UNIVERSIDAD TECNOLÓGICA DE LOS ANDES

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

Tesis

Implementación de un servidor de monitoreo para optimizar los servicios TI en la empresa EGEMSA Cusco, 2025

Asesor:

Mg. Cusihuaman Phocco, Roger Mario

Autores:

Olivera Antitupa, Jonathan Manuel

Vargas Callapiña, Adriano José

Para optar el Título Profesional de:

Ingeniero de Sistemas e Informática

Cusco - Cusco - Perú

2026

UNIVERSIDAD TECNOLÓGICA DE LOS ANDES

FACULTAD DE INGENIERIA

ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS E INFORMATICA

Acta N°: 05

ACTA DE SUSTENTACIÓN DE TÍTULO PROFESIONAL

En la ciudad de Cusco, a los 15 días del mes de julio del 2026, siendo las 09:00 horas, se reunieron los integrantes del Jurado designado por Resolución Sub Directoral N° 060-2026-UTEA-FC-FI-EPISeI-SD. de la Escuela Profesional de Ingeniería de Sistemas e Informática, Facultad de Ingeniería:

Presidente	:	Mg. Anaya Bellido, Tula
Dictaminante	:	Dra. Huaman Vargas, Jaqueline
Replicante	:	Mg. Roldan Medina, Moises

Para evaluar la sustentación, en la modalidad de:

☒ Tesis ☐ Trabajo de suficiencia profesional

Titulada:

Implementación de un servidor de monitoreo para optimizar los servicios TI en la empresa EGEMSA Cusco, 2025

Desarrollado por el (los) Bachiller (es):

Br.: Olivera Antitupa, Jonathan Manuel
(Apellidos y Nombres)

Br.: Vargas Callapiña, Adriano José
(Apellidos y Nombres)

Para optar el Tituló Profesional de:

Ingeniero de Sistemas e Informática
(Denominación del Título)

Concluido el acto, el Jurado dictaminó que el (la) (los) mencionado(a) (s) bachiller (es) fue (ron) APROBADO(S) ☒ o DESAPROBADO(S) ☐:

Emitiéndose el calificativo final de:

Bachiller (Apellidos y Nombres)	Nota	Detalle (**)
Br. Olivera Antitupa Jonathan Manuel	14	Aprobado
Br. Vargas Callapiña Adriano José	14	Aprobado

Siendo las 10:50 horas concluyó la sesión, firmando los integrantes del Jurado.

Presidente: Mg. Anaya Bellido, Tula
(Dr. Mg.). (Apellidos y Nombres) (Firma)

Dictaminante: Dra. Huaman Vargas, Jaqueline
(Dr. Mg.). (Apellidos y Nombres) (Firma)

Replicante: Mg. Roldan Medina, Moises
(Dr. Mg.). (Apellidos y Nombres) (Firma)

Nota: Desaprobado: 0-10; **Aprobado:** 11-20

(**): 0 a 10: Desaprobado, 11 a 15: Aprobado, 16 a 18: Aprobado Notable, 19 y 20: Aprobado con Distinción, Art. 18 RGGAT.

12% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto citado
- Coincidencias menores (menos de 10 palabras)

Fuentes principales

10% Fuentes de Internet
2% Publicaciones
10% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

Metadatos

Datos del autor		
Apellidos y Nombres	:	Olivera Antitupa, Jonathan Manuel
Tipo de documento de identidad	:	DNI
Número de documento de identidad	:	70420384
URL ORCID	:	https://orcid.org/0009-0003-4142-5910
Datos del autor		
Apellidos y Nombres	:	Vargas Callapiña, Adriano José
Tipo de documento de identidad	:	DNI
Número de documento de identidad	:	48536536
URL ORCID	:	https://orcid.org/0009-0002-7118-353X
Datos del asesor		
Apellidos y Nombres	:	Mg. Cusihuaman Phocco, Roger Mario
Tipo de documento de identidad	:	DNI
Número de documento de identidad	:	74570513
URL ORCID	:	https://orcid.org/0000-0002-6240-5818
Datos de la Investigación		
Facultad	:	Ingeniería
Escuela Profesional	:	Ingeniería de Sistemas e Informática
Línea de Investigación	:	Informática, Sociedad y Gestión de Conocimiento
Rango de años en que se realizó la investigación	:	Diciembre 2024 – diciembre 2025
Fuente de financiamiento	:	Auto financiado
Porcentaje de similitud	:	12 %
URL de OCDE	:	https://purl.org/pe-repo/ocde/ford - 2.02.04

Dedicatoria

A mis padres y mi hermana por el apoyo incondicional, en especial para mi madre, tu esfuerzo y sacrificio hicieron que todo esto se materialice, te amo, gracias por estar siempre a mi lado.

Para mi hija Catalina, tu ternura y curiosidad hacen que mis días tengan sentido, gracias por llenar mi vida con amor y para Pieri, mi compañera de vida, gracias por tu perseverancia y paciencia en este camino, las amo infinitamente. Esta tesis se las dedico con mucho amor, gracias totales.

Jonathan Manuel Olivera Antitupa

Dedico este trabajo a quienes acompañaron este camino con paciencia y comprensión, estando presentes de distintas maneras a lo largo de todo el proceso. Su apoyo, muchas veces silencioso y constante, se convirtió en un sostén que permitió avanzar incluso en los momentos en que la exigencia y el esfuerzo parecían mayores.

Este trabajo es también reflejo de un recorrido construido con constancia, aprendizaje y compromiso. A lo largo de ese camino hubo instantes que ayudaron a mantener el equilibrio, pequeñas pausas que acompañaron la concentración, rutinas que dieron continuidad al esfuerzo y una cercanía especial que, de forma discreta, aportó motivación y sentido a cada paso. Todo ello forma parte de lo que hoy se concreta en este trabajo concluido.

Adriano José Vargas Callapiña

Agradecimiento

Agradezco a todas las personas que, de manera directa o indirecta, contribuyeron a la realización y culminación de este trabajo. Su apoyo, colaboración y disposición, brindados en distintos momentos, hicieron posible llegar a este resultado.

De manera especial, expreso mi agradecimiento a quienes facilitaron el acceso a la información y a los recursos necesarios para el desarrollo del estudio, así como a quienes brindaron su tiempo y colaboración durante el proceso. Asimismo, reconozco los aportes y sugerencias recibidas, que contribuyeron a fortalecer el presente trabajo.

Jonathan Manuel Olivera Antitupa

Mi agradecimiento especial a mi Universidad, docentes, compañeros con los que compartí. A mi asesor de tesis por su orientación. Para terminar un agradecimiento especial a las personas que nos apoyaron en todo el proceso de realización de la tesis.

Adriano José Vargas Callapiña

Resumen

La presente tesis tiene como objetivo implementar un servidor de monitoreo para optimizar los servicios TI en la empresa EGEMSA Cusco, 2025, demostrando que existen mejoras consistentes en cada aspecto analizado, hallando disminuciones en los tiempos de respuesta, en la duración de los incidentes, mayor disponibilidad de los servicios, y uso más eficiente de los recursos de red y del servidor.

El estudio utiliza un enfoque cuantitativo, con diseño pre-experimental basado en pretest y postest, evaluando cuatro dimensiones fundamentales de los servicios TI: eficiencia operativa, disponibilidad del servicio, rendimiento de la infraestructura de red y rendimiento de la infraestructura del servidor. Asimismo, para el análisis inferencial, se aplica la prueba U de Mann–Whitney, por la naturaleza no paramétrica de los datos.

Los resultados evidencian mejoras significativas en todas las dimensiones evaluadas, destacando disminuciones en los tiempos de respuesta a incidentes, incremento de la disponibilidad de los servicios TI, disminución en la duración de fallas de red y optimización del uso de CPU, memoria, almacenamiento y temperatura del servidor. Además, los valores de significancia son $p < .001$, lo que permite rechazar las hipótesis nulas y confirmar que la implementación del servidor de monitoreo produce efectos positivos reales y medibles.

Se concluye que la intervención optimiza integralmente los servicios TI de la empresa, contribuyendo a una operación más estable, eficiente y confiable de su infraestructura tecnológica.

Palabras clave: Servidor de monitoreo, servicios TI, eficiencia operativa, disponibilidad, infraestructura de red.

Abstract

The objective of this thesis is to implement a monitoring server to optimize IT services at EGEMSA Cusco, 2025, demonstrating consistent improvements in each aspect analyzed, reflecting significant reductions in response times, shorter incident durations, greater service availability, and more efficient use of network and server resources.

The study uses a quantitative approach, with a pre-experimental design based on pre-test and post-test measurements, evaluating four fundamental dimensions of IT services: operational efficiency, service availability, network infrastructure performance, and server infrastructure performance. Likewise, the Mann–Whitney U test is applied for inferential analysis, due to the non-parametric nature of the data.

The results show significant improvements in all dimensions evaluated, highlighting notable reductions in incident response times, increased IT service availability, decreased network outage duration, and optimized CPU, memory, storage, and server temperature usage. In all cases, the significance values are $p < .001$, which allows us to reject the null hypotheses and confirm that the implementation of the monitoring server produces real and measurable positive effects.

We conclude that the intervention comprehensively optimizes the company's IT services, contributing to a more stable, efficient, and reliable operation of its technological infrastructure.

Keywords: Monitoring server, IT services, operational efficiency, availability, network infrastructure.

Índice

Portada i
Acta de sustentación ii
Reporte de similitud iii
Metadatos iv
Dedicatoria v
Agradecimiento vi
Resumen vii
Abstract viii
Índice ix
Índice de tablas xi
Índice de figuras xiii
Índice de anexos xiv
I. **Introducción** 15
II. **Problema de investigación** 18
2.1. Descripción y formulación del problema 18
2.2. Objetivos 22
2.2.1. Objetivo General 22
2.2.2. Objetivos Específicos 23
2.3. Justificación e importancia 23
2.4. Hipótesis 24
2.5. Variables 25
III. **Marco teórico** 28
3.1. Antecedentes 28
3.2. Bases teóricas 34
3.3. Definición de términos 48
IV. **Metodología** 51

4.1. Tipo y nivel de investigación 51
4.2. Ámbito temporal y espacial 52
4.3. Población y muestra 52
4.4. Instrumentos 53
4.5. Procedimientos 54
4.6. Análisis de datos 55
V. **Resultados y discusión** 57
VI. **Conclusiones** 114
VII. **Recomendaciones** 116
VIII. **Referencias bibliográficas** 118
IX. **Anexos** 125

Índice de tablas

Tabla 1 Operacionalización de la variable independiente 26
Tabla 2 Operacionalización de la variable dependiente 27
Tabla 3 Población accesible 53
Tabla 4 Caracterización de la intervención: implementación del servidor de monitoreo 58
Tabla 5 Características técnicas de la intervención según indicadores 58
Tabla 6 Indicador cumplimiento de guías y estándares de fabricantes 59
Tabla 7 Indicador hardening aplicado 60
Tabla 8 Indicador dispositivos monitoreados 61
Tabla 9 Indicador servicios supervisados 62
Tabla 10 Indicador uptime del contenedor Docker 63
Tabla 11 Indicador uso de recursos promedio 64
Tabla 12 Indicador Aplicación de actualizaciones, firewall y auditorías 65
Tabla 13 Síntesis general del servidor de monitoreo 66
Tabla 14 Resultados pretest de la dimensión eficiencia operativa según fuente de detección 67
Tabla 15 Resultados postest de la dimensión eficiencia operativa según fuente de detección 68
Tabla 16 Resultados pretest y postest de la dimensión eficiencia operativa según fuente de detección 69
Tabla 17 Resultados pretest de la dimensión disponibilidad del servicio según fuente de detección 71
Tabla 18 Resultados postest de la dimensión disponibilidad del servicio según fuente de detección 73
Tabla 19 Resultados pretest y postest de la dimensión disponibilidad del servicio según fuente de detección 74
Tabla 20 Resultados pretest de la disponibilidad estimada según equipo de red 76
Tabla 21 Resultados postest de la disponibilidad estimada según equipo de red 77
Tabla 22 Resultados pretest y postest de la disponibilidad estimada según equipo de red 78
Tabla 23 Resultados pretest de la duración según equipo de red 79
Tabla 24 Resultados postest de la duración según equipo de red 80
Tabla 25 Resultados pretest y postest de la duración según equipo de red 81
Tabla 26 Resultados postest y postest según recursos 82

Tabla 27 Resultados postest y postest según recursos 85
Tabla 28 Prueba de normalidad 89
Tabla 29 Resultados por dimensión de la variable servicios TI 91
Tabla 30 Rangos de la dimensión eficiencia operativa en el pretest y postest 92
Tabla 31 Estadísticos de la prueba U de Mann–Whitney de la dimensión eficiencia operativa entre el pretest y postest 93
Tabla 32 Rangos de la dimensión disponibilidad del servicio en el pretest y postest 94
Tabla 33 Estadísticos de la prueba U de Mann–Whitney de la dimensión disponibilidad del servicio entre el pretest y postest 94
Tabla 34 Rangos de la dimensión rendimiento de la infraestructura de red en el pretest y postest de duración y disponibilidad estimada 96
Tabla 35 Estadísticos de la prueba U de Mann–Whitney de la dimensión rendimiento de la infraestructura de red entre el pretest y postest de duración y disponibilidad estimada 97
Tabla 36 Rangos de la dimensión rendimiento de la infraestructura de red en el pretest y postest según recursos 98
Tabla 37 Estadísticos de la prueba U de Mann–Whitney de la dimensión rendimiento de la infraestructura de red entre el pretest y postest según recursos 99
Tabla 38 Rangos de la dimensión rendimiento de la infraestructura del servidor en el pretest y postest 100
Tabla 39 Estadísticos de la prueba U de Mann–Whitney de la dimensión rendimiento de la infraestructura del servidor entre el pretest y postest 101
Tabla 40 Tamaño del efecto según r de Rosenthal 102
Tabla 41 Matriz de consistencia 126

Índice de figuras

Figura 1 Resultados pretest y postest de la dimensión eficiencia operativa según fuente de detección 70

Figura 2 Resultados pretest y postest de la dimensión disponibilidad del servicio según fuente de detección 75

Figura 3 Resultados pretest y postest de la disponibilidad estimada por equipo de red 78

Figura 4 Resultados pretest y postest de la duración por equipo red 81

Figura 5 Resultados pretest y postest del estado de CPU 82

Figura 6 Resultados pretest y postest del estado de memoria 83

Figura 7 Resultados pretest y postest del estado de almacenamiento interno 83

Figura 8 Resultados pretest y postest del uso de CPU por servidor afectado 86

Figura 9 Resultados pretest y postest del uso de memoria RAM por servidor afectado 86

Figura 10 Resultados pretest y postest del uso de almacenamiento por servidor afectado 87

Figura 11 Resultados pretest y postest de la temperatura de CPU por servidor afectado .. 87

Índice de anexos

Anexo 1. Matriz de consistencia 126

Anexo 2. Matriz de instrumentos 127

Anexo 3. Instrumentos de recolección de datos 128

Anexo 4. Validación de experto 134

Anexo 5. Evidencia de la implementación del servidor de monitoreo 137

Anexo 6. Resultados eficiencia operativa pretest 143

Anexo 7. Resultados eficiencia operativa postest 145

Anexo 8. Resultados disponibilidad del servicio pretest 147

Anexo 9. Resultados disponibilidad del servicio postest 149

Anexo 10. Resultados rendimiento de la infraestructura de red pretest 151

Anexo 11. Resultados rendimiento de la infraestructura de red postest 153

Anexo 12. Resultados rendimiento de la infraestructura de servidor pretest 155

Anexo 13. Resultados rendimiento de la infraestructura de servidor postest 158

I. Introducción

En la actualidad, la transformación digital ha incrementado la dependencia de las organizaciones respecto de sus infraestructuras tecnológicas, convirtiendo a los servicios TI en un componente esencial para garantizar la continuidad operativa y la eficiencia de los procesos institucionales. En este contexto, las inversiones en tecnologías de la información permiten a las organizaciones optimizar sus operaciones, mejorar la toma de decisiones y fortalecer su competitividad en entornos cada vez más dinámicos (Bessen, 2020).

Dentro del ámbito internacional, diversas investigaciones han demostrado que la implementación de servidores de monitoreo contribuye significativamente a la mejora de la gestión de servicios TI. Montero (2022), en una empresa avícola ecuatoriana, evidenció que la incorporación de una plataforma de monitoreo permitió optimizar la gestión de incidentes y elevar la satisfacción de los usuarios. De manera similar, Robledo (2023), en Colombia, reportó mejoras en la estabilidad, seguridad y rendimiento de la infraestructura tecnológica mediante la implementación de soluciones de monitoreo basadas en Ubuntu Server Linux.

En el contexto nacional, Lizárraga y Ponce (2021) identificaron que la ausencia de monitoreo generaba deficiencias en la gestión tecnológica; sin embargo, tras la implementación de un servidor de monitoreo, lograron incrementos significativos en el control del tráfico de red, la atención de incidencias y la supervisión de servicios críticos. Asimismo, Guevara (2023) determinó que la implementación de un sistema de monitoreo en una universidad pública permitió mejorar la operatividad de los recursos tecnológicos y reducir considerablemente los tiempos de detección de incidentes.

En el ámbito local, la Empresa de Generación Eléctrica Machupicchu S.A. (EGEMSA) enfrenta desafíos relacionados con la supervisión de su infraestructura tecnológica, evidenciados en incidentes recurrentes asociados a la conectividad de usuarios, servicios de telefonía IP, acceso a sistemas y dispositivos de red. Esta situación se ha visto

incrementada por la ampliación de la infraestructura tecnológica de la empresa y por la ausencia de mecanismos sistemáticos para el seguimiento de indicadores de operatividad, disponibilidad y rendimiento de los servicios TI. En consecuencia, la implementación de un servidor de monitoreo se plantea como una alternativa tecnológica orientada a fortalecer la gestión de la infraestructura informática, mejorar la detección temprana de fallas y contribuir a la continuidad operativa de la organización.

Conforme a esta problemática el objetivo general de determinar de qué manera la implementación de un servidor de monitoreo optimiza los servicios TI en la empresa EGEMSA S.A. Cusco, 2025., lo que dio sentido a la estructura metodológica de la investigación como el análisis comparado entre el pretest y el postest, siendo así posible poder identificar el impacto de la intervención en relación a los principales indicadores de desempeño tecnológico.

La presente tesis se desarrolla bajo un enfoque cuantitativo, de diseño prexperimental, utilizando mediciones antes y después de la implementación del sistema de monitoreo, por eso, se evaluaron cuatro dimensiones como la eficiencia operativa, disponibilidad del servicio, rendimiento de la infraestructura de red y rendimiento de la infraestructura del servidor. Además, los datos recolectados fueron procesados mediante estadísticos descriptivos y la prueba U de Mann–Whitney, lo que permitió determinar si las diferencias entre las etapas pre y post implementación fueron estadísticamente significativas.

La presente tesis se estructura en siete capítulos. El Capítulo I presenta la introducción de la investigación; el Capítulo II desarrolla el problema de investigación, incluyendo la formulación del problema, objetivos, hipótesis y operacionalización de variables; el Capítulo III expone los antecedentes y las bases teóricas relacionadas con el monitoreo y los servicios TI; el Capítulo IV describe la metodología empleada para el

desarrollo del estudio; el Capítulo V presenta el análisis de los resultados obtenidos y su respectiva discusión; el Capítulo VI contiene las conclusiones derivadas de la investigación; y el Capítulo VII formula las recomendaciones orientadas a fortalecer la gestión de los servicios TI. Finalmente, se incluyen las referencias bibliográficas y los anexos que sustentan el desarrollo de la investigación.

II. Problema de investigación

2.1. Descripción y formulación del problema

En un mundo cada vez más globalizado, el crecimiento de las tecnologías de la información (TI) de las empresas competitivas está transformando radicalmente el panorama empresarial durante las últimas décadas. Estas tecnologías han permitido que las empresas puedan, entre otras cosas, perfeccionar sus procesos operativos, aumentar la efectividad en el proceso de decisiones y alcanzar un mayor potencial de adaptación dentro del ámbito global dinámico. En este marco, las empresas que tienen una fuerte inversión en la infraestructura basada en las TI no solo pasan a ser mucho más ágiles y competitivas, sino que además soportan una concentración de mercado provocada por la implantación de software a medida y sistemas propios, lo que las lleva a obtener ventajas competitivas frente a sus rivales (Bessen, 2020).

