidores VPN en lugar de uno, proporcionando una capa extra de cifrado y seguridad para mejorar la privacidad del usuario.

Esta clasificación no es rígida, pero ayuda a comprender los diferentes usos y ventajas de cada tipo de VPN (Viteri & Orbe, 2005).

2.2.8. Ventajas de una VPN Site-to-Site

Las VPN de sitio a sitio ofrecen varios beneficios clave, especialmente en contextos corporativos y empresariales. Aquí te detallo algunos de los principales beneficios:

- **Conexión segura entre sucursales**: Las VPN de sitio a sitio permiten que diferentes oficinas o sucursales de una empresa estén conectadas a través de una red privada y segura, lo que mejora la comunicación interna y la

transferencia de datos entre distintas ubicaciones geográficas sin exponer la información a redes públicas.

- **Costos reducidos**: A diferencia de las conexiones dedicadas, que pueden ser costosas, las VPN de sitio a sitio utilizan la infraestructura de Internet pública para crear una conexión privada, lo que reduce significativamente los costos de implementación y mantenimiento.
- **Escalabilidad**: Las VPN de sitio a sitio son fácilmente escalables. A medida que una empresa crece, puede agregar más sitios o sucursales a la red privada sin necesidad de cambios costosos en la infraestructura.
- **Mejora en la seguridad**: Las VPN de sitio a sitio utilizan métodos de cifrado robustos, como IPSec (Internet Protocol Security), para asegurar la confidencialidad e integridad de los datos transmitidos entre los puntos de la red, lo que hace que las comunicaciones sean mucho más seguras frente a posibles interceptaciones.
- **Reducción de la complejidad en la gestión**: Una vez configurada la VPN de sitio a sitio, la gestión de la red se simplifica, ya que las conexiones entre las distintas ubicaciones están automatizadas y no requieren intervención manual continua.

Acceso remoto seguro a la red interna: Aunque las VPN de sitio a sitio suelen ser para conectar oficinas físicas, pueden permitir que usuarios remotos o de oficina en casa accedan de manera segura a los recursos internos de la empresa (Calatayud, 2014a).

2.2.9. Funcionamiento de Tunelización Site-to-Site

En la tunelización Site-to-Site, el tráfico de datos se encripta en un extremo (la red de origen) y se envía a través de un "túnel" seguro hasta el otro extremo (la red de destino), donde se descifra. Este túnel se establece mediante protocolos de seguridad como IPSec (Internet Protocol Security) o SSL/TLS (Secure Sockets Layer/Transport Layer Security). Los routers o dispositivos de seguridad en ambos extremos de la conexión actúan como puertas de enlace que cifran y descifran los datos.

El proceso básico de funcionamiento incluye:

- **Establecimiento del Túnel**: Las dos redes (o sitios) se configuran para que cada una tenga un dispositivo que actúe como "puerta de enlace" (router o firewall). Estos dispositivos negocian las claves de cifrado y autentican la conexión, creando un túnel seguro.
- **Cifrado de Datos**: Una vez establecido el túnel, el tráfico entre las dos redes se cifra utilizando un algoritmo de cifrado (por ejemplo, AES o 3DES), asegurando que los datos sean ilegibles para cualquier atacante que intente interceptarlos.
- **Transporte Seguro de Datos**: El tráfico cifrado viaja a través de Internet (o cualquier red pública) de manera segura. Aunque los datos transiten por redes no confiables, el cifrado garantiza que no sean accesibles ni modificados.
- **Descifrado de Datos**: Al llegar al destino, el dispositivo receptor descifra el tráfico utilizando la misma clave de cifrada acordada en el proceso de establecimiento del túnel, permitiendo que los datos se reciban en su forma original (Calatayud, 2014b).

2.2.10. Protocolo IPsec

IPsec (Internet Protocol Security) es un conjunto de protocolos diseñados para garantizar la seguridad de las comunicaciones a través de redes IP. Su implementación permite establecer túneles cifrados que protegen los datos contra accesos no autorizados, garantizando confidencialidad, integridad y autenticidad. Para lograr este objetivo, se configuran diversos parámetros que rigen el comportamiento y las características del túnel. A continuación, se presenta una descripción de los elementos más relevantes en la configuración de un túnel IPsec, divididos en las fases de negociación y transporte (Marqués, 2016a).

2.2.11. Parámetros de Configuración del protocolo IPsec

Parámetros de la negociación IKE

La negociación IKE (Internet Key Exchange) es el proceso mediante el cual se establecen los parámetros iniciales para la creación de un canal seguro. Este proceso se organiza en dos versiones principales: IKEv1 e IKEv2, siendo esta última la más utilizada debido a sus mejoras en eficiencia, seguridad y simplicidad.

- Versión de IKE: Este parámetro define la versión del protocolo utilizada para la negociación.

  IKEv1: Es la versión original, ampliamente soportada, pero con limitaciones en términos de eficiencia y seguridad.

  IKEv2: Introduce mejoras significativas, como una negociación más rápida y mejor manejo de errores.

- Algoritmo de cifrado: Este algoritmo se utiliza para proteger la confidencialidad de los datos negociados. Un ejemplo común es AES-CBC-256, que emplea el estándar avanzado de cifrado (AES) con una longitud de clave de 256 bits y opera en modo de encadenamiento de bloques (CBC).
- Algoritmo de integridad: Garantiza que los datos intercambiados no sean alterados durante la transmisión, mediante la creación de un valor hash. Entre los algoritmos más utilizados se encuentra SHA-1 (Secure Hash Algorithm 1), aunque existen alternativas más robustas, como SHA-256.
- Grupo Diffie-Hellman (DH): Este grupo determina el tamaño de las claves utilizadas en el intercambio seguro, contribuyendo a la creación de claves de sesión. Los grupos con valores más altos, como modp3072 o modp8192, ofrecen mayor seguridad a costa de un mayor consumo de recursos computacionales.
- Duración de la asociación de seguridad (SA Lifetime): Representa el tiempo durante el cual las asociaciones de seguridad (SA) permanecen activas antes de ser renegociadas. Usualmente, este valor se configura en segundos; por ejemplo, 3600 segundos equivalen a 1 hora.
- Clave precompartida (Pre-Shared Key): Es una clave secreta que se utiliza para autenticar los extremos durante la fase inicial de negociación.

Parámetros de la fase de transporte IPsec

Una vez finalizada la negociación IKE, se establece la configuración para proteger los datos transmitidos a través del túnel, lo que se conoce como la fase de transporte.

- Algoritmo de cifrado: Protege la confidencialidad de los datos mediante algoritmos como ESP-GCM-256, que combina cifrado y autenticación en un solo proceso.
- Algoritmo de integridad: Este parámetro asegura la integridad de los paquetes transmitidos, garantizando que los datos no sean modificados.
- Grupo de PFS (Perfect Forward Secrecy): Este grupo asegura que cada sesión utilice claves únicas generadas mediante un nuevo intercambio Diffie-Hellman, lo que incrementa la seguridad.
- Duración de la asociación de seguridad: Similar al SA Lifetime de la fase IKE, este parámetro define el tiempo de validez de las asociaciones de seguridad en la fase de transporte.

Configuración de BGP en un túnel IPsec

En aplicaciones avanzadas, como las redes corporativas o híbridas, se habilita el protocolo de enrutamiento dinámico BGP (Border Gateway Protocol) para optimizar el intercambio de rutas entre los extremos conectados. Esto permite una mayor flexibilidad en el manejo del tráfico, especialmente en configuraciones complejas con múltiples redes.

Relación entre las fases de IKE e IPsec

La configuración de un túnel IPsec se divide en dos fases principales:

- Fase 1: Se establece un canal seguro inicial mediante la negociación IKE, definiendo los parámetros de autenticación y cifrado entre los extremos.
- Fase 2: Se utiliza el canal seguro para configurar los parámetros de cifrado y autenticación que protegerán los datos transmitidos (Marqués, 2016b).

2.2.12. Monitoreo en Nube

El monitoreo en la nube se refiere al proceso de supervisar, rastrear y gestionar los recursos y servicios que se ejecutan en una infraestructura de nube, ya sea pública, privada o híbrida. Este monitoreo es esencial para obtener una visibilidad completa del rendimiento de las aplicaciones y sistemas, y ayuda a identificar problemas antes de que afecten a los usuarios. Entre las plataformas más utilizadas para este fin se encuentran Microsoft Azure, Amazon Web Services (AWS), y Google Cloud Monitoring (Ward & Barker, 2014).

Importancia y Ventajas del Monitoreo en Nube

El monitoreo en nube es muy importante y ofrece diversas ventajas a los usuarios, entre ellas:

- Visibilidad del rendimiento: Permite rastrear en tiempo real métricas clave, como el uso de CPU, memoria y el tráfico de red, lo que facilita la optimización de recursos y la detección de problemas antes de que escalen.
- Seguridad mejorada: El monitoreo continuo ayuda a identificar accesos no autorizados, ataques de denegación de servicio (DDoS) y otras amenazas. Esto es crucial para garantizar la seguridad de los datos y aplicaciones en la nube.
- Escalabilidad: Los sistemas en la nube suelen ser dinámicos y pueden crecer o disminuir según la demanda. El monitoreo permite escalar recursos de manera eficiente y evitar costos innecesarios al ajustar el uso de recursos en tiempo real.
- Automatización: Muchas herramientas permiten acciones automáticas, como la corrección de errores o la provisión de más recursos cuando se detectan problemas, lo que minimiza la intervención manual (Ward & Barker, 2014).

Beneficios frente al Monitoreo Local

El monitoreo en nube cuenta con mayores beneficios, respecto a un monitoreo local. Algunos parámetros son los siguientes:

- Accesibilidad: Las soluciones en la nube permiten a los administradores acceder a las métricas y datos desde cualquier lugar con conexión a internet, facilitando la gestión remota.
- Reducción de costos: En lugar de mantener hardware y software local, el monitoreo en la nube suele ser más rentable, ya que los costos de infraestructura son asumidos por el proveedor del servicio.
- Mejora de la seguridad: Al centralizar el monitoreo, las organizaciones pueden detectar y responder rápidamente a amenazas distribuidas en múltiples entornos.
- Automatización y eficiencia operativa: El monitoreo en la nube facilita la automatización de procesos y la implementación de soluciones rápidas para problemas de rendimiento o seguridad (Ward & Barker, 2014)

2.2.13. Infraestructura como Servicio o IaaS

La infraestructura como servicio (IaaS) es un modelo de computación en la nube que proporciona recursos de procesamiento, almacenamiento y redes bajo demanda, permitiendo a las organizaciones reducir costos en hardware y mantenimiento de centros de datos locales. Este enfoque ofrece flexibilidad para escalar recursos TI según las necesidades y facilita el aprovisionamiento de nuevas aplicaciones. IaaS evita la complejidad de gestionar servidores físicos, ya que los proveedores como Microsoft Azure, Amazon Web Services (AWS) y Google Cloud Monitoring, manejan la infraestructura, mientras que los usuarios administran su propio software (IBM, 2021).

2.2.14. Plataformas de servicios en Nube

Microsoft Azure

Microsoft Azure es una plataforma de servicios en la nube que permite a las empresas construir, implementar y gestionar aplicaciones a través de una red global de centros de datos. Ofrece una amplia variedad de servicios, desde computación y almacenamiento hasta análisis de datos y redes. Azure se destaca

por su integración con herramientas de Microsoft, como Office 365 y Dynamics, y su capacidad para soportar soluciones híbridas que combinan infraestructuras locales y en la nube, facilitando una transición más suave para las organizaciones. (Microsoft, 2024).

Amazon Web Services

Es una plataforma de servicios en la nube que proporciona a las empresas acceso a una infraestructura escalable y flexible. Ofrece una extensa gama de servicios, incluyendo almacenamiento, computación y bases de datos, así como herramientas avanzadas de análisis y machine learning. AWS es conocido por su modelo de pago por uso, que permite a las empresas pagar solo por los recursos que utilizan, optimizando costos y permitiendo una fácil escalabilidad según las necesidades del negocio (AWS, 2023).

Google Cloud

Google Cloud es una plataforma integral de servicios en la nube que se centra en ofrecer infraestructura, análisis de datos y herramientas de inteligencia artificial. Destaca por su enfoque en el big data y machine learning, proporcionando soluciones innovadoras para el procesamiento de datos a gran escala. Google Cloud también ofrece una experiencia de colaboración mejorada con herramientas como Google Workspace, y se beneficia de su infraestructura global altamente eficiente, permitiendo a las empresas optimizar el rendimiento y la disponibilidad de sus aplicaciones (Google Cloud, s. f.).

2.2.15. Software Libre

El software libre se refiere a la libertad de los usuarios para ejecutar, estudiar, modificar y distribuir el software, y no a su precio. Esto incluye cuatro libertades clave: la libertad de usar el programa con cualquier fin (libertad 0), la libertad de estudiar y modificar el código fuente (libertad 1), la libertad de distribuir copias del software (libertad 2) y la libertad de mejorar el programa y compartir esas mejoras

(libertad 3). Para garantizar estas libertades, el acceso al código fuente es esencial. El software libre puede ser comercializado, y su distribución no debe imponer restricciones que limiten estas libertades (Stallman, 2004).

2.2.16. Plataformas de Gestión Web

Una plataforma de gestión es un software alojado en un servidor, cuyo propósito principal es ofrecer una funcionalidad general para administrar dispositivos de red. Existen diferentes tipos de plataformas de gestión, entre las más utilizadas son Zabbix, Nagios y PRTG Network Monitor (wakkeit, 2024).

2.2.16.1. Plataforma Zabbix

Zabbix fue creado por Alexei Vladishev y es actualmente dirigido por Zabbix SIA. Su propósito es brindar una solución para el monitoreo de redes, dispositivos, máquinas virtuales, servidores, bases de datos, sitios web, aplicaciones en la nube, entre otros, permitiendo registrar y visualizar el estado en tiempo real y su historial. Cabe resaltar que Zabbix es un software de código abierto de nivel empresarial, lo que significa que su código fuente es gratuito y accesible para el público. Además, cuenta con un sistema de notificaciones flexible que permite a los usuarios configurar alertas mediante correo electrónico y plataformas como Telegram o WhatsApp para cualquier evento anómalo, facilitando una respuesta rápida ante problemas en servidores o dispositivos monitoreados. Con una correcta instalación y configuración, Zabbix es clave para organizaciones de cualquier tamaño, como Maxxnet, ya que, al ser software libre, se pueden evitar costos de licencias sin sacrificar la calidad del producto comparado con sistemas con licencia (Zabbix, 2021a)

2.2.16.2. Funcionamiento de Zabbix

Para este proyecto, Zabbix se instaló en un servidor Ubuntu 22.04, el cual se encargará de recolectar y monitorear información de los equipos Kaise utilizando el protocolo SNMP. Además, Zabbix ofrece una interfaz web que presenta de

manera gráfica toda la información recopilada y almacenada de los dispositivos gestionados por el sistema.

Zabbix cuenta con agentes compatibles con sistemas operativos como Linux, Mac y Windows, que se instalan en los servidores o estaciones de trabajo que serán monitoreados. También permite supervisar en tiempo real el estado de impresoras, routers, switches, sensores de temperatura y humedad, entre otros dispositivos.

Algunas de las principales funcionalidades de Zabbix incluyen:

- Alertas configurables.
- Visualización de gráficos en tiempo real.
- Capacidad avanzada de monitoreo.
- Almacenamiento de datos históricos.
- Configuración dinámica.
- Recopilación eficiente de datos (Zabbix, 2021b)

2.2.16.3. Ventajas y Características de Zabbix

Zabbix es una solución de código abierto que ofrece varias ventajas para el monitoreo de redes. Entre ellas se incluye el acceso al código fuente y la integración de componentes como Linux, Apache, MySQL/PostgreSQL y PHP. Proporciona una gestión centralizada a través de una interfaz web, permitiendo controlar todos los dispositivos de la red desde un solo lugar. Cuenta con un sistema de gestión de usuarios con autenticación, y notificaciones automáticas que se envían vía correo electrónico o SMS ante cualquier incidente.

Zabbix soporta diversos protocolos, como SNMP (v1, v2, v3), facilitando la detección y monitoreo de dispositivos como routers, switches, servidores, impresoras y otros periféricos. Además, ofrece capacidades avanzadas de visualización y limpieza de datos, lo que asegura un entorno organizado y actualizado.

Entre sus principales características de monitorización se encuentran:

- Configuración y acceso centralizados.
- Escalabilidad probada con hasta 100,000 dispositivos monitorizados y 1,000,000 chequeos.
- Monitoreo en tiempo real con alertas y notificaciones personalizables.
- Auto detección de dispositivos mediante SNMP y rangos IP.
- Monitoreo proactivo sin agentes, con soporte para múltiples protocolos.
- Seguridad avanzada con permisos flexibles, autenticación IP y protección contra ataques de fuerza bruta.

Zabbix también incluye funciones administrativas como ping y traceroute a hosts (Zabbix, 2021c).

2.2.17. Sistema de Alimentación Ininterrumpida o UPS

Un sistema de alimentación ininterrumpida o también conocido como UPS por sus siglas en inglés Uninterrumptible Power Supply, es un equipo diseñado para proporcionar energía de respaldo a cargas críticas en caso de interrupciones del suministro eléctrico. Su función principal es proteger los dispositivos conectados contra perdidas de energía o fluctuaciones en la corriente eléctrica.

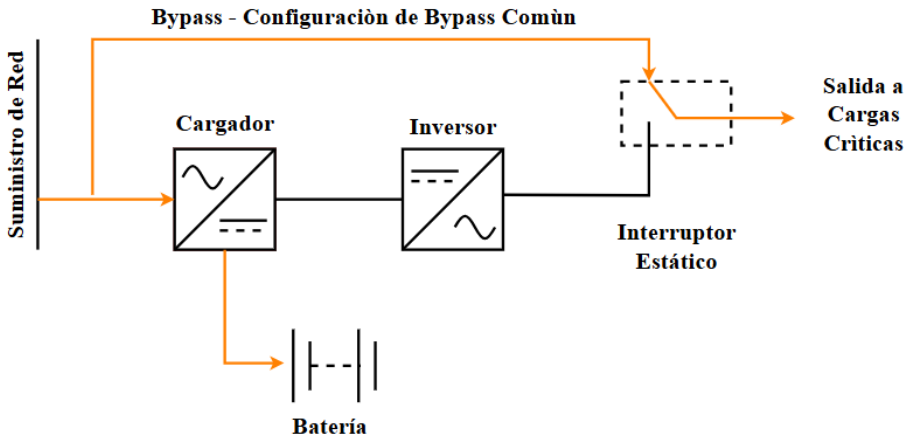
2.2.18. Tipos de UPS

UPS Offline

El UPS Offline o de Standby es el modelo más básico de sistemas de alimentación ininterrumpida. Solo activa su batería cuando se detecta una interrupción total del suministro eléctrico. En las figuras (Figuras 2, 3 y 4) se explica los modos de operación.

Figura 2

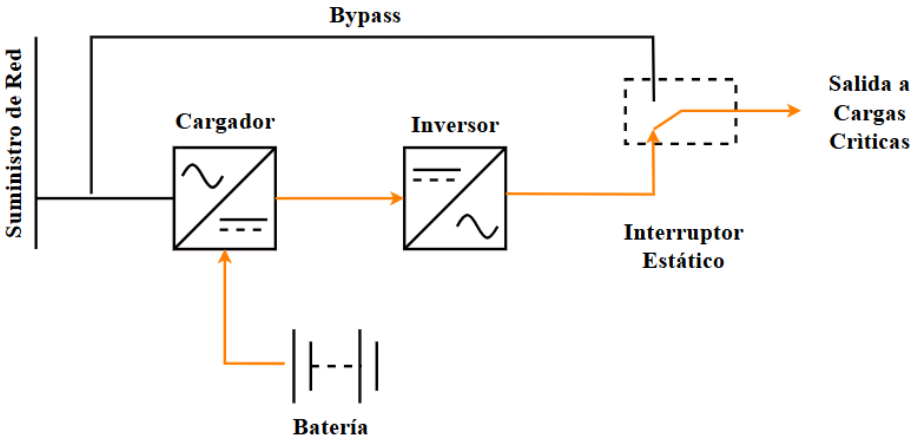
UPS Offline: Operación Normal



Nota. El diagrama muestra la configuración típica de un bypass en un sistema UPS, donde el inversor y el cargador trabajan en conjunto para garantizar la alimentación ininterrumpida de las cargas críticas.

Figura 3

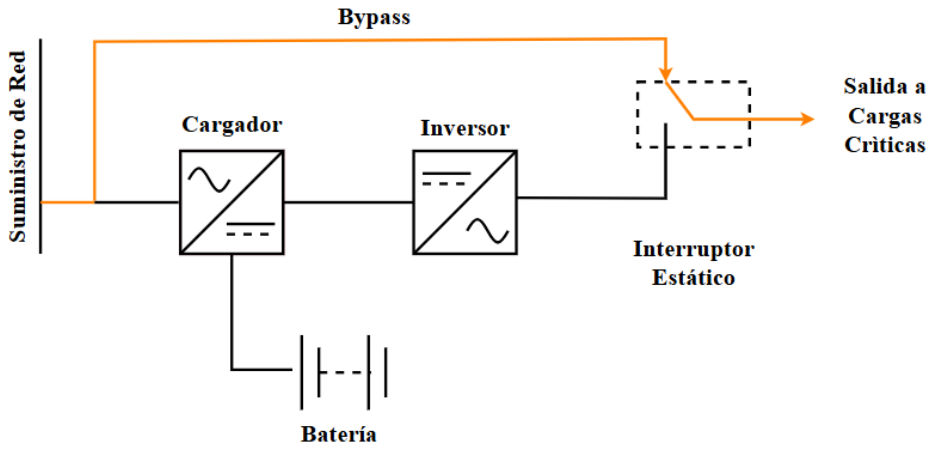
UPS Offline: Falla de Red



Nota. El diagrama muestra cómo el inversor utiliza la energía de la batería para alimentar las cargas críticas, con el bypass inactivo y el sistema completamente dependiente del respaldo del UPS.

Figura 4

UPS Offline: Falla de UPS



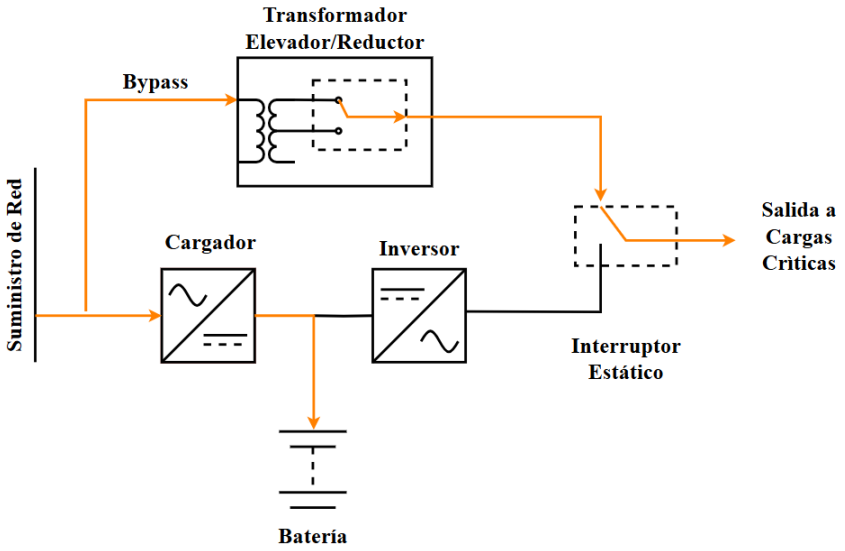
Nota. El diagrama muestra cómo, en caso de una falla interna del UPS, la energía fluye directamente desde la red a las cargas críticas a través del bypass, mientras que el UPS y la batería permanecen inactivos.