Por ello, la implementación de servidores de monitoreo es considerada una práctica que se viene gestionando tanto en el sector público como en el privado, logrando la mejora en los servicios TI, como demuestra la investigación de Montero (2022), que implementó un servidor de monitoreo en una empresa avícola ecuatoriana “POFASA S. A.” logrando mayor eficiencia en la gestión de incidentes, aumentando en la satisfacción y confianza del usuario, y una reducción significativa en las quejas, aportando evidencia no solo sobre la mejora de los indicadores específicos de los servicios TI, sino también sobre como este se relaciona con la satisfacción del usuario.

Así mismo, la investigación de Robledo (2023), realizada en Risaralda Colombia, ha obtenido resultados positivos que mejoraron la estabilidad, seguridad y rendimiento optimizando la gestión de la red. Esta investigación aporta la comparación de la implementación entre un servidor en Windows y otro en Ubuntu Server Linux, lo que

permitió ver las ventajas de Ubuntu Server Linux en la realización de las tareas de monitoreo.

Así mismo en el Perú, en el estudio de Lizárraga y Ponce (2021), realizada en la empresa “Precisa” de la ciudad de Lima, contaban con una gestión ineficiente de los servicios TI por la falta de un monitoreo adecuado impactando negativamente a la empresa, lo cual generaba costos adicionales y una baja calidad del servicio. Sin embargo, con la implementación de un servidor de monitoreo mejoró significativamente la gestión de sus servicios TI. Se constató un incremento del 45.53% en el control de saturación del tráfico de red, un aumento del 40.91% en la atención de incidencias de dispositivos Networking y un incremento del 30.3% en el control de servicios caídos, destacando el impacto positivo de estas herramientas en la gestión tecnológica.

Por otro lado, el estudio de Guevara (2023), se enfrentó a serios desafíos en la gestión de la infraestructura tecnológica, en la Universidad Nacional de Cajamarca, debido a la ausencia de un sistema de monitoreo efectivo. La falta de herramientas adecuadas resultó en procesos de seguimiento manual, dependientes de la experiencia del personal, lo que limitaba la capacidad de detectar y resolver incidentes en tiempo real. La implementación de un sistema de monitoreo de infraestructura de TI mejoró significativamente el soporte a la gestión de recursos tecnológicos con una mejora en la funcionalidad del sistema, en la satisfacción del usuario y en la operatividad de los recursos de tecnologías de la información o TI. Ello se traduce en un incremento del 13% en funcionalidad, un aumento del 15% en satisfacción de usuarios, un incremento del 10% en operatividad de los recursos de TI, y una reducción del 99,99% en los tiempos de detección de incidentes, destacando el impacto positivo de estos sistemas en la gestión de recursos tecnológicos.

Por otro lado, en el estudio de Fernández (2019), en la Unidad de Gestión Educativa Local de Huamanga (UGEL Huamanga), enfrentaban problemas debido a la expansión de

su red de datos, lo que resultó en una congestión del tráfico y una saturación del ancho de banda, afectando la calidad del servicio para sus trabajadores y también el uso de herramientas limitadas como Wireless Network Watcher no era suficiente para manejar la creciente complejidad de la red. Entonces, la implementación del servidor de monitoreo y gestión permitió una mejora significativa en la administración de la red de datos, logrando una mayor eficiencia en la gestión del tráfico de red, la detección de intrusos y la supervisión del consumo de ancho de banda.

Es en este sentido, la presente investigación pretende abordar una problemática actual de la “Empresa de Generación Eléctrica Machupicchu S.A.” (EGEMSA), dicha entidad enfrenta importantes desafíos relacionados con la gestión y optimización de sus servicios TI. A pesar de ser una organización clave en el sector energético de la ciudad del Cusco, su infraestructura tecnológica presenta limitaciones que afectan la continuidad y calidad de los servicios. Entre los principales incidentes resaltan fallos en la conexión de usuarios a sistemas, problemas con teléfonos IP, y dificultades con el acceso de dispositivos como impresoras. Esto refleja una problemática recurrente en la empresa relacionada con la falta de supervisión proactiva en la conectividad de los servicios clave, lo que puede impactar la continuidad operativa.

Además, se dan incidentes de supervisión y acceso, lo que indica posibles fallas en la gestión de recursos críticos. Un servidor de monitoreo podría aportar significativamente al identificar interrupciones de red, supervisar el estado de los dispositivos conectados y enviar alertas tempranas para prevenir fallos en los servicios de comunicación y sistemas esenciales. La cantidad de incidentes relacionados con estas fallas pasaron del 24.3%, del total de incidentes reportados en Julio del 2024, al 48.6% en diciembre del 2024, motivado principalmente por la ampliación de la infraestructura física de EGEMSA con la consiguiente cobertura de nuevos equipos para las nuevas oficinas. Cabe resaltar que no se

realiza el seguimiento de indicadores de operatividad de servicios y rendimiento de red o servidores en la actualidad en EGEMSA.

Asimismo, la dependencia de sistemas informáticos complejos en la gestión administrativa, operativa y de seguridad en EGEMSA resalta la necesidad de una supervisión constante y eficiente. Los sistemas involucrados incluyen el almacenamiento mediante VEAM Backup, que permite compartir y resguardar grandes cantidades de información generada; servidores de bases de datos que brindan servicios críticos bajo un modelo cliente-servidor; y servicios esenciales como el servidor web, que maneja la entrega de información a los usuarios, además de servicios DHCP, DNS y Active Directory, fundamentales para la administración de la red interna. También se cuenta con un sistema de antivirus, actualmente Kaspersky Security Endpoint, para mitigar amenazas de archivos maliciosos.

Sin embargo, la gestión actual de esta infraestructura TI no responde adecuadamente a las crecientes demandas de eficiencia, seguridad y escalabilidad. A pesar de inversiones en servidores modernos, sistemas de almacenamiento y un ERP, persisten brechas significativas en la capacidad de monitoreo y respuesta. Esta situación no solo limita la productividad interna, sino que también puede dañar la reputación externa de la empresa, reduciendo la confianza de los clientes en su capacidad de ofrecer servicios confiables.

Por lo tanto, las consecuencias de estos problemas pueden ser las interrupciones en los servicios, pérdida de información crítica y disminución de la eficiencia operativa. Así también, la caída de servicios afecta directamente los procesos estratégicos y operativos, impactando tanto en la productividad interna como en la percepción externa de EGEMSA. Además, la falta de un registro centralizado de eventos impide una adecuada correlación de datos, lo que retrasa la toma de decisiones y complica la implementación de soluciones preventivas.

En los motivos expuestos en el párrafo anterior la implementación de un servidor de monitoreo se presenta como una solución integral para abordar estos desafíos tecnológicos Esta accione podría contribuir en la mejora de la productividad posicionando a EGEMSA como una empresa más competitiva y tecnológicamente eficiente.

2.1.1. Problema General

¿De qué manera la implementación del servidor de monitoreo optimiza los servicios TI en la empresa EGEMSA Cusco, 2025?

2.1.2. Problemas Específicos

- ¿De qué manera la implementación del servidor de monitoreo optimiza la eficiencia operativa en la empresa EGEMSA S.A. Cusco, 2025?
- ¿De qué manera la implementación del servidor de monitoreo optimiza la disponibilidad del servicio en la empresa EGEMSA S.A. Cusco, 2025?
- ¿De qué manera la implementación del servidor de monitoreo optimiza el rendimiento de la infraestructura de red en la empresa EGEMSA S.A. Cusco, 2025?
- ¿De qué manera la implementación del servidor de monitoreo optimiza el rendimiento de la infraestructura del servidor en la empresa EGEMSA S.A. Cusco, 2025?

2.2. Objetivos

2.2.1. Objetivo General

Determinar de qué manera la implementación de un servidor de monitoreo optimiza los servicios TI en la empresa EGEMSA S.A. Cusco, 2025.

2.2.2. Objetivos Específicos

- Determinar de qué manera la implementación de un servidor de monitoreo optimiza la eficiencia operativa en la empresa EGEMSA S.A. Cusco, 2025.
- Determinar de qué manera la implementación de un servidor de monitoreo optimiza la disponibilidad del servicio en la empresa EGEMSA S.A. Cusco, 2025.
- Determinar de qué manera la implementación de un servidor de monitoreo optimiza el rendimiento de la infraestructura de red en la empresa EGEMSA S.A. Cusco, 2025.
- Determinar de qué manera la implementación de un servidor de monitoreo optimiza el rendimiento de la infraestructura del servidor en la empresa EGEMSA S.A. Cusco, 2025.

2.3. Justificación e importancia

La implementación de un servidor de monitoreo en EGEMSA presenta una justificación desde diversas perspectivas. Desde un enfoque económico, la implementación reducirá los costos operativos vinculados con la gestión de los incidentes, ya que se puede optimizar la eficiencia operativa al disminuir los tiempos de respuesta y resolución de problemas, esto puede contribuir a mejorar la disponibilidad en los servicios TI, reduciendo las pérdidas económicas. De manera operativa, se puede centrar en el control y seguimiento de los recursos tecnológicos, mejorando la supervisión en tiempo real de los servicios críticos y también permitirá identificar y solucionar incidentes de manera proactiva, optimizando la infraestructura de red y del servidor al detectar puntos críticos que puedan afectar el rendimiento.

Desde un enfoque social y práctico, esta optimización de los servicios TI puede beneficiar a los trabajadores, a los clientes y a toda la comunidad garantizando una mayor estabilidad en el servicio y una mayor confiabilidad, al mismo tiempo fortalecería la imagen de EGEMSA como empresa eficiente en cuanto a los servicios TI y de tecnología avanzada, contribuyendo así al desarrollo económico y social de la región.

En cuanto a la metodología, la investigación se desarrolla con un enfoque cuantitativo, de nivel causal y con un diseño pre-experimental, el cual permite evaluar el impacto de la implementación del servidor de monitoreo en los servicios TI para ello se compara los resultados de esta variable antes y después de su implementación, para ello, se hace uso de instrumentos realizados en función a la literatura académica existente que fueron validados por juicios de expertos para su aplicación y para una recolección de información confiable. Asimismo, esta investigación aporta un caso de estudio valioso para el campo de TI, el cual sirve como referencia para futuras aplicaciones en contextos similares y destacando la adaptabilidad y eficacia de estas tecnologías en la gestión de infraestructuras complejas.

Siguiendo este razonamiento el estudio se lleva a cabo en la empresa EGEMSA en la subgerencia de TI, ubicada en Cusco, Perú. Además, el estudio se realiza durante el año 2025.

2.4. Hipótesis

2.4.1. Hipótesis general

La implementación del servidor de monitoreo optimiza los servicios TI mediante la eficiencia operativa, disponibilidad del servidor y rendimiento de la red y del servidor en la empresa EGEMSA S.A. Cusco, 2025.

2.4.2. Hipótesis específicas

- La implementación del servidor de monitoreo optimiza la eficiencia operativa en la empresa EGEMSA S.A. Cusco, 2025.
- La implementación del servidor de monitoreo optimiza la disponibilidad del servicio en la empresa EGEMSA S.A. Cusco, 2025.
- La implementación del servidor de monitoreo optimiza la infraestructura de red en la empresa EGEMSA S.A. Cusco, 2025.
- La implementación del servidor de monitoreo optimiza la infraestructura del servidor en la empresa EGEMSA S.A. Cusco, 2025.

2.5. Variables

2.5.1. Variable independiente

Servidor de monitoreo: Un servidor de monitoreo es un sistema dedicado a supervisar y analizar el estado, rendimiento y salud de diversos componentes de una red informática y sus recursos asociados (Junco y Rabelo, 2018).

2.5.2. Variable dependiente

Servicios TI: Los servicios de TI pueden definirse como un grupo de tareas proporcionadas por un sistema de TI o un departamento de TI , es decir, el servicio de TI puede caracterizarse como la aplicación de capacidades especializadas en activos de TI (Serrano et al., 2021).

2.5.3. Operacionalización de variables

Tabla 1

Operacionalización de la variable independiente

Variable independiente	Dimensiones	Indicadores	Ítems	Escala de medición
Implementación de servidor de monitoreo Un servidor de monitoreo es un sistema dedicado a supervisar y analizar el estado, rendimiento y salud de diversos componentes de una red informática y sus recursos asociados (Junco y Rabelo, 2018).	Unidimensional	Presencia o ausencia de servidor de monitoreo	Ficha de registro	Dicotómica

Tabla 2

Operacionalización de la variable dependiente

Variable dependiente	Dimensiones	Indicadores	Ítems	Escala de medición
Servicios TI Los servicios de TI pueden definirse como un grupo de tareas proporcionadas por un sistema de TI o un departamento de TI , es decir, el servicio de TI puede caracterizarse como la aplicación de capacidades especializadas en activos de TI (Serrano et al., 2021).	**Dimensión 1** **Eficiencia operativa** La eficiencia operativa en los servicios TI es la capacidad de la infraestructura tecnológica para responder de manera oportuna a incidentes, reduciendo tiempos de respuesta y minimizando el impacto negativo en las operaciones de la organización (Serrano et al., 2021).	Tiempo promedio de resolución de incidentes Porcentaje de eventos detectados	Ficha 1	De razón
	Dimensión 2 **Disponibilidad del servicio** La disponibilidad del servicio es la capacidad de los sistemas TI para permanecer operativos y accesibles durante periodos prolongados, ya que cualquier interrupción puede generar pérdidas significativas y afectar operaciones críticas (Serrano et al., 2021).	Tiempo de actividad de los servicios TI Frecuencia de interrupciones de servicio	Ficha 2	De razón
	Dimensión 3 **Rendimiento de la infraestructura de red** El rendimiento de la infraestructura de red se refiere a la capacidad de la red para manejar cargas de tráfico de manera efectiva, minimizar la pérdida de datos y garantizar una disponibilidad continua de los servicios TI (Serrano et al., 2021).	Disponibilidad de la red Saturación Estado del equipo de red	Ficha 3, 4, 5	De razón
	Dimensión 4 **Rendimiento de la infraestructura del servidor** El rendimiento de la infraestructura del servidor es la capacidad del servidor para gestionar eficazmente las demandas de procesamiento, almacenamiento y disponibilidad de las aplicaciones críticas, asegurando estabilidad y escalabilidad de los servicios tecnológicos (González et al., 2021).	Uso de recursos Temperatura de CPU	Ficha 6	De razón

III. Marco teórico

3.1. Antecedentes

A nivel internacional se encuentra el estudio de Montero (2022), titulado "Implementación de un sistema de monitoreo y control de la infraestructura de TI para la gestión de incidencias en la red interna de la empresa avícola Pollo Favorito S.A. (POFASA)", desarrollado en la Escuela Politécnica Nacional de Ecuador. La investigación tuvo como objetivo implementar un sistema de monitoreo y control de infraestructura TI para la gestión de incidencias mediante el análisis de servicios y dispositivos críticos. El estudio fue de tipo aplicada, nivel descriptivo-explicativo y diseño experimental, empleando la metodología PDCA. Los resultados evidenciaron una reducción significativa en los tiempos de atención de incidentes, pasando de más de 4 horas en el 69% de los casos a 30 minutos en el 89% tras la implementación. Asimismo, la satisfacción de los usuarios alcanzó un 95% de valoraciones entre bueno y excelente, mientras que la confianza en el sistema aumentó de un 11% a un 95%. También se redujeron las quejas de un promedio de tres por semana a una por semana en el 78% de los casos. Se concluyó que la implementación de Zabbix tuvo un impacto significativo en la gestión de la infraestructura TI de POFASA.

Este antecedente coincide con la presente investigación al demostrar que la implementación de sistemas de monitoreo contribuye significativamente a la mejora de la gestión de servicios TI, especialmente en la reducción de tiempos de atención de incidentes y el incremento de la satisfacción de los usuarios. Sin embargo, el estudio se desarrolló en una empresa del sector avícola y se enfocó principalmente en la gestión de incidencias, mientras que la presente investigación aborda además indicadores relacionados con la disponibilidad del servicio y el rendimiento de la infraestructura tecnológica. Por ello, sus resultados constituyen evidencia relevante sobre los beneficios operativos del monitoreo,

aunque persiste la necesidad de validar estos efectos en organizaciones con características y requerimientos tecnológicos distintos, como EGEMSA.

Robledo (2023), en su investigación titulada “Implementación de un Servidor de Monitoreo de Telecomunicaciones en la Gobernación de Risaralda”, realizada en la Universidad Católica de Pereira (Colombia), tuvo como objetivo implementar un servidor para la gestión de la infraestructura de telecomunicaciones de dicha entidad. La investigación fue de tipo aplicada, nivel descriptivo-explicativo y diseño experimental. Los resultados evidenciaron que Ubuntu Server Linux presentó un desempeño superior frente a Windows en la detección y respuesta ante incidentes. En las pruebas realizadas, Ubuntu detectó dispositivos conectados en un promedio de 48 segundos, mientras que Windows requirió entre 3 y 5 minutos. Asimismo, ante eventos como desconexión de patch cord, fallas eléctricas y desconexiones masivas, Ubuntu registró tiempos de detección entre 27 y 51 segundos, superando ampliamente a Windows, cuyos tiempos excedieron los 3 minutos en la mayoría de los casos. Se concluyó que la implementación de Cacti sobre Ubuntu Server Linux optimiza significativamente la monitorización y gestión de redes, destacando por su rapidez en la detección de problemas.

Esta investigación coincide con el presente estudio al evidenciar que las herramientas de monitoreo permiten mejorar la detección temprana de fallas y optimizar la gestión de la infraestructura tecnológica. Como diferencia, el estudio centra su análisis en la comparación del desempeño entre sistemas operativos para la implementación del servidor de monitoreo, mientras que la presente investigación evalúa el impacto de la implementación sobre los servicios TI. Esta diferencia permite identificar un vacío relacionado con la medición de indicadores organizacionales posteriores a la implementación, aspecto que se desarrolla en la presente investigación.

En el territorio nacional se tienen investigaciones como el de Lizarraga y Ponce (2021), en su tesis de pregrado realizada bajo el título: “Implementación de un servidor de monitoreo para optimizar la gestión de servicios TI en la empresa Precisa, 2021”, desarrollada en la Universidad César Vallejo, en Lima Callao, tuvo como objetivo determinar la influencia de la implementación de un servidor de monitoreo en la gestión de servicios TI de la empresa Precisa. La investigación fue de tipo aplicada y se desarrolló bajo el diseño pre-experimental con el uso del enfoque cuantitativo. Por medio de los resultados se pudo observar que hubo un aumento del porcentaje en el nivel de control de saturación del tráfico de red de 42.35% antes de la implementación a 87.88% después, un aumento del 45.53%. En cuanto al nivel de atención de incidencias de dispositivos Networking, se mejoró de 52.27% a 93.18%, reflejando un aumento del 40.91%. Finalmente, el nivel de control de servicios caídos mejoró de 60.61% a 90.91%, un aumento del 30.3%, por tanto, se concluyó que por medio de la utilización del servidor, operando con Ubuntu Linux y las herramientas de monitoreo Nagios y Cacti, destacando la eficacia de la implementación del servidor de monitoreo como una herramienta crítica para la administración eficiente de la infraestructura TI en la empresa.

Este antecedente presenta una similitud con la presente investigación debido a que evalúa la influencia de un servidor de monitoreo sobre la gestión de servicios TI mediante un diseño preexperimental. Los resultados obtenidos evidencian mejoras en el control del tráfico de red, atención de incidencias y supervisión de servicios críticos, coincidiendo con la hipótesis planteada en el presente estudio. Sin embargo, la investigación se desarrolló en una empresa privada con características organizacionales diferentes a las de una empresa del sector energético, por lo que resulta pertinente analizar si dichos beneficios pueden replicarse en el contexto de EGEMSA.