UPS Interactivo

El UPS Línea Interactiva incorpora un regulador de voltaje que permite corregir pequeñas caídas o picos en la tensión sin recurrir a la batería, como se observa en la Figura 5, mientras que en la Figura 6 se observa el funcionamiento ante una falla del suministro eléctrico. Este modelo es más avanzado que el standby y es adecuado para servidores medianos, estaciones de trabajo o sistemas de telecomunicaciones. Es un equilibrio entre costo y funcionalidad, ofreciendo mayor protección frente a variaciones comunes en el suministro de energía.

Figura 5

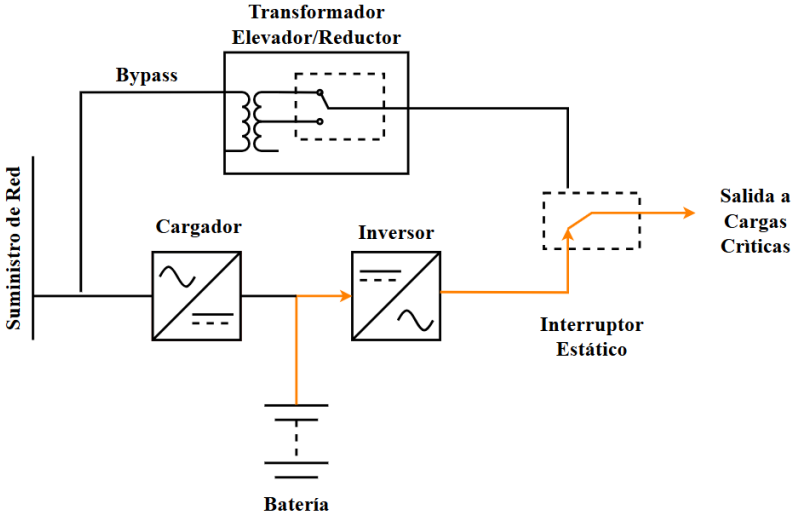
UPS Interactivo: Operación Normal



Nota. El diagrama muestra cómo el regulador de voltaje corrige pequeñas variaciones en la tensión, protegiendo las cargas sin afectar la autonomía del sistema.

Figura 6

UPS Interactivo: Falla de Red



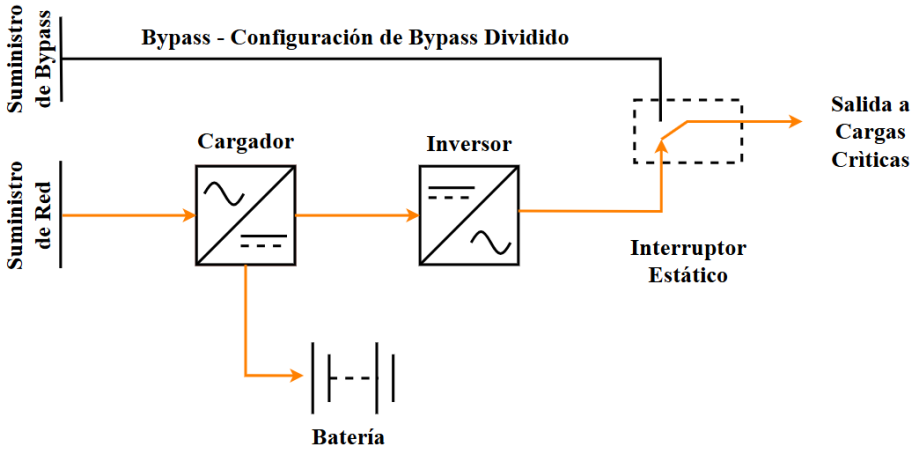
Nota. El diagrama muestra cómo el UPS Interactivo regula el voltaje y, en ausencia de suministro de red, utiliza la batería para garantizar la continuidad de la alimentación a las cargas críticas.

UPS Online

El UPS Online o de Doble Conversión ofrece la mayor protección, ya que convierte constantemente la energía de entrada de CA a CC y nuevamente a CA, eliminando cualquier irregularidad en el suministro eléctrico, según se aprecia en los diagramas de las figuras (Figura 7, 8 y 9). Este tipo de UPS es ideal para aplicaciones de misión crítica como centros de datos, hospitales y sistemas financieros, ya que garantiza un suministro continuo y limpio, independiente de las condiciones de la red eléctrica.

Figura 7

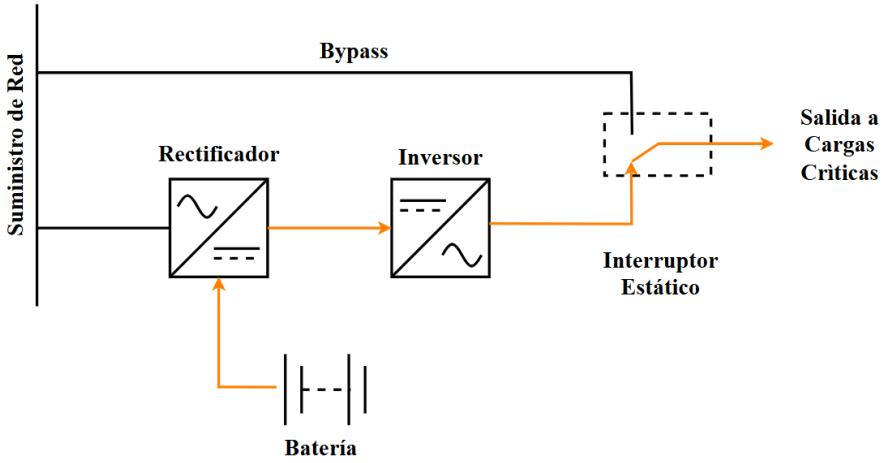
UPS Online: Operación Normal



Nota. El diagrama muestra la operación del UPS en modo online, utilizando doble conversión para asegurar una salida de energía limpia y estable a las cargas críticas.

Figura 8

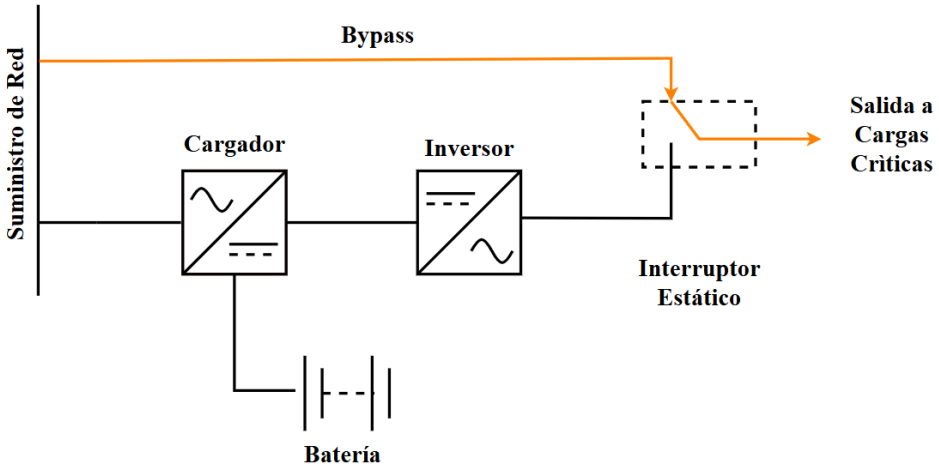
UPS Online: Falla de Red



Nota. El diagrama ilustra el modo batería, donde el inversor alimenta las cargas críticas desde la batería, con el bypass desconectado, asegurando continuidad de energía durante fallas de la red.

Figura 9

UPS Online: Falla de UPS



Nota. En el modo bypass, la energía fluye directamente desde la red hacia las cargas críticas, desconectando el inversor y la batería para reducir el consumo energético.

2.2.19. Aplicaciones para UPS

Los UPS tienen una amplia gama de aplicaciones en diversas áreas donde es esencial garantizar la continuidad del suministro eléctrico. Aquí algunos ejemplos:

- Centros de datos y servidores: Los UPS protegen los equipos críticos de los centros de datos de caídas de tensión, apagones y fluctuaciones, asegurando que la infraestructura informática se mantenga operativa sin interrupciones.

- Hospitales y equipos médicos: En entornos médicos, los UPS son esenciales para mantener el funcionamiento de equipos críticos como ventiladores, monitores de pacientes y máquinas de resonancia magnética, donde la falta de energía podría poner en riesgo vidas.

- Sistemas de telecomunicaciones: Las empresas de telecomunicaciones utilizan los UPS para garantizar la operatividad continua de sus estaciones base y equipos de redes, esenciales para mantener la conectividad y las comunicaciones.

- Industrias y procesos de manufactura: En la industria, los UPS garantizan que los procesos automatizados, las líneas de producción y los sistemas de control no se vean afectados por cortes eléctricos que puedan interrumpir o dañar la maquinaria.
- Equipos de oficina: Los UPS protegen computadoras, impresoras y otros dispositivos críticos en oficinas para prevenir la pérdida de datos y daños ante interrupciones eléctricas.

- Sistemas de seguridad y videovigilancia: Las cámaras de seguridad y los sistemas de alarma suelen depender de UPS para continuar operando durante fallas de energía, garantizando la seguridad en instalaciones residenciales y comerciales.

- Infraestructura crítica: Los UPS son esenciales para proteger infraestructuras como estaciones eléctricas, instalaciones gubernamentales y aeropuertos, donde una interrupción de energía podría tener consecuencias importantes para la seguridad y la operatividad.

- Aplicaciones domésticas: Aunque menos comunes que en el sector industrial, los UPS se utilizan en hogares para proteger equipos electrónicos sensibles como computadoras, routers y televisores ante fluctuaciones eléctricas o cortes inesperados. El tipo de UPS interactivos es más común para esta aplicación.

2.2.20. Monitoreo de UPS

El monitoreo de un UPS es fundamental para asegurar su correcta operación y prevenir fallos en los sistemas eléctricos que protege. Algunos de los parámetros críticos que deben monitorearse son:

- Tensión de entrada y salida: Es esencial verificar que la tensión suministrada a los dispositivos conectados sea estable y dentro de los rangos aceptables, evitando sobrecargas o subidas de tensión que puedan dañar el equipo.

- Corriente: El monitoreo de la corriente consumida ayuda a detectar si los dispositivos conectados al UPS están operando dentro de sus límites de consumo o si hay alguna sobrecarga que ponga en riesgo el sistema.

- Temperatura: Un aumento en la temperatura interna del UPS puede indicar problemas de ventilación o sobrecarga, lo que afecta la vida útil de sus componentes. Monitorear la temperatura es crucial para evitar el sobrecalentamiento y posibles fallos.

- Estado de la batería: Es clave revisar la capacidad de carga de la batería, su nivel de carga y tiempo de autonomía. La batería es uno de los componentes más vulnerables en un UPS, por lo que su monitoreo constante garantiza que esté lista para suministrar energía cuando sea necesario.

- Frecuencia: Tanto la frecuencia de entrada como de salida (normalmente 50/60 Hz) deben mantenerse estables. Variaciones en la frecuencia pueden afectar el rendimiento de los dispositivos conectados.

- Ciclos de carga/descarga: Es útil monitorear el número de ciclos que ha realizado la batería, lo cual es importante para prever cuándo será necesario reemplazarla, ya que su vida útil depende de estos ciclos.

- Alarmas y notificaciones: Un sistema UPS bien monitoreado debe emitir alertas automáticas para fallos inminentes, sobrecargas o cambios en el estado operativo del sistema, permitiendo la toma de acciones inmediatas.

Estos parámetros ayudan a maximizar la eficiencia y confiabilidad del UPS, previniendo interrupciones imprevistas en el suministro de energía y extendiendo la vida útil del equipo.

2.2.21. Mantenimiento Preventivo de UPS

Los mantenimientos preventivos son importantes por que permiten a los técnicos la oportunidad detectar y reparar posibles fallas antes de que se presenten. De hecho, los estudios muestran que el mantenimiento preventivo rutinario de los UPS reduce significativamente la probabilidad de tiempo de inactividad inducido por el UPS. Un estudio reveló que los clientes que no realizan un mantenimiento preventivo tienen casi cuatro veces más probabilidades de sufrir una falla del SAI que aquellos que realizan las dos visitas de mantenimiento preventivo recomendadas por año (Tamberg, 2024).

2.2.22. UPS Kaise

Los UPS Kaise, fabricados por Tempel Group, destacan por su tecnología avanzada y su capacidad para cumplir con una amplia variedad de necesidades en entornos críticos. A continuación, se presentan las características técnicas más relevantes de su tecnología:

- Avanzada tecnología de control DSP: La incorporación de procesadores de señal digital (DSP) permite un control más preciso y rápido del sistema, mejorando la estabilidad y eficiencia del UPS.

- Corrección Activa de Factor de Potencia (APFC): El factor de potencia de entrada puede llegar hasta 0.99, lo que optimiza la eficiencia energética, reduce pérdidas y mejora la calidad de la energía suministrada.

- Factor de potencia de salida de 0.99: Esto garantiza una mayor capacidad para manejar cargas críticas sin comprometer el rendimiento, ideal para equipos de alta demanda energética.

- Arranque en frío y entrada dual: Estas funcionalidades permiten que el UPS inicie sin conexión a la red eléctrica, garantizando una mayor flexibilidad y continuidad de operación en escenarios de emergencia.

- Amplio rango de voltaje de entrada: Con un rango de entre 190V y 485V, los UPS Kaise son capaces de operar en condiciones de suministro fluctuante, garantizando la estabilidad del sistema.
- Frecuencia autoajustable: La capacidad de ajustar la frecuencia de operación a 50 o 60 Hz de forma automática permite una mayor adaptabilidad en distintas redes eléctricas.

- Alta eficiencia en modo ECO: En modo de ahorro de energía (ECO), los UPS pueden alcanzar eficiencias de hasta el 98%, lo que reduce considerablemente el consumo energético en comparación con otros modelos.

- Display LCD+LED: Permite una interfaz intuitiva para el usuario, ofreciendo información visual clara sobre el estado del UPS y las alarmas.

- Capacidad de carga rápida: Es una característica clave para asegurar que las baterías estén disponibles rápidamente después de una descarga, mejorando la continuidad operativa.

- Advanced Battery Management (ABM): Un algoritmo inteligente gestiona la descarga de las baterías, lo que ayuda a extender su vida útil y mejorar la eficiencia operativa.

- Transistores IGBT: La avanzada técnica de control con transistores de efecto de campo (IGBT) mejora la calidad de la energía y minimiza las pérdidas de conmutación, haciendo el sistema más robusto.

- Apagado remoto (EPO): Una función de seguridad que permite apagar el UPS en casos de emergencia.

- Puertos de comunicación: Los UPS Kaise incluyen múltiples interfaces de comunicación como RS232, USB, Ethernet y RS485, lo que facilita la integración con sistemas de monitoreo como SNMP y AS400, permitiendo una gestión remota eficiente (Kaise, 2018).

ESTANDARES

2.2.23. ISO 27017

Con el incremento de las soluciones en la nube, la seguridad de la información se ha convertido en una prioridad crítica para las organizaciones. La norma ISO 27017 ofrece una guía específica sobre los controles de seguridad aplicables a entornos de computación en la nube. Esta normativa es parte de la familia ISO 27000, conocida por establecer estándares de seguridad de la información. Sin embargo, la ISO 27017 se centra exclusivamente en la seguridad en la nube, abordando los desafíos y riesgos específicos que surgen al gestionar y almacenar datos en infraestructuras en la nube (iso.org, 2015).

2.2.24. IEC/EN 62040-1

La norma IEC/EN 62040-1, publicada por la Comisión Electrotécnica Internacional (IEC), dispone los requerimientos de seguridad para los sistemas de alimentación ininterrumpida (UPS) con almacenamiento de energía en corriente continua. Su objetivo es asegurar la continuidad de la energía eléctrica en sistemas de distribución de baja tensión, asegurando la seguridad ante riesgos como incendios, descargas eléctricas y peligros mecánicos. Aplica a UPS con tensiones de salida hasta 1000 V de corriente alterna o 1500 V de corriente continua, y cubre tanto la instalación como la operación y el mantenimiento según las definiciones del fabricante (IEC, 2021).

2.3. Definición de términos básicos

- **ANSI/TIA-942B:** Norma que establece los requisitos de infraestructura para centros de datos en áreas como conectividad y seguridad (ANSI, 2005).

- **Dashboard:** Sección de la interfaz web que muestra información importante mediante widgets visuales (Ortiz, 2023).

- **Eficiencia energética:** Metodologías para utilizar menos energía para realizar la misma tarea, optimizando recursos sin perder rendimiento. Esto reduce el consumo, los costos y el impacto ambiental (gob.pe, 2021).

- **Host:** Dispositivo o conjunto de parámetros monitoreados, ya sea físico o virtual (msmk, 2024).

- **IGBT:** Dispositivo semiconductor que controla eficientemente la energía en aplicaciones de alta potencia, como inversores y convertidores (Darnell, 2022).

- **IP:** Conjunto de reglas que permite la comunicación entre dispositivos en una red, asignando una dirección única a cada uno (Castillo, 2020).

- **LAN:** Red de área local que conecta dispositivos en un área limitada para compartir recursos (Hwang, 2021).

- **Linux:** Sistema operativo de código abierto basado en Unix, conocido por su seguridad y estabilidad, usado en diversas plataformas (Acero, 2005).

- **Servidores:** Computadoras que proporcionan recursos o servicios, como almacenamiento y procesamiento, a otros dispositivos en una red (Marchionni, 2011).

- **SNMP:** Protocolo para gestionar y monitorear dispositivos en redes IP, permitiendo recopilar datos y enviar alertas sobre el estado de estos (Misra, 2004).

- **Switch:** Dispositivo de red que conecta varios dispositivos, facilitando la comunicación eficiente entre ellos (Rodriguez, 2023).
- **Template:** Conjunto de elementos de monitoreo predefinidos aplicables a uno o varios hosts para facilitar la configuración (zabbix, 2024).

- **Trigger:** Expresión lógica que define un umbral de problema y evalúa datos para indicar estados de "Ok" o "Problema" (Hernandez, 2020).

CAPÍTULO III: DESARROLLO DEL TRABAJO PROFESIONAL

3.1. Determinación y análisis del problema

La adopción de los UPS Kaise se vio incrementada en el mercado eléctrico en los últimos dos años hasta en un 50%, por lo que la cantidad de solicitudes de soporte ha crecido significativamente en un 75%, lo que agrava el problema, ya que el personal de soporte técnico es limitado y cuentan con otras funciones a su cargo.

El enfoque de soporte técnico dependía de la intervención humana directa y carecía de herramientas tecnológicas avanzadas que facilitaran la identificación y resolución de problemas sin intervención física, por lo que se encontraba con una limitación tecnológica para la detección y prevención de fallas.

La carencia de un sistema de monitoreo remoto y en tiempo real para los UPS Kaise genera varios retos para Tempel y sus clientes:

- Tiempo de respuesta prolongado: El equipo técnico debe realizar diagnósticos a distancia o desplazarse físicamente, lo que aumenta el tiempo necesario para resolver problemas.
- Gastos operativos elevados: Los desplazamientos físicos y el uso constante de recursos para soporte remoto incrementan los gastos en sobretiempo y movilidad.
- Impacto en la operatividad del cliente: La ineficiencia en el soporte técnico puede provocar que los equipos UPS permanezcan fuera de servicio por períodos prolongados, afectando la continuidad de las operaciones del cliente, especialmente en industrias que dependen de la energía ininterrumpida.

Para visualizar de manera cuantitativa estas actividades, se presenta la Tabla 1, que resume los aspectos clave y sus valores actuales en relación con el soporte de los UPS Kaise.

Tabla 1

Diagnóstico Cuantitativo de la Situación Actual en el Soporte de UPS Kaise

Aspecto	**Cuantificación Actual**
Tiempo de respuesta promedio	8-10 horas por incidente
Gastos operativos (mensuales)	S/. 1,950 en movilidad y sobretiempo
Inactividad del cliente promedio	4-6 horas por incidente
Volumen de solicitudes de soporte	25-30 solicitudes al mes
Diagnósticos físicos	75% de los incidentes requiere desplazamiento físico

Nota. Datos basados en registros de soporte y operativos de Tempel Perú.

3.1.1. Problema General

Carencia de un sistema de monitoreo en nube para los Sistemas de Alimentación Ininterrumpida (UPS) Kaise de Tempel Perú

3.1.2. Problemas Específicos

- Falta de un diseño centralizado para monitorear los UPS Kaise en tiempo real.
- Ausencia de un sistema centralizado para monitorear los UPS Kaise en tiempo real.
- Déficit de historial operativo de parámetros eléctricos y alertas configurables para notificar eventos críticos en tiempo real de los UPS Kaise.

3.1.3. Necesidades

- Se identifico la necesidad de implementar un sistema que permitiera la supervisión continua de los UPS en tiempo real.
- Era fundamental contar con una solución que redujera los tiempos de respuesta ante cualquiera falla y/o alarmas del equipo

- La empresa requería una herramienta que reduzca la necesidad de desplazamientos físicos y mejore la eficiencia del soporte.
- Era necesario contar con un sistema de monitoreo con historial de funcionamiento que ayude al personal de soporte a tomar decisiones, ya sea de reparación, cambio de pieza, mantenimiento o aplicación de garantía.
- El área de soporte técnico necesitaba de una mayor visibilidad del estado de los UPS para adelantarse a posibles problemas que afecten las cargas del cliente.
- Era importante contar con una configuración de alarmas por correo que notifique al usuario la presencia de algún evento en el equipo.
- Surgió la necesidad de brindar un valor agregado a los UPS Kaise para mantener el liderazgo en el mercado eléctrico.