Fernández (2019), en su tesis titulada “Implementación de un servidor como gestión y monitoreo de servicios para la red de datos en la UGEL Huamanga, 2018”, desarrollada en la Universidad Nacional de San Cristóbal de Huamanga, tuvo como objetivo implementar un servidor de monitoreo para la gestión de dispositivos y servicios de red mediante el protocolo SNMP y tecnologías de virtualización en CentOS 7 y NethServer 7. La investigación fue de tipo aplicada, enfoque cuantitativo y diseño observacional. Los resultados evidenciaron que la interfaz ens33 concentró el mayor tráfico de red, alcanzando picos de 5.51 Mbps, predominando protocolos como SSL_No_Cert, HTTP y SSDP. Asimismo, se identificaron los principales orígenes y destinos del tráfico de datos, permitiendo una supervisión más eficiente de la infraestructura. Se concluyó que el sistema implementado constituyó una herramienta valiosa para la administración proactiva de la red, facilitando intervenciones oportunas y contribuyendo a la operatividad y seguridad de la infraestructura tecnológica.

Esta investigación coincide con el presente estudio en la importancia atribuida al monitoreo continuo para garantizar la operatividad y seguridad de la infraestructura tecnológica. Sin embargo, su enfoque estuvo orientado principalmente al análisis del tráfico de red y consumo de ancho de banda, mientras que la presente investigación incorpora además indicadores de eficiencia operativa, disponibilidad de servicios y rendimiento de servidores. Esta diferencia evidencia la necesidad de estudios más integrales que permitan evaluar el impacto general de los sistemas de monitoreo sobre los servicios TI.

Guevara (2023), con título “Sistema de monitoreo de infraestructura de TI para soporte a la gestión de recursos de la Oficina de Tecnologías de la Información de la Universidad Nacional de Cajamarca” realizada en la Universidad Nacional de Cajamarca, se desarrolló con el objetivo de determinar la influencia del sistema de monitoreo de infraestructura de TI en el soporte de la gestión de recursos en la oficina de tecnologías de

la información de la UNC, esta investigación fue de tipo aplicada y de diseño experimental, los resultados tras la implementación del sistema Zabbix mostraron en el nivel de funcionalidad una mejora del 13% desde el porcentaje anterior 61,71%, el nivel de satisfacción del usuario aumentó en un 15% en comparación del porcentaje previa a la implementación que era de 65%, y el nivel de operatividad de los recursos de TI mostró un incremento del 10% desde el porcentaje previo que bordeaba el 69.74%. Además, se observó una mejora en la detección de incidencias, reduciendo los tiempos en un 99,99%. Se concluye que el impacto positivo de la implementación del sistema de monitoreo en la infraestructura de TI en la oficina de tecnologías de la información de UNC.

Los resultados obtenidos en este estudio guardan relación directa con la presente investigación, ya que evidencian mejoras en la funcionalidad, operatividad y satisfacción de los usuarios tras la implementación de un sistema de monitoreo. Asimismo, ambos estudios comparten el interés por evaluar el efecto de estas herramientas sobre la gestión tecnológica institucional. Sin embargo, la investigación fue desarrollada en una institución universitaria, por lo que aún existe la necesidad de generar evidencia en organizaciones pertenecientes a otros sectores estratégicos, como el energético, donde la continuidad de los servicios tecnológicos resulta crítica.

Garay (2018), realizada bajo el título: “Implementación de la herramienta centreon para el monitoreo de la infraestructura de T.I. en la empresa América Móvil Perú S.A.C” realizada en la Universidad Autónoma del Perú. Esta investigación tuvo como objetivo implementar la herramienta Centreon para el control de la infraestructura de TI en la empresa América Móvil Perú S.A.C., la investigación estuvo dentro del desarrollo de un proyecto de una duración de 3 meses de tipo aplicado y de enfoque cuantitativo. Los resultados evidenciaron que la herramienta de monitoreo Centreon posee una gran efectividad frente a las demandas de la infraestructura de TI de la empresa América Móvil Perú S.A.C, por

consiguiente, la empresa obtuvo una visibilidad mejorada y mayor control sobre el hardware y software.

Este estudio coincide con la presente investigación al demostrar que las herramientas de monitoreo incrementan la visibilidad y control sobre la infraestructura tecnológica. No obstante, la investigación se enfoca principalmente en la implementación tecnológica de la solución y en sus beneficios operativos generales, sin evaluar de manera específica indicadores asociados a la optimización de los servicios TI, esta limitación justifica la necesidad de investigaciones que cuantifiquen de forma objetiva el impacto de estas herramientas sobre variables específicas del desempeño tecnológico.

Casas y Sempértegui (2018), en la investigación titulada “Implementación de un Sistema de Monitoreo y Supervisión de la Infraestructura y Servicios de Red para Optimizar la Gestión de TI en la Universidad Nacional Pedro Ruiz Gallo”, desarrollada en Lambayeque, tuvieron como objetivo implementar un sistema de monitoreo y supervisión para optimizar la administración de la red de datos y el monitoreo de la infraestructura y servicios de red. El estudio fue de tipo experimental. Los resultados evidenciaron una reducción significativa en los tiempos de detección y notificación de incidentes, registrando caídas de infraestructura en 70 segundos y de servicios de red en 42 segundos, con notificaciones enviadas en menos de dos minutos. Asimismo, actividades de supervisión que anteriormente se realizaban de forma manual pasaron a ejecutarse en línea y en tiempo real. Se concluyó que la implementación del sistema mejoró significativamente el monitoreo, diagnóstico y gestión de la infraestructura y servicios de red.

Este antecedente coincide con la presente investigación al evidenciar que la implementación de sistemas de monitoreo reduce significativamente los tiempos de detección y notificación de incidentes, contribuyendo a una gestión más eficiente de la infraestructura tecnológica. Además, como diferencia, el estudio se concentra

principalmente en la optimización de los procesos de supervisión y diagnóstico de redes, mientras que la presente investigación amplía el análisis hacia indicadores de eficiencia operativa, disponibilidad y rendimiento de infraestructura. En consecuencia, sus resultados constituyen una base importante para sustentar la efectividad de las soluciones de monitoreo en distintos entornos organizacionales.

3.2. Bases teóricas

3.2.1. Variable independiente

3.2.1.1. Servidor de monitoreo

Para Junco y Rabelo (2018), un servidor de monitoreo es un sistema dedicado a supervisar y analizar el estado, rendimiento y salud de diversos componentes de una red informática y sus recursos asociados.

Por lo tanto, un servidor de monitoreo es una plataforma que permite la observación continua y sistemática de la infraestructura de TI, incluyendo servidores, dispositivos de red, aplicaciones y servicios. Este tipo de servidor consulta, recoge y analiza datos de rendimiento y estado, generando alarmas en modo real y generando reportes detallados sobre el procesamiento y salud de los componentes monitoreados.

Por otro lado, según Oppenheimer (2010), un servidor de monitoreo se utiliza para "supervisar la infraestructura de red y los sistemas de TI, asegurando que todos los componentes funcionen dentro de los parámetros normales y que cualquier anomalía o fallo sea detectado y reportado inmediatamente".

Asimismo, Stallings (2017), se describe que "los servidores de monitoreo son esenciales para mantener la disponibilidad y el rendimiento de los servicios de TI, ya que proporcionan una vigilancia constante y alertan a los administradores sobre problemas potenciales antes de que se conviertan en fallos críticos". Además, Laudon y Laudon (2019) señalan que "un servidor de monitoreo no solo recoge datos de rendimiento, sino que

también analiza patrones y tendencias, permitiendo a las organizaciones predecir y prevenir problemas, mejorando así la eficiencia operativa y la satisfacción del usuario final".

En la práctica, un servidor de monitoreo suele integrarse en la arquitectura de gestión de TI como parte de un Centro de Operaciones de Red, estos sistemas pueden ser de código abierto o comerciales, y a menudo siguen estándares y buenas prácticas de la industria (por ejemplo, ITIL en gestión de servicios). Además, herramientas populares como Nagios, Zabbix, PRTG o Centreon cumplen estas funciones, permitiendo supervisar dispositivos on-premise, en la nube o en entornos híbridos, y generando alertas para el personal de TI cuando algo se desvía de la norma. Por consiguiente, un buen servidor de monitoreo ofrece a los administradores una visibilidad completa de la infraestructura, hace el mapeo de los componentes que están conectados, monitoriza el rendimiento de las aplicaciones y la infraestructura asociada, y prueba de optimizar el flujo de datos al detectar cuellos de botella (IBM, 2021).

El monitoreo de servidores es imprescindible para obtener buenas experiencias de los usuarios y buenos resultados de negocio, a medida que la infraestructura de TI se vuelve más compleja, ello implica entornos de nube híbridos y arquitecturas distribuidas, el monitoreo efectivo ayuda a los equipos de TI a mantener operaciones confiables y evitar que los problemas escalen sin ser detectados (IBM, 2023a). En la actualidad, la tendencia va más allá del monitoreo tradicional hacia el concepto de observabilidad, el cual no solo indica cuándo algo anda mal, sino que también brinda información sobre qué está sucediendo y el por qué; permitiendo identificar la causa raíz y resolver problemas de forma proactiva (IBM, 2023c).

3.2.1.2. Etapas del servidor de monitoreo

3.2.1.2.1. Configuración inicial

La configuración inicial de un sistema de monitoreo se encuentra orientada a la definición de parámetros técnicos básicos que incidan en el aseguramiento del correcto funcionamiento del sistema, lo que incluye la disposición de guías y lineamientos entendidos como estándares que han sido formalizados por fabricantes como Microsoft o Linux. Dichas guías incluyen los lineamientos necesarios para asegurar el correcto funcionamiento, la estabilidad y la seguridad del sistema. Estas guías son fundamentales para establecer políticas de configuración inicial que minimicen riesgos de seguridad y optimicen el desempeño del sistema. Además, los estándares de hardening, como los recomendados por CIS Benchmarks y OpenSCAP, se aplican durante esta fase para reforzar la protección frente a vulnerabilidades comunes (Center for Internet Security, 2022).

La configuración inicial también incluye la implementación del hardening, un proceso técnico que implica deshabilitar servicios no esenciales, configurar correctamente permisos y aplicar políticas de seguridad robustas. Según Red Hat (2023), estas prácticas aseguran que el servidor esté preparado para operaciones seguras desde su instalación, donde esta dimensión establece la base para que el servidor opere en un entorno controlado y seguro.

De manera complementaria, Sasidharan (2022) evidencia, mediante un estudio de caso sobre hardening en sistemas Windows, que las organizaciones que aplican los controles CIS logran establecer una línea base de seguridad confiable que protege la infraestructura frente a amenazas externas e internas. Asimismo, Govindappa y Singh (2024) señalan que la estandarización de configuraciones mediante benchmarks CIS no solo fortalece la postura de seguridad, sino que también

facilita la integración de herramientas automatizadas para la verificación continua del cumplimiento, lo cual es especialmente relevante en entornos con múltiples servidores.

Se enfatiza la importancia de seguir lineamientos oficiales de configuración, por ejemplo, las guías de hardening de Windows Server o Linux, que aseguren que el servidor opere bajo condiciones óptimas y con las debidas medidas de seguridad; el cumplimiento de estándares recomendados (como las políticas de seguridad de Microsoft o los benchmarks de CIS para sistemas operativos) es un indicador fundamental en esta etapa, pues minimiza riesgos de vulnerabilidades por configuraciones débiles o incorrectas. En definitiva, hardening es aplicar configuraciones seguras y estrictas con el fin de aplacar las vulnerabilidades: desactivar funcionalidades no utilizadas, restringir los accesos o seguir las guías de confianza (Hatt, 2025).

El hardening, consistente en desactivar servicios no requeridos, mejorar los permisos y aplicar alguna de las configuraciones de seguridad que existe para poner en producción un servidor, es un aspecto clave de la configuración inicial, para ejecutar un hardening efectivo, existen organismos especialistas como el Center for Internet Security (2022) que proporcionan guías de hardening que, al ser aplicadas, disminuyen la superficie de ataque del servidor y mejoran la postura de seguridad del mismo desde el arranque.

Indicadores:

- **Cumplimiento de guías y estándares de fabricantes**

Este indicador mide el grado en que se aplican los lineamientos técnicos proporcionados por los fabricantes del sistema operativo y otros componentes del

servidor, por ello, su importancia radica en establecer configuraciones estandarizadas que aseguren un funcionamiento óptimo desde el inicio.

- **Hardening aplicado (seguridad básica configurada)**

Evalúa el porcentaje que ha implementado solo las configuraciones de seguridad más recomendadas, esto incluye la desactivación de servicios innecesarios, configuraciones de acceso y actualizaciones de seguridad. Según el Center for Internet Security (2022), aplicar hardening reduce la superficie de ataque y fortalece el sistema contra amenazas.

3.2.1.2.2. Cobertura de supervisión

La cobertura de supervisión se refiere a la capacidad del servidor para monitorear de manera eficiente dispositivos y servicios críticos dentro de una red informática, entonces, esta dimensión garantiza la detección oportuna de problemas y la optimización de recursos mediante herramientas como Nagios y Zabbix, que facilitan la supervisión en tiempo real (Nagios, 2023). Según la documentación oficial de Ubuntu Server (Canonical, 2023), un sistema de supervisión efectivo debe incluir métricas claras y relevantes para evitar interrupciones en los servicios.

La cobertura de supervisión es clave para identificar cuellos de botella en la red y priorizar recursos hacia elementos críticos. Además, esta dimensión asegura que los dispositivos y servicios supervisados se encuentren en cumplimiento con las políticas establecidas por la organización, minimizando riesgos operativos (Zabbix, 2023).

Un aspecto importante de la cobertura es evitar zonas sin monitoreo (*blind spots*), por ello, una visibilidad incompleta de la infraestructura puede permitir que ciertas fallas pasen desapercibidas. En este sentido, las buenas prácticas indican que

se debe eliminar cualquier brecha de monitoreo para garantizar una conciencia situacional completa de la red y reducir la superficie de ataque (Selector, 2023).

Indicadores:

- **Porcentaje de dispositivos supervisados por el servidor**

Este indicador mide la proporción de dispositivos monitoreados en relación con el total conectado a la red, entonces, un alto porcentaje indica una cobertura adecuada que reduce la posibilidad de dispositivos sin supervisar (Nagios, 2023).

- **Cantidad de servicios críticos supervisados por el servidor**

Representa el número de servicios signigicativos monitoreados y asegura la continuidad de operaciones. Según Zabbix (2023) enfatiza que identificar servicios críticos es importante para mantener la estabilidad del sistema.

3.2.1.2.3. Rendimiento operativo

El rendimiento operativo evalúa la capacidad del servidor para operar sin interrupciones y gestionar recursos de manera eficiente bajo diferentes niveles de carga, además, la tasa de operación ininterrumpida, o *uptime*, es un indicador crucial que mide la fiabilidad del sistema. Según Nagios (2023), mantener altos niveles de *uptime* es fundamental para garantizar la disponibilidad de servicios críticos. Por otro lado, el uso eficiente de CPU, memoria y almacenamiento refleja la capacidad del servidor para manejar tareas bajo condiciones de estrés (Zabbix, 2023).

La mejora del rendimiento operativo está ligada a una adecuada configuración inicial y a un monitoreo constante. Documentos de Red Hat (2023) destacan que un servidor con buen rendimiento no solo asegura la continuidad operativa, sino que también optimiza costos al utilizar eficientemente los recursos disponibles.

La eficiencia del rendimiento operativo resulta indudablemente destacable en la capacidad de respuesta del servidor de supervisión ante múltiples eventos; en grandes entornos pueden procesarse cientos de alertas u otras consultas por minuto, de forma que un buen diseño (ya sea software optimizado, bases de datos tipo time-series eficientes, etc.) permite procesar esos eventos en tiempo real sin retrasos. También se indica que sistemas de monitoreo bien afinados pueden manejar millones de puntos de datos por segundo gracias a arquitecturas distribuidas y algoritmos de procesamiento en tiempo real (Choudhury, 2024).

Un diseño óptimo (ya sea mediante software afinado, uso de bases de datos de series de tiempo eficientes, o arquitecturas distribuidas con múltiples nodos de monitoreo) permite procesar eventos en tiempo real sin retrasos perceptibles. Por ejemplo, en industrias con altísimas exigencias, se busca una disponibilidad del 99.99% (“cinco nueves”) en sus sistemas, lo cual equivale a apenas unos 5 minutos de inactividad al año. Solo las arquitecturas más robustas logran este nivel de desempeño, típicamente a través de eliminación de puntos únicos de falla, failover automatizado y escalamiento horizontal (IBM, 2023b).

Ahmad et al. (2020) complementan esta visión al indicar que una infraestructura de red bien gestionada no solo optimiza el flujo de información, sino que también reduce el tiempo de respuesta en la resolución de problemas, lo cual es significativo para la continuidad operativa. Además, González et al. (2021) subrayan que una red confiable mejora de manera directa la experiencia del usuario y la productividad organizacional, particularmente en entornos de alta dependencia tecnológica.

Indicadores:

- **Tiempo de operación ininterrumpida del servidor (uptime)**

Este indicador mide la cantidad de tiempo que el servidor ha estado operativo sin interrupciones, siendo una alta tasa de uptime un estándar de calidad en infraestructuras TI (Nagios, 2023).

- **Uso de recursos promedio bajo carga del servidor**

Evalúa el porcentaje de utilización de CPU, memoria y almacenamiento durante operaciones normales y bajo estrés, por eso, un servidor eficiente mantiene estos valores dentro de rangos aceptables (Zabbix, 2023).

3.2.1.2.4. Seguridad operativa

La seguridad operativa se centra en mantener la protección del sistema mediante la actualización de parches de seguridad, la implementación de configuraciones seguras de acceso y la realización periódica de análisis de vulnerabilidades. Según Nessus (2023), estas prácticas son esenciales para prevenir ataques cibernéticos y mitigar riesgos, los parches de seguridad garantizan que el sistema esté protegido contra vulnerabilidades conocidas, mientras que las configuraciones de firewall y accesos seguros establecen barreras contra accesos no autorizados.

La seguridad operativa también incluye un enfoque proactivo mediante análisis de vulnerabilidades realizados con herramientas como OpenVAS, que identifican debilidades en el sistema antes de que sean explotadas (OpenVAS, 2023), este enfoque integral asegura que el servidor de monitoreo se mantenga protegido en un entorno de amenazas dinámico, sirviendo como un guardián fiable de la infraestructura de TI. No obstante, hay que mencionar que el 60% de los compromisos en seguridad de las empresa son consecuencia de vulnerabilidades

conocidas que no han sido parcheadas a tiempo (Field, 2024). Por su parte, Govindappa y Singh (2024) señalan que la integración de herramientas automatizadas de análisis de vulnerabilidades, alineadas con los controles CIS, permite a las organizaciones mantener una postura de seguridad dinámica que se adapta a un entorno de amenazas en constante evolución.

Indicadores:

- **Actualización de parches de seguridad**

Mide el porcentaje de actualizaciones aplicadas respecto al total disponible, la documentación de Microsoft se resalta que la aplicación oportuna de parches reduce significativamente los riesgos de seguridad.

- **Configuración de acceso seguro (firewall y usuarios)**

Este indicador evalúa la proporción de accesos configurados de manera segura, garantizando que las políticas de acceso estén alineadas con los estándares de seguridad (Red Hat, 2023).

- **Análisis de vulnerabilidades**

Mide la frecuencia con la que se realizan análisis de vulnerabilidades para identificar y corregir debilidades del sistema. Nessus (2023) señala que el monitoreo constante reduce los riesgos de ciberataques.

3.2.2. Variable dependiente

3.2.2.1. Servicios TI

Según Serrano et al. (2021), los servicios de TI pueden definirse como un grupo de tareas proporcionadas por un sistema de TI o un departamento de TI, es decir, el servicio de TI puede caracterizarse como la aplicación de capacidades especializadas en activos de TI.

Los servicios de TI son una fuente reconocida de ventaja competitiva para organizaciones de todos los tamaños y para lograr esta ventaja competitiva, es fundamental comprender tanto la filosofía del servicio de TI en su totalidad como los procesos para gestionar dichos servicios. Por lo tanto, estos aspectos son importantes a medida que aumenta la dependencia de las empresas en los servicios de TI y la complejidad de la gestión de procesos para los mismos. Por otro lado, la gestión de servicios de TI utiliza un enfoque orientado al servicio y de procesos para la gestión de TI y se ha argumentado que es importante para las organizaciones entender los beneficios de los procesos efectivos de la gestión de servicios de TI, también, la expansión del número de estudios en esta área es una indicación del creciente interés de los académicos en la gestión de servicios de TI (Shrestha, 2019).

3.2.2.2. Dimensiones de servicios TI

3.2.2.2.1. Eficiencia operativa

La eficiencia operativa en los servicios TI se refiere a la capacidad de la infraestructura tecnológica para responder de manera oportuna a incidentes, minimizando el tiempo de inactividad y optimizando el uso de recursos. Serrano et al. (2021) destacan que la eficiencia operativa está directamente relacionada con la capacidad de los sistemas de monitoreo para detectar fallos y responder proactivamente, minimizando los impactos negativos sobre las operaciones de la organización. En esta línea, Ahmad et al. (2020) definen el tiempo promedio de resolución de incidentes como el período transcurrido desde la detección de un incidente hasta la implementación de una acción para mitigarlo, incluyendo las fases de percepción, comprensión del impacto y proyección de estados futuros, y señalan que un menor tiempo de respuesta resulta crucial para limitar el impacto sobre la disponibilidad de los servicios.

Indicadores:

- **Tiempo promedio de resolución de incidentes**

Según Ahmad et al. (2020) es el período de tiempo transcurrido desde el momento en que se detecta un incidente en la red hasta que se implementa una acción para mitigarlo o resolverlo, por eso, este tiempo incluye las fases de percepción del incidente, la comprensión de su naturaleza y su impacto en los objetivos de la organización, y la proyección de posibles estados futuros y un menor tiempo de respuesta es crucial para limitar el impacto de los incidentes en la red y mantener la disponibilidad de los servicios de TI y la protección de los datos.

- **Porcentaje de eventos destacados**

El porcentaje de eventos detectados es un indicador clave para medir la capacidad de un sistema de monitoreo de identificar anomalías en los servicios TI. Según González et al. (2021), la detección activa de eventos críticos permite a las organizaciones prevenir interrupciones en el servicio y mejorar el rendimiento general de la infraestructura. En contraste, Shrestha et al. (2019) resaltan que los sistemas basados en inteligencia artificial y análisis de predicción son fundamentales para mejorar la precisión de las detecciones.

3.2.2.2.2. Disponibilidad del servicio

La disponibilidad del servicio representa la capacidad de los sistemas TI para estar operativos y accesibles para los usuarios durante períodos prolongados. Serrano et al. (2021) enfatizan que una alta disponibilidad es importante para las operaciones de carácter crítico, ya que cualquier interrupción puede resultar en pérdidas significativas. Asimismo, González et al. (2021) afirman que las estrategias de redundancia y recuperación ante desastres son cruciales para mantener la continuidad del servicio.

Otro aspecto relevante de la disponibilidad es la evaluación del tiempo de actividad en comparación con el tiempo total de operación. Kumar et al. (2023) indican que el monitoreo continuo de los servicios TI facilitan datos valiosos para identificar y corregir vulnerabilidades que afectan la disponibilidad. De manera similar, Ahmad et al. (2020) sostienen que las métricas de tiempo de actividad permiten a las organizaciones establecer objetivos claros y medir su desempeño frente a estándares internacionales.

Indicadores:

- **Tiempo de actividad de los servicios TI**

El tiempo de actividad es una métrica que evalúa el porcentaje del tiempo en que los sistemas están disponibles para los usuarios. Según Serrano et al. (2021), esta métrica es un reflejo directo de la calidad y confiabilidad de los servicios TI. Serrano et al. (2021) señalan que un tiempo de actividad elevado requiere una infraestructura robusta, combinada con estrategias de monitoreo activo.

- **Frecuencia de interrupciones del servicio**

La frecuencia de interrupciones mide la cantidad de eventos que resultan en la pérdida de disponibilidad de los servicios TI. Ahmad et al. (2020) indican que una menor frecuencia de interrupciones es un indicador de una infraestructura estable y bien gestionada. Por su parte, Shrestha et al. (2019) subrayan que las interrupciones frecuentes pueden indicar problemas relacionadas con la red o en los sistemas de gestión de recursos.

3.2.2.2.3. Rendimiento de la infraestructura de red

El rendimiento de la infraestructura de red es un aspecto crítico para garantizar que los servicios TI funcionen de manera eficiente y confiable. Serrano et al. (2021) afirman que este concepto incluye la capacidad de la red para manejar

cargas de tráfico de manera efectiva, minimizar la pérdida de datos y garantizar la disponibilidad continua. Por su parte, Ahmad et al. (2020) indican que una infraestructura de red bien gestionada no solo optimiza el flujo de información, sino que también reduce el tiempo de respuesta en la resolución de problemas, lo cual es significativa para la continuidad operativa.

Además, la evaluación del rendimiento de la red permite identificar cuellos de botella y puntos de mejora en su operación. Kumar et al. (2023) afirman que las herramientas de monitoreo activo son esenciales para obtener datos en tiempo real sobre la salud de la red, lo que facilita la toma de decisiones informadas. Según González et al. (2021) subrayan que una red confiable mejora de manera directa la experiencia del usuario y la productividad organizacional, particularmente en entornos de alta dependencia tecnológica.

Indicadores:

- **Disponibilidad de la red**

La disponibilidad de la red mide el porcentaje del tiempo en que esta permanece operativa y accesible para los usuarios. Según Serrano et al. (2021), mantener altos niveles de disponibilidad es esencial para garantizar la entrega de servicios de calidad. Por otro lado, Ahmad et al. (2020) destacan que la falta de disponibilidad, incluso por períodos cortos, puede tener un impacto significativo en la productividad de las organizaciones.

- **Saturación**

La saturación ocurre cuando la demanda de tráfico o procesamiento supera la capacidad disponible de los recursos de la red (como el ancho de banda o los equipos de conmutación y encaminamiento), llevando a que se alcancen o excedan sus límites operativos y esto produce una disminución del rendimiento reflejada en retrasos,

incremento en los tiempos de respuesta e incluso pérdida de paquetes, comprometiendo la calidad general del servicio y la experiencia del usuario.

- **Estado del equipo de red**

El rendimiento de la infraestructura de red es un aspecto crítico para garantizar que los servicios TI funcionen de manera eficiente y confiable. Serrano et al. (2021) afirman que este concepto incluye la capacidad de la red para manejar cargas de tráfico de manera efectiva, minimizar la pérdida de datos y garantizar la disponibilidad continua. Ahmad et al. (2020) complementan esta visión al indicar que una infraestructura de red bien gestionada no solo optimiza el flujo de información, sino que también reduce el tiempo de respuesta en la resolución de problemas, lo cual es significativo para la continuidad operativa. Además, González et al. (2021) subrayan que una red confiable mejora de manera directa la experiencia del usuario y la productividad organizacional, particularmente en entornos de alta dependencia tecnológica.

3.2.2.2.4. Rendimiento de la infraestructura del servidor

El rendimiento de la infraestructura del servidor es un factor clave para garantizar la operatividad de los servicios TI. Según González et al. (2021) explican que un servidor bien gestionado debe manejar eficazmente las demandas de procesamiento, almacenamiento y disponibilidad de las aplicaciones críticas. En consecuencia, Ahmad et al. (2020) destacan que una infraestructura del servidor con un rendimiento óptimo contribuye a la estabilidad y escalabilidad de los servicios tecnológicos, lo cual es fundamental en entornos empresariales dinámicos.

Además, el monitoreo continuo del servidor permite anticipar fallas y optimizar el uso de recursos. Para Serrano et al. (2021) afirman que herramientas avanzadas de supervisión pueden proporcionar datos en tiempo real sobre el estado

del hardware y software, facilitando la detección temprana de problemas. De manera similar, Kumar et al. (2023) afirman que la automatización en la gestión del servidor reduce significativamente el riesgo de interrupciones inesperadas, lo que mejora la experiencia del usuario y la continuidad del negocio.

Indicadores:

- **Uso de recursos**

El uso de recursos mide la eficiencia con que los servidores utilizan su capacidad de procesamiento, memoria y almacenamiento. Según Serrano et al. (2021), el monitoreo proactivo del uso de recursos es esencial para identificar cuellos de botella y evitar sobrecargas en los servidores. Por su parte, Ahmad et al. (2020) señalan que una gestión eficiente de los recursos garantiza que las aplicaciones críticas estén siempre disponibles para los usuarios.

- **Temperatura de CPU**

La temperatura de la CPU es un indicador clave del estado de los servidores, ya que niveles excesivos pueden provocar fallas en el hardware y afectar la continuidad del servicio. Para Serrano et al. (2021) explican que el monitoreo constante es importante para prevenir sobrecalentamientos y garantizar el rendimiento óptimo del sistema. Por otro lado, González et al. (2021) destacan que una temperatura elevada puede ser resultado de una ventilación insuficiente o una carga excesiva de trabajo en el servidor.

3.3. Definición de términos

3.3.1. Monitoreo

Proceso de recolección y análisis de datos para evaluar el desempeño de las áreas de una empresa y tomar decisiones informadas (Corado, 2022).

3.3.2. Monitoreo activo

Introducción de paquetes de prueba en la red para medir tiempos de respuesta y rendimiento, agregando tráfico adicional (Junco y Rabelo, 2018).

3.3.3. Monitoreo pasivo

Recolección y análisis del tráfico de red existente sin introducir tráfico adicional, utilizando herramientas como SNMP y NetFlow (Junco y Rabelo, 2018).

3.3.4. Servidor de monitoreo

Plataforma dedicada a supervisar y analizar el estado y rendimiento de componentes de la red, proporcionando alertas y generando informes (Oppenheimer, 2010).

3.3.5. Nagios

Herramienta de monitoreo de sistemas y redes que permite la supervisión continua de dispositivos y servicios, alertando sobre problemas. Nagios ofrece notificaciones en tiempo real, lo que permite a los administradores de sistemas tomar medidas correctivas de manera rápida. Además, proporciona informes detallados sobre el rendimiento y la disponibilidad, ayudando a mantener la infraestructura tecnológica en óptimas condiciones (Nagios Enterprises, s.f.).

3.3.6. Cacti

Plataforma de monitoreo de red que utiliza Round-Robin Database Tool (RRDTool) para almacenar datos de rendimiento y generar gráficos, ideal para visualizar y detectar tendencias en la red (Cacti.net, s.f.).

3.3.7. Eficiencia operativa

Proceso de maximización de la efectividad de los recursos tecnológicos para mejorar la toma de decisiones, reducir desperdicios y optimizar procesos clave dentro de una organización (Seun et al., 2023).

3.3.8. Infraestructura TI

Se refiere al conjunto de servicios tecnológicos que sustentan las operaciones dentro de una organización, incluyendo la creación, mantenimiento y soporte de aplicaciones, así como el apoyo a la infraestructura tecnológica. En este contexto, la gestión de servicios de TI (ITSM, por sus siglas en inglés) busca alinear las necesidades empresariales con las capacidades del departamento de TI para garantizar la eficiencia, eficacia y calidad de los servicios proporcionado (Gunawan et al. 2024).

IV. Metodología

4.1. Tipo y nivel de investigación

4.1.1. Tipo de investigación

La presente investigación fue de tipo aplicada. De acuerdo con Lozada (2014) “las investigaciones aplicadas buscan originar nuevo conocimiento con la aplicación de manera directa a aquellas problemáticas referentes al área productiva o también a la sociedad en general”. El estudio se consideró de tipo aplicada porque su propósito principal fue implementar un servidor de monitoreo para optimizar los servicios TI en la empresa EGEMSA, alineándose con el objetivo general de ofrecer una solución práctica y funcional a un problema específico de la organización

4.1.2. Nivel de investigación

Esta investigación fue de nivel causal. Según Hernández y Mendoza (2018), este se centró en establecer las causas y efectos de los fenómenos estudiados, identificando relaciones causales entre las variables. Este nivel busca no solo describir o correlacionar variables, sino también entender y explicar por qué y cómo ocurren los eventos.

4.1.3. Diseño de investigación

El método usado fue experimental bajo un diseño pre-experimental con un solo grupo empleando la técnica de la observación, según Hernández y Mendoza (2018), es una metodología de investigación en la cual se manipula al menos una variable para observar su efecto en una o más variables dependientes, sin la utilización de un grupo de control, siendo útil para obtener una primera aproximación a la relación entre variables.

En la implementación del servidor de monitoreo en EGEMSA, se empleó un diseño pre-experimental para evaluar los efectos de esta implementación en los servicios TI. Se utilizó la técnica de observación directa como método principal, y se aplicaron instrumentos como la ficha de observación, destinada a registrar datos de la variable dependiente

(servicios TI) mediante un pretest y un postest, permitiendo comparar los resultados antes y después del monitoreo; y la ficha de registro, enfocada en verificar que la implementación del sistema de monitoreo se haya llevado a cabo de manera correcta. Este enfoque garantiza un análisis objetivo y confiable de los cambios observados tras la implementación.

Diseño pre-experimental:

$$O1 – X – O2$$

Donde:

O1 = Pretest

X = Implementación del servidor de monitoreo

O2 = Postest

4.2. Ámbito temporal y espacial

El ámbito temporal de la investigación comprende el periodo desarrollado entre los meses de agosto de 2025 y octubre de 2025, etapa en la cual se efectuó el diagnóstico inicial de los servicios TI, la implementación del servidor de monitoreo y la recolección de datos correspondientes al pretest y postest.

En cuanto al ámbito espacial, el estudio se llevó a cabo en la empresa EGEMSA S.A., ubicada en la ciudad del Cusco. La investigación se desarrolló específicamente en el área de TI.

4.3. Población y muestra

Según Hernández y Mendoza (2018), la población se define como el conjunto total de elementos que comparten ciertas características y sobre los cuales se desea hacer inferencias. Por consiguiente, el estudio no consideró una muestra ya que el total de la población es accesible y estuvo compuesta por la infraestructura de TI de la empresa EGEMSA Cusco como se describe a continuación:

Tabla 3

Población accesible

Infraestructura tecnológica	**Cantidad**
SW	25
SW CORE	2
SVR FÍSICO	5
SVR VIRTUALIZADOS	20
Soluciones tecnológicas de EGEMSA	**Cantidad**
Almacenamiento	2
Servicio tecnológico	3

La unidad de análisis estadístico estuvo conformada por los eventos o incidentes registrados por el sistema de monitoreo durante los periodos de evaluación pretest y postest. Cada evento constituyó una observación independiente, asociada a condiciones operativas específicas de la infraestructura tecnológica. En este contexto, los dispositivos de red, servidores, sistemas de almacenamiento y servicios tecnológicos representaron el entorno de observación sobre el cual se generaron los registros.

4.4. Instrumentos

Según Hernández y Mendoza (2018), una técnica de investigación es el conjunto de procedimientos y métodos que se emplean para recolectar datos necesarios para un estudio.

La técnica utilizada en este estudio fue la observación. Esta técnica permitió recopilar datos directos sobre el uso y rendimiento de los servicios TI, así como sobre la interacción de los usuarios con estos servicios antes y después de la implementación del servidor de monitoreo, permitiendo una evaluación precisa de los cambios.

El instrumento utilizado fue la ficha de observación, el cual se utilizó para registrar de manera sistemática y estructurada las observaciones realizadas. Este instrumento incluyó una lista de indicadores y criterios específicos relacionados con los servicios TI. La ficha de

observación permitió una evaluación objetiva y consistente de los datos observados, facilitando la comparación antes y después de la implementación del servidor de monitoreo. Así mismo, se empleó la ficha de registro, la cual se empleó para verificar de manera estructurada el cumplimiento del sistema de monitoreo, asegurando una implementación precisa y consistente.

Para garantizar la validez de los instrumentos de recolección de datos en esta investigación, se llevó a cabo una validación mediante juicio de expertos. La validación por juicio de expertos implicó la revisión de los instrumentos por especialistas en tecnologías de la información, quienes evaluaron su pertinencia y capacidad para medir las variables del estudio (Anexo D).

4.5. Procedimientos

El desarrollo de la presente investigación se llevó a cabo siguiendo una secuencia metodológica organizada en varias etapas. En primer lugar, se realizó un diagnóstico descriptivo de los servicios TI de la empresa EGEMSA S.A., identificando las principales limitaciones operativas, los incidentes recurrentes y la ausencia de un sistema automatizado de monitoreo. Posteriormente, se procedió a definir los instrumentos de recolección de datos, los cuales incluyeron fichas de observación estructuradas para registrar tiempos de respuesta, disponibilidad del servicio, rendimiento de la red y desempeño del servidor antes de la implementación del sistema.

Luego, se ejecutó la medición pretest, recopilando información durante un periodo establecido para obtener una línea base representativa del funcionamiento real de la infraestructura TI sin herramientas de monitoreo, para finalizar este proceso, se implementó el servidor de monitoreo, configurando sus componentes principales (Zabbix, Docker, Grafana, agentes de supervisión y reglas de alerta) y documentando el proceso técnico correspondiente.

Una vez operativo el servidor, se desarrolló la fase postest, en la cual se registraron nuevamente los indicadores de desempeño utilizando los mismos instrumentos aplicados en el pretest. Es así que, esta etapa permitió evaluar el comportamiento de los servicios TI bajo un esquema de supervisión automatizada. Finalmente, se procedió a ordenar, tabular y validar la información recolectada, resguardando la coherencia entre los instrumentos aplicados y la matriz de operacionalización de variables. Por ello, los procedimientos permitieron comparar ambos periodos y determinar el impacto del servidor de monitoreo en los servicios TI de la empresa.

4.6. Análisis de datos

Para el análisis de los datos obtenidos se siguió un proceso estadístico estructurado. En una primera etapa, se efectuó un análisis descriptivo, mediante el cual se determinaron frecuencias, porcentajes y medidas de tendencia central correspondientes a las variables evaluadas tanto en el pretest como en el postest. Esto permitió identificar patrones y comportamientos iniciales en los tiempos de respuesta, la disponibilidad de los servicios, el rendimiento de la red y la carga del servidor.

Posteriormente, debido a la naturaleza no paramétrica de los datos y al carácter pre-experimental del diseño, se aplicó la prueba U de Mann–Whitney, utilizada para comparar las diferencias entre los valores del pretest y postest en cada una de las dimensiones e indicadores. Esta prueba permitió determinar si las mejoras observadas tras la implementación del servidor de monitoreo eran estadísticamente significativas. El análisis se efectuó con un nivel de significancia del 5 % ($\alpha = 0.05$), estableciendo como criterio que valores de $p < 0.05$ indican diferencias significativas entre ambos periodos.

El procesamiento de los datos se llevó a cabo utilizando herramientas informáticas como Microsoft Excel y SPSS, permitiendo realizar la tabulación, el cálculo de los estadísticos y la representación gráfica de los resultados. Finalmente, los hallazgos fueron

interpretados y contrastados con las hipótesis planteadas, lo que permitió determinar el efecto del servidor de monitoreo sobre los servicios TI evaluados.

V. Resultados y discusión

5.1. Resultados

5.1.1. Implementación del servidor de monitoreo

La implementación del servidor de monitoreo se desarrolló sobre una arquitectura basada en Ubuntu Server, utilizando Docker como plataforma para desplegar los servicios principales, entre ellos Zabbix Server, Zabbix Agent, MySQL y Grafana. Esta infraestructura permitió asegurar un entorno estable y fácilmente escalable, durante el proceso de implementación se configuraron políticas técnicas de acuerdo con las recomendaciones de los fabricantes y guías de seguridad como CIS Benchmarks; asimismo, se habilitaron mecanismos de observabilidad mediante agentes SNMP y métricas internas del sistema operativo. A su vez, se aplicaron medidas de hardening tales como el ajuste del firewall UFW, la restricción de puertos, la protección de SSH y auditorías periódicas con herramientas como Lynis y RKHunter. Por consiguiente, la integración de Zabbix y Grafana permitió consolidar un entorno de monitoreo en tiempo real, facilitando la supervisión de servicios esenciales, dispositivos de red, servidores físicos y virtuales, así como el análisis de rendimiento del sistema. Todo este proceso quedó documentado mediante fichas de registro diarias, lo que permitió evaluar el comportamiento y la estabilidad del servidor.