3.2. Modelo de solución propuesto

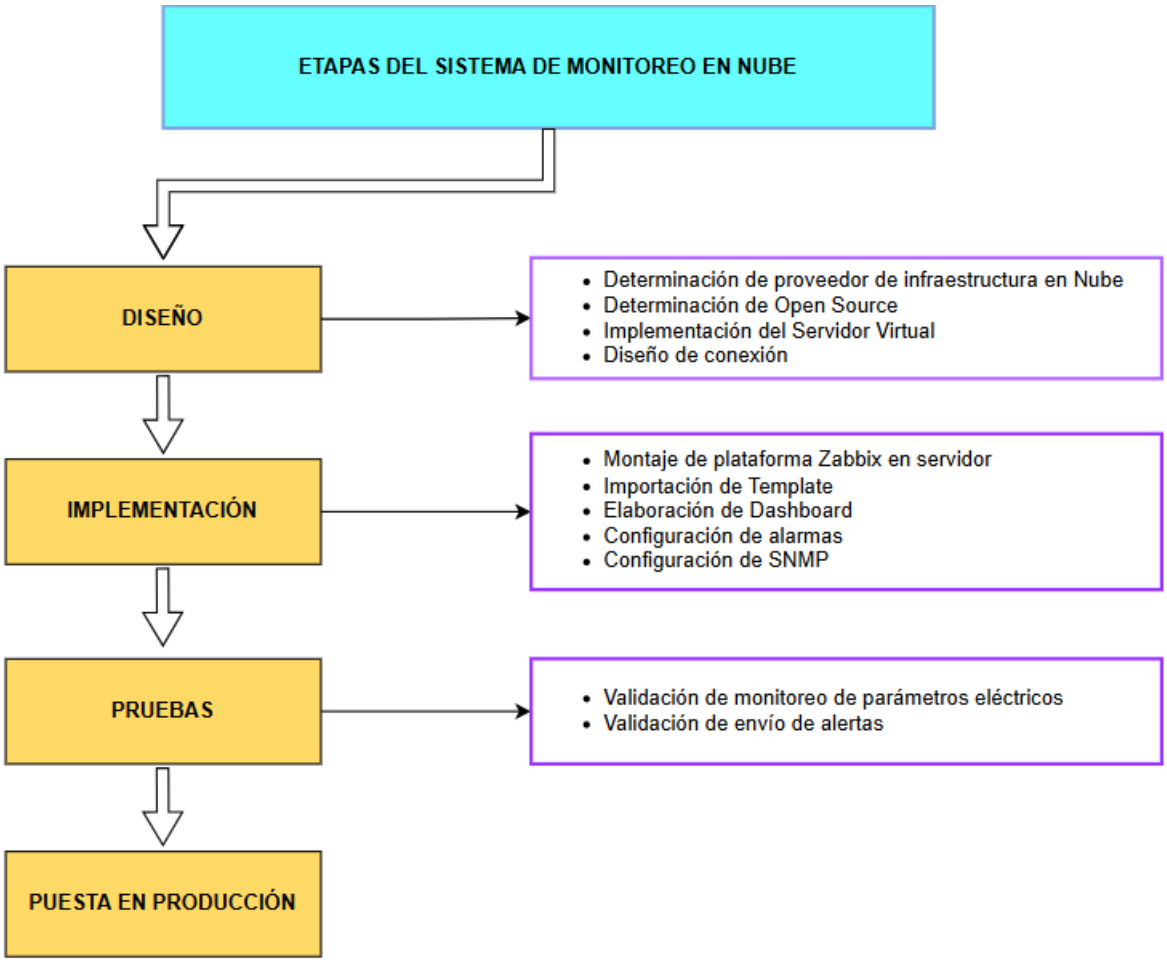
El desarrollo e implementación de un sistema de monitoreo en la nube para los Sistemas de Alimentación Ininterrumpida (UPS) de Tempel Perú se estructura en cuatro etapas clave: diseño, implementación, pruebas y puesta en producción. Estas etapas aseguran una transición eficiente desde la planificación inicial hasta la operación final del sistema, optimizando la supervisión en tiempo real y mejorando la respuesta ante incidentes críticos.

En la etapa de diseño, se determina el proveedor de infraestructura en la nube y la plataforma de monitoreo de código abierto más adecuada, tomando en cuenta factores como la compatibilidad con los UPS, la escalabilidad y los costos. La etapa de implementación abarca la configuración técnica del sistema, incluyendo el montaje del servidor virtual, la creación de plantillas, el diseño del dashboard y la configuración de alarmas para garantizar un monitoreo integral. Posteriormente, en la fase de pruebas, se valida el correcto funcionamiento del sistema mediante la verificación del monitoreo de parámetros eléctricos y el envío de alertas configurables. Finalmente, la puesta en producción asegura la integración completa del sistema y su operación en un entorno real.

En la Figura 10 se presentan de forma esquemática las etapas del sistema de monitoreo en la nube, destacando las actividades principales realizadas en cada fase.

Figura 10

Etapas del sistema de monitoreo en la nube



Nota. El flujograma presenta las etapas clave del proceso, que abarcan el diseño, la implementación, las pruebas y la puesta en producción. Cada fase se desglosa en sus respectivas tareas y secuencias.

3.2.1. Etapa de Diseño

Análisis de la Situación Actual

Los UPS Kaise, desarrollados y fabricados por Tempel Group, se monitoreaban de manera local mediante una tarjeta SNMP, específicamente el modelo NetAgent 9 (véase anexo 1). Esta tarjeta, fabricada por Net Agent, que es un integrador de la marca Kaise, añadía funciones de administración y monitoreo de red. La tarjeta se insertaba en la ranura de expansión de comunicación del UPS y se conectaba a la red mediante un puerto RJ45, compatible con velocidades Fast Ethernet (10/100 Mbps), lo cual garantizaba una transmisión de datos suficiente para la supervisión remota en tiempo real. La tarjeta utiliza el puerto UDP 161 para recibir y enviar comandos de monitoreo y el puerto 162 para la recepción de notificaciones de eventos (traps). En la Figura 11 se muestra físicamente la tarjeta SNMP NetAgent instalada en el UPS, destacando el puerto RJ45 de conexión de red.

Figura 11

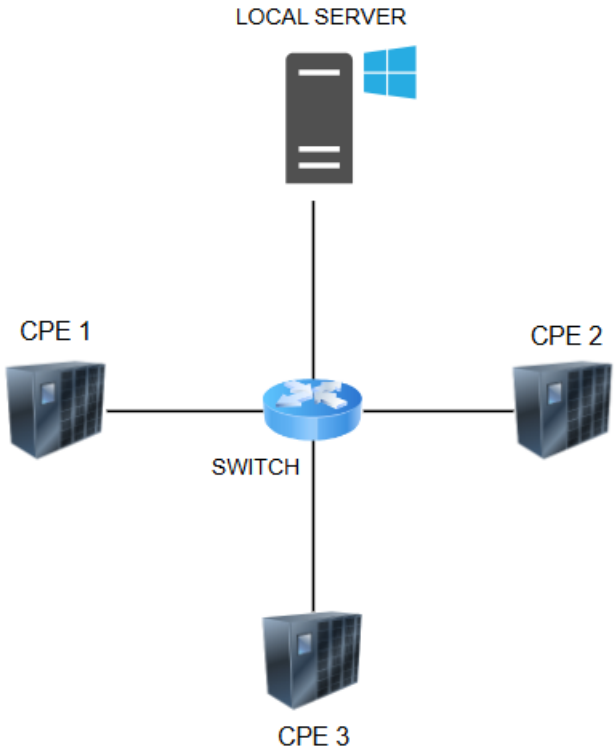
Tarjeta SNMP-CY54-03

Nota. Vista frontal de la tarjeta SNMP del fabricante NetAgent.

En la Figura 12 se ilustra la topología originaria de monitoreo, donde cada UPS Kaise se operaba de forma independiente, sin una plataforma centralizada, lo que limita la visibilidad y obliga al equipo técnico a realizar diagnósticos locales o desplazarse al sitio del cliente.

Figura 12

Topología LAN de monitoreo UPS Kaise

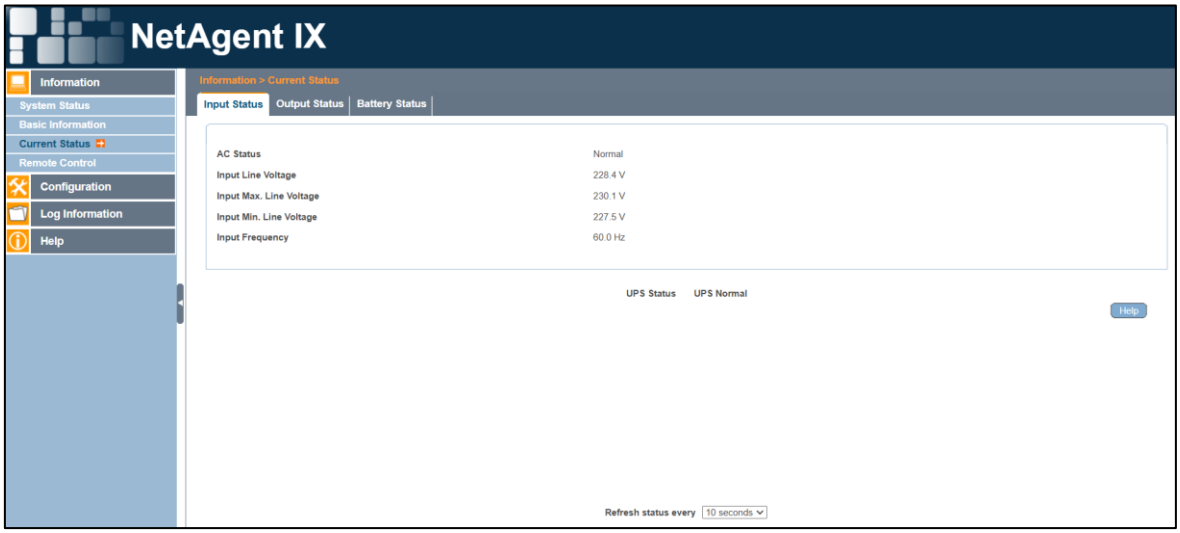


Nota. El esquema ilustra cómo los UPS se conectaban en una red común y eran monitoreados de esta misma.

Además, en la Figura 13 se presenta una captura de la plataforma de monitoreo de NetAgent, la cual ofrece una interfaz básica que muestra solo parámetros limitados y no cuenta con gráficos o historial de datos detallados, dificultando el análisis y la identificación de patrones de comportamiento.

Figura 13

Interfaz de plataforma NetAgent IX

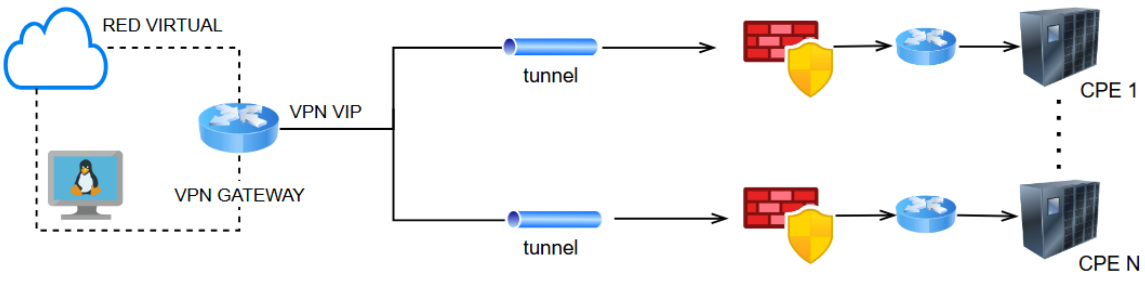


Nota. Captura extraída de la interfaz web de NetAgent.

Para superar estas limitaciones, se implementó una nueva topología en la nube, mostrada en la Figura 14, que centraliza el monitoreo de todos los UPS Kaise en nube.

Figura 14

Topología en Nube de monitoreo UPS Kaise

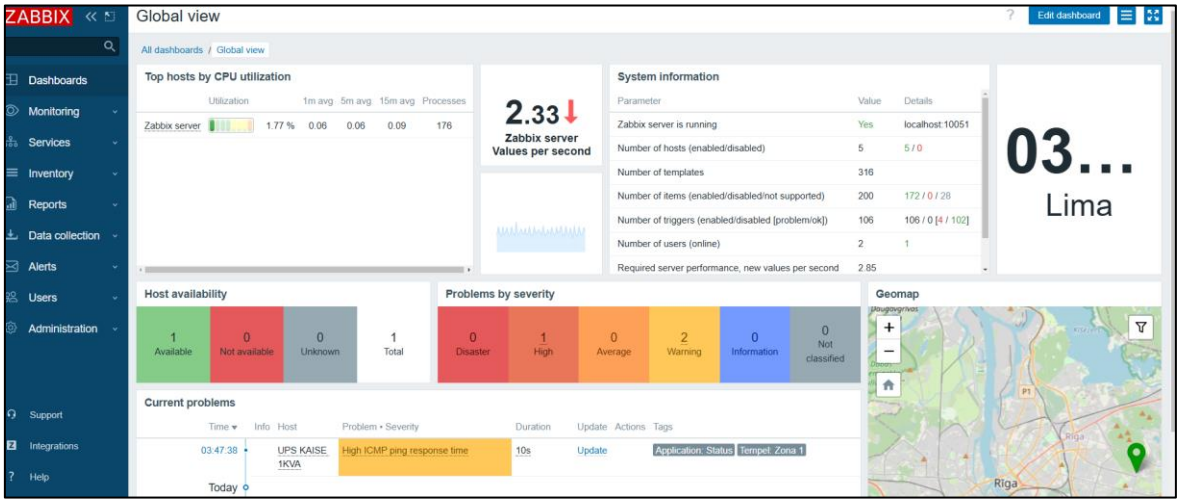


Nota. El esquema ilustra la nueva topología propuesta para el monitoreo de los UPS.

Este nuevo sistema permite monitorear en tiempo real desde una interfaz central, con gráficos históricos y alertas configurables, optimizando la eficiencia operativa y mejorando la respuesta ante incidentes como se muestra en la Figura 15.

Figura 15

Plataforma de monitoreo en Zabbix



Nota. Captura extraída de la interfaz web de Zabbix, donde se puede visualizar un dasboard general por defecto.

Parámetros Críticos a Monitorear y su Importancia

Para garantizar una supervisión eficiente y resolver las deficiencias del sistema anterior, se definieron los siguientes parámetros críticos:

Tensión de Entrada y Salida

- Descripción: Verifica que los voltajes suministrados al UPS y a los dispositivos conectados estén dentro de los rangos aceptables.
- Importancia: Detectar subtensiones o sobrevoltajes permite evitar daños en los equipos conectados. Por ejemplo, una subtensión podría provocar apagones en los dispositivos, mientras que un sobrevoltaje puede dañar circuitos sensibles.
- Acción preventiva: Generar alertas automáticas cuando los valores estén fuera de los rangos establecidos (p. ej., 200-240V para entrada y 220V +/- 10V para salida).

Corriente de Carga

- Descripción: Mide la cantidad de corriente consumida por las cargas conectadas al UPS.

- Importancia: Detectar sobrecargas puede prevenir fallos críticos en el UPS. Por ejemplo, si la corriente supera el límite del equipo, podría generar un sobrecalentamiento y un apagado forzado.
- Acción preventiva: Configurar notificaciones al superar el 90% de la capacidad de corriente nominal.

Estado de la Baterías

- Descripción: Evalúa el nivel de carga, capacidad de la batería y ciclos de carga/descarga.
- Importancia: Detectar baterías agotadas o con baja capacidad es crucial para garantizar el respaldo energético durante interrupciones del suministro eléctrico.
- Acción preventiva: Planificar el reemplazo de baterías antes de que alcancen niveles críticos de desgaste.

Temperatura interna:

- Descripción: Monitorea la temperatura de los componentes internos del UPS.
- Importancia: Un aumento anómalo en la temperatura puede indicar problemas de ventilación, sobrecarga o fallos en los componentes internos. Por ejemplo, temperaturas superiores a 70°C podrían dañar los transistores o los circuitos de control.
- Acción preventiva: Configurar alarmas para temperaturas que excedan los rangos seguros y programar mantenimientos preventivos.

Frecuencia de entrada y salida:

- Descripción: Mide la estabilidad de la frecuencia eléctrica, normalmente 50 o 60 Hz.
- Importancia: Variaciones significativas pueden afectar el rendimiento de los dispositivos conectados, como motores o sistemas electrónicos sensibles.
- Acción preventiva: Ajustar la frecuencia automáticamente dentro del rango permitido.

Alarmas por Eventos Críticos:

- Descripción: Registro y notificación de fallos como pérdida de energía, fluctuaciones extremas o errores internos del UPS.
- Importancia: La generación de alertas en tiempo real permite actuar rápidamente para mitigar impactos negativos.

Análisis de Elección de Proveedor en la Nube: Microsoft Azure

La elección de un proveedor de nube es un aspecto crítico en la infraestructura de sistemas de monitoreo modernos, especialmente para aplicaciones que requieren disponibilidad continua y escalabilidad en tiempo real. La computación en la nube permite una gestión eficiente de datos, reducción de gastos en infraestructura y accesibilidad global, lo que la convierte en una solución atractiva para empresas de todos los tamaños (Armbrust et al., 2010). En este proyecto, la selección de un proveedor de nube compatible con Zabbix fue fundamental para implementar un sistema de monitoreo centralizado y eficiente para los SAI Kaise, garantizando una supervisión en tiempo real, seguridad de datos y una integración fluida con la plataforma de monitoreo.

Microsoft Azure fue el proveedor elegido debido a su rendimiento comprobado en entornos de misión crítica, escalabilidad ajustable y precedentes de integración con Zabbix, lo que ha demostrado ser una solución confiable en proyectos similares (Microsoft Azure, 2023). Otros proveedores como Amazon Web Services (AWS) y Google Cloud Platform (GCP) también fueron evaluados, considerando factores clave como compatibilidad, escalabilidad, seguridad y costos a largo plazo, cada uno de ellos puntualmente comparado según su capacidad para satisfacer los requisitos del proyecto.

La Tabla 2 presenta una comparativa cuantificada que destaca los criterios de selección relevantes para este sistema de monitoreo y la puntuación asignada a cada proveedor en función de su adecuación a las necesidades del proyecto.

Tabla 2

Comparativa de Proveedores de Infraestructura en Nube

Criterio de Selección	Microsoft Azure	Amazon Web Services (AWS)	Google Cloud Platform (GCP)
Compatibilidad e integración con Software libre	5	4	4
Escalabilidad para múltiples dispositivos	5	5	4
Seguridad y cumplimiento normativo	5	5	4
Alta disponibilidad y tolerancia a fallos	5	5	4
Costo inicial y a largo plazo	4	3	4
Soporte técnico y facilidad de uso	4	4	5
Puntuación Total (Máximo 30)	28	26	25

Nota. La comparativa presentada se basa en un análisis general de las características y capacidades de los proveedores de infraestructura en la nube, considerando factores como compatibilidad, escalabilidad, seguridad, costo y soporte técnico. Las puntuaciones y valoraciones se han asignado de manera subjetiva y aproximada en función de las funcionalidades conocidas de cada servicio.

Análisis de la Comparativa:

Microsoft Azure: Con una puntuación total de 28/30, Azure sobresale en la mayoría de los criterios debido a su integración comprobada con Zabbix y su infraestructura segura y escalable. Su capacidad para adaptarse al crecimiento de la red de monitoreo y sus certificaciones de seguridad global lo convierten en una opción óptima para aplicaciones empresariales críticas (Microsoft Azure, 2023).

Amazon Web Services (AWS): AWS también es una solución robusta, logrando 26/30 en la evaluación. Su amplia gama de servicios y escalabilidad global son sus principales fortalezas, aunque presenta costos superiores en comparación con Azure y una integración menos fluida con Zabbix para este tipo de aplicaciones (Rimal et al., 2009)

Google Cloud Platform (GCP): Google Cloud obtuvo 25/30, siendo una opción competitiva en términos de accesibilidad y costos. Sin embargo, su enfoque principal en Big Data y aplicaciones de machine learning limita sus capacidades en la gestión de aplicaciones críticas de monitoreo en tiempo real en comparación con Azure (Zhang et al., 2010).

Conclusión: La elección de Microsoft Azure responde a la necesidad de una infraestructura confiable y escalable que permita una integración óptima con Zabbix, favoreciendo la continuidad operativa y el monitoreo en tiempo real. La combinación de seguridad avanzada, disponibilidad global y compatibilidad hacen de Azure la opción más adecuada para el sistema de monitoreo de UPS Kaise.

Análisis de Elección de Plataforma de Monitoreo

La plataforma de monitoreo es el núcleo del sistema, permitiendo la recopilación y análisis de datos de los UPS en tiempo real. En la Tabla 3, se compararon varias opciones de plataformas de código abierto y de pago, incluyendo Zabbix, Nagios, y PRTG Network Monitor.

Tabla 3

Evaluación de plataformas de monitoreo de código abierto

Sistema de Monitoreo	Versión	Código Abierto	Precio	Facilidad de Instalación	Facilidad de Uso	Soporte
Nagios	XI Free	Sí	Gratuito	No	Sí	Comunidad Gratuita
PRTG	Empresarial	No	$ 1550.00	Sí	Sí	Soporte comercial
Zabbix	Core (Única)	Sí	Gratuito	Sí	Sí	Comunidad y comercial

Nota: La evaluación presentada en la tabla se basa en una comparación general de las plataformas de monitoreo de código abierto, considerando aspectos como la versión, si el código es abierto, precio, facilidad de instalación, facilidad de uso y

soporte. Las valoraciones y características mostradas se basan en la información disponible públicamente sobre cada plataforma.

Justificación de la Elección: La decisión final fue optar por Zabbix debido a su robustez, flexibilidad y capacidades avanzadas para la gestión de grandes volúmenes de dispositivos. Zabbix permite una integración completa mediante SNMP, lo que era fundamental para monitorear en tiempo real los UPS Kaise. Su capacidad de almacenar datos históricos y generar gráficos detallados facilita la identificación de patrones y la planificación de mantenimientos predictivos.

Beneficios Específicos de Zabbix:

- Alertas configurables y personalizables: Posibilidad de ajustar parámetros críticos y recibir notificaciones en tiempo real.
- Historial de datos extenso: Ideal para análisis de rendimiento a largo plazo, crucial para el soporte de equipos como los UPS.
- Costos reducidos: Al ser una solución de código abierto, Zabbix permite ahorrar en costos de licencia, optimizando el presupuesto sin comprometer la funcionalidad.

La fase de diseño estableció las bases técnicas y estratégicas para el desarrollo del sistema de monitoreo en la nube, identificando Microsoft Azure y Zabbix como las herramientas más adecuadas por su compatibilidad, escalabilidad y eficiencia. Este diseño responde a las necesidades actuales y garantiza una implementación alineada con los objetivos del proyecto.

Con esta etapa finalizada, se da paso a la fase de implementación, donde se integrarán y configurarán las tecnologías seleccionadas para optimizar el monitoreo en tiempo real.

Diseño de la Infraestructura en Nube

La creación de la infraestructura en la nube en Microsoft Azure se llevó a cabo de manera secuencial, desde la configuración inicial de la suscripción hasta la creación de la máquina virtual que alojará los servicios del sistema de monitoreo. Este enfoque asegura una estructura sólida y escalable para las necesidades del proyecto.

Creación de la suscripción

La suscripción es el primer paso para establecer la infraestructura en Azure. Este componente asigna un espacio en la nube y define los costos asociados al uso de los recursos. Se realizó la configuración inicial para:

- Centralizar el control financiero del proyecto.
- Administrar los permisos necesarios para los equipos técnicos.

La Figura 16 muestra el entorno del portal de Azure durante la configuración de la suscripción.