Tabla 4

Caracterización de la intervención: implementación del servidor de monitoreo

Elemento	Descripción
Variable independiente	Implementación del servidor de monitoreo
Naturaleza metodológica	Intervención o tratamiento técnico aplicado sobre la infraestructura TI de la empresa EGEMSA S.A. Cusco en un diseño preexperimental de pretest y postest en un solo grupo.
Condición de análisis	Pretest = sin implementación del servidor de monitoreo; Postest = con implementación del servidor de monitoreo.
Componentes de ejecución de la intervención	Configuración inicial, cobertura de supervisión, rendimiento operativo y seguridad operativa.
Medios de verificación	Fichas de registro, reportes de Zabbix, Grafana, Docker, Lynis, RKHunter y evidencias técnicas de implementación.
Propósito de la intervención	Optimizar los servicios TI mediante supervisión continua, detección oportuna de incidentes y mejora en la gestión operativa de la infraestructura tecnológica.

Tabla 5

Características técnicas de la intervención según indicadores

Características técnicas de la solución implementada	Indicadores	Escala de medición
Configuración inicial	Cumplimiento de guías y estándares de fabricantes Hardening aplicado (seguridad básica configurada)	De razón
Cobertura de supervisión	Cantidad de dispositivos supervisados por el servidor Cantidad de servicios críticos supervisados por el servidor	De razón
Rendimiento operativo	Tiempo operación ininterrumpida del servidor (uptime) Uso de recursos promedio bajo carga del servidor	De razón
Seguridad Operativa	Actualización de parches de seguridad Configuración de acceso seguro (firewall y usuarios) Análisis de vulnerabilidades	De razón

5.1.1.1. Configuración inicial del servidor de monitoreo implementado

Tabla 6

Indicador cumplimiento de guías y estándares de fabricantes

Día	% Cumplimiento	Nivel de desempeño	Observación técnica
10/01/2025	84	Alto	Revisión inicial de políticas Docker y Zabbix completada.
10/02/2025	85	Alto	Validación de configuración de red del servidor.
10/03/2025	86	Alto	Ajuste de parámetros en zabbix_agentd.conf.
10/04/2025	85	Alto	Aplicación parcial de guías CIS en Ubuntu Server.
10/05/2025	87	Alto	Comprobación del cumplimiento de políticas de contraseñas.
10/06/2025	88	Alto	Corrección en permisos de acceso SSH y logs.
10/07/2025	86	Alto	Auditoría de estándares Docker Bench Security.
10/08/2025	85	Alto	Ajuste de métricas SNMP en Zabbix.
10/09/2025	84	Alto	Validación manual de reglas de configuración.
10/10/2025	86	Alto	Verificación final de estándares técnicos.

El análisis del cumplimiento de guías y estándares técnicos muestra que el servidor de monitoreo mantuvo un desempeño alto durante todo el periodo evaluado, con valores que oscilaron entre 84 % y 88 %, ubicándose cada día dentro del nivel de desempeño “Alto”. Estos resultados evidencian que las configuraciones iniciales del entorno Zabbix–Docker–Ubuntu Server fueron aplicadas de manera correcta y bajo criterios técnicos adecuados. Las observaciones registradas reflejan una ejecución continua de actividades clave, como la verificación de la configuración de red, el ajuste de parámetros del agente Zabbix, la aplicación parcial de guías CIS, la validación de políticas de contraseñas y la corrección de permisos SSH, lo cual indica un proceso de configuración estable y progresivo. Asimismo, la inclusión de auditorías como Docker Bench Security y revisiones manuales de reglas de configuración mejora la consistencia de las buenas prácticas implementadas.

Tabla 7

Indicador hardening aplicado

Día	% Cumplimiento	Nivel de desempeño	Observación técnica
10/01/2025	68	Medio	Ejecución inicial de auditoría con Lynis.
10/02/2025	70	Medio	Actualización de paquetes y desactivación de servicios no esenciales.
10/03/2025	72	Medio	Configuración de fail2ban y revisión de puertos abiertos.
10/04/2025	71	Medio	Restricción de permisos de usuario root.
10/05/2025	70	Medio	Evaluación de logs de seguridad en /var/log/auth.log.
10/06/2025	73	Medio	Ajuste de política de contraseñas en PAM.
10/07/2025	74	Medio	Aplicación de reglas UFW más restrictivas.
10/08/2025	71	Medio	Auditoría automática parcial con RKHunter.
10/09/2025	72	Medio	Eliminación de servicios innecesarios.
10/10/2025	73	Medio	Revisión de permisos y usuarios del sistema.

El análisis del indicador referido al hardening del servidor muestra un cumplimiento promedio de 71.4 %, correspondiente a un nivel de desempeño Medio, lo que indica que, si bien se aplicaron medidas de seguridad esenciales, aún existen aspectos que necesitan un fortalecimiento para alcanzar un nivel óptimo de protección, los registros muestran que durante el periodo evaluado se ejecutaron acciones fundamentales, como auditorías iniciales con Lynis, actualización de paquetes, desactivación de servicios innecesarios, configuración de fail2ban, revisión de puertos abiertos, aplicación de reglas UFW más restrictivas y auditorías parciales con RKHunter. Estas actividades evidencian un proceso de mejora de la seguridad del sistema. No obstante, el rango de cumplimiento entre 68 % y 74 % refleja que varias de las prácticas implementadas aún no alcanzan un nivel avanzado, especialmente en lo relacionado con la automatización del monitoreo de vulnerabilidades, el endurecimiento completo de permisos, la gestión avanzada de usuarios o la adopción total de estándares CIS.

5.1.1.2. Cobertura de supervisión del servidor de monitoreo implementado

Tabla 8

Indicador dispositivos monitoreados

Día	% Dispositivos supervisados	Nivel	Observación técnica
10/01/2025	98	Óptimo	Todos los hosts principales activos.
10/02/2025	99	Óptimo	Validación de agentes en servidores físicos.
10/03/2025	100	Óptimo	Sin pérdida de conectividad entre nodos.
10/04/2025	100	Óptimo	Sin alertas por latencia.
10/05/2025	100	Óptimo	Supervisión estable en Zabbix dashboard.
10/06/2025	100	Óptimo	Integración completa de agentes SNMP.
10/07/2025	100	Óptimo	Todos los equipos reportando métricas.
10/08/2025	100	Óptimo	Sin errores en consulta de métricas.
10/09/2025	99	Óptimo	Revisión de reconexión de un host.
10/10/2025	100	Óptimo	Supervisión completa operativa.

El indicador correspondiente a la supervisión de dispositivos muestra un desempeño sobresaliente, con un promedio de 99.6 %, clasificado en el nivel Óptimo, lo que evidencia que prácticamente la totalidad de los equipos previstos fueron monitoreados de manera continua durante el periodo evaluado. Los registros diarios confirman que los agentes instalados en los servidores físicos y virtuales operaron correctamente, permitiendo la recolección estable de métricas y la integración completa de los dispositivos mediante SNMP. Asimismo, no se identificaron pérdidas de conectividad entre nodos ni errores en la consulta de métricas, lo cual refleja una infraestructura robusta y correctamente enlazada al sistema de monitoreo. Incluso en los días donde el porcentaje se redujo levemente a 98 % y 99 %, las observaciones técnicas señalan que estos valores estuvieron asociados únicamente a procesos de reconexión puntual de un host, sin afectar la continuidad del servicio.

Tabla 9

Indicador servicios supervisados

Día	% Servicios supervisados	Nivel	Observación técnica
10/01/2025	88	Alto	Verificación de monitoreo HTTP/SMTP.
10/02/2025	89	Alto	Configuración de alertas para base de datos.
10/03/2025	91	Alto	Supervisión activa de contenedores Docker.
10/04/2025	90	Alto	Alerta resuelta en servicio web secundario.
10/05/2025	92	Alto	Integración de métricas de rendimiento de CPU.
10/06/2025	91	Alto	Supervisión de servicios críticos completa.
10/07/2025	90	Alto	Registro de disponibilidad en Grafana actualizado.
10/08/2025	92	Alto	Alertas procesadas automáticamente.
10/09/2025	91	Alto	Mantenimiento de plantilla SNMP.
10/10/2025	90	Alto	Revisión final de servicios monitoreados.

El indicador referente a la supervisión de servicios muestra un desempeño consistentemente alto, con valores que se sitúan entre el 88 % y el 92 %, manteniéndose durante todo el periodo evaluado en el nivel de desempeño Alto, estos resultados evidencian que el servidor de monitoreo logró supervisar de manera estable la mayoría de los servicios críticos de la infraestructura tecnológica, también, las observaciones técnicas registradas indican que se evidenció correctamente el monitoreo de protocolos esenciales como HTTP y SMTP, se configuraron alertas para servicios de base de datos y se mantuvo una supervisión activa de contenedores Docker. Asimismo, la integración de métricas de rendimiento de CPU, el registro actualizado de disponibilidad en Grafana y el procesamiento automático de alertas reflejan un sistema maduro en términos de observabilidad, aunque el indicador no alcanzó el nivel Óptimo, los rangos obtenidos muestran un funcionamiento

adecuado y sin interrupciones relevantes, lo que permite concluir que el servidor garantiza una supervisión fiable de los servicios críticos, contribuyendo a la continuidad operacional.

5.1.1.3. Rendimiento operativo del servidor de monitoreo implementado

Tabla 10

Indicador uptime del contenedor Docker

Día	% Uptime	Nivel	Observación técnica
10/01/2025	99.3	Óptimo	Sin reinicios en contenedores.
10/02/2025	99.5	Óptimo	Uptime continuo en Zabbix container.
10/03/2025	99.4	Óptimo	Docker service operativo sin fallas.
10/04/2025	99.6	Óptimo	Sin interrupciones registradas.
10/05/2025	99.7	Óptimo	Monitoreo estable en todos los contenedores.
10/06/2025	99.5	Óptimo	Contenedor Zabbix operativo al 100 %.
10/07/2025	99.4	Óptimo	Pequeña latencia de red corregida.
10/08/2025	99.6	Óptimo	Operación ininterrumpida.
10/09/2025	99.5	Óptimo	Sin eventos de reinicio.
10/10/2025	99.5	Óptimo	Uptime constante verificado.

El análisis del uptime del contenedor Docker evidencia un desempeño altamente estable, con un promedio de 99.5 %, clasificado dentro del nivel Óptimo, lo que demuestra que el servidor de monitoreo operó de manera prácticamente ininterrumpida durante todo el periodo evaluado, también, los registros diarios indican que no se presentaron reinicios inesperados en los contenedores, y que tanto el servicio Docker como el contenedor de Zabbix funcionaron sin fallas significativas, incluso los días en los que se reportaron pequeñas incidencias, como una leve latencia de red, estas fueron corregidas oportunamente sin afectar la continuidad del servicio y la ausencia de interrupciones, la verificación

constante del estado de los contenedores y la operación estable reflejan un entorno bien configurado y con recursos adecuados para mantener la disponibilidad del sistema.

Tabla 11

Indicador uso de recursos promedio

Día	% Utilización promedio	Nivel	Observación técnica
10/01/2025	94	Alto	CPU al 40 %, RAM al 45 %, Disco al 50 %.
10/02/2025	96	Óptimo	Equilibrio entre recursos bajo carga.
10/03/2025	95	Óptimo	CPU estable, sin sobreuso de RAM.
10/04/2025	94	Alto	Incremento leve en disco (55 %).
10/05/2025	97	Óptimo	Buen rendimiento global.
10/06/2025	96	Óptimo	Métricas estables en Grafana.
10/07/2025	95	Óptimo	CPU promedio de 35 %, memoria 42 %.
10/08/2025	94	Alto	Leve pico en almacenamiento temporal.
10/09/2025	96	Óptimo	Sistema balanceado.
10/10/2025	95	Óptimo	Desempeño continuo sin alertas.

El indicador de uso de recursos promedio evidencia un desempeño eficiente del servidor de monitoreo, alcanzando un promedio de 95.2 %, clasificado en el nivel Óptimo, lo que refleja una adecuada administración de CPU, memoria RAM y almacenamiento durante el periodo evaluado y las observaciones técnicas muestran que el sistema mantuvo valores estables, con promedios de uso de CPU entre 35 % y 40 %, memoria entre 42 % y 45 %, y almacenamiento entre 50 % y 55 %, cifras que se encuentran dentro de los rangos recomendados para entornos de monitoreo basados en contenedores, incluso en los días donde se evidenciaron ligeros incrementos en el uso de disco o picos temporales en el

almacenamiento, estos no representaron riesgos operativos ni generaron alertas de saturación.

5.1.1.4. Seguridad operativa del servidor de monitoreo implementado

Tabla 12

Indicador Aplicación de actualizaciones, firewall y auditorías

Día	% Cumplimiento	Nivel	Observación técnica
10/01/2025	95	Alto	Aplicación de parches semanales.
10/02/2025	96	Óptimo	Verificación de unattended-upgrades.
10/03/2025	97	Óptimo	Auditoría automática Lynis ejecutada.
10/04/2025	96	Óptimo	Actualización de firmas RKHunter.
10/05/2025	95	Alto	Revisión manual de firewall UFW.
10/06/2025	97	Óptimo	SSH endurecido, sin accesos externos.
10/07/2025	98	Óptimo	Monitoreo de puertos activo.
10/08/2025	96	Óptimo	Validación de logs de seguridad.
10/09/2025	95	Alto	Tareas cron verificadas.
10/10/2025	97	Óptimo	Auditoría mensual completada.

El indicador relacionado con la aplicación de actualizaciones, la gestión del firewall y la ejecución de auditorías refleja un desempeño altamente consistente, alcanzando un promedio de 96.2 %, lo que lo ubica dentro del nivel Óptimo. Los resultados indican actividades fundamentales para garantizar la seguridad operativa del servidor, como la aplicación regular de parches, la verificación del servicio unattended-upgrades, la ejecución de auditorías automáticas con Lynis y la actualización de firmas de RKHunter. Del mismo modo, se llevaron a cabo revisiones manuales del firewall UFW, se reforzó la seguridad del servicio SSH evitando accesos externos, y se mantuvo un monitoreo activo de puertos y de logs de seguridad, las tareas fueron verificadas y se completó la auditoría correspondiente, lo que demuestra un control constante de los procesos internos del sistema.

5.1.1.5. Indicadores del servidor de monitoreo implementado

Tabla 13

Síntesis general del servidor de monitoreo

Características técnicas de la solución implementada	**Indicador**	**Promedio (%)**	**Nivel de desempeño**
Configuración inicial	Hardening aplicado	71.4	Alto
Cobertura de supervisión	Dispositivos monitoreados	99.6	Medio
	Servicios supervisados	90.4	Óptimo
Rendimiento operativo	Uptime del contenedor Docker	99.5	Alto
	Uso de recursos promedio	95.2	Óptimo
Seguridad operativa	Actualizaciones, firewall y auditorías	96.2	Óptimo
Promedio total		**92.05**	**Óptimo**

La tabla presenta la síntesis general de los indicadores técnicos del servidor de monitoreo implementado, consolidando los resultados obtenidos durante el periodo de evaluación postest, en cuanto a la configuración inicial el hardening aplicado alcanzó un promedio de 71.4% clasificado en un nivel alto, lo que refleja una aplicación sólida de medidas de seguridad base, aunque con margen de mejora en controles más avanzados. Respecto a la cobertura de supervisión la cantidad de dispositivos monitoreados obtuvo un promedio de 99.6% con nivel medio, mientras que los servicios supervisados alcanzaron el 90.4% con nivel óptimo evidenciando una cobertura prácticamente total de la infraestructura TI. En el rendimiento operativo el uptime del contenedor Docker registró un 99.5% en nivel alto, demostrando una operación casi ininterrumpida del servidor, en tanto que el uso de recursos promedio fue de 95.2% con nivel óptimo, lo cual indica una utilización eficiente de

los recursos de cómputo disponibles. Finalmente, la seguridad operativa, que integra actualizaciones, configuración de firewall y auditorías periódicas, obtuvo un 96.2% con nivel óptimo, confirmando una gestión robusta de los riesgos operativos. En conjunto, el promedio total de 92.05% con nivel óptimo evidencia que la implementación del servidor de monitoreo cumplió satisfactoriamente con los criterios técnicos establecidos, consolidando una infraestructura de supervisión estable, segura y funcional para la empresa EGEMSA S.A. Cusco.

5.1.2. Análisis descriptivo de la variable servicios TI

5.1.2.1. Dimensión eficiencia operativa

Tabla 14

Resultados pretest de la dimensión eficiencia operativa según fuente de detección

Tiempo de respuesta	Detección manual (TI)		Detección manual por personal TI		Detección manual por técnico		Reporte de usuario		Total	
	f	%	*f*	%	*f*	%	*f*	%	*f*	%
1:10:00	0	0.0%	0	0.0%	1	3.0%	0	0.0%	1	3.0%
1:20:00	1	3.0%	0	0.0%	0	0.0%	2	6.1%	3	9.1%
1:25:00	0	0.0%	1	3.0%	1	3.0%	1	3.0%	3	9.1%
1:30:00	1	3.0%	0	0.0%	1	3.0%	4	12.1%	6	18.2%
1:35:00	0	0.0%	0	0.0%	0	0.0%	1	3.0%	1	3.0%
1:40:00	1	3.0%	0	0.0%	1	3.0%	5	15.2%	7	21.2%
1:45:00	0	0.0%	0	0.0%	1	3.0%	2	6.1%	3	9.1%
1:50:00	0	0.0%	1	3.0%	0	0.0%	2	6.1%	3	9.1%
1:55:00	0	0.0%	0	0.0%	1	3.0%	1	3.0%	2	6.1%
2:00:00	0	0.0%	0	0.0%	0	0.0%	1	3.0%	1	3.0%
2:10:00	0	0.0%	0	0.0%	0	0.0%	1	3.0%	1	3.0%
2:20:00	0	0.0%	0	0.0%	0	0.0%	2	6.1%	2	6.1%
Total	**3**	**9.1%**	**2**	**6.1%**	**6**	**18.2%**	**22**	**66.7%**	**33**	**100.0%**

Análisis e interpretación:

Los resultados del pretest evidencian que, antes de la implementación del servidor de monitoreo, la eficiencia operativa de los servicios TI era limitada y dependía en gran medida del reporte del usuario, que representó el 66.7 % de las detecciones, así, el tiempo de respuesta se concentra entre 1:30:00 y 1:40:00 horas, reflejando procesos de atención prolongados. Esta situación se confirma con incidentes significativos registrados durante el periodo, como la caída temporal del servidor de correo, fallos en la carga de archivos del sistema, la congestión de red en el enlace principal, reinicios inesperados del servidor de autenticación y errores en la conexión a la base de datos, todos ellos con tiempos de resolución que alcanzaron entre 1:40:00 y 2:20:00 horas.

Incluso problemas frecuentes como la lentitud general del sistema, la interrupción en el acceso a sistemas institucionales y fallos de impresión en red superaron en varios casos las 1:50:00 horas. La detección manual por el personal TI o técnicos fue minoritaria, representando solo el 33.3 % de los casos, lo que evidencia la ausencia de herramientas que permiten una supervisión interna continua. Se concluye que, estos resultados muestran que, en la etapa previa, la organización operaba bajo un modelo reactivo, con limitada capacidad de detección temprana y tiempos prolongados para la resolución de incidentes.

Tabla 15

Resultados postest de la dimensión eficiencia operativa según fuente de detección

Tiempo de respuesta	**Alerta del sistema de monitoreo**		**Supervisión directa (TI)**		**Total**	
	f	**%**	***f***	**%**	***f***	**%**
0:10:00	3	8.6%	0	0.0%	3	8.6%
0:15:00	17	48.6%	4	11.4%	21	60.0%
0:20:00	9	25.7%	2	5.7%	11	31.4%
Total	**29**	**82.9%**	**6**	**17.1%**	**35**	**100.0%**

Análisis e interpretación:

Los resultados del postest evidencian una mejora notable en la eficiencia operativa, ya que el 82.9 % de los incidentes fueron detectados por el sistema de monitoreo, lo que demuestra una transición hacia un proceso de detección automática y proactiva. Asimismo, los tiempos de respuesta muestran una reducción significativa, concentrándose principalmente en el intervalo de 0:15:00 minutos, que representa el 60.0 % de los casos atendidos. También se registraron tiempos aún más breves, como 0:10:00 minutos, lo que refuerza la capacidad del sistema para agilizar la atención y la supervisión directa del personal de TI representa solo el 17.1 % de las detecciones, lo cual indica que la dependencia del monitoreo manual disminuyó considerablemente. Por consiguiente, estos resultados reflejan que, tras la implementación del servidor de monitoreo, la empresa alcanzó una respuesta más rápida y eficiente frente a los incidentes, logrando una detección temprana y una atención más oportuna.

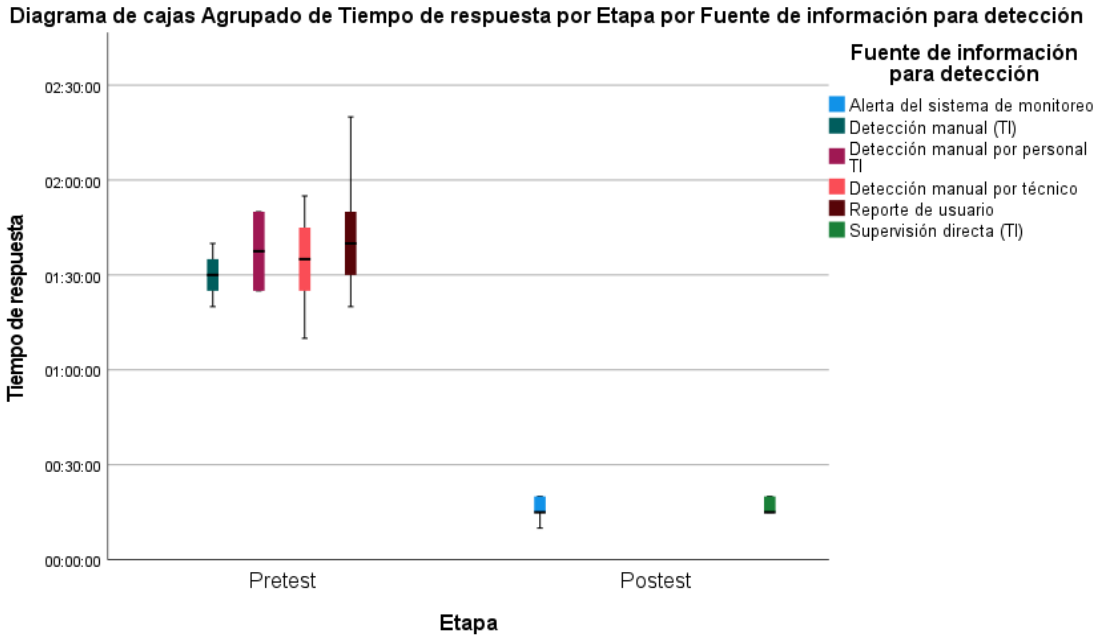
Tabla 16

Resultados pretest y postest de la dimensión eficiencia operativa según fuente de detección

		Tiempo de respuesta	**Media**
Pretest	Fuente de información para detección	Detección manual (TI)	01:30:00
		Detección manual por personal TI	01:37:30
		Detección manual por técnico	01:34:10
		Reporte de usuario	01:43:24
		Media	**01:40:09**
Postest	Fuente de información para detección	Alerta del sistema de monitoreo	00:16:02
		Supervisión directa (TI)	00:16:40
		Media	**00:16:08**

Figura 1

Resultados pretest y postest de la dimensión eficiencia operativa según fuente de



detección

Análisis e interpretación:

La comparación entre los resultados del pretest y postest muestra una mejora sustancial en la eficiencia operativa de los servicios TI. En el pretest, los tiempos de respuesta eran considerablemente altos, con un promedio general de 01:40:09 horas, y con detecciones que dependían mayoritariamente del reporte del usuario, alcanzando tiempos de hasta 01:43:24 horas. Además, las detecciones manuales realizadas por el personal de TI y técnicos también mostraban tiempos prolongados, superiores a 01:30:00 horas, lo que indica un proceso poco eficiente. En contraste, en el postest, tras la implementación del servidor de monitoreo, los tiempos de respuesta disminuyeron drásticamente a un promedio general de 00:16:08 minutos, siendo la mayoría de los incidentes detectados automáticamente por las alertas del sistema en solo 00:16:02 minutos. Esta disminución evidencia que la detección temprana y automatizada permite iniciar la atención de manera inmediata, reduciendo significativamente los retrasos operativos. En síntesis, los resultados confirman que el

sistema de monitoreo tuvo un impacto positivo directo en la eficiencia operativa, mejorando tanto la capacidad de detección como la velocidad de respuesta ante incidentes.

5.1.2.2. Dimensión disponibilidad del servicio

Tabla 17

Resultados pretest de la dimensión disponibilidad del servicio según fuente de detección

Tiempo de respuesta	Detección manual por técnico		Reporte de usuario		Supervisión directa (TI)		Total	
	f	%	*f*	%	*f*	%	*f*	%
1:15:00	0	0.0%	1	4.0%	0	0.0%	1	4.0%
1:25:00	0	0.0%	1	4.0%	0	0.0%	1	4.0%
1:30:00	0	0.0%	4	16.0%	0	0.0%	4	16.0%
1:35:00	0	0.0%	3	12.0%	0	0.0%	3	12.0%
1:40:00	1	4.0%	3	12.0%	0	0.0%	4	16.0%
1:45:00	1	4.0%	1	4.0%	0	0.0%	2	8.0%
1:50:00	1	4.0%	4	16.0%	0	0.0%	5	20.0%
1:55:00	0	0.0%	2	8.0%	1	4.0%	3	12.0%
2:20:00	1	4.0%	0	0.0%	1	4.0%	2	8.0%
Total	**4**	**16.0%**	**19**	**76.0%**	**2**	**8.0%**	**25**	**100.0%**

Análisis e interpretación:

La tabla muestra que, antes de la implementación del servidor de monitoreo, los tiempos de respuesta asociados a la recuperación de servicios críticos presentaban una tendencia a superar la hora y media. El rango de 1:50:00 fue la hora más frecuente, concentrando el 20.0% de los incidentes, seguido de tiempos de 1:40:00 y 1:30:00 con un 16.0% cada uno. Asimismo, el 76.0% de los eventos fue detectado por reporte de usuario,

mientras que solo el 16.0% y el 8.0% fueron identificados mediante detección manual por técnico y supervisión directa del área TI, respectivamente.

Los tiempos observados en la tabla son consistentes con incidentes relevantes ocurridos durante el periodo evaluado, donde servicios esenciales como Internet institucional, correo corporativo, intranet, VPN y sistemas administrativos presentaron interrupciones prolongadas, en muchos de estos casos, las afectaciones incluyeron caídas completas de servicios clave, por ejemplo, fallas en el servidor de archivos, la plataforma de videoconferencia o la aplicación web de matrícula, llegando algunos a superar las dos horas de inactividad. Por ello, la recurrencia de incidentes de lentitud, interrupción o caída total evidencia que la infraestructura carecía de mecanismos automáticos de alerta capaces de detectar y reportar anomalías en tiempo real. Asimismo, se observa que la mayoría de los eventos fueron identificados únicamente cuando los usuarios reportaron la interrupción, lo que generó demoras adicionales entre el inicio del incidente y el inicio de la atención.

Tabla 18

Resultados postest de la dimensión disponibilidad del servicio según fuente de detección

Tiempo de respuesta	Alerta del sistema de monitoreo		Supervisión directa (TI)		Total	
	f	%	*f*	%	*f*	%
0:15:00	20	58.8%	8	23.5%	28	82.4%
0:20:00	1	2.9%	0	0.0%	1	2.9%
0:25:00	1	2.9%	1	2.9%	2	5.9%
0:35:00	3	8.8%	0	0.0%	3	8.8%
Total	**25**	**73.5%**	**9**	**26.5%**	**34**	**100.0%**

Análisis e interpretación:

Los resultados de la tabla muestran que, tras la implementación del servidor de monitoreo, la disponibilidad del servicio experimentó una mejora sustancial, especialmente en lo referente a los tiempos de respuesta ante interrupciones. El 82.4% de los incidentes fueron atendidos en un máximo de 15 minutos, lo cual constituye el rango más representativo del periodo evaluado. Adicionalmente, el 73.5% de los eventos fue detectado directamente mediante alertas del sistema de monitoreo, mientras que el 26.5% restante requirió supervisión directa del personal TI. También se registraron tiempos aislados de atención de 20, 25 y 35 minutos, aunque con frecuencias bajas (entre 2.9% y 8.8%). En síntesis, los datos reflejan un esquema de recuperación ágil y predominantemente automatizado.

Durante este periodo, se identificaron incidentes relevantes que afectaron servicios clave como Internet institucional, correo corporativo, sistemas contables, autenticación de dominio, servidores de archivos, NAS, intranet corporativa, Wi-Fi administrativo y aplicaciones web internas. A diferencia de la etapa previa, donde los tiempos de atención

superaban habitualmente la hora y media, la mayoría de estos incidentes fueron resueltos en apenas 15 minutos, incluso cuando se trataba de servicios de alta criticidad.

La mayoría de las alertas automatizadas revela que el servidor de monitoreo permitió detectar caídas, lentitudes o fallas intermitentes de forma inmediata, reduciendo significativamente el tiempo que transcurría entre el inicio de un incidente y su identificación, esto evitó que los servicios permanecieran inactivos durante largos periodos y disminuyó el impacto sobre las operaciones diarias.

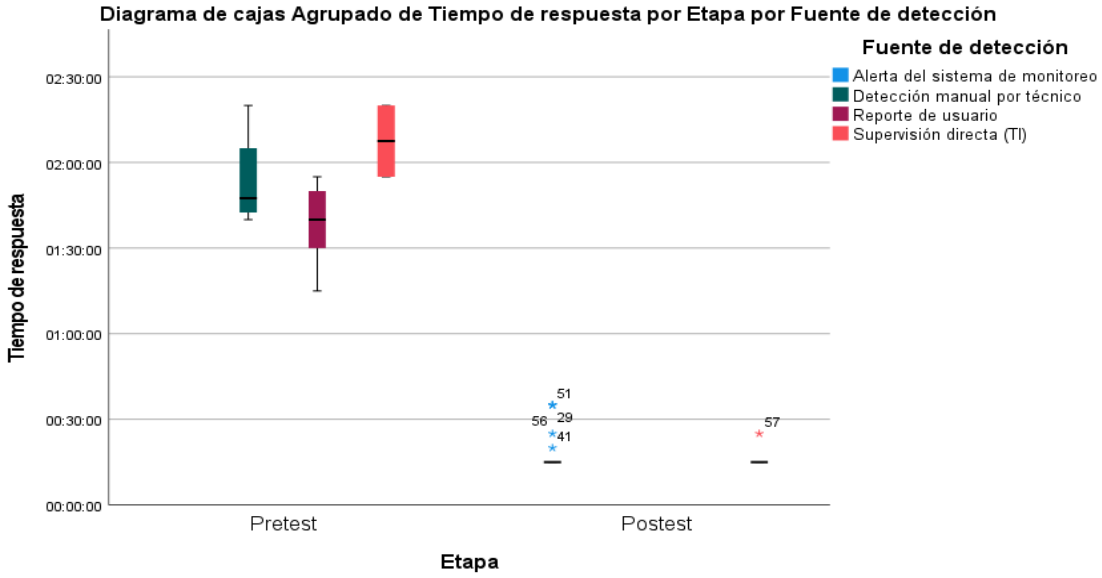
Tabla 19

Resultados pretest y postest de la dimensión disponibilidad del servicio según fuente de detección

		Tiempo de respuesta	Media
Pretest	Fuente de detección	Detección manual por técnico	1:53:45
		Reporte de usuario	1:38:56
		Supervisión directa (TI)	2:07:30
		Total	1:43:36
Postest	Fuente de detección	Alerta del sistema de monitoreo	0:18:00
		Supervisión directa (TI)	0:16:06
		Total	0:17:30

Figura 2

Resultados pretest y postest de la dimensión disponibilidad del servicio según



fuente de detección

Análisis e interpretación:

La tabla muestra una mejora sustancial en la disponibilidad del servicio tras la implementación del servidor de monitoreo, evidenciada por la reducción importante en los tiempos de respuesta. En la etapa pretest, los tiempos promedios fueron elevados y reflejaron un proceso reactivo: la supervisión directa del personal TI demoró 2:07:30 en promedio, la detección manual por técnico 1:53:45 y los reportes de usuario 1:38:56, alcanzando un promedio general de 1:43:36. En contraste, en el postest la detección automatizada mediante alertas del sistema disminuyó el tiempo promedio a solo 0:18:00, mientras que la supervisión directa mejoró a 0:16:06, obteniéndose un promedio general de 0:17:30. Esta disminución superior al 80% evidencia la transición de un modelo de detección manual y tardío a uno automatizado, oportuno y continuo, lo que permitió intervenir de manera inmediata ante incidencias y mejorar significativamente la disponibilidad de los servicios TI.

5.1.2.3. Dimensión rendimiento de la infraestructura de red

Tabla 20

Resultados pretest de la disponibilidad estimada según equipo de red

Disponibilidad estimada (%)	Equipo de red - Pretest												Total	
	Core Principal		Core Respaldo		Switch A1		Switch A2		Switch A3		Switch A4			
	f	%	*f*	%	*f*	%	*f*	%	*f*	%	*f*	%	*f*	%
99,00	1	6.7%	0	0.0%	1	6.7%	1	6.7%	2	13.3%	1	6.7%	6	40.0%
99,10	0	0.0%	2	13.3%	1	6.7%	1	6.7%	0	0.0%	1	6.7%	5	33.3%
99,30	3	20.0%	1	6.7%	0	0.0%	0	0.0%	0	0.0%	0	0.0%	4	26.7%
Total	**4**	**26.7 %**	**3**	**20.0 %**	**2**	**13.3 %**	**2**	**13.3 %**	**2**	**13.3 %**	**2**	**13.3 %**	**15**	**100.0 %**

La tabla evidencia que, antes de la implementación del servidor de monitoreo, la disponibilidad estimada de los equipos de red presentó resultados con niveles que, si bien se mantienen cercanos al 99%, reflejan variaciones que pueden comprometer la estabilidad global de la infraestructura, y se observa que el valor más frecuente fue el 99,00%, concentrando el 40,0% de los registros, distribuido principalmente en el Core Principal, Switch A1, A2, A3 y A4, lo cual indica que múltiples dispositivos experimentaron el mismo nivel de disponibilidad reducida. Un 33,3% de los equipos alcanzó una disponibilidad de 99,10%, siendo el Core de Respaldo el dispositivo con mayor concentración en este nivel, mientras que solo el 26,7% obtuvo 99,30%, principalmente en el Core Principal. La distribución revela que ningún equipo alcanzó valores superiores a 99,30%, lo que sugiere la presencia de variaciones en conectividad o episodios breves de inactividad que afectaron la estabilidad operativa.

Tabla 21

Resultados postest de la disponibilidad estimada según equipo de red

Disponibilidad estimada (%)	Equipo de red - Postest												Total	
	Core Principal		Core Respaldo		Switch A1		Switch A2		Switch A3		Switch A4			
	f	%	*f*	%	*f*	%	*f*	%	*f*	%	*f*	%	*f*	%
99,60	0	0.0%	0	0.0%	0	0.0%	1	4.8%	0	0.0%	0	0.0%	1	4.8%
99,70	0	0.0%	1	4.8%	0	0.0%	0	0.0%	2	9.5%	1	4.8%	4	19.0%
99,80	3	14.3%	3	14.3%	2	9.5%	2	9.5%	1	4.8%	1	4.8%	12	57.1%
99,90	3	14.3%	0	0.0%	0	0.0%	0	0.0%	0	0.0%	1	4.8%	4	19.0%
Total	**6**	**28.6 %**	**4**	**19.0 %**	**2**	**9.5 %**	**3**	**14.3 %**	**3**	**14.3 %**	**3**	**14.3 %**	**21**	**100.0 %**

La tabla muestra que, tras la implementación del servidor de monitoreo, la disponibilidad estimada de los equipos de red experimentó una mejora notable, concentrándose principalmente en valores superiores al 99,70%. El nivel más frecuente fue 99,80%, alcanzado por el 57,1% de los registros y distribuido de forma amplia entre el Core Principal, el Core de Respaldo y varios switches, lo que refleja una estabilidad operativa significativamente mayor en comparación con el pretest. Asimismo, un 19,0% de los equipos alcanzó un valor de 99,90%, evidenciando un desempeño casi óptimo, especialmente en el Core Principal, lo que indica una reducción considerable de caídas breves y si bien valores como 99,60% y 99,70% estuvieron presentes en menor medida de 4,8% y 19,0% respectivamente, estos porcentajes continúan representando altos niveles de disponibilidad.

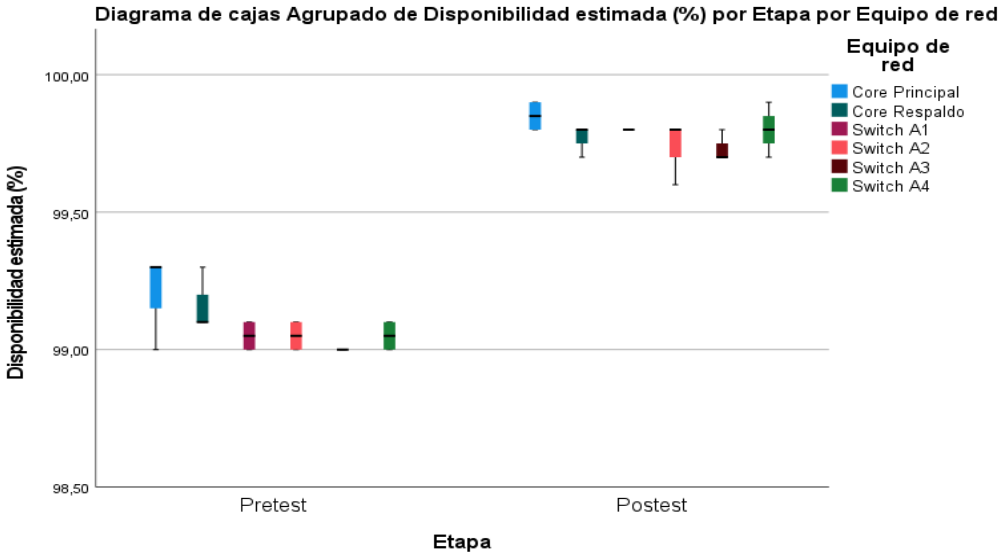
Tabla 22

Resultados pretest y postest de la disponibilidad estimada según equipo de red

Disponibilidad estimada (%)	Equipo de red						
	Core Principal	Core Respaldo	Switch A1	Switch A2	Switch A3	Switch A4	Total
Pretest	99.23	99.17	99.05	99.05	99.00	99.05	99.11
Postest	99.85	99.78	99.80	99.73	99.73	99.80	99.79
Diferencias	0.625	0.6083	0.75	0.6833	0.7333	0.75	0.6771
Media	0.63	0.61	0.75	0.68	0.73	0.75	0.68

Figura 3

Resultados pretest y postest de la disponibilidad estimada por equipo de red



La comparación entre el pretest y el postest muestra que la disponibilidad de todos los equipos de red mejoró notablemente después de implementar el servidor de monitoreo. En el pretest, los valores promedio de disponibilidad se encontraban alrededor del 99,11%, con algunos equipos, como los switches, ligeramente por debajo debido a interrupciones frecuentes y tras la implementación, la disponibilidad general aumentó hasta 99,79%, registrándose incrementos entre 0,61% y 0,75% en todos los dispositivos, donde los mayores avances se dieron en los switches A1 y A4, que elevaron su disponibilidad en 0,75%. Estos

resultados confirman que el monitoreo permitió detectar fallos con mayor rapidez, reducir las caídas y mantener la red más estable y operativa.