Figura 16

Configuración inicial de la suscripción en Azure

Nota: Captura de pantalla generada en el entorno de Microsoft Azure.

Creación del grupo de recursos

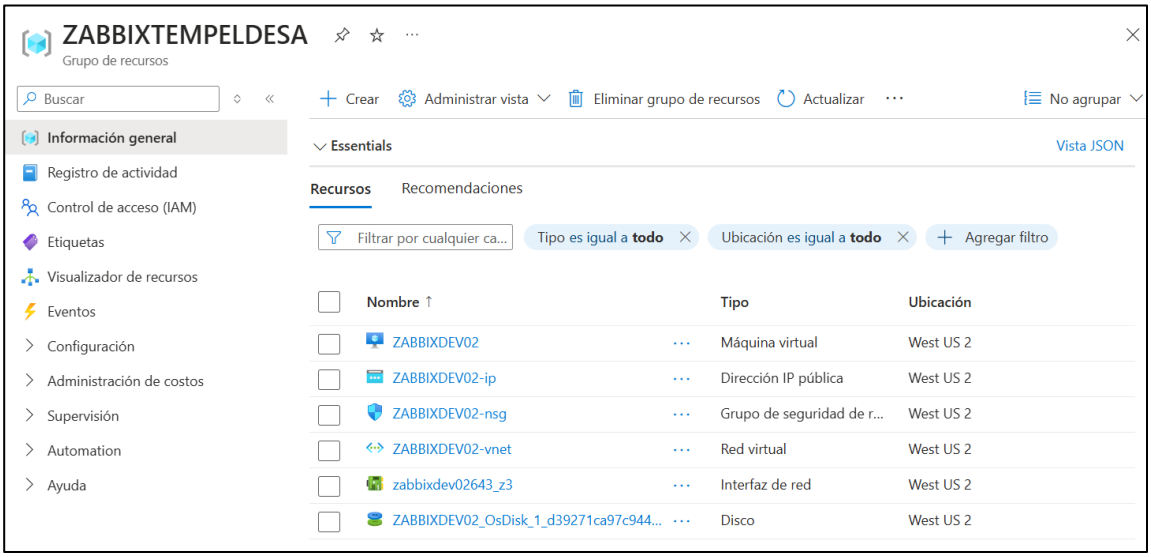
Se configuró un grupo de recursos que agrupa los componentes necesarios del proyecto, como redes, puertas de enlace y máquinas virtuales. Esto permite:

- Una administración lógica y organizada de los recursos.
- Aplicación de políticas de seguridad y gestión centralizada.

En la Figura 17 se observa la estructura inicial del grupo de recursos configurado.

Figura 17

Grupo de recursos en Azure



Nota: Captura de pantalla generada en el entorno de Microsoft Azure.

Configuración de la red virtual

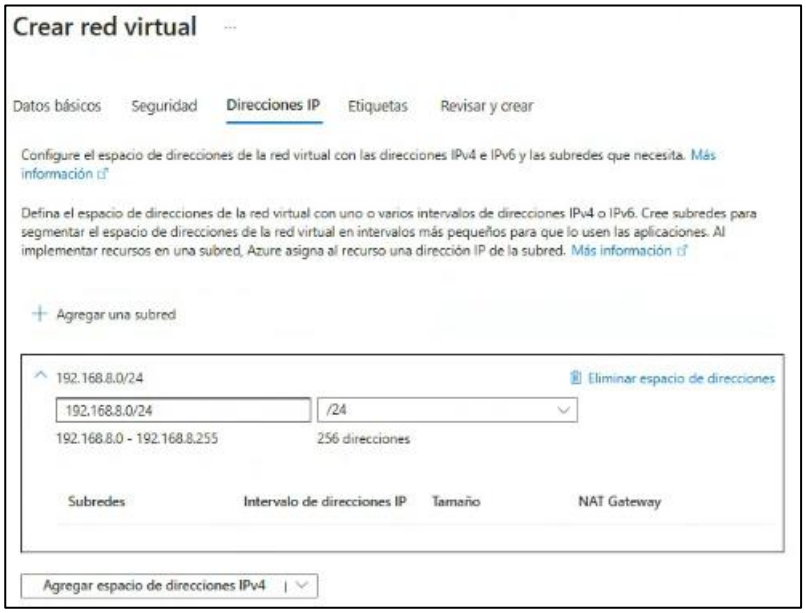
La red virtual (VNet) fue diseñada para soportar el sistema de monitoreo, asegurando conectividad segura y segmentada. Los pasos técnicos incluyeron:

- ✓ Dimensionamiento de la red:
  Espacio de direcciones: rango IP privado asignado según las necesidades del cliente.
- ✓ Creación de subredes:
  - Subred para el servidor Zabbix.
  - Subred GatewaySubnet para la configuración de la VPN.

Según las mejores prácticas de Azure, la GatewaySubnet es necesaria para el protocolo Site-to-Site, que conectará la red local y la nube. En la Figura 18 y en la Figura 19 se muestra el diseño de la red virtual con las subredes configuradas.

Figura 18

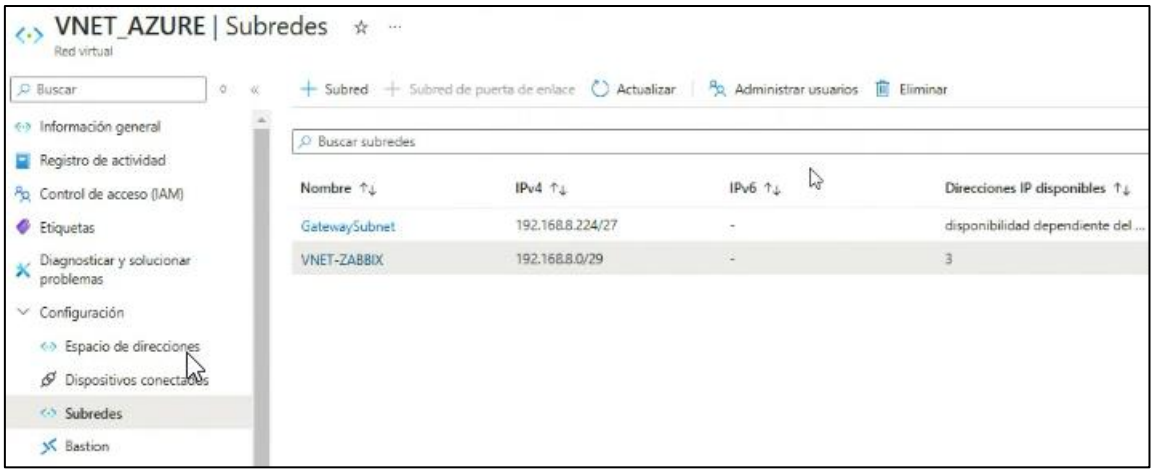
Diseño de la red virtual



Nota: Captura de pantalla generada en el entorno de Microsoft Azure.

Figura 19

Diseño de la subred GatewaySubnet y subred para Zabbix



Nota: Captura de pantalla generada en el entorno de Microsoft Azure.

Configuración de la puerta de enlace de red local

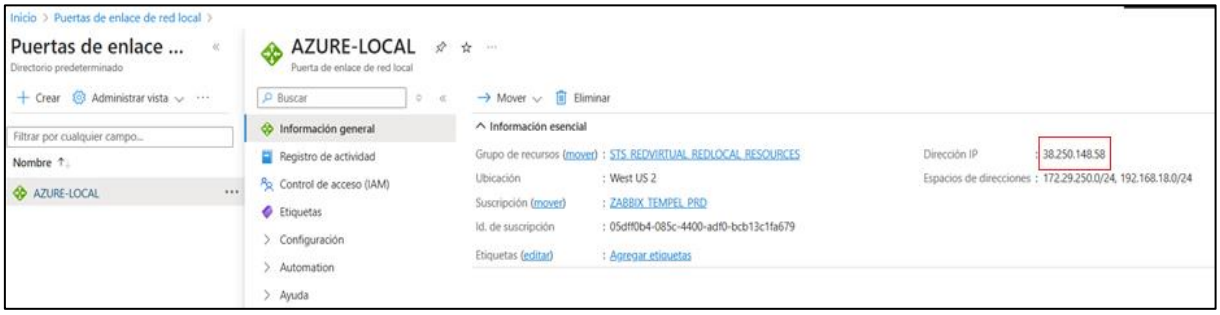
La puerta de enlace de red local define los parámetros de la red física del cliente para su integración con la nube. Se configuraron los siguientes elementos:

- Dirección IP pública del cliente: 38.250.148.58.
- Segmentos de red local para dispositivos SAI y otros equipos físicos.

Este paso asegura que el túnel VPN Site-to-Site pueda comunicarse correctamente con la infraestructura en Azure. En Figura 20 se detalla la configuración de la puerta de enlace local.

Figura 20

Configuración de la puerta de enlace de red local



Nota: Captura de pantalla generada en el entorno de Microsoft Azure.

Configuración de la puerta de enlace de red virtual

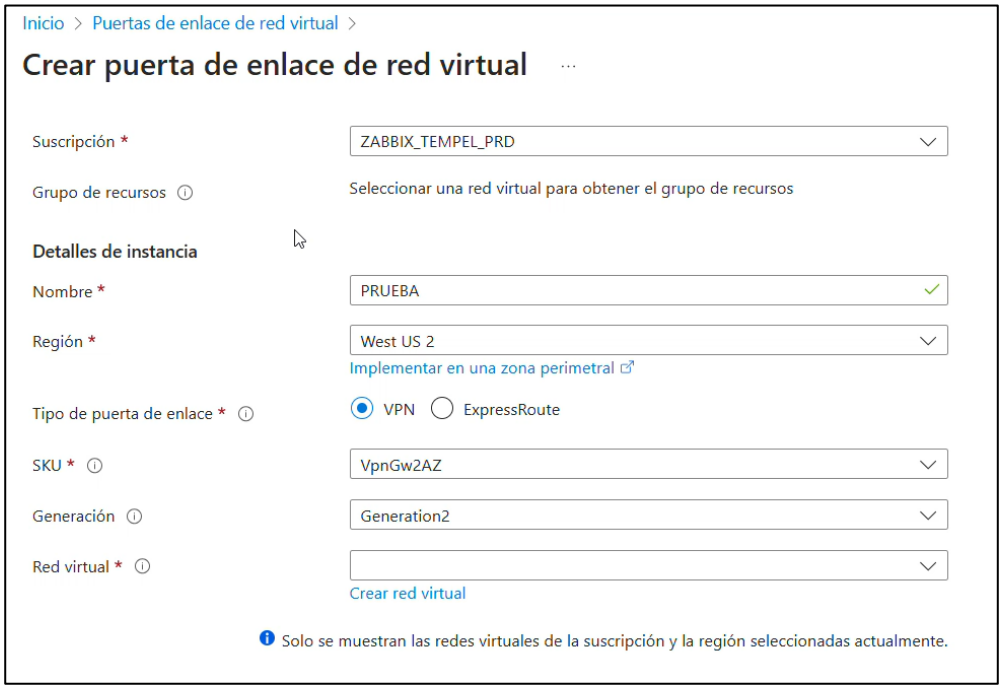
La puerta de enlace de red virtual conecta la infraestructura en la nube con el túnel VPN. Se configuraron los siguientes parámetros:

- **SKU**: Basic, optimizada para un tráfico de red moderado.
- **Asignación de IP pública**: Generada automáticamente por Azure para el acceso externo.

Este componente es esencial para enrutar el tráfico entre los segmentos de la red virtual y la red local. La Figura 21 ilustra el proceso de configuración de la puerta de enlace virtual.

Figura 21

Configuración de la puerta de enlace de red virtual



Nota: Captura de pantalla generada en el entorno de Microsoft Azure.

Configuración del túnel Site-to-Site

El túnel Site-to-Site se configuró para garantizar una conexión segura entre la red local y la infraestructura en la nube. Este paso incluyó:

✓ Configuración en Azure:

Dirección IP pública de la red local: 38.250.148.58.

Segmentos de red locales proporcionados por el cliente.

✓ Configuración en el MikroTik RB750:

Protocolo: IPsec.

Métodos de autenticación: Clave compartida (pre-shared key).

Encriptación: AES-CBC-256.

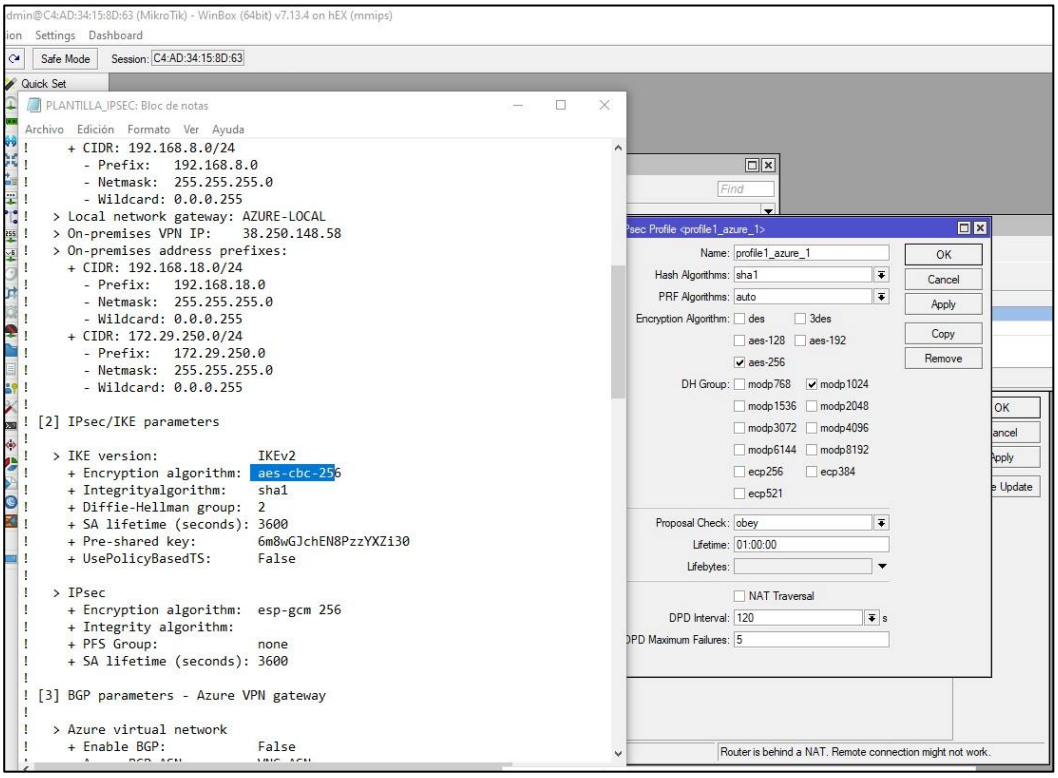
Algoritmo de integridad: SHA-1.

Grupo Diffie-Hellman: Grupo 2.

En la Figura 22 se detalla la configuración de IPsec en el dispositivo MikroTik, mostrando el estado operativo del túnel.

Figura 22

Configuración del túnel IPsec en MikroTik RB750

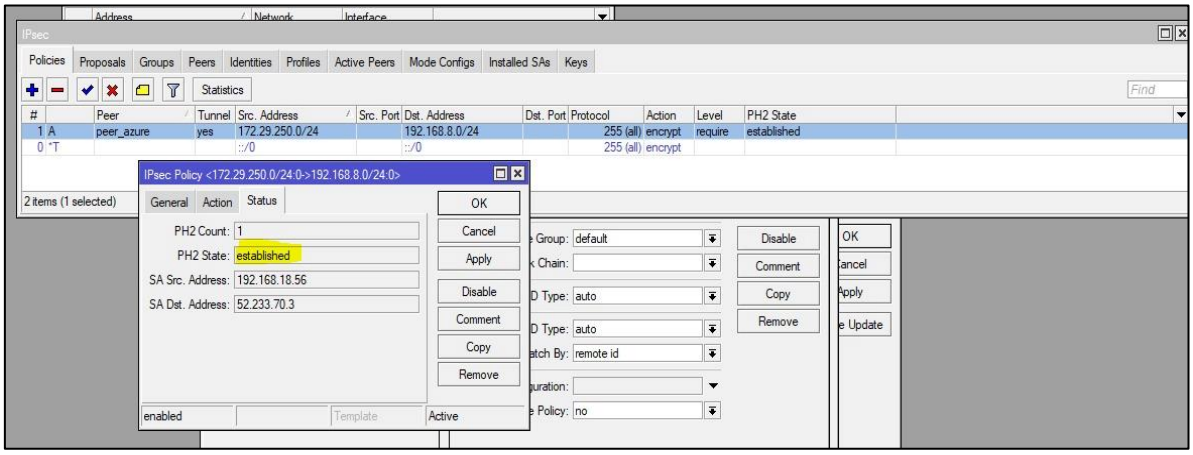


Nota: Captura de pantalla generada en la consola de administración del Mikrotik RB750.

Una vez establecidos los parámetros de configuración en Azure y en el dispositivo MikroTik RB750, el túnel Site-to-Site quedó operativo y funcional. En la Figura 23 se presenta el estado operativo del túnel, validado mediante el protocolo IPsec. El estado established confirma que la conexión entre la red virtual en Azure y la red local se encuentra activa y encriptada.

Figura 23

Estado operativo del túnel Site-to-Site configurado con IPsec en MikroTik RB750



Nota: Captura de pantalla generada en plataforma del Mikrotik RB750.

Con este último paso, se garantizó la comunicación segura y estable entre ambos entornos, lo que permitió proceder a la siguiente etapa: la creación y configuración de la máquina virtual que alojará el sistema de monitoreo.

Creación de la máquina virtual

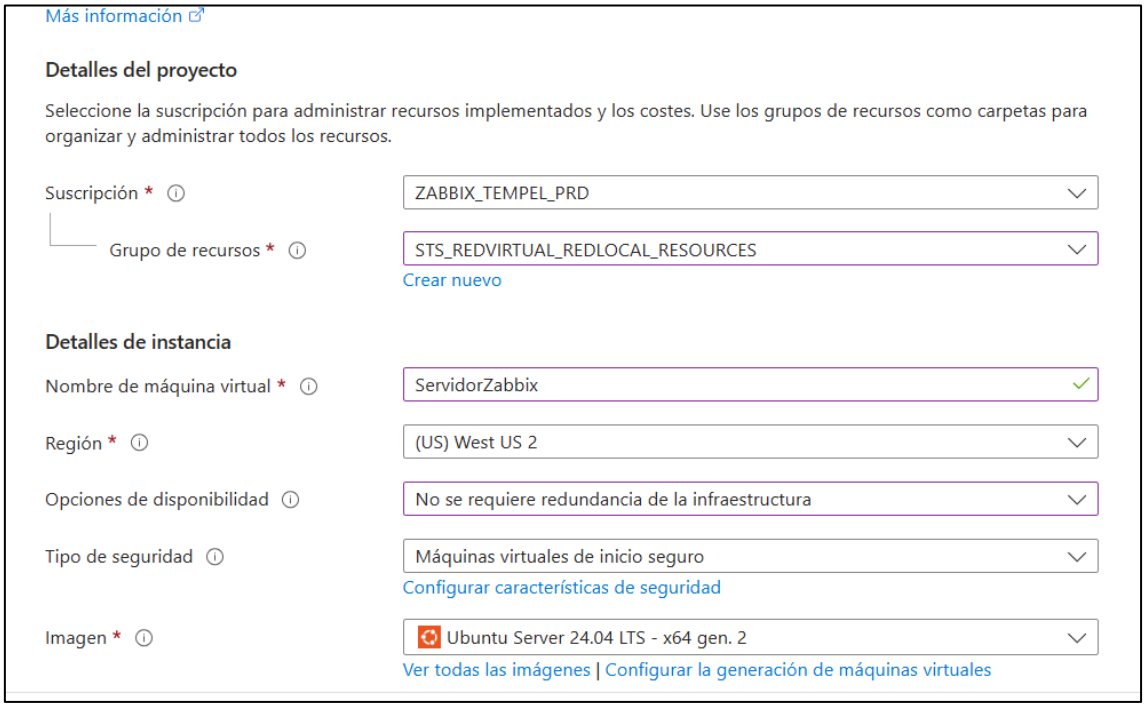
La máquina virtual es el núcleo de la infraestructura, diseñada para alojar los servicios del sistema de monitoreo. Se configuraron los siguientes parámetros técnicos:

- **Tipo de máquina**: *Standard B2ms* (2 vCPUs, 8 GB RAM), adecuada para sistemas de monitoreo con cargas moderadas.
- **Sistema operativo**: Ubuntu 22.04, optimizado para servidores Zabbix.
- **Almacenamiento**: Disco SSD de 100 GB para garantizar un alto rendimiento.
- **Red**: Conexión directa a la subred definida para el servidor.

En la Figura 24 se detalla el entorno de configuración de la máquina virtual, incluida la asignación de recursos y la conectividad.

Figura 24

Vista de la máquina virtual configurada en Azure



Nota: Captura de pantalla generada en el entorno de Microsoft Azure.

3.2.2. Etapa de Implementación

En esta etapa, se llevó a cabo la implementación y configuración de la plataforma Zabbix, enfocándose en habilitar su capacidad de monitoreo para los UPS. Este proceso incluyó la configuración de los hosts, protocolos de comunicación (como SNMP), y la personalización de alertas y dashboards para garantizar una supervisión precisa y en tiempo real. Adicionalmente, se incluyó una fase de pruebas para validar el correcto funcionamiento de las configuraciones realizadas y asegurar la fiabilidad del sistema en un entorno operativo.

Montaje de Plataforma Zabbix

En esta sección se describirá el paso a paso de los comandos utilizados para la instalacion del Zabbix en el servidor Ubuntu 22.04.

✓ **Instalación de Apache y MariaDB**

Se digita el comando: "***sudo apt install apache2 mariadb-server -y***", el cual instala Apache, un servidor web que permitirá servir la interfaz gráfica de Zabbix, y MariaDB, el sistema de gestión de bases de datos necesario para almacenar datos de monitoreo. Al estar acompañado del "***-y***", automatiza el proceso aceptando todas las solicitudes de confirmación.

✓ **Agregar el repositorio para PHP**

Se digito el comando: "***sudo apt install ca-certificates apt-transport-https software-properties-common***".

Estos paquetes aseguran que el sistema pueda manejar conexiones HTTPS para agregar repositorios seguros y administrar fuentes adicionales de software.

Además, se digito el comando "***sudo add-apt-repository ppa:ondrej/php***" que agrega un repositorio confiable que contiene versiones modernas de PHP, necesarias para la instalación de Zabbix.

✓ **Actualización del sistema**

Para este punto se ejecutó los comandos "***sudo apt update -y && sudo apt upgrade -y***".

En este caso es importante, por lo siguiente:

apt update: Actualiza la lista de paquetes disponibles en el sistema.

apt upgrade: Instala las versiones más recientes de los paquetes instalados para garantizar que el sistema esté actualizado.