Tabla 23

Resultados pretest de la duración según equipo de red

Duración	Equipo de red - Pretest												Total	
	Core Principal		Core Respaldo		Switch A1		Switch A2		Switch A3		Switch A4			
	f	%	*f*	%	*f*	%	*f*	%	*f*	%	*f*	%	*f*	%
0:30:00	3	20.0%	1	6.7%	0	0.0%	0	0.0%	0	0.0%	0	0.0%	4	26.7%
0:40:00	0	0.0%	2	13.3%	1	6.7%	1	6.7%	0	0.0%	1	6.7%	5	33.3%
0:45:00	0	0.0%	0	0.0%	1	6.7%	1	6.7%	0	0.0%	1	6.7%	3	20.0%
0:50:00	1	6.7%	0	0.0%	0	0.0%	0	0.0%	2	13.3%	0	0.0%	3	20.0%
Total	**4**	**26.7%**	**3**	**20.0%**	**2**	**13.3%**	**2**	**13.3%**	**2**	**13.3%**	**2**	**13.3%**	**15**	**100.0%**

Los resultados del pretest muestran que los equipos de red presentaron tiempos de duración de incidencias relativamente prolongados, con valores que oscilaron entre 30 y 50 minutos. El mayor número de casos se concentró en la duración de 40 minutos, representando el 33,3% del total, afectando principalmente al Core de Respaldo, el Switch A1, el Switch A2 y el Switch A4. Por su parte, el Core Principal registró tiempos de 30 y 50 minutos, evidenciando también tiempos considerables de afectación. Estos niveles reflejan que, antes de la implementación del servidor de monitoreo, la interrupción de los servicios de red permanecía activa por periodos relativamente largos debido a la detección tardía de fallos y la ausencia de alertas automáticas, lo que dificultaba la atención inmediata. En conclusión, los datos evidencian un escenario de baja eficiencia operativa, donde la red funcionaba con tiempos moderados de indisponibilidad que afectaban la continuidad del servicio.

Tabla 24

Resultados postest de la duración según equipo de red

Duración	Equipo de red - Pretest												Total	
	Core Principal		Core Respaldo		Switch A1		Switch A2		Switch A3		Switch A4			
	f	%	*f*	%	*f*	%	*f*	%	*f*	%	*f*	%	*f*	%
0:07:00	1	4.8%	0	0.0%	0	0.0%	0	0.0%	0	0.0%	0	0.0%	1	4.8%
0:08:00	2	9.5%	0	0.0%	0	0.0%	0	0.0%	0	0.0%	1	4.8%	3	14.3%
0:10:00	3	14.3%	3	14.3%	2	9.5%	2	9.5%	1	4.8%	1	4.8%	12	57.1%
0:12:00	0	0.0%	1	4.8%	0	0.0%	0	0.0%	1	4.8%	0	0.0%	2	9.5%
0:13:00	0	0.0%	0	0.0%	0	0.0%	0	0.0%	1	4.8%	1	4.8%	2	9.5%
0:15:00	0	0.0%	0	0.0%	0	0.0%	1	4.8%	0	0.0%	0	0.0%	1	4.8%
Total	**6**	**28.6%**	**4**	**19.0%**	**2**	**9.5%**	**3**	**14.3%**	**3**	**14.3%**	**3**	**14.3%**	**21**	**100.0%**

Los resultados del postest evidencian una mejora significativa en la duración de las incidencias de red tras la implementación del servidor de monitoreo. Los tiempos se reducen de manera notable, ubicándose ahora entre 7 y 15 minutos, con una clara concentración en los 10 minutos, que representan el 57,1% del total de los casos. Esta duración de 10 minutos se registró de forma consistente en casi todos los equipos de red, incluyendo el Core Principal, Core Respaldo y los switches A1, A2, A3 y A4, lo que evidencia una reducción uniforme del tiempo de afectación en toda la infraestructura. Además, solo unos pocos equipos presentaron tiempos ligeramente superiores, como 12 o 13 minutos, lo cual sigue indicando un contexto altamente eficiente. En general, los datos muestran que la red pasó de tener interrupciones prolongadas a tiempos muy breves, gracias a la detección automática y oportuna de fallos, lo que permitió una intervención inmediata y una mejora sustancial en la continuidad operativa.

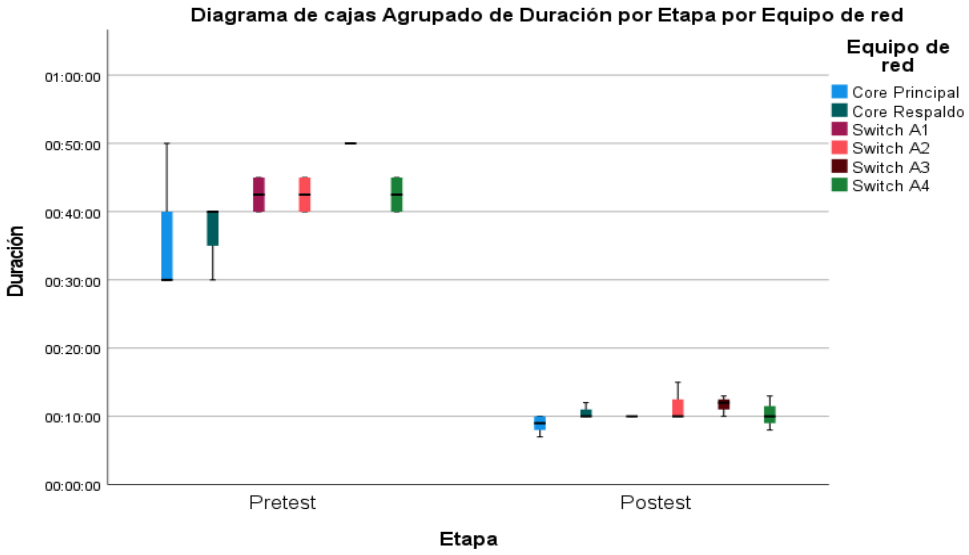
Tabla 25

Resultados pretest y postest de la duración según equipo de red

Duración	Equipo de red						
	Core Principal	Core Respaldo	Switch A1	Switch A2	Switch A3	Switch A4	Total
Pretest	0:35:00	0:36:40	0:42:30	0:42:30	0:50:00	0:42:30	0:40:20
Postest	0:08:50	0:10:30	0:10:00	0:11:40	0:11:40	0:10:20	0:10:17
Diferencias	-00:26:10	-00:26:10	-00:32:30	-00:30:50	-00:38:20	-00:32:10	-00:30:03

Figura 4

Resultados pretest y postest de la duración por equipo red



La comparación entre el pretest y el postest muestra una mejora sustancial en la duración de las incidencias de red tras la implementación del servidor de monitoreo. Durante el pretest, los tiempos promedio por equipo variaron entre 35 y 50 minutos, evidenciando interrupciones prolongadas en equipos críticos como el Switch A3 (50 min) y los Switches A1, A2 y A4 (42 min). Sin embargo, en el postest, estos tiempos se reducen drásticamente a valores que oscilan solo entre 8 y 12 minutos, con un promedio general de 10:17 minutos, lo que representa reducciones de entre 26 y 38 minutos por equipo siendo el más beneficiado el Switch A3, que redujo su tiempo de afectación en 38 minutos, mientras que los demás

equipos también muestran mejoras consistentes superiores a los 26 minutos. Entonces, los datos confirman que la detección temprana y automatizada permitió acortar significativamente la duración de las interrupciones en toda la infraestructura de red.

Tabla 26

Resultados postest y postest según recursos

Etapa	Recurso	Equipo de red						
		Core Principal	Core Respaldo	Switch A1	Switch A2	Switch A3	Switch A4	Total
Pretest	CPU (%)	87	90	87	91	90	93	89
	Memoria (%)	77	82	76	83	82	85	80
	Almacenamiento interno (%)	69	72	69	73	72	73	71
Postest	CPU (%)	68	73	69	75	74	78	72
	Memoria (%)	60	65	63	66	65	70	64
	Almacenamiento interno (%)	56	59	56	59	58	61	58
Diferencias	CPU (%)	-20	-18	-17	-15	-16	-14	-17
	Memoria (%)	-17	-17	-14	-16	-17	-15	-16
	Almacenamiento interno (%)	-14	-14	-12	-14	-14	-12	-13

Figura 5

Resultados pretest y postest del estado de CPU

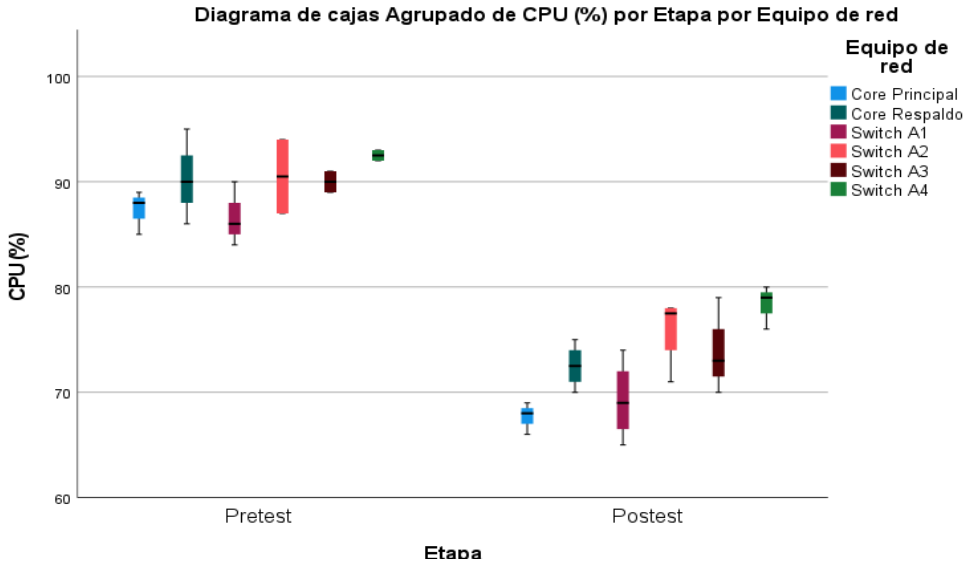


Figura 6

Resultados pretest y postest del estado de memoria

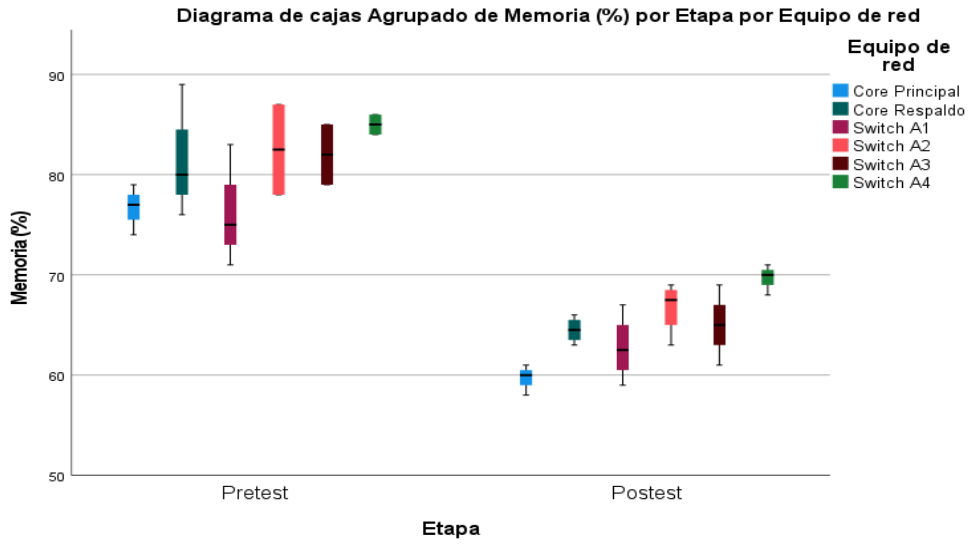
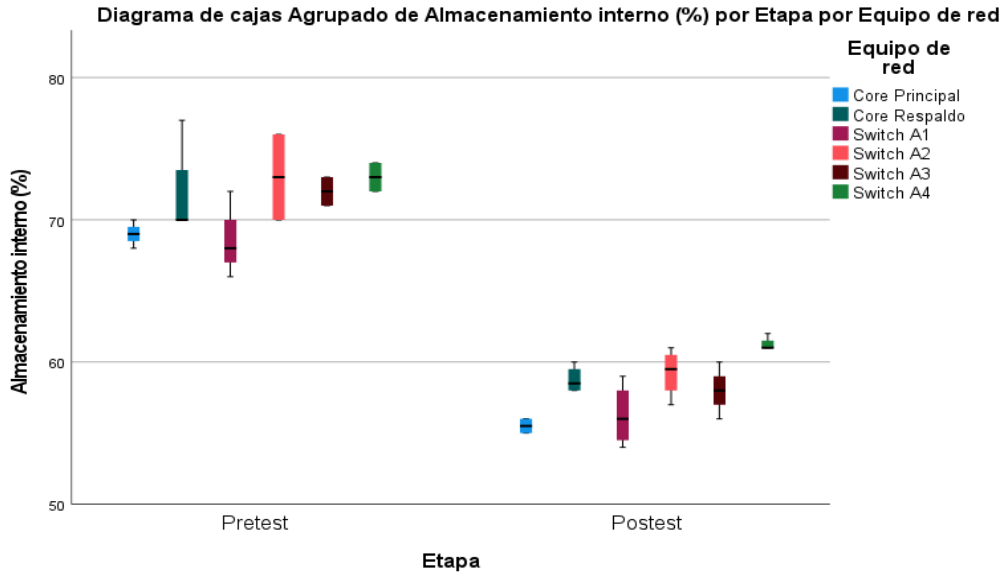


Figura 7

Resultados pretest y postest del estado de almacenamiento interno



Los resultados muestran una mejora significativa en el rendimiento de los equipos de red luego de la implementación del servidor de monitoreo, reflejada en la reducción del uso de CPU, memoria y almacenamiento interno. En la etapa pretest, los valores eran elevados, con promedios de 89% en CPU, 80% en memoria y 71% en almacenamiento, lo cual evidenciaba una operación cercana a los límites recomendados, especialmente en el Core de Respaldo y el Switch A4. Tras la implementación, el postest registra una

disminución consistente en todos los equipos, alcanzando promedios de 72% en CPU, 64% en memoria y 58% en almacenamiento, lo que representa reducciones globales de 17%, 16% y 13% respectivamente. Estas mejoras indican que el monitoreo continuo permitió gestionar adecuadamente las cargas de trabajo y detectar comportamientos anómalos antes de que saturaran los sistemas. Por ello, los resultados confirman que el servidor de monitoreo optimizó el uso de recursos en toda la infraestructura, reduciendo la sobrecarga y favoreciendo un funcionamiento más eficiente y estable.

5.1.2.4. Dimensión rendimiento de la infraestructura del servidor

Tabla 27

Resultados postest y postest según recursos

Etapa	Indicador	Servidor afectado									
		Servidor respaldos	**Servidor académico**	**Servidor contable**	**Servidor de archivos**	**Servidor de correo**	**Servidor de directorio activo**	**Servidor de respaldos**	**Servidor intranet**	**Servidor web**	**Total**
Pretest	Uso de CPU	92.00%	83.00%	85.86%	74.00%	78.60%	84.75%	68.80%	87.33%	87.14%	81.50%
	Uso de Memoria RAM	80.00%	79.33%	83.43%	73.80%	81.40%	71.25%	64.60%	74.00%	77.00%	76.18%
	Uso de Almacenamiento	77.00%	71.67%	74.14%	91.80%	68.40%	67.75%	91.00%	70.00%	74.00%	76.65%
	Temperatura de CPU (°C)	82.00	80.33	80.57	79.60	78.80	80.25	79.40	80.67	81.57	80.25
Postest	Uso de CPU	62.83%	56.80%	60.67%	63.00%	57.50%	63.00%	59.43%	58.00%	61.00%	60.11%
	Uso de Memoria RAM	69.17%	63.60%	66.33%	62.00%	63.25%	66.00%	64.00%	66.00%	66.60%	65.26%
	Uso de Almacenamiento	61.83%	68.20%	59.67%	58.33%	64.75%	60.00%	60.71%	65.00%	62.40%	62.49%
	Temperatura de CPU (°C)	63.67	61.60	62.00	62.33	61.25	64.00	61.71	60.00	61.20	62.00
Diferencias	Uso de CPU	-29.2%	-26.2%	-25.2%	-11.0%	-21.1%	-21.8%	-9.4%	-29.3%	-26.1%	-21.4%
	Uso de Memoria RAM	-10.8%	-15.7%	-17.1%	-11.8%	-18.2%	-5.2%	-0.6%	-8.0%	-10.4%	-10.9%
	Uso de Almacenamiento	-15.2%	-3.5%	-14.5%	-33.5%	-3.7%	-7.8%	-30.3%	-5.0%	-11.6%	-14.2%
	Temperatura de CPU (°C)	-18.33	-18.73	-18.57	-17.27	-17.55	-16.25	-17.69	-20.67	-20.37	-18.25

Figura 8

Resultados pretest y postest del uso de CPU por servidor afectado

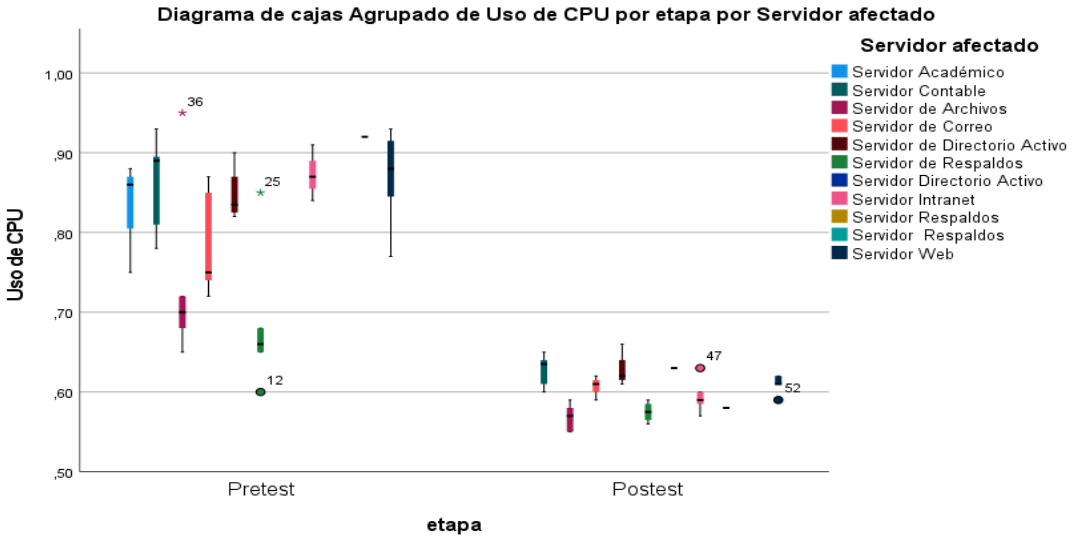


Figura 9

Resultados pretest y postest del uso de memoria RAM por servidor afectado

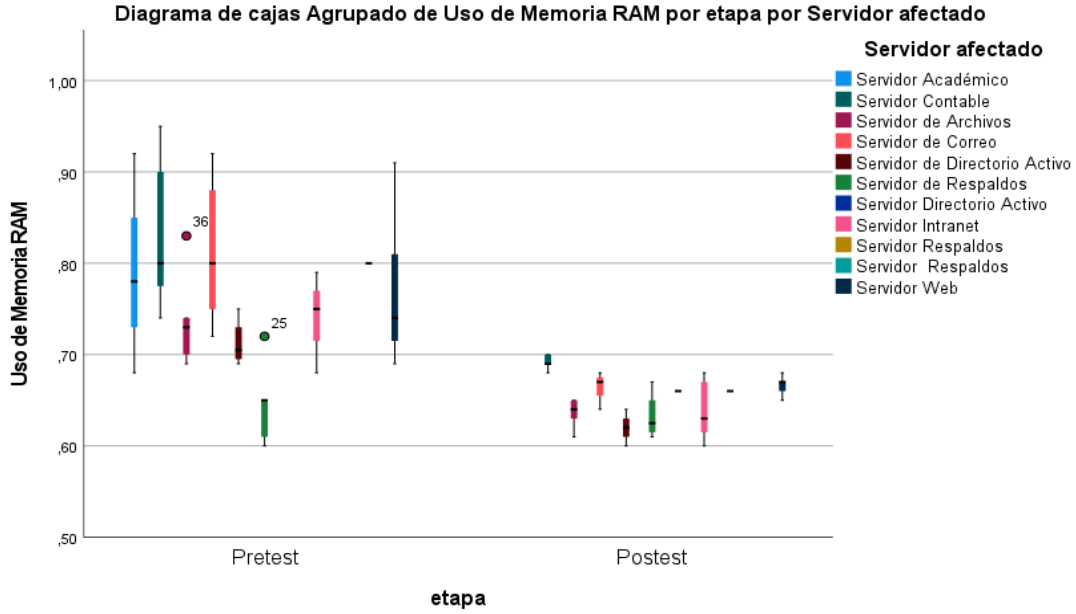


Figura 10

Resultados pretest y postest del uso de almacenamiento por servidor afectado

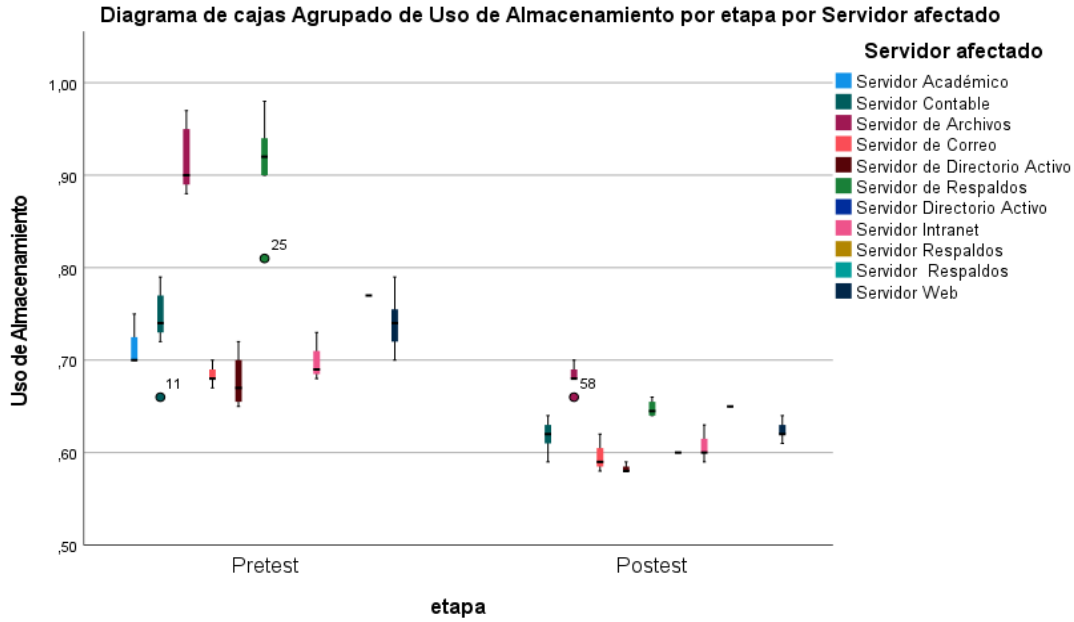
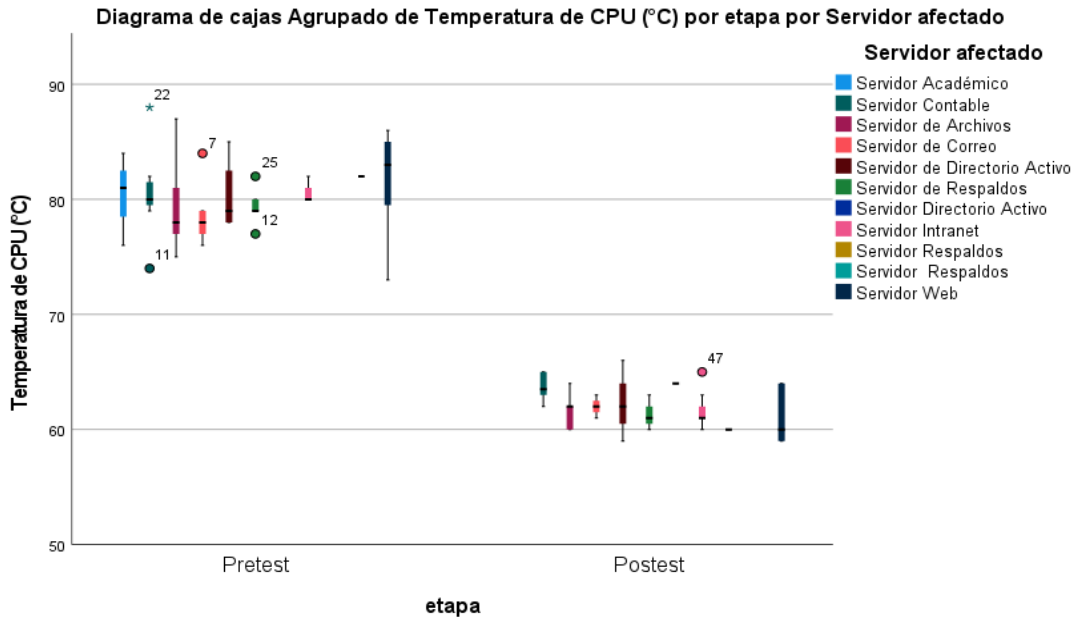


Figura 11

Resultados pretest y postest de la temperatura de CPU por servidor afectado



Los resultados muestran una mejora significativa en el rendimiento de todos los servidores tras la implementación del sistema de monitoreo. En el periodo pretest, los servidores presentaban niveles elevados de uso de CPU, memoria RAM y almacenamiento, alcanzando promedios de 81.50 %, 76.18 % y 76.65 % respectivamente, lo que evidenciaba una carga operativa alta y riesgo de saturación. Asimismo, las temperaturas promedio de CPU se situaban alrededor de 80.25 °C, un valor cercano a niveles de sobrecalentamiento en equipos de uso continuo.

En el postest, luego de implementar el servidor de monitoreo, todos los indicadores mostraron disminuciones considerables. El uso promedio de CPU se redujo a 60.11 %, la memoria RAM descendió a 65.26 % y el almacenamiento bajó a 62.49 %, reflejando una infraestructura más equilibrada y con menor probabilidad de fallas por sobrecarga. De igual manera, la temperatura promedio del CPU disminuyó a 62.00 °C, lo cual evidencia una operación más estable y segura.

Las diferencias entre ambos periodos confirman esta mejora: el uso de CPU se redujo en –21.4 %, la memoria RAM en –10.9 %, el almacenamiento en –14.2 % y la temperatura en –18.25 °C. De manera puntual, servidores críticos como el servidor de respaldos, el servidor académico y el servidor web mostraron reducciones superiores al 25 % en el uso de CPU, lo que indica una optimización significativa del rendimiento. Del mismo modo, el servidor de archivos y el servidor de respaldos registraron las mayores reducciones en uso de almacenamiento, con descensos de –33.5 % y –30.3 %, lo que sugiere una mejor gestión del espacio y procesos internos.

En conclusión, estos valores evidencian que el sistema de monitoreo permitió identificar eventos anómalos, optimizar recursos, equilibrar procesos y mejorar la eficiencia operativa de los servidores, reforzando su disponibilidad y prolongando su vida útil.

5.1.3. Contrastación de hipótesis

5.1.3.1. Prueba de normalidad

Antes de aplicar las pruebas estadísticas, fue necesario evaluar la distribución de los datos con el fin de determinar si estos seguían una distribución normal. Para ello, se empleó la prueba de normalidad de Shapiro–Wilk, recomendada para muestras pequeñas y medianas, así como para estudios de tipo pre-experimental donde se analizan indicadores continuos relacionados con desempeño tecnológico.

Tabla 28

Prueba de normalidad

	Kolmogorov-Smirnov[a]			**Shapiro-Wilk**		
	Estadístico	**gl**	**Sig.**	**Estadístico**	**gl**	**Sig.**
Tiempo de respuesta	0.315	68	0.000	0.798	68	0.000
Tiempo de respuesta	0.286	59	0.000	0.761	59	0.000
Duración	0.288	36	0.000	0.786	36	0.000
Disponibilidad estimada (%)	0.262	36	0.000	0.798	36	0.000
CPU (%)	0.115	37	,200*	0.933	37	0.028
Memoria (%)	0.123	37	0.172	0.937	37	0.038
Almacenamiento interno (%)	0.198	37	0.001	0.901	37	0.003
Uso de CPU	0.187	75	0.000	0.874	75	0.000
Uso de Memoria RAM	0.176	75	0.000	0.896	75	0.000
Uso de Almacenamiento	0.155	75	0.000	0.875	75	0.000
Temperatura de CPU (°C)	0.212	75	0.000	0.861	75	0.000

Análisis e interpretación:

Los resultados obtenidos mediante la prueba de Shapiro–Wilk muestran que todos los indicadores presentan valores de significancia $p < 0.05$, lo cual indica que sus datos no siguen una distribución normal cuyos valores de $p < .001$. Esta prueba confirma la ausencia

de normalidad ($p < 0.05$), determinando que los datos no cumplen con los supuestos de normalidad necesarios para aplicar pruebas paramétricas, justificando el uso del estadístico U de Mann–Whitney para comparar las mediciones del pretest y postest en la investigación.

Es pertinente precisar la elección de la prueba U de Mann–Whitney como estadístico de contraste, si bien el diseño de la investigación es pre-experimental con mediciones pretest y postest la unidad de registro en cada fase no corresponde a sujetos medidos en dos momentos, sino a eventos o incidentes independientes ocurridos durante cada periodo de observación. Esto genera tamaños de muestra diferentes entre el pretest y el postest, por ejemplo: 33 registros en el pretest y 35 en el postest para la dimensión de eficiencia operativa, o 15 y 21 para la dimensión de rendimiento de la infraestructura de red, lo cual imposibilita el emparejamiento necesario para la prueba de rangos con signo de Wilcoxon. La prueba U de Mann–Whitney es la alternativa no paramétrica adecuada cuando se comparan dos muestras independientes que no cumplen el supuesto de normalidad. En consecuencia, dado que las observaciones de cada fase son estructuralmente independientes y los datos no siguen una distribución normal según lo evidenciado por la prueba de Shapiro–Wilk con $p < .001$, la prueba U de Mann–Whitney resulta el estadístico apropiado para este estudio.

5.1.3.2. Prueba de hipótesis general

Tabla 29

Resultados por dimensión de la variable servicios TI

Dimensión	Prueba estadística	p-valor	Decisión estadística
Eficiencia operativa	U de Mann–Whitney	0.000	Se rechaza H_0 y se acepta H_1
Disponibilidad del servicio	U de Mann–Whitney	0.000	Se rechaza H_0 y se acepta H_1
Rendimiento de la infraestructura de red	U de Mann–Whitney	0.000	Se rechaza H_0 y se acepta H_1
Rendimiento de la infraestructura del servidor	U de Mann–Whitney	0.000	Se rechaza H_0 y se acepta H_1
Hipótesis general	**Todas las dimensiones muestran mejora significativa**	0.000	**Se confirma el cumplimiento de la hipótesis general**

Análisis e interpretación:

La tabla evidencia que en todas las dimensiones evaluadas de los servicios TI, eficiencia operativa, disponibilidad del servicio, rendimiento de la infraestructura de red y rendimiento de la infraestructura del servidor, se registran diferencias estadísticamente significativas entre el pretest y el postest. Esto se indica en que los rangos del postest son menores o mayores según la naturaleza del indicador, mostrando mejoras en los tiempos de respuesta, en la continuidad de los servicios, en la estabilidad de la red y en el uso eficiente de los recursos del servidor. Además, en todos los casos el valor de significancia obtenido fue $p < .001$, inferior al nivel de significancia de 0.05, lo que conlleva al rechazo de la hipótesis nula y a la aceptación de la hipótesis alterna correspondiente. Entonces, estos resultados confirman que la implementación del servidor de monitoreo generó mejoras significativas en todas las áreas analizadas, permitiendo concluir que la hipótesis general se

cumple, dado que los servicios TI fueron optimizados de manera integral en la empresa EGEMSA S.A. Cusco, 2025.

5.1.3.3. Prueba de hipótesis específicas

Hipótesis específica 1

Tabla 30

Rangos de la dimensión eficiencia operativa en el pretest y postest

	Etapa	N	Rango promedio	Suma de rangos
Tiempo de respuesta	Pretest	33	52.00	1716.00
	Postest	35	18.00	630.00
	Total	**68**		

Análisis e interpretación:

En la tabla de rangos se observa una diferencia marcada entre el pretest y el postest respecto al tiempo de respuesta de los incidentes. El pretest presenta un rango promedio de 52.00, lo que indica tiempos de atención significativamente más altos. En contraste, el postest muestra un rango promedio de 18.00, evidenciando una reducción sustancial del tiempo requerido para detectar y atender un incidente. Esta variación sugiere que, tras la implementación del servidor de monitoreo, los incidentes fueron identificados más rápidamente y gestionados con mayor eficiencia, incluso antes del análisis estadístico inferencial.

Tabla 31

Estadísticos de la prueba U de Mann–Whitney de la dimensión eficiencia operativa entre el pretest y postest

Estadísticos de prueba[a]	Tiempo de respuesta
U de Mann-Whitney	0.000
W de Wilcoxon	630.000
Z	-7.217
Sig. asin. (bilateral)	0.000

a. Variable de agrupación: Etapa

Análisis e interpretación:

Hipótesis nula (H_0): La implementación del servidor de monitoreo no optimiza la eficiencia operativa en la empresa EGEMSA S.A. Cusco, 2025.

Hipótesis alterna (H_1): La implementación del servidor de monitoreo sí optimiza la eficiencia operativa en la empresa EGEMSA S.A. Cusco, 2025.

Nivel de significancia: 5% ($\alpha = 0.05$)

U de Mann–Whitney: 0.000

p–valor: 0.000 (< 0.05)

Conclusión: Al analizar los resultados, se observa que el valor obtenido de $p < .001$, menor que el nivel de significancia de 0.05. En consecuencia, se rechaza la hipótesis nula (H_0) y se acepta la hipótesis alterna (H_1).

Por lo tanto, se concluye que la implementación del servidor de monitoreo optimiza significativamente la eficiencia operativa, reduciendo de manera notable el tiempo de respuesta ante los incidentes en la empresa EGEMSA S.A. Cusco durante el año 2025.

Hipótesis específica 2

Tabla 32

Rangos de la dimensión disponibilidad del servicio en el pretest y postest

	Etapa	N	Rango promedio	Suma de rangos
Tiempo de respuesta	Pretest	25	47.00	1175.00
	Postest	34	17.50	595.00
	Total	**59**		

Análisis e interpretación:

En la tabla de rangos se observa una diferencia clara entre el pretest y el postest en relación con el tiempo de respuesta relacionado a la disponibilidad del servicio. El pretest presenta un rango promedio de 47.00, lo que indica mayores tiempos de afectación cuando se registraban interrupciones o caídas de los servicios TI. En contraste, el postest muestra un rango promedio considerablemente menor (17.50), lo que refleja que, después de la implementación del servidor de monitoreo, los tiempos para restablecer los servicios fueron significativamente más cortos. Esta comparación indica una mejora significativa en la disponibilidad del servicio incluso antes de aplicar el análisis estadístico.

Tabla 33

Estadísticos de la prueba U de Mann–Whitney de la dimensión disponibilidad del servicio entre el pretest y postest

Estadísticos de prueba[a]	**Tiempo de respuesta**
U de Mann-Whitney	0.000
W de Wilcoxon	595.000
Z	-6.904
Sig. asin. (bilateral)	0.000

a. Variable de agrupación: Etapa

Análisis e interpretación:

Hipótesis nula (H_0): La implementación del servidor de monitoreo no optimiza la disponibilidad del servicio en la empresa EGEMSA S.A. Cusco, 2025.

Hipótesis alterna (H_1): La implementación del servidor de monitoreo sí optimiza la disponibilidad del servicio en la empresa EGEMSA S.A. Cusco, 2025.

Nivel de significancia: 5% ($\alpha = 0.05$)

U de Mann–Whitney: 0.000

p–valor: 0.000 (< 0.05)

Conclusión: Por lo tanto, se identifica que el valor de significancia obtenido ($p < .001$) es menor que el nivel de significancia de 0.05; por lo tanto, se rechaza la hipótesis nula (H_0) y se acepta la hipótesis alterna (H_1).

Este resultado indica que existen diferencias estadísticamente significativas entre el pretest y el postest, mostrando una mejora notable en los tiempos de recuperación de los servicios TI después de la implementación del servidor de monitoreo.

Por consiguiente, se concluye que la implementación del servidor de monitoreo optimiza significativamente la disponibilidad del servicio en la empresa EGEMSA S.A. Cusco, 2025, cumpliéndose la hipótesis específica.

Hipótesis específica 3

Tabla 34

Rangos de la dimensión rendimiento de la infraestructura de red en el pretest y postest de duración y disponibilidad estimada

	Etapa	N	Rango promedio	Suma de rangos
Duración	Pretest	15	29.00	435.00
	Postest	21	11.00	231.00
	Total	**36**		
Disponibilidad estimada (%)	Pretest	15	8.00	120.00
	Postest	21	26.00	546.00
	Total	**36**		

Análisis e interpretación:

En primer lugar, para el indicador de duración, el pretest presenta un rango promedio de 29.00, lo que indica mayores tiempos de afectación cuando la red sufría congestiones, lentitud o caídas. En contraste, el postest obtiene un rango promedio de 11.00, reflejando una notable reducción en el tiempo que los incidentes impactan a la infraestructura de red después de la implementación del servidor de monitoreo.

Por otro lado, la disponibilidad estimada de la red muestra la tendencia inversa: en el pretest el rango promedio es 8.00, mientras que en el postest asciende a 26.00, lo que evidencia un aumento significativo en la proporción de tiempo en que la red permaneció operativa y estable.

Tabla 35

Estadísticos de la prueba U de Mann–Whitney de la dimensión rendimiento de la infraestructura de red entre el pretest y postest de duración y disponibilidad estimada

Estadísticos de prueba[a]	Duración	Disponibilidad estimada (%)
U de Mann-Whitney	0.000	0.000
W de Wilcoxon	231.000	120.000
Z	-5.165	-5.179
Sig. asin. (bilateral)	0.000	0.000
Significación exacta [2*(sig. unilateral)]	,000[b]	,000[b]

a. Variable de agrupación: Etapa

b. No corregido para empates.

Análisis e interpretación:

Hipótesis nula (H_0): La implementación del servidor de monitoreo no optimiza el rendimiento de la infraestructura de red en la empresa EGEMSA S.A. Cusco, 2025.

Hipótesis alterna (H_1): La implementación del servidor de monitoreo sí optimiza el rendimiento de la infraestructura de red en la empresa EGEMSA S.A. Cusco, 2025.

Nivel de significancia: 5% ($\alpha = 0.05$)

En ambos casos, p - valor< 0.05.

Conclusión: Dado que los valores p obtenidos (0.000) son menores que el nivel de significancia establecido (0.05), se rechaza la hipótesis nula (H_0) y se acepta la hipótesis alterna (H_1).

Esto indica que existen diferencias estadísticamente significativas entre el pretest y el postest en los dos indicadores evaluados, se observa una disminución significativa en la duración de los incidentes y un incremento notable en la disponibilidad de la red después de la implementación del servidor de monitoreo.

Por lo tanto, se concluye que, la implementación del servidor de monitoreo optimiza de manera significativa el rendimiento de la infraestructura de red en la empresa EGEMSA S.A. Cusco, 2025, cumpliéndose la hipótesis específica.

Tabla 36

Rangos de la dimensión rendimiento de la infraestructura de red en el pretest y postest según recursos

Recursos	Etapa	N	Rango promedio	Suma de rangos
CPU (%)	Pretest	15	30.00	450.00
	Postest	22	11.50	253.00
	Total	**37**		
Memoria (%)	Pretest	15	29.97	449.50
	Postest	22	11.52	253.50
	Total	**37**		
Almacenamiento interno (%)	Pretest	15	30.00	450.00
	Postest	22	11.50	253.00
	Total	**37**		

La tabla muestra que, en los tres recursos evaluados (CPU, memoria y almacenamiento interno), los valores registrados en el pretest presentan rangos promedio más altos en comparación con el postest, cuyos rangos promedio se sitúan alrededor de 11.50. Esta diferencia evidencia que, antes de la implementación del sistema de monitoreo, los equipos de red operaban con mayores niveles de uso y carga, lo que reflejaba una infraestructura más exigente y cercana a niveles de saturación. En contraste, los rangos menores del postest indican que, tras la implementación del