✓ **Instalación de PHP y extensiones necesarias**

Se digito el comando: "***sudo apt install php8.3 libapache2-mod-php8.3 php8.3-common php8.3-fpm php8.3-cgi php8.3-bcmath php8.3-gd php8.3-imap php8.3-intl php8.3-apcu php8.3-cli php8.3-mbstring php8.3-curl php8.3-mysql php8.3-xml unzip -y***"

Básicamente instalo PHP en la versión 8.3 y todas las extensiones requeridas por Zabbix, como:

- ***php8.3-curl**:* Para manejar solicitudes HTTP.
- ***php8.3-mysql**:* Para interactuar con la base de datos MariaDB.
- ***php8.3-cli**:* Herramientas de línea de comandos necesarias para ejecutar scripts PHP.

✓ **Verificar la instalación de PHP**

Se digita el comando "***php -v***" para que muestre la versión de PHP instalada, confirmando que se instaló correctamente.

Posteriormente ejecutar "***sudo service apache2 restart***" para reiniciar el Apache y asegurar que reconozca la nueva configuración PHP y sus extensiones.

✓ **Configuración de acceso remoto para MariaDB**

El comando "***sudo nano /etc/mysql/mariadb.conf.d/50-server.cnf***" edita el archivo de configuración de MariaDB para permitir conexiones externas.

*Se cambia bind-address = 127.0.0.1 a bind-address = 0.0.0.0, lo que permite aceptar conexiones desde cualquier dirección IP.

Luego "***sudo service mysql restart***" para reiniciar Maria DB y validar los cambios en el archivo de configuración.

✓ **Agregar el repositorio de Zabbix**

El comando "***wget https://repo.zabbix.com/zabbix/6.4/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.4-1+ubuntu22.04_all.deb***" descarga el archivo de iinstalacióndel repositorio de Zabbix para Ubuntu 22.04.

Luego se instala el paquete descargado con el comando "***sudo dpkg -i zabbix-release_6.4-1+ubuntu22.04_all.deb***", habilitando el repositorio de Zabbix en el sistema.

Finalmente actualizar nuevamente con el comando "***sudo apt update"*** para asegurar que el sistema reconozca los paquetes disponibles desde el nuevo repositorio.

✓ **Instalar Zabbix**

El comando "***sudo apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent****".* Incluye la siguiente instalación:

- ***zabbix-server-mysql****:* Configura el servidor Zabbix para interactuar con MariaDB.
- ***zabbix-frontend-php****:* Proporciona la interfaz gráfica de Zabbix.
- ***zabbix-apache-conf****:* Configura Apache para servir la interfaz de Zabbix.
- ***zabbix-agent****:* Permite monitorear la máquina donde se instala Zabbix.

✓ **Configuración de la base de datos para Zabbix**

Accedemos a MariaDB como usuario administrador con el comando "***mysql -uroot -p***".

Creamos la base de datos configurada para manejar caracteres multilingües y datos complejos con el comando: "***create database zabbix character set utf8mb4 collate utf8mb4_bin***"

Se creo un usuario para Zabbix: Proporcionándole permisos completos sobre la base de datos, por ejemplo:

create user zabbix@localhost identified by 'zabbix';
grant all privileges on zabbix.* to zabbix@localhost;

Finalmente, con el comando "***zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-character-set=utf8mb4 -uzabbix -p zabbix",*** se Importa las tablas y datos iniciales necesarios para Zabbix.

✓ **Configurar Zabbix**

Para especificar la contraseña, aplicamos "***sudo nano /etc/zabbix/zabbix_server.conf***"

Por ejemplo, **"*DBPassword=zabbix***"

✓ **Inicia los servicios de Zabbix**

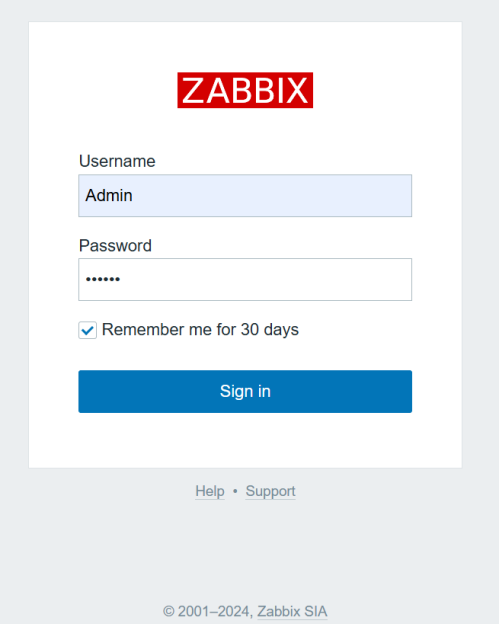
Reiniciamos los servicios para aplicar los cambios y se configuro los servicios para que inicien automáticamente al encender el sistema con los comandos: ***"sudo systemctl restart zabbix-server zabbix-agent apache2"***
"sudo systemctl enable zabbix-server zabbix-agent apache2"

✓ **Resultado final:**

Finalmente se accede a la interfaz de Zabbix desde el navegador:
http://<dirección_IP>/zabbix
Con esto, se tuvo un sistema de monitoreo funcional basado en Zabbix, configurado para monitorear y administrar dispositivos en tiempo real listo para usar, como se muestra en la Figura 25.

Figura 25

Interfaz de Registro de Zabbix



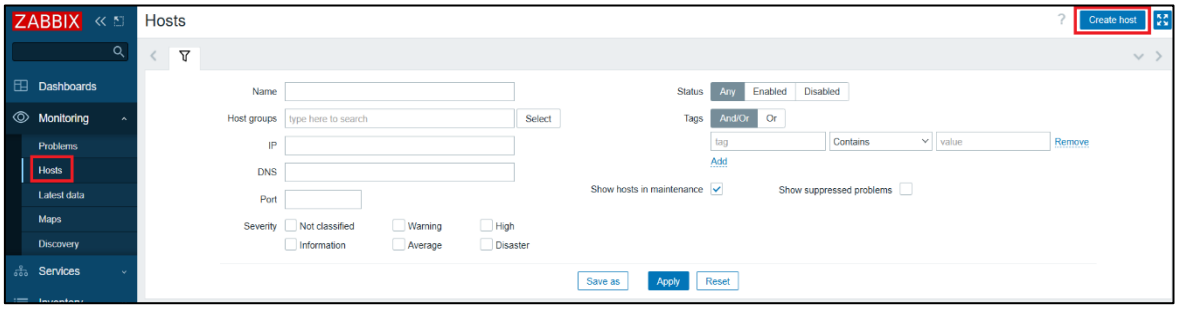
Nota: Captura de pantalla generada en el entorno del software Zabbix (versión 6.4.19).

Creación de Host

En la Figura 26 se ilustra el menú de configuración de Zabbix. Para crear un nuevo Host, es necesario acceder a la opción Hosts, como se observa en la figura. A continuación, se debe hacer clic en el botón Create host.

Figura 26

Menú de Configuración en Zabbix



Nota: Captura de pantalla extraída del entorno del software Zabbix (versión 6.4.19).

Luego, como se observa en la figura 27 se completan los campos requeridos, tales como:

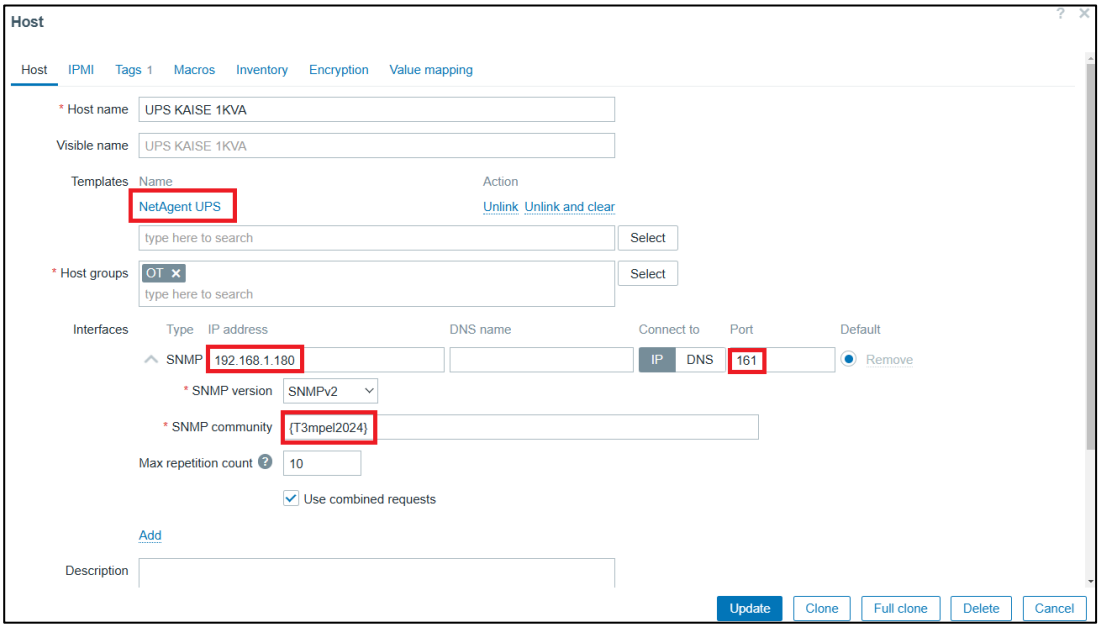
- **Host name:** Nombre del dispositivo o equipo a monitorear.
- **Visible name:** Nombre que será mostrado en la interfaz de Zabbix.
- **Groups:** Grupo al cual pertenecerá el host.
- **Template:** Plantilla que contiene las métricas y configuraciones predefinidas para el monitoreo del host.
- **Interfaces:** Permite especificar el método de monitoreo (por Agente, SNMP, JMX o IPMI).
- **Descripción:** Campo opcional para añadir información adicional sobre el host.

En este caso se usará la interface SNMP donde se tendrá que digitar el IP del UPS a monitorear. Para este caso se hizo pruebas con el IP 192.168.1.180.

Finalmente, se debe hacer clic en el botón Add para guardar y agregar el host al sistema.

Figura 27

Creación de Host en Zabbix



Nota: Captura de pantalla extraída del entorno del software Zabbix (versión 6.4.19).

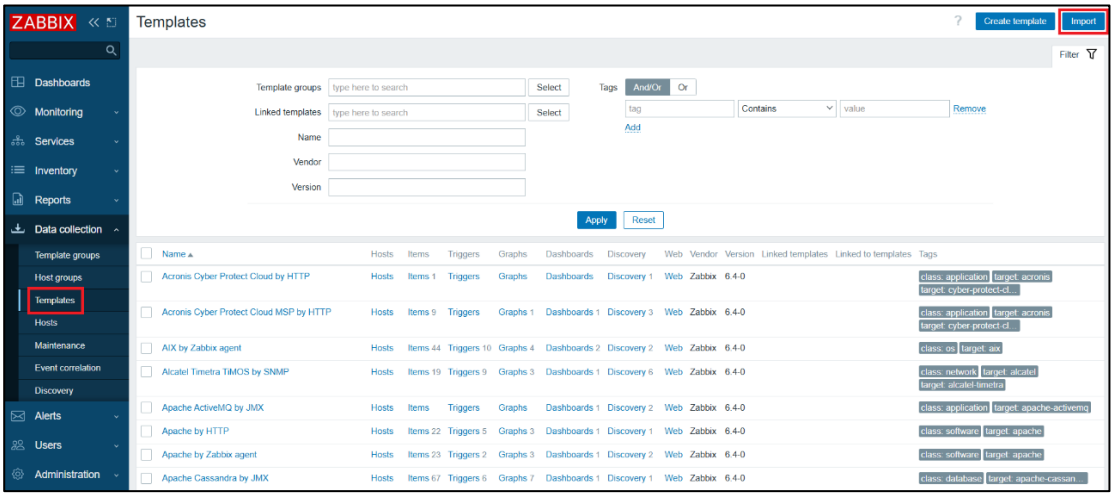
Importación de Plantilla

La asociación de plantillas en Zabbix permitió definir las métricas y configuraciones predefinidas para el monitoreo de los hosts. En este caso, se realizó el proceso de importación y asociación de una plantilla proporcionada por el fabricante de la tarjeta SNMP, Net Agent, siguiendo un enfoque técnico y sistemático.

Primero, se accedió a la sección de plantillas desde la interfaz de Zabbix. Para ello, se inició sesión en el sistema y se navegó al menú principal, seleccionando la opción Configuration > Templates. Una vez en esta sección, se hizo clic en el botón Import, ubicado en la parte superior derecha como se muestra en la Figura 28.

Figura 28

Captura de la sección Plantillas en Zabbix

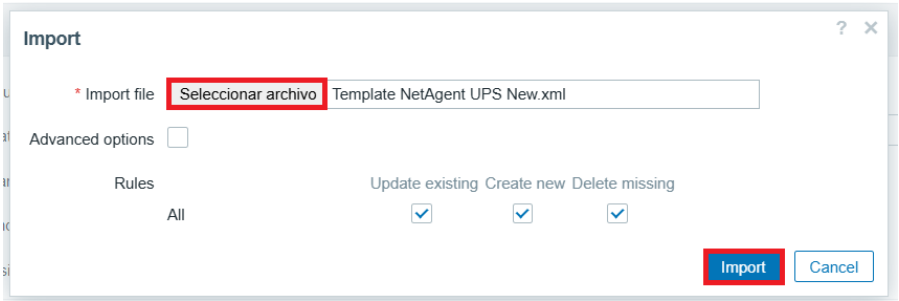


Nota: Captura de pantalla extraída del entorno del software Zabbix (versión 6.4.19).

Posteriormente, en la ventana emergente que apareció, se seleccionó el archivo del template descargado previamente desde el sitio oficial de Net Agent, utilizando el botón Select file para elegir el archivo en formato .xml. Antes de proceder con la importación, se revisaron las opciones predefinidas para garantizar que estuvieran correctamente configuradas. Una vez verificados los datos, se presionó el botón Import, completando así la carga del template en Zabbix. La Figura 29 muestra el formulario de importación con el archivo del template seleccionado.

Figura 29

Formulario de importación de plantillas en Zabbix



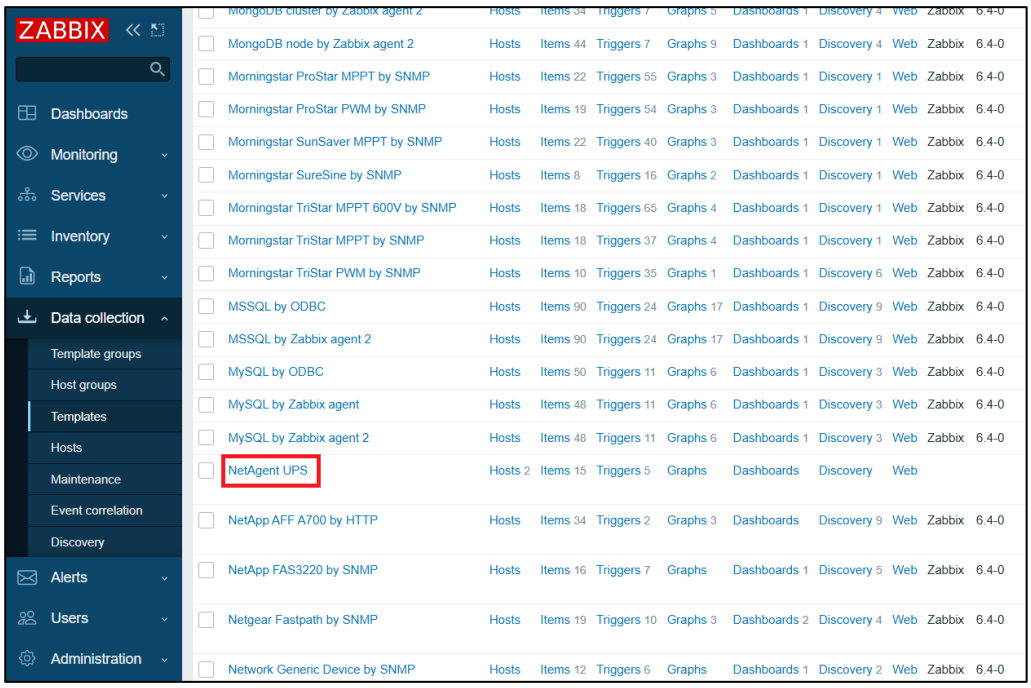
Nota: Captura de pantalla extraída del entorno del software Zabbix (versión 6.4.19).

Tras completar el proceso, se verificó que la plantilla se hubiera cargado correctamente. Esta validación se realizó observando la lista de plantillas

disponibles en la misma sección Templates y utilizando el buscador para localizar la plantilla por su nombre como se observa en la Figura 30.

Figura 30

Verificación de plantilla importada en Zabbix

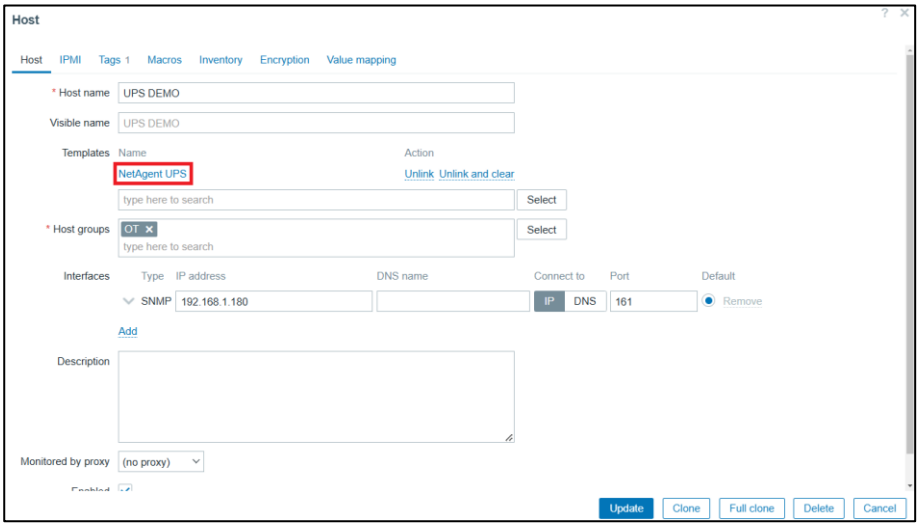


Nota: Captura de pantalla extraída del entorno del software Zabbix (versión 6.4.19).

El siguiente paso fue asociar el template al host correspondiente. Para ello, se accedió a la sección Configuration > Hosts y se seleccionó el host al que se deseaba vincular el template. En la pestaña Templates, se hizo clic en Link new templates, se buscó el nombre del template importado (por ejemplo, “Net Agent”) y se seleccionó. Finalmente, se guardaron los cambios presionando el botón Update. La Figura 31 muestra el formulario de configuración del host con el template asociado.

Figura 31

Asociación de plantilla al host en Zabbix

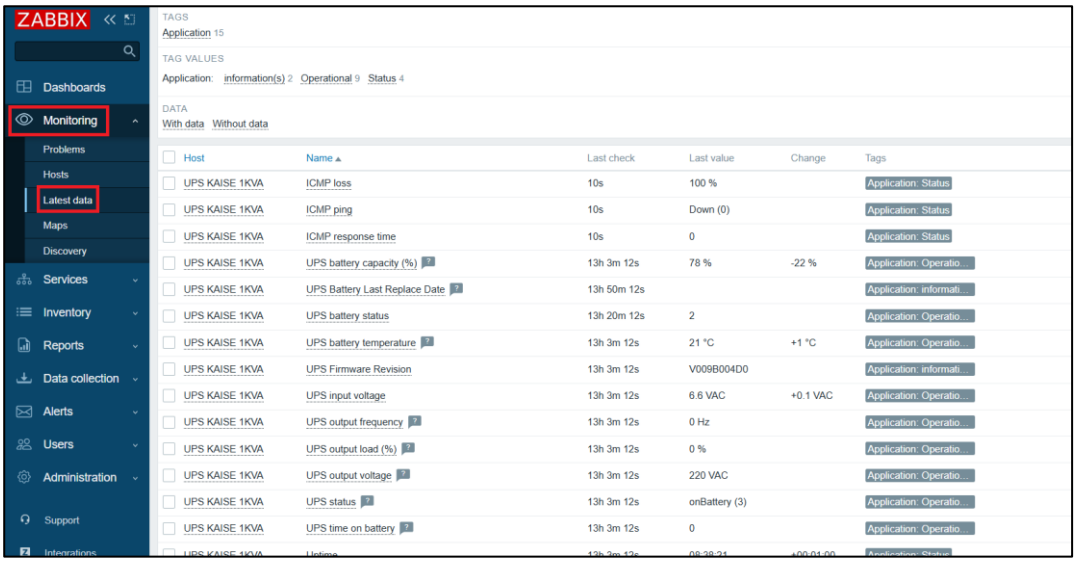


Nota: Captura de pantalla extraída del entorno del software Zabbix (versión 6.4.19).

Para validar la correcta asociación del template, se accedió a Monitoring > Latest data, donde se seleccionó el host configurado. En esta sección, se verificó que las métricas definidas en el template fueran visibles y que Zabbix estuviera recibiendo información del dispositivo monitoreado. La Figura 32 muestra un ejemplo de las métricas monitoreadas del host en la sección Latest data.

Figura 32

Métricas monitoreadas en la sección Latest data de Zabbix



Nota: Captura de pantalla extraída del entorno del software Zabbix (versión 6.4.19).

Es importante destacar que se aseguró la compatibilidad del archivo del template con la versión de Zabbix instalada. Adicionalmente, se verificó la correcta configuración del protocolo SNMP en el dispositivo y en el host para garantizar la recolección de datos. En caso de problemas, los logs de Zabbix se revisaron para identificar y resolver posibles errores de configuración. Con este procedimiento, el host quedó configurado con las métricas y parámetros definidos en la plantilla del fabricante.

Configuración SNMP en el UPS

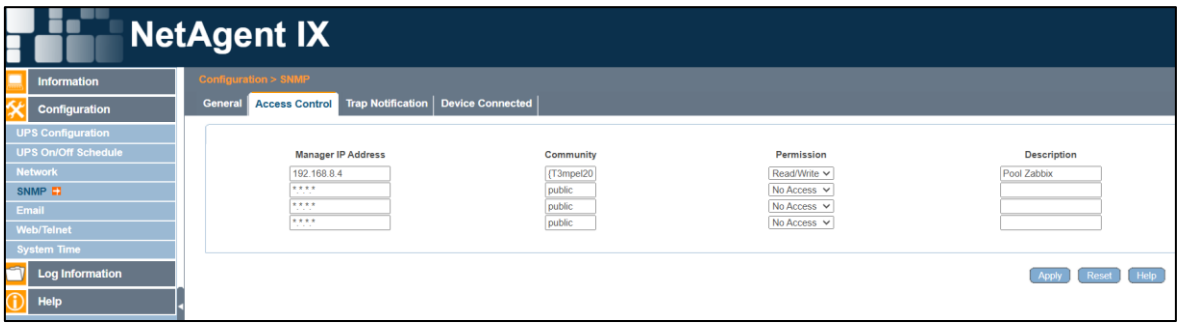
El protocolo SNMP (Simple Network Management Protocol) permite la supervisión y gestión remota de los UPS Kaise. Para habilitar el monitoreo desde el servidor alojado en la nube, se configuró la tarjeta SNMP del UPS utilizando la plataforma de administración remota proporcionada por el fabricante, NetAgent. Esta plataforma permite activar el protocolo SNMP y establecer la comunicación con la dirección IP pública del servidor Zabbix.

El procedimiento comenzó con la conexión física del UPS a una red LAN mediante su tarjeta de red. Una vez conectado, se identificó la dirección IP asignada al UPS dentro de la red local. Con esta información, se accedió a la consola remota del dispositivo a través de un navegador web, donde se realizó la configuración presentada que corresponde a la sección SNMP > Access Control de la interfaz de administración NetAgent IX del UPS. En esta configuración, se define la dirección IP del servidor Zabbix (192.168.8.4) como gestor autorizado para comunicarse con el UPS mediante el protocolo SNMP. Se asigna la comunidad {T3mpel2024} con permisos de lectura y escritura (Read/Write), lo que permite al servidor tanto consultar métricas como ejecutar comandos de configuración en el SAI. Las demás comunidades están restringidas (No Access) para garantizar la seguridad y limitar el acceso únicamente al servidor autorizado. Además, la descripción "Pool Zabbix" identifica el propósito de esta configuración, destinada exclusivamente al sistema de monitoreo. Esta configuración que se observa en la figura 33 asegura una integración segura y eficiente entre el UPS y el servidor Zabbix, permitiendo un

monitoreo en tiempo real de métricas clave como el estado de la batería, tensión de entrada/salida y alarmas.

Figura 33

Configuración SNMP en la interfaz NetAgent IX del UPS

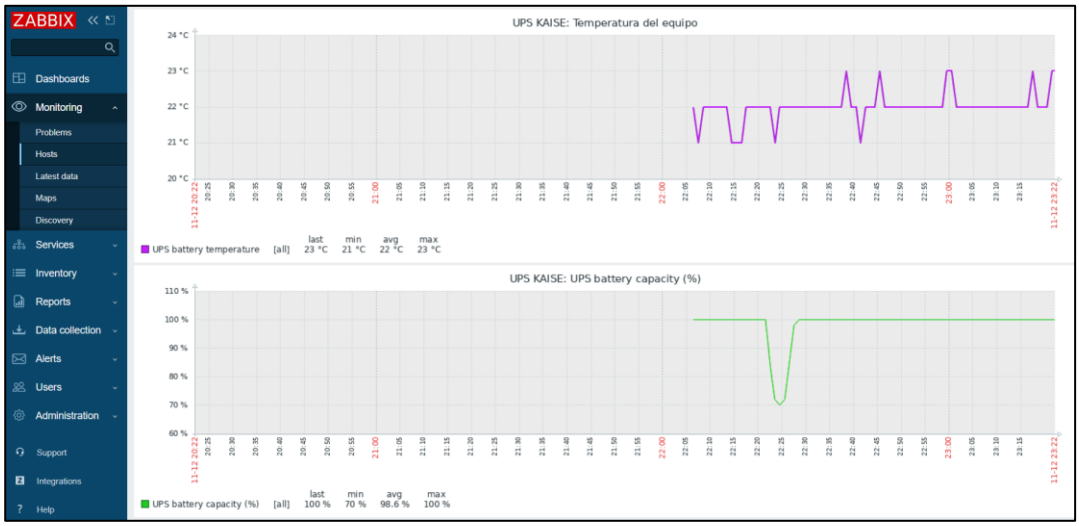


Nota: Captura de pantalla extraída del entorno de la interfaz de NetAgent.

La Figura 34 muestra la validación del registro de logs correspondiente a los ítems configurados en la plantilla importada en Zabbix. Este proceso permite verificar que las métricas definidas en la plantilla, como tensión de entrada, estado de la batería y temperatura interna del UPS, están siendo recolectadas correctamente por el sistema. Los logs confirman que los datos se están registrando en tiempo real y que no existen errores en la comunicación entre el dispositivo monitoreado y el servidor Zabbix, lo que asegura la fiabilidad del monitoreo configurado.

Figura 34

Validación del registro de logs de los ítems en la plantilla importada



Nota: Captura de pantalla extraída del entorno del software Zabbix (versión 6.4.19).

Creación de Triggers en el UPS

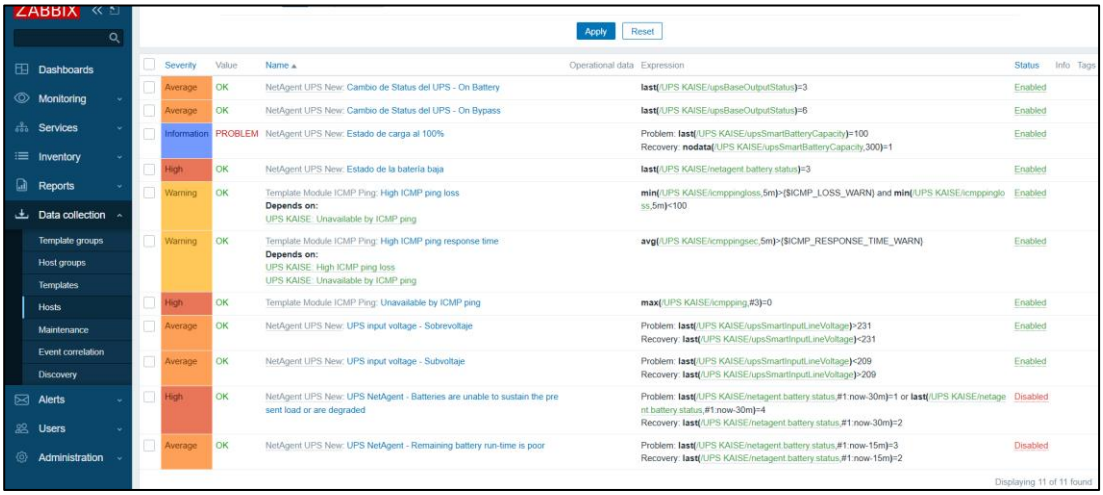
En la Figura 35 se muestra los triggers configurados en Zabbix para el host UPS KAISE, cada uno asociado a métricas críticas del dispositivo, como el estado de la batería, voltajes de entrada/salida y pérdida de paquetes ICMP. Los triggers permiten automatizar el monitoreo mediante la definición de condiciones lógicas o umbrales que, al ser alcanzados, cambian su estado a "problema" y notifican al administrador.

Para crear un trigger en Zabbix, primero se debe tener un ítem configurado que recolecte datos del dispositivo. Luego, en la sección de configuración de triggers, se define una expresión lógica basada en esos datos. Por ejemplo, en este caso, se configuró un trigger que monitorea el voltaje de entrada y alerta sobre sobrevoltaje si excede los 231V o subvoltaje si desciende por debajo de 209V. Además, se configuraron triggers para alertar sobre la capacidad de la batería y el tiempo restante de respaldo.

La personalización de los triggers facilita una respuesta proactiva ante condiciones críticas del UPS, mejorando la eficiencia del monitoreo. Los valores actuales y estados de cada trigger se pueden visualizar y gestionar desde esta interfaz.

Figura 35

Visualización de triggers configurados en Zabbix para el host UPS Kaise



Nota: Captura de pantalla extraída del entorno del software Zabbix (versión 6.4.19).

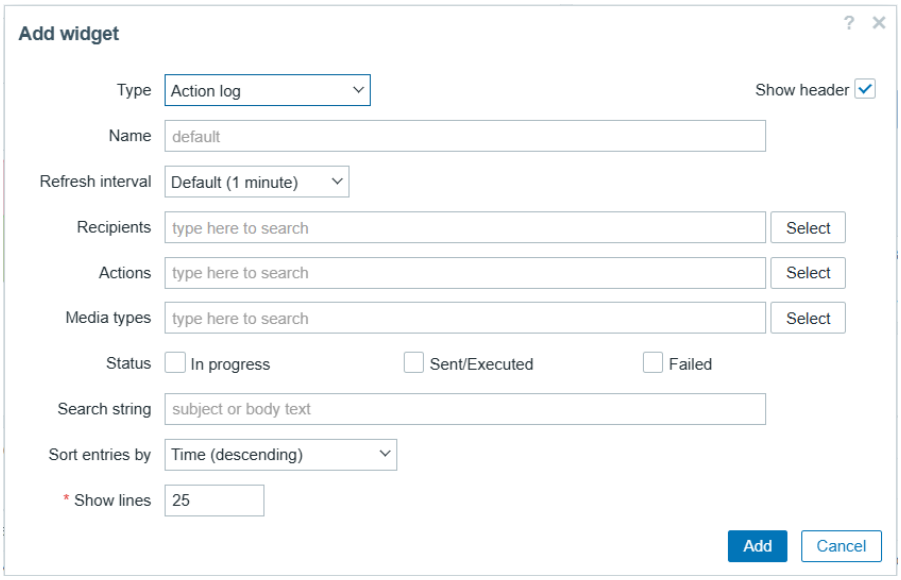
Creación de Dashboard en Zabbix

El dashboard en Zabbix fue diseñado para ofrecer una visualización centralizada y en tiempo real de las métricas clave del UPS Kaise. Se configuraron widgets específicos que permiten monitorear aspectos críticos como tensión de entrada y salida, nivel de batería, temperatura interna, y el estado general del dispositivo. También se incluyeron paneles de alarmas activas para facilitar la identificación rápida de problemas.

En la Figura 36 se visualiza los pasos principales:

Figura 36

Formulario para creación de Widget para Dashboard



Nota: Captura de pantalla extraída del entorno del software Zabbix (versión 6.4.19).

- Selección de widgets relevantes: Se añadieron gráficos históricos, indicadores en tiempo real y un listado de triggers activos.
- Diseño del layout: El dashboard fue organizado para mostrar métricas en secciones claramente diferenciadas.
- Configuración de actualizaciones: Se programó una actualización automática cada 30 segundos para garantizar que los datos reflejen el estado actual del dispositivo.

3.2.3. Etapa de Pruebas

La etapa de pruebas validó el correcto funcionamiento del sistema de monitoreo implementado, evaluando aspectos clave como la recolección de métricas, la configuración de triggers, la personalización del dashboard y las notificaciones automáticas. En la Tabla 4, se resumen los procedimientos realizados junto con sus resultados, complementados por evidencias visuales presentadas en las figuras correspondientes.

Tabla 4

Resumen de la Etapa de Pruebas

Aspecto Evaluado	Procedimiento	Resultado
Pruebas de Métricas	Recolección de datos de ítems configurados, como tensión de entrada y frecuencia de salida.	✓
	Validación de plantillas importadas y monitoreo continuo de dispositivos.	✓
Pruebas de Trigger	Configuración de triggers basados en umbrales: batería baja (<20%) y sobrevoltaje (>240V).	✓
	Simulación de condiciones críticas para observar el cambio de estado del trigger a "problema".	✓
Pruebas de Dashboard	Revisión del diseño y funcionalidad del dashboard en Zabbix	✓
	Validación de la actualización en tiempo real de gráficos y widgets configurados.	✓
Pruebas de Notificaciones	Configuración de correos electrónicos para recibir alertas.	✓
	Simulación de eventos críticos como batería baja y sobrevoltaje.	✓

Nota: En la tabla adjunta se valida el éxito de las pruebas.

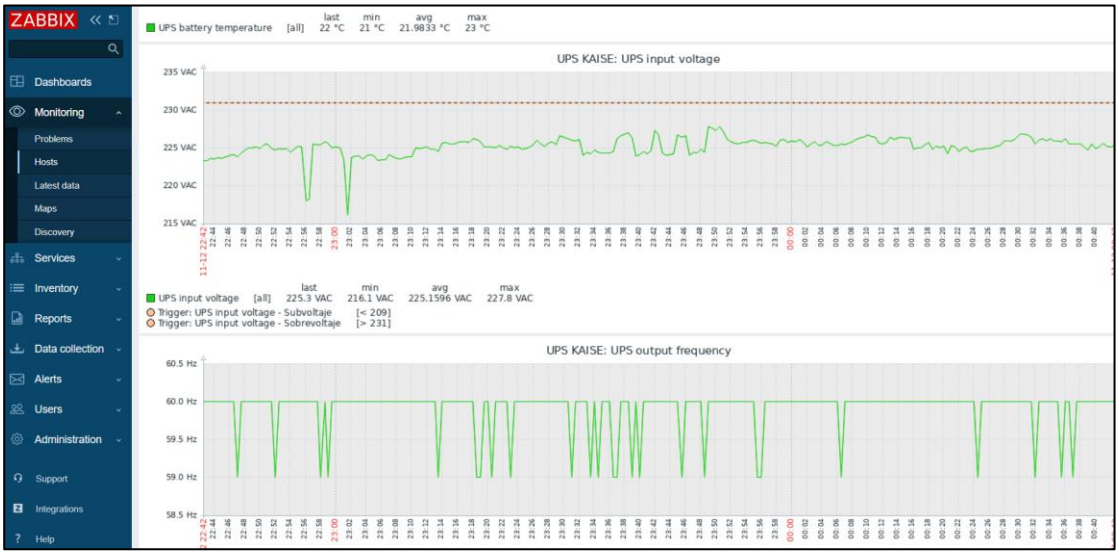
Las siguientes figuras ilustran los resultados obtenidos durante la etapa de pruebas:

Pruebas de Métricas

La Figura 37 muestra la recolección de métricas del UPS Kaise en Zabbix, incluyendo la tensión de entrada/salida y el estado de la batería, validadas en tiempo real.

Figura 37

Visualización de métricas del UPS Kaise en Zabbix



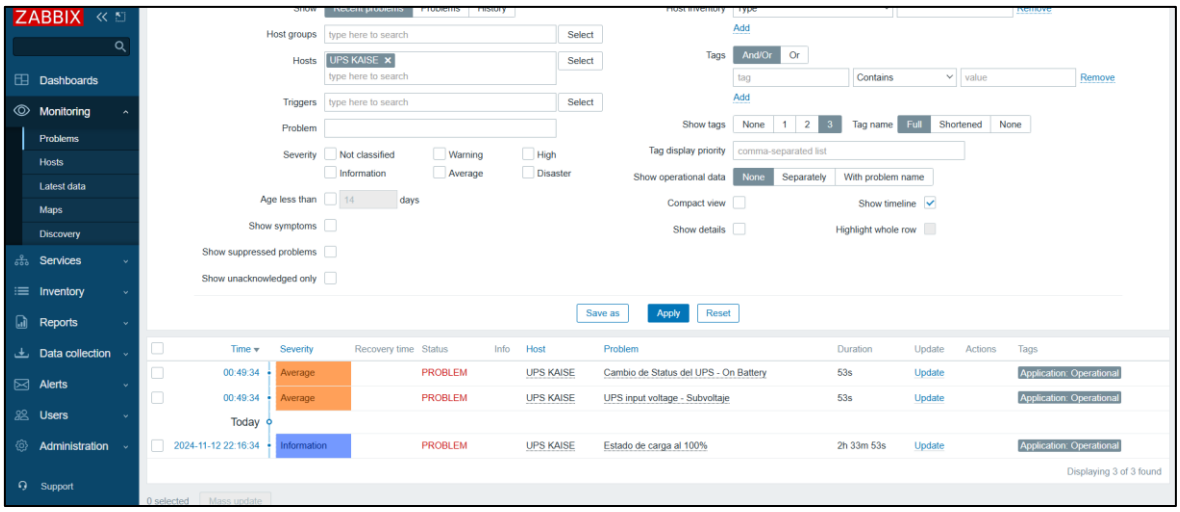
Nota: Captura de pantalla extraída del entorno del software Zabbix (versión 6.4.19).

Pruebas de Triggers

En la Figura 38, se observa la activación de un trigger por cambio de status (On Baterry), lo que generó un cambio automático de estado a "problema".

Figura 38

Activación de Trigger por Cambio de Status del UPS



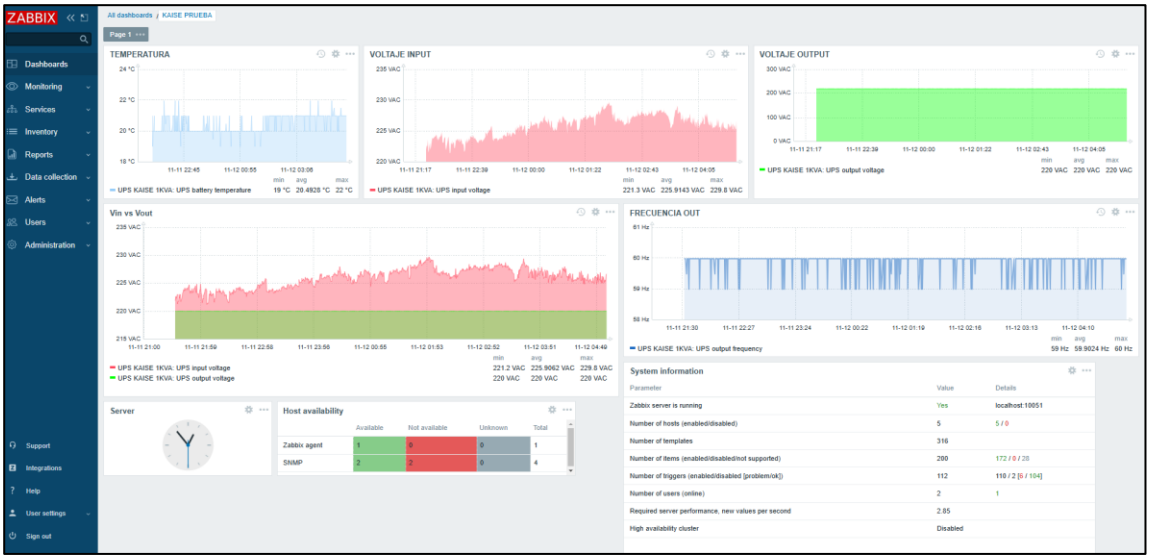
Nota: Captura de pantalla extraída del entorno del software Zabbix (versión 6.4.19).

Pruebas de Dashboards

La Figura 39 presenta el dashboard configurado en Zabbix, mostrando métricas clave y alarmas activas en tiempo real.

Figura 39

Dashboard personalizado en Zabbix con métricas en tiempo real



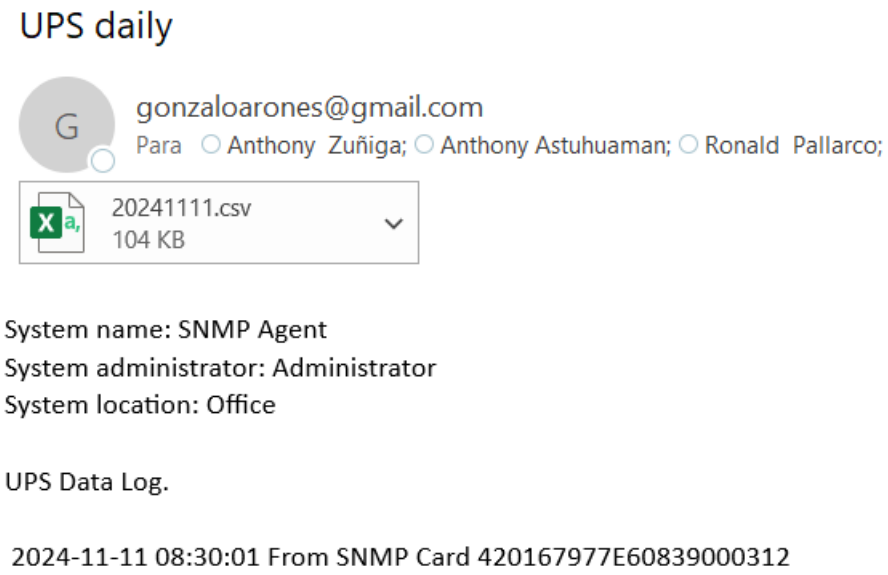
Nota: Captura de pantalla extraída del entorno del software Zabbix (versión 6.4.19).

Pruebas de Notificaciones

La Figura 40 evidencia una notificación enviada automáticamente por Zabbix, describiendo el evento crítico detectado y el host afectado.

Figura 40

Notificación por correo electrónico generada por Zabbix



Nota: Captura de pantalla extraída del entorno del outlook.

Con la etapa de pruebas finalizada, se valida exitosamente el diseño e implementación del sistema de monitoreo en la nube para los SAI Kaise. Las pruebas realizadas confirmaron que el sistema cumple con los objetivos planteados, permitiendo la supervisión en tiempo real, la detección proactiva de problemas mediante triggers, y la centralización de métricas clave en un dashboard intuitivo. Además, se verificó la funcionalidad de las notificaciones automáticas, asegurando una respuesta eficiente ante eventos críticos.

Tras esta validación, el sistema se encuentra listo para pasar a producción. En esta etapa, la operación del software será gestionada directamente por el área de soporte técnico, quienes estarán a cargo del monitoreo continuo, la interpretación de métricas, y la atención de alertas generadas por los dispositivos monitoreados. Esto garantiza la continuidad del servicio y la optimización del desempeño de los equipos.

3.2.4. Contribución en Competencias y Habilidades Adquiridas

El desarrollo del sistema de monitoreo en nube para los UPS Kaise representó una experiencia integral que permitió fortalecer y aplicar competencias clave en Ingeniería Electrónica y Telecomunicaciones. Este proyecto no solo cumplió con los objetivos técnicos, sino que también impulsó el crecimiento en habilidades blandas y de gestión, esenciales en un entorno laboral dinámico y orientado a la innovación tecnológica.

Diseño e implementación de sistemas tecnológicos avanzados:

- La implementación del sistema utilizando Zabbix demostró la capacidad para integrar herramientas de monitoreo avanzadas y personalizarlas según las necesidades específicas del cliente.
- Se adquirió dominio en el manejo de protocolos de comunicación como SNMP, destacando su uso para la recopilación y transmisión de datos en tiempo real.
- El despliegue de infraestructura en la nube mediante Microsoft Azure reforzó habilidades en la configuración de redes virtuales, seguridad en la nube y tunelización segura (Site-to-Site VPN), garantizando la estabilidad y eficiencia del sistema.

Análisis de datos y toma de decisiones:

- La capacidad de monitorear variables críticas como voltaje, corriente y temperatura permitió desarrollar competencias en el análisis y gestión de datos en tiempo real.
- El uso de gráficos históricos y alertas configurables fortaleció la toma de decisiones basada en datos, optimizando procesos de mantenimiento preventivo y correctivo.

Gestión de proyectos tecnológicos:

- La estructuración del proyecto en etapas (diseño, implementación, pruebas y resultados) evidenció una planificación estratégica efectiva y una ejecución alineada con las mejores prácticas de la industria.
- La integración de estándares internacionales como IEC/EN 62040-1 e ISO 27017 validó el cumplimiento normativo y la calidad técnica del sistema desarrollado.

3.3 Resultados

La implementación del sistema de monitoreo en nube para los UPS Kaise de Tempel Perú logró superar las problemáticas identificadas en la etapa de diagnóstico situacional, cumpliendo con los objetivos planteados en el proyecto. En la tabla 5, se detallan los beneficios alcanzados y las mejoras cuantificadas tras la implementación:

Tabla 5

Comparativa de Resultados Antes y Después de la Implementación

Aspecto Evaluado	Antes	Después	Mejora
Tiempo de respuesta promedio	8-10 horas	2-3 horas	70% de mejora
Gastos operativos (mensuales)	S/. 1,950.00	S/. 1230.00	37% de reducción
Inactividad promedio por incidente	4-6 horas	1 hora	80% de reducción
Vida útil estimada de los equipos	7 años	12 años	Incremento del 43%
Volumen de diagnósticos físicos	75%	25%	Reducción significativa

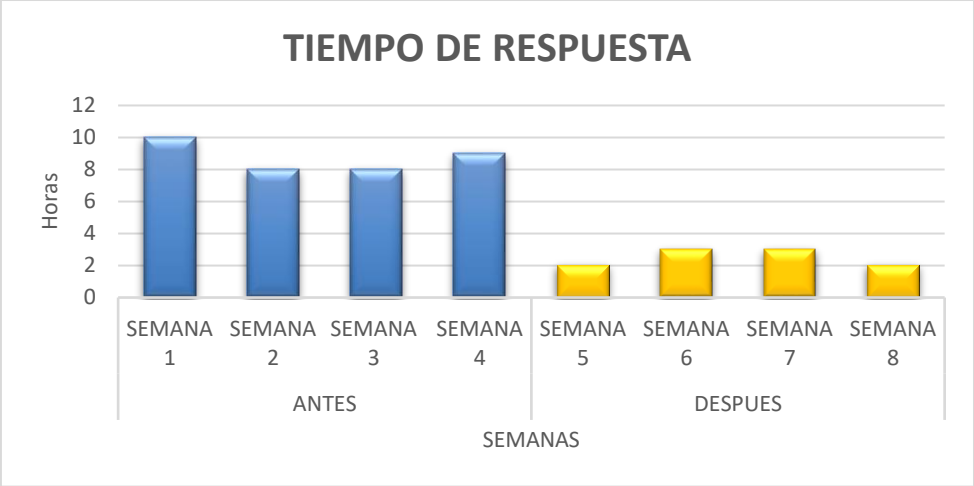
Mejoras obtenidas:

<u>Reducción en el tiempo de respuesta</u>

En la Figura 41 muestra una comparación del tiempo de respuesta antes y después de la implementación del sistema de monitoreo, donde se observa la optimización de los tiempos de respuesta de un 70%.

Figura 41

Comparativa del Tiempo de Respuesta antes y después.



Nota. El grafico representa el tiempo de respuesta semanal ante incidentes. Durante las primeras 4 semanas, antes de la implementación del sistema, el tiempo fue de 9 horas por incidente. Consecutivamente, tras la implementación, se alcanzó reducir significativamente el tiempo de respuesta a un promedio de 2.5 horas por incidente, mostrando una mejora esencial en la eficiencia de respuesta.

Reducción de gastos operativos

En la Figura 42 se visualiza la comparativa de los gastos operativos antes y después de la implementación del sistema de monitoreo, donde se evidencia la reducción de estos hasta en un 37%. El retorno de inversión del sistema (véase anexo 1) resulto en 3.55 meses.

Figura 42

Comparativa de la reducción de gastos operativos antes y después

Nota. El grafico representa la reducción de gastos operativos ante la atención de averías, fallas y alarmas de los UPS. Antes de la existencia del sistema de monitoreo se alcanzaba un monto de S/. 1,950 mensuales. Posteriormente, tras la implementación, se alcanzó reducir los gastos en un 37%, alcanzando un promedio mensual de S/. 1230.

Disminución de inactividad operativa

En la figura 43 se observa la comparación del tiempo de inactividad operativa de los UPS antes y después de la implementación del sistema de monitoreo, donde se observa una mejora del 80% en la continuidad de los equipos.

Figura 43

Comparativa del tiempo de inactividad de los UPS antes y después

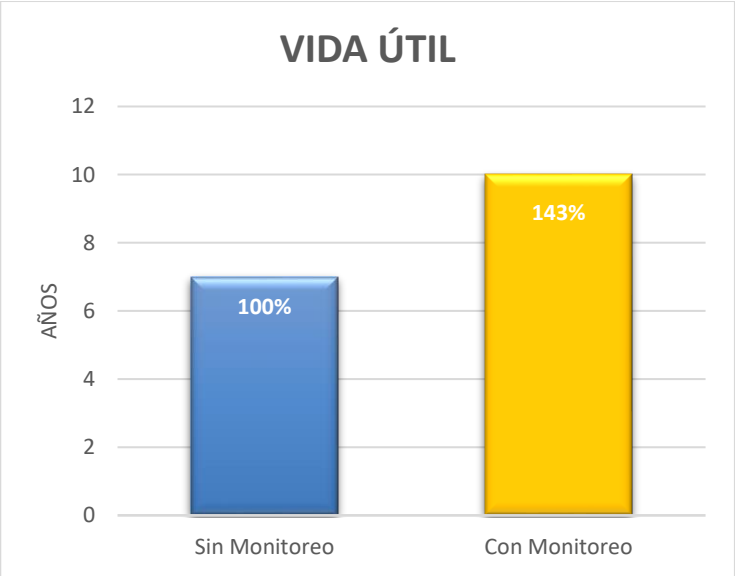
Nota. El grafico representa el tiempo de inactividad semanal ante incidentes. Durante las primeras 4 semanas, antes de la implementación del sistema, el tiempo fue de inactividad de los UPS por incidentes era de 4 a 6 horas. Tras la implementación, se alcanzó reducir significativamente el tiempo de inactividad promedio de 1 hora por incidente. Logrando disminuir en un 80% la continuidad de equipos.

Optimización del mantenimiento preventivo

La vida útil promedio de un UPS de calidad es de 6 años, pero esto puede extenderse si se realiza un buen mantenimiento. En la figura 44 se observa la comparación entre la vida útil de los UPS Kaise antes y después de implementar el sistema de monitoreo.

Figura 44

Comparativa de vida útil de los UPS Kaise antes y después



Nota. El grafico muestra la comparación de la vida útil de los UPS Kaise, donde tras la implementación del monitoreo histórico permitió identificar patrones de uso y desgaste, incrementando la vida útil de los equipos en un 43%.

Centralización y automatización

Gracias al sistema Zabbix, todos los UPS fueron integrados en una única interfaz de monitoreo, con alertas automáticas configuradas para eventos críticos lo que reducido significativamente las atenciones en sitio, como se muestra en la Figura 45.

Figura 45

Dashboard centralizado y automatizado para los UPS Kaise en Zabbix

Nota: Captura de pantalla extraída del entorno del software Zabbix (versión 6.4.19).

CONCLUSIONES

- El diseño incluyo la creación de una infraestructura en la nube mediante Microsoft Azure, integrada con la plataforma Zabbix, lo que permitió centralizar el monitoreo y establecer una solución escalable y segura, cumpliendo los parámetros críticos identificados, como tensión, corriente, temperatura y estado de la batería.

- Se configuró y puso en funcionamiento Zabbix, integrando los UPS mediante el protocolo SNMP, además se implementaron dashboards personalizados y triggers automáticos para alertas, logrando una supervisión remota eficiente, puesto que la infraestructura se probó en condiciones reales, validando la comunicación entre los dispositivos y el servidor en la nube.

- La etapa de pruebas confirmo que el sistema cumpliera con los objetivos planteados, asegurando su confiabilidad para la puesta en producción, específicamente se validó la reducción en el tiempo de respuesta (de 8-10 horas a 2-3 horas), una disminución del 80% en la inactividad operativa, y la optimización del mantenimiento preventivo, lo que extendió la vida útil de los equipos en un 25%.

RECOMENDACIONES

- Capacitar al personal de soporte técnico en el manejo de la plataforma en nube, enfocándose en la gestión de alertas, interpretación de datos y resolución de problemas. Esto permitirá un uso eficiente del sistema y una respuesta oportuna a los incidentes.

- Realizar un mantenimiento preventivo cada seis meses que incluya la actualización del software, revisión de la infraestructura y configuraciones, y evaluación de la seguridad para prevenir vulnerabilidades y garantizar la continuidad del sistema.

- Elaborar un algoritmo basado en recolección, análisis y procesamiento de datos operativos para identificar patrones de fallas en los UPS y poder estructurar un plan de mantenimiento preventivo.

- Evaluar la implementación de un sistema hibrido que combine la infraestructura de la nube con los servidores locales que permita la resiliencia operativa y garantice la continuidad del servicio en caso de que una de estas falle.

REFERENCIAS BIBLIOGRÁFICAS

Acero Fino, N. (2005). ¿Qué es Linux? *REVISTA GUARRACUCO*, *1*(12), Article 12.

ANSI. (2005). *Telecomunications Infraestructure Standard for Data Center-TIA-942*. https://tiaonline.org/products-and-services/tia942certification/ansi-tia-942-standard/

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. *Commun. ACM*, *53*(4), 50-58. https://doi.org/10.1145/1721654.1721672

AWS. (2023). *¿Qué es AWS? - Computación en la nube con Amazon Web Services*. https://aws.amazon.com/es/what-is-aws/

Bernuy Ramirez, J. G., & Villarreal Marcelo, R. J. (2023). Diseño de un sistema de alarmas de monitoreo ambiental utilizando la plataforma ZABBIX para el centro de datos de la empresa WOW PERU. *Universidad Peruana de Ciencias Aplicadas (UPC)*. https://repositorioacademico.upc.edu.pe/handle/10757/670948

Bibbs, E., & Matt, B. (2006). *Comparison of SNMP Versions 1, 2 and 3*.

Calatayud Giner, Jorge. (2014). Universitat Politècnica de València. *Ingeniería del agua*, *18*(1), ix. https://doi.org/10.4995/ia.2014.3293

Castillo, J. A. (2020). *Protocolo TCP/IP - ¿Qué es y cómo funciona?* https://repositorio.usam.ac.cr/xmlui/handle/11506/localhost/xmlui/handle/11506/2181

Castro González, J. S. (2020). *Implementación en la Nube de un Sistema de Monitoreo de Eventos de Fallas para Infraestructura de Redes y de Seguridad Informática Utilizando la Integración de Zabbix, Grafana y Zammad* [Thesis, ESPOL. FIEC.]. http://www.dspace.espol.edu.ec/handle/123456789/56359

Darnell Pascual, G. (2022). *Análisis Térmico de un convertidor basado en IGBT de un vehículo eléctrico* [Bachelor thesis, Universitat Politècnica de Catalunya]. https://upcommons.upc.edu/handle/2117/367431

Diana Hwang. (2021). *¿Qué es Red de área local o LAN? - Definición en Computer Weekly*. ComputerWeekly.es. https://www.computerweekly.com/es/definicion/Red-de-area-local-o-LAN

Enciso Cochachi, H. G. (2020). *Diseño E Implementación De Un Sistema De Monitoreo Del Centro De Datos Para La Red Del Inictel-Uni Utilizando Software Libre*. https://repositorio.untels.edu.pe/jspui/handle/123456789/581

gob.pe. (2021). *¿Qué Es La Eficiencia Energética?* https://www.gob.pe/institucion/regionpiura-drem/noticias/618472-que-es-la-eficiencia-energetica

Google Cloud. (s. f.). *Ventajas de Google Cloud*. Google Cloud. Recuperado 26 de octubre de 2024, de https://cloud.google.com/why-google-cloud

Hernandez, A. (2020, agosto 8). *Triggers, qué son y para qué sirven*. https://ed.team/blog/triggers-que-son-y-para-que-sirven

IBM. (2021, octubre 20). *¿Qué es la IaaS ? (Infraestructura como servicio)*. https://www.ibm.com/mx-es/topics/iaas

IDC. (2022). *IDC - Crecimiento de la nube pública y privada en Latinoamérica*. IDC: The premier global market intelligence company. https://www.idc.com/latam_es/analysts/blog/detail?id=3bc61a9d432062f984b1

IEC. (2021). *IEC 62040-1:2017+AMD1:2021 CSV*. https://webstore.iec.ch/en/publication/69012

Instituto Nacional de Estadística e Informática. (2022). *Acceso a los Servicios Básicos en el Perú, 2021*. https://www.gob.pe/institucion/inei/informes-publicaciones/3570539-acceso-a-los-servicios-basicos-en-el-peru-2021

iso.org. (2015). *ISO/IEC 27017:2015(en), Information technology—Security techniques—Code of practice for information security controls based on ISO/IEC 27002 for cloud services*. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27017:ed-1:v1:en

Kaise. (2018). *UPS – Kaise*. https://kaise.pe/ups/

Kaise. (2020). *Kaise – UPS y Baterías Industriales*. https://kaise.pe/, https://kaise.pe/

Lezama, C. R. Q. (2024). La Transición Energética como Estrategia para el Posicionamiento del Perú en la Región: Retos en la Política de Seguridad y Defensa Nacional. *Revista Cuadernos de Trabajo*, *28*, Article 28. https://doi.org/10.58211/nkrzvk06

MandiOhlinger. (2023, diciembre 11). *¿Qué es la administración de dispositivos?* https://learn.microsoft.com/es-es/mem/intune/fundamentals/what-is-device-management

Manrique-Villafuerte, C. J., Márquez-Vélez, G. M., & Herrera-Tapia, J. (2021). Herramientas de código abierto para el monitoreo de redes LAN. *Revista Científica de Informática ENCRIPTAR - ISSN: 2737-6389.*, *4*(8), Article 8.

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

MarketsandMarkets. (2024). *Cloud Analytics Market—Global Forecast to 2029* (No. TC 3598). https://www.marketsandmarkets.com/Market-Reports/cloud-based-business-analytics-market-959.html

Marqués, G. (2016). *IPsec y redes privadas virtuales*. Lulu.com.

Microsoft. (2024). *What Is Cloud Computing? | Microsoft Azure*. https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-cloud-computing

Microsoft Azure. (2023). *Servicios de informática en la nube | Microsoft Azure*. https://azure.microsoft.com/es-es/

Ministerio de Energía y Minas. (2015). *Plan Energético Nacional 2014- 2025*. https://www.gob.pe/institucion/minem/informes-publicaciones/4821287-plan-energetico-nacional-2014-2025

Misra, K. (2004). Network Management Using SNMP. En K. Misra (Ed.), *OSS for Telecom Networks: An Introduction to Network Management* (pp. 27-40). Springer. https://doi.org/10.1007/978-0-85729-400-5_4

msmk. (2024, septiembre 5). ¿Qué es un host? | MSMK University. *MSMK*. https://msmk.university/que-es-un-host-msmk-university/

Nagios. (2023). *Descripción general | Nagios de código abierto*. https://www.nagios.org/about/overview/

Ortiz, D., & Cyberclick. (2023). *¿Qué es un dashboard y para qué se usa? (2025)*. https://www.cyberclick.es/numerical-blog/que-es-un-dashboard

Quispe, J. (2019). *Implementación de un prototipo de monitoreo de dispositivos de comunicación y usuarios finales utilizando el protocolo SNMP basada en software libre para una empresa e-Commerce* [Universidad Nacional Mayor de San Marcos]. https://cybertesis.unmsm.edu.pe/item/f2171fdd-b3f0-4cee-9310-469f6b147638

Rimal, B. P., Choi, E., & Lumb, I. (2009). A Taxonomy and Survey of Cloud Computing Systems. *2009 Fifth International Joint Conference on INC, IMS and IDC*, 44-51. https://doi.org/10.1109/NCM.2009.218

Rodero, J. (2023, marzo 2). *Cloud en el sector energético—Digital Biz Magazine*. https://www.digitalbizmagazine.com/cloud-en-el-sector-energetico/

Rodriguez, A. (2023, febrero 24). ¿Qué es un Switch de Red y cómo funciona? *instaladoresdetelecomhoy.com*. https://www.instaladoresdetelecomhoy.com/que-es-un-switch-de-red-y-como-funciona/

Soriano, M. (2014). *Seguridad en redes y seguridad de la información*.

Stallings, W. (2014). *Data and computer communications* (Tenth edition). Pearson.

Stallman, R. M. (2004). *Software libre para una sociedad libre*. https://www.gnu.org/philosophy/fsfs/free_software.es.pdf

Tamberg, M. (2024, mayo 14). *Maximizing Efficiency and Reliability with UPS Preventive Maintenance Services*. Unified Power. https://unifiedpowerusa.com/maximizing-efficiency-and-reliability-with-ups-preventive-maintenance-services/

Tempel Group. (2024). *Home*. Tempel Group. https://www.tempelgroup.pe/

Toapanta Carvajal, Á. S. (2023). *Implementación de un sistema integral de monitoreo en tiempo real en la red core con SNMPv3 utilizando el software zabbix, para la empresa Maxxnet.* http://dspace.espoch.edu.ec/handle/123456789/20907

Viteri Guillén, S., & Orbe Torres, F. (2005). *Análisis comparativo de tipos de redes virtuales privadas (VPN) y diseño de una solución VPN para la PUCE-Q*. https://repositorio.puce.edu.ec/handle/123456789/26536

wakkeit. (2024, febrero 28). ¿Zabbix o Nagios? *Wakke IT*. https://wakkeit.com/2024/02/zabbix-o-nagios/

Ward, J. S., & Barker, A. (2014). Observing the clouds: A survey and taxonomy of cloud monitoring. *Journal of Cloud Computing*, *3*(1), 24. https://doi.org/10.1186/s13677-014-0024-2

Zabbix. (2021a). *2 ¿Qué es Zabbix?* https://www.zabbix.com/documentation/current/en/manual/introduction/about

Zabbix. (2021b). *2 Requisitos*. https://www.zabbix.com/documentation/current/en/manual/installation/requirements

Zabbix. (2021c). *3 características de Zabbix*. https://www.zabbix.com/documentation/current/en/manual/introduction/features

Zabbix. (2023). *About Zabbix LLC*. https://www.zabbix.com/about

zabbix. (2024). *8 Plantillas y grupos de plantillas*. https://www.zabbix.com/documentation/current/es/manual/config/templates

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: State-of-the-art and research challenges. *Journal of Internet Services and Applications, 1*(1), Article 1. https://doi.org/10.1007/s13174-010-0007-6

ANEXOS

Anexo 1. Hoja Técnica de Tarjeta SNMP-CY54-03

1. General Specification

CPU	ARM 266MHz 32Bit
System Clock	208MHz
Flash Memory	8M Byte
SDRAM	32M Byte
LED	5
Watch Dog	Yes
USB Port	No
Environment Port	No
Real Time Clock	Yes
LCD Display	No
LAN Interface	10M/100M UTP
Ethernet Throughput	1620K Byte per seconds
Ethernet Latency	0.759 milliseconds

2. Power Specification

NetAgent 9

ITEM	Minimum	Maximum
DC Input Voltage	+5.3V	+40V
DC Input Current		3W Maximum

3. Pin Assignment

Pin	Input/Output	Description
P1 GND	GND	Ground PIN
P2 PowerIn	Input	DC power input.
P3 RS232_TXD	Output	+5.5V and -5.5V Voltage level for RS232
P4 RS232_RXD	Input	-3V to -15V for logic '1', +3V to +15V for logic '0'
P5-P7 No USE		
P8 SNMPSIG		NetAgent card plug in detect, connect to PIN 10
P9 GND	GND	Ground PIN
P10 SNMPSIG		NetAgent card plug in detect, connect to PIN 8
P11 RS232_DCD	Input	+/-3V to +/-15V for RS232
P12 RS232_DTR	Output	+5.5V and -5.5V for RS232

P13 No Use		
P14 RS232_RTS	Output	+5.5V and -5.5V for RS232
P15 RS232_CTS	Input	+/-3V to +/-15V for RS232
P16-P26 No Use		

4. Signal Specification

Receiver Inputs

PARAMETER	CONDITIONS	MIN	TYP	MAX
Input Voltage Range		-25V		+25 V
Input Threshold Low	TA = +25°C	+0.6V	+1.2V	
Input Threshold High	TA = +25°C		+1.5V	+2.4V
Input Hysteresis			0.3 V	
Input Resistance	TA = +25°C	3 k ohm	5 k ohm	7k ohm

Transmitter Outputs

PARAMETER	CONDITIONS	MIN	TYP	MAX
Output Voltage Swing	All transmitter outputs loaded with 3k ohm to ground	±5.0V	±5.4V	
Output Resistance	TA = +25°C	300	10M	
Output Short-Circuit Current			±35 mA	±60 mA

5. Environment Specification

PARAMETER	CONDITIONS	Minimum	Maximum
Operating Temperature		0 °C	60 °C
Storage Temperature		-40 °C	125 °C
Operating Humidity	Non-Condensing	10% RH	90% RH
Storage Humidity	Non-Condensing	5% RH	95% RH

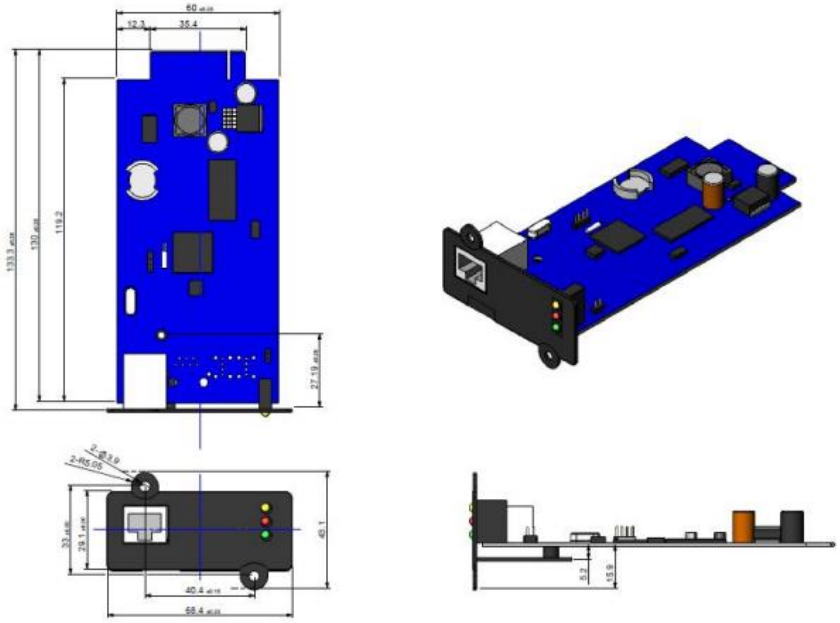
EMI
FCC Class B, CE

6. Dimension and Outlook

The whole package includes the following items.

A. NetAgent 9 Internal Card

Dimension	133.3mm(L) x 68.4mm(W) x 43.1mm(H)
Weight	70.0g±2g
Connector	26pin gold finger.

Dimension


Outlook

Top view

Bottom view

Front Panel

Anexo 2. Hoja Técnica de UPS Kaise 1-3kVA

UPS
Kaise 1 - 3 kVA

CARACTERÍSTICAS

- Tecnología de doble conversión en línea de alta frecuencia
- Tecnología de control DSP (procesadores de señal digital)
- Corrección activa del factor de potencia (APFC), factor de potencia de entrada de hasta 0.99
- Factor de potencia de salida 0.9
- Amplio rango de voltaje de entrada (110V ~ 300 Vac) y rango de frecuencia (40~70Hz)
- Frecuencia de detección automática
- Conversión de frecuencia 50 / 60Hz
- Inicio en frío
- Diseño de ventilación trasera y ventilador de velocidad variable
- Protección efectiva de software y hardware
- Carga rápida y estable, 90% de capacidad restaurada en 3 h (UPS modelo estándar)
- Reducción lineal en la entrada de bajo voltaje que reduce los tiempos de descarga de la batería
- Inicio diferido configurable cuando se restablece la energía
- Gestión avanzada de baterías (ABM)
- Múltiples funciones configurables a través de LCD: voltaje de salida, EOD, inicio automático, modo bypass, modo ECO y modo de conversión de frecuencia
- Comunicaciones multiplataforma: RS232 (estándar), USB / RS485 / SNMP / contactos secos (opcional)

Opciones Disponibles

- USB opcional, tarjeta RS485, contactos secos AS400, tarjeta SNMP, alarmas SMS, función EPO, cargador 12A (solo 2-3KVA) y transformador de aislamiento incorporado

PANEL TRASERO

1- Protección contra sobrecorriente
2- AC input
3- Modem/tel/fax
4- DC input
5- Toma de corriente
6- Ventilador
7- RS232
8- USB (opcional)
9- EPO (opcional)
10- SNMP/AS400 (opcional)

friendly tech

tempel group

Kaise®

ESPECIFICACIONES TÉCNICAS

MODEL	KTPE901PS	KTPE901PH	KTPE902PS	KTPE902PH	KTPE903PS	KTPE903PH
Capacity	1 KVA / 900 W		2 KVA / 1800 W		3 KVA / 2700 W	
INPUT						
Rated voltage	208 V / 220 V / 230 V / 240 Vac					
Voltage range	110 ~ 176 Vac (linear derating between 50% and 100% load); 176 ~ 280 Vac (no derating); 280 ~ 300 Vac (derating 50%)					
Frequency	40 ~ 70 Hz (auto-sense)					
Power factor	⩾ 0.99					
Bypass voltage range	-25% ~ +15% (settable)					
OUTPUT						
Voltage	208 V / 220 V / 230 V / 240 Vac (settable via LCD)					
Voltage regulation	± 1%					
Frequency	45 ~ 55 Hz or 55 ~ 65 Hz (synchronized range); 50 / 60 Hz ± 0.1 Hz (battery mode)					
Waveform	Sinusoidal					
Crest factor	3:1					
Harmonic distortion	⩽ 2% (linear load); ⩽ 5% (non-linear load)					
Transfer time	Mains mode to battery mode: 0 ms Inverter mode to bypass mode: 4 ms (typical)					
Overload capability	105% ~ 125%: transfer to bypass in 1 min; 125% ~ 150%: transfer to bypass in 30 s; > 150%: transfer to bypass in 300 ms					
EFFICIENCY						
Mains mode	⩾ 90%		⩾ 91%		⩾ 92%	
Battery mode	⩾ 85%		⩾ 86%		⩾ 87%	
ECO mode	⩾ 95%		⩾ 96%		⩾ 97%	
BATTERIES						
DC voltage	24 V	36 V	36 V	48 V	72 V	72 V	72 V	96 V	96 V
Inbuilt battery	2 × 9 Ah	3 × 7 Ah	/	4 × 9 Ah	6 × 7 Ah	/	6 × 9 Ah	8 × 7 Ah	/
Charging current (max.)	1 A		6 A	1 A		6 A	1 A		6 A
Recharge time	8 h								
ALARMS									
Utility failure	4 s per beep								
Low battery	1 s per beep								
Overload	1 s twice beep								
UPS fault	Long beep								
COMMUNICATIONS									
RS232 (standard) / USB (optional)	Supports Windows® 98 / 2000 / 2003 / XP / Vista / 2008 / Windows® 7 / 8 / 10								
SNMP (optional)	Power management from SNMP manager and web browser								
OTHERS									
Operating temperature	0 ~ 40℃								
Relative Humidity	0 ~ 90% (non-condensing)								
Noise level	⩽ 50 dB (1m)								
Dimensions (W × D × H) (mm)	144 × 336 × 214	144 × 414 × 214	144 × 336 × 214	191 × 418 × 335				191 × 464 × 335	191 × 418 × 335
Packaged dimensions (W × D × H) (mm)	232 × 417 × 318	231 × 492 × 316	232 × 417 × 318	318 × 533 × 471				320 × 573 × 471	318 × 533 × 471
Net weight (kg)	9.5	13	6	18	25.7	10.5	27.2	32	11
Gross weight (kg)	10.5	14.2	7	19.5	27.4	12	29	34	12.5

- Derate capacity to 70% in CUCF mode and to 90% when the output voltage is adjusted to 208Vac.
- S means standard model, H means long time model.
- All specifications subject to change without notice.
- Custom-made specifications are acceptable.

Anexo 3. Hoja Técnica de UPS Kaise 10-30kVA

UPS Kaise 10-30kVA 3:3
MODELO . CARACTERÍSTICAS . ESPECIFICACIONES TÉCNICAS

Kaise®

UPS
Kaise 10-30kVA 3:3

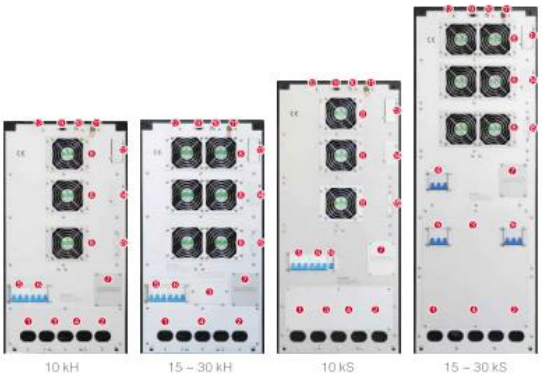
CARACTERÍSTICAS

- Tecnología de control digital DSP
- Corrección activa del factor de potencia (APFC), factor de potencia de entrada de hasta 0.99
- Factor de potencia de salida 0.9
- Inicio fresco
- Entrada dual
- Amplio rango de voltaje de entrada (190V - 485V)
- Frecuencia de detección automática
- Modo de conversión de frecuencia de 50/60 Hz
- Eficiencia laboral de hasta el 98% en modo ECO
- Control automático de la velocidad del ventilador cuando las cargas varían
- Encendido / apagado automático de acuerdo con la capacidad de carga establecida por los usuarios
- Configuración de batería flexible para usar baterías de 14/16/18/20 piezas
- Diseño interno compacto, miniaturiza la unidad completa para un tamaño reducido
- Pantalla LCD + LED, operación de teclas multifuncionales, interfaz amigable hombre-máquina
- Potente software en segundo plano para la configuración de parámetros y la actualización en línea
- Duplicando la velocidad de carga de la batería, 90% de capacity restaurada en 4 horas (UPS modelo estándar)
- Reducción lineal en la entrada de bajo voltaje, lo que reduce los tiempos de descarga de la batería y prolonga la vida útil de la batería.
- Gestión avanzada de la batería (ABM), control automático de carga flotante / ecualizador, control de latencia del cargador

Panel frontal

Opcional: Pantalla táctil a color de 5"

1- Mains Input
2- DC Input
3- Bypass Input
4- Output
5- Mains Input Breaker
6- Bypass Input Breaker
7- Maintenance Bypass
8- Fan
9- RS232
10- USB
11- EPO
12- Battery temperature Compensation (Optional)
13- Intelligent Slot 1 (SNMP /AS400 / RS485 Optional)
14- Intelligent Slot 2 (Optional)
15- Parallel Card (optional)
16- Battery Breaker



10 kH | 15 – 30 kH | 10 kS | 15 – 30 kS

friendly tech

tempel group

MODEL	KTPE9010P	KTPE9015P	KTPE9020P	KTPE9030P
Capacity	10 kVA / 9 kW	15 kVA / 13.5 kW	20 kVA / 18 kW	30 kVA / 27 kW
INPUT				
Rated voltage	360 / 380 / 400 / 415 Vac			
Voltage range	277 ~ 485 Vac (no derating); 190 ~ 277 Vac (linear derating between 50% and 100% load)			
Rated frequency	50 / 60 Hz (auto-sense)			
Frequency range	40 ~ 70 Hz			
Power factor	≥ 0.99			
Bypass voltage range	– 40% ~ + 15% (settable)			
Total harmonic distortion (THDi)	≤ 5%			
OUTPUT				
Rated Voltage	360 / 380 / 400 / 415 Vac (settable)			
Voltage regulation	± 1%			
Frequency	45 ~ 55 Hz or 55 ~ 65 Hz (synchronized range); 50 / 60 Hz ± 0.1 Hz (battery mode)			
Waveform	Sinusoidal			
Power Factor	0.9			
Total harmonic distortion (THDv)	≤ 2% (linear load), ≤ 5% (non-linear load)			
Crest factor	3:1			
Overload (Inverter)	102% ~ 125% for 10 min, 125% ~ 150% for 1 min, > 150% for 0.5 s			
Overload (Bypass)	102% ~ 125% for 20 min, 125% ~ 150% for 2 min, > 150% for 1 s			
BATTERIES				
DC voltage	Standard model: 240 Vdc; Long time model: 192 Vdc (168 / 192 / 216 / 240V optional)			
Inbuilt battery of standard model	20 × 7 Ah	40 × 7 Ah	40 × 9 Ah	60 × 9 Ah
Charging current	Long time model: 7 A supplied (additional 7 A is optional) Standard model: 1 A, 2 A, 3.5 A settable			
Recharge time	Standard model: 90% capacity restored in 4 hours; Long time model: depend on the capacity of battery			
SYSTEM				
Efficiency	≥ 93%, ECO mode 98%			
Transfer time	0 ms			
Max. number of parallel connections	6			
Protections	Short-circuit, overload, overtemperature, battery low voltage, overvoltage, undervoltage and fan failure			
Communications	RS232 / USB (standard), RS485 / dry contacts / SNMP (optional)			
Display	LCD+LED			
Standards	EN 62040-1, EN 62040-2, EN 61000-3-12, EN 61000-3-2, EN 61000-3-11, IEC 61000-4-2, IEC 61000-4-3, IEC 61000-4-4, IEC 61000-4-5, IEC 61000-4-6, IEC 61000-4-8, IEC 61000-4-11, IEC 61000-2-2			
OTHERS				
Operating temperature	0℃ ~ 40℃			
Storage temperature	–25℃ ~ 55℃ (without batteries)			
Relative humidity	0 ~ 95% (non-condensing)			
Altitude	≤ 1000 m, derating 1% for each additional 100 m			
IP rating	IP 20			
Noise level at 1 m	≤ 60 dB	≤ 65 dB		
Online thermal dissipation	3504 BTU/hr	5773 BTU/hr	8281 BTU/hr	9929 BTU/hr
Dimensions (W × D × H) (mm)	350 × 655 × 732 (H)			
	350 × 785 × 858 (S)	350 × 785 × 1078 (S)		
Packaged dimensions (W × D × H) (mm)	472 × 780 × 920 (H)			
	472 × 910 × 1050 (S)	472 × 910 × 1260 (S)		
Net weight (kg)	55 (H), 115 (S)	60 (H), 155 (S)	61 (H), 175 (S)	65 (H), 235 (S)
Gross weight (kg)	65 (H), 125 (S)	70 (H), 170 (S)	71 (H), 190 (S)	75 (H), 250 (S)

- Derate capacity to 90% when the output voltage is adjusted to 360 Vac.
- S means standard model, H means long time model.
- All specifications subject are to change without notice.
- Custom-made specifications are acceptable.

Anexo 4. Hoja Técnica de UPS Kaise 40-120kVA

UPS
Kaise 40-120kVA 3:3

CARACTERÍSTICAS

- Factor de potencia de salida 1.0
- Diseño interno compacto, tamaño reducido
- Eficiencia de trabajo de hasta el 99% en modo ECO
- Modo de conversión de frecuencia de 50 Hz / 60 Hz
- Tecnología avanzada de control DSP de doble núcleo y tecnología de 3 niveles
- Tecnología de corrección del factor de potencia activa, factor de potencia de entrada de hasta 0.99
- La eficiencia del sistema mejoró al 96%, la tasa de ahorro de energía se duplicó
- Diseño de entrada dual, compatible con bypass independiente
- Tecnología digital y paralela avanzada, que proporciona mayor confiabilidad que un solo sistema
- Amplio rango de voltaje de entrada, frecuencia de detección automática de 50/60 Hz
- La velocidad del ventilador varía de manera inteligente con la temperatura, lo que reduce el ruido y extiende su vida útil.
- Presenta una fuerte tolerancia a fallas, un ventilador dañado toma el 50% de la carga, dos ventiladores dañados toman el 30% de la carga
- Tecnología de recubrimiento conforme para hacer que UPS funcione en entornos hostiles durante mucho tiempo
- Protección efectiva de hardware y software, función de autodiagnóstico robusta, abundante evento para verificación futura
- Reducción lineal en la entrada de bajo voltaje que reduce los tiempos de descarga de la batería
- Configuración de batería flexible, números de batería seleccionables: 30 - 46 piezas
- Cargador controlado digitalmente (Máx. 36A)
- Posibilidad de encender el UPS con batería en ausencia de alimentación de red (arranque en frío)
- Tiempo de conmutación cero para el modo de suministro de energía del UPS cuando la alimentación de la red es inestable, asegurando que la salida no se interrumpa
- Tiempo de inicio diferido configurable cuando se restablece la alimentación de red
- Pantalla táctil colorida LCD de 5 pulgadas, interfaz amigable para humanos y máquinas
- Potente software de fondo para la configuración de parámetros y actualización en línea
- Comunicación multiplataforma avanzada para monitoreo de UPS: RS232, USB, RS485, NET, contactos secos, tarjeta SNMP, tarjeta Wi-Fi y tarjeta GPRS
- Gestión inteligente de la batería, control de carga flotante y ecualizado automático, control de latencia del cargador, mejora la fiabilidad del cargador y prolonga la vida útil de la batería.
- Opciones y accesorios: RS232, USB, RS485, NET, paralelo, LBS, contactos secos, EPO e interfaces de compensación de temperatura de batería suministradas; Tarjeta SNMP opcional, tarjeta Wi-Fi, tarjeta GPRS, sensor de temperatura de la batería, detector EMD y alarmas SMS

friendly tech

tempel group

MODEL	KTPE9940	KTPE9960	KTPE9980	KTPE99120
Capacity	40 kVA / 40 kW	60 kVA / 60 kW	80 kVA / 80 kW	120 kVA / 120 kW
INPUT				
Input wiring	Three-phase five-wire (3Φ + N + PE)			
Rated voltage	380 / 400 / 415 Vac			
Voltage range	304 ~ 485 Vac (no downgrading), 138 ~ 304 Vac (linear downgrading between 40% ~ 100% load)			
Rated frequency	50 / 60 Hz (auto-sensing)			
Frequency range	40 ~ 70 Hz			
Power factor	≥ 0.99			
Bypass voltage range	–60% ~ +20% (settable)			
Total harmonic distortion (THDi)	≤3%			
OUTPUT				
Output wiring	Three-phase five-wire (3Φ + N + PE)			
Rated voltage	380 / 400 / 415 Vac			
Voltage regulation	± 1%			
Frequency	Synchronized with utility in mains mode,50 / 60 Hz ± 0.1% in battery mode			
Waveform	Sinusoidal			
Power factor	1			
Total harmonic distortion (THDv)	≤ 1% (linear load); ≤ 5% (non-linear load)			
Crest factor	3:1			
Overload	105% ~110% for 60 min, 110% ~ 125% for 10 min, 125% ~ 150% for 1 min, >150% for 0.2 s			
BATTERIES				
DC voltage	± 192 Vdc (± 180 ~ ± 276 Vdc settable)			
Number of battery	32 pcs (30 ~ 46 pcs settable)			
Charging current (max.)	12 A	24 A		36 A
Recharge time	Depend on the capacity of battery			
SYSTEM				
Efficiency	Max. 96% in online mode, 99% in ECO mode			
Transfer time	0 ms			
Protections	Short-circuit, overload, overtemperature, excessive low battery, overvoltage, undervoltage, fans failure			
Max. number of parallel connections	4			
Communications	Standard configuration: RS232, USB, RS485, NET, dry contacts; Optional configuration: SNMP card, Wi-Fi card, GPRS card			
Display	5 inches colorful LCD touch screen			
OTHERS				
Operating temperature	0℃ ~ 40℃			
Storage temperature	–25℃ ~ 55℃ (without battery)			
Relative humidity	0% ~ 95% (non-condensing)			
Altitude	≤ 1000 m; above 1000 m, downgrading 1% for each additional 100 m			
IP rating	IP 20			
Noise level at 1 m	≤ 65 dB			
Dimensions (W × D × H) (mm)	360 × 850 × 950		360 × 850 × 1200	440 × 850 × 1200
Packaged dimensions (W × D × H) (mm)	460 × 950 × 1113		460 × 950 × 1363	540 × 950 × 1363
Net weight (kg)	93	125	157	192
Gross weight (kg)	106	138	170	207

- All specifications are subject to change without notice.
- Custom-made specifications are acceptable.
- Derate capacity to 90% when the number of batteries is set to 30 pcs.

Anexo 5. Hoja Técnica de Mikrotik RB750

hEX

hEX is a five port gigabit ethernet router for locations where wireless connectivity is not required. The device has a USB 2.0 port. This new updated revision of the hEX brings several improvements in performance.

- hEX (revision 3)
- 880 MHz CPU, 2 cores and 4 threads
- 256 MB RAM
- microSD slot for "Dude Server" support
- Full size USB
- IPsec hardware acceleration ~450 Mbps
- Same form factor
- Same price

It is affordable, small and easy to use, but at the same time comes with a very powerful dual core 880MHz CPU and 256MB RAM, capable of all the advanced configurations that RouterOS supports. IPsec Hardware encryption (~450Mbps) and dude server package is supported, microSD slot on it also provides improved r/w speed for database storage on microSD card.

Performance comparison

Previous r2	64 byte	1518 byte	1400 byte
Bridging	396 Mbps	986 Mbps	986 Mbps
Routing	373 Mbps	986 Mbps	986 Mbps
AES-128	9 Mbps	52 Mbps	50 Mbps

New r3	64 byte	1518 byte	1400 byte
Bridging	523 Mbps	1972 Mbps	1972 Mbps
Routing	530 Mbps	1972 Mbps	1972 Mbps
AES-128	21 Mbps	472 Mbps	450 Mbps

Specifications

Product code	RB750Gr3
CPU nominal frequency	880 MHz
CPU core count	2
Size of RAM	256 MB
10/100/1000 Ethernet ports	5
PoE in	Yes
Supported input voltage	8 - 30 V
PCB temperature monitor	Yes
Voltage Monitor	Yes
USB	Yes, type A 2.0
Hardware encryption	Yes
Dude server package support	Yes
Dimensions	113x89x28mm
License level	4
Operating System	RouterOS
CPU	MT7621A
Max Power consumption	5 W
Suggested price	$59.95

Included

24V 0.38A Power adapter

RETORNO DE INVERSION DEL SISTEMA DE MONITOREO EN NUBE PARA LOS UPS KAISE

CAPEX	S/ 1,420.00
OPEX MENSUAL	S/ 320.00
AHORRO MENSUAL	S/ 720.00
AHORRO NETO MENSUAL	S/ 400.00
PAYBACK (MESES)	3.55

Gastos mensual	Sin Sistema de Monitoreo	Con Sistema de Monitoreo
Movilidad	S/ 600.00	S/ 300.00
Horas Hombre	S/ 840.00	S/ 420.00
Suministros	S/ 160.00	S/ 160.00
Viaticos	S/ 350.00	S/ 350.00
Gasto Total Mensual	S/ 1,950.00	S/ 1,230.00

PROYECCIÓN A UN AÑO													
Flujo	**Mes 0**	**Mes 01**	**Mes 02**	**Mes 03**	**Mes 04**	**Mes 05**	**Mes 06**	**Mes 07**	**Mes 08**	**Mes 09**	**Mes 10**	**Mes 11**	**Mes 12**	**TOTAL**
Inversión	-S/ 1,420.00													-S/ 1,420.00
Ahorro		S/ 720.00	S/ 720.00	S/ 720.00	S/ 720.00	S/ 720.00	S/ 720.00	S/ 720.00	S/ 720.00	S/ 720.00	S/ 720.00	S/ 720.00	S/ 720.00	S/ 8,640.00
OPEX		-S/ 320.00	-S/ 320.00	-S/ 320.00	-S/ 320.00	-S/ 320.00	-S/ 320.00	-S/ 320.00	-S/ 320.00	-S/ 320.00	-S/ 320.00	-S/ 320.00	-S/ 320.00	-S/ 3,840.00
Flujo Neto	-S/ 1,420.00	S/ 400.00	S/ 400.00	S/ 400.00	S/ 400.00	S/ 400.00	S/ 400.00	S/ 400.00	S/ 400.00	S/ 400.00	S/ 400.00	S/ 400.00	S/ 400.00	S/ 4,800.00
Total	3,380													
Ahorro Total	4,800													
Payback	3.55													
Saldo	-S/ 1,420.00	-S/ 1,020.00	-S/ 620.00	-S/ 220.00	S/ 180.00	S/ 580.00	S/ 980.00	S/ 1,380.00	S/ 1,780.00	S/ 2,180.00	S/ 2,580.00	S/ 2,980.00	S/ 3,380.00	

Anexo 6. Cálculo de Retorno de Inversión

Anexo 7. Carta de autorización de Tempel Perú

tempel group

tempel Perú sac
Calle Dionisio Derteano 184 - Oficina 704
Tel. +511 271 9445
San Isidro [Lima] - Perú
www.tempelgroup.com
lima@tempelgroup.com

Lima, 25 de noviembre de 2024

Señores
UNIVERSIDAD NACIONAL TECNOLOGICA DE LIMA SUR –UNTELS
Presente.

De mi consideración:

Es grato dirigirme a ustedes en mi calidad de Representante Legal de la empresa TEMPEL PERU S.A.C con RUC Nº 20552258429, para comunicar que el señor **Anthony Adolfo Zúñiga Huamani** identificado con DNI Nº 76530297, desempeña el cargo de Ingeniero de Oficina Técnica, por ello otorgamos la autorización de presentar y desarrollar el proyecto de suficiencia profesional titulado: "Diseño e implementación de un sistema de monitoreo en nube para los sistemas de alimentación ininterrumpida Kaise de Tempel Perú" en el VII Programa de Titulación por la Modalidad de Trabajo de Suficiencia Profesional 2024 de su institución.

Atentamente,

TEMPEL PERU S.A.C. R.U.C. 20552258429 V°B° ADMINISTRACIÓN

Jorge Pareja Rojas
Representante Legal
TEMPEL PERU S.A.C

Jorge Aristides Pareja Rojas
Representante Legal
Tempel Peru S.A.C 20552258429

UNIVERSIDAD NACIONAL TECNOLOGICA DE LIMA SUR
E.P. INGENIERIA ELECTRONICA Y TELECOMUNICACIONES
25 NOV. 2024
RECIBIDO
EXP. N°: FOLIO(S):
HORA: FIRMA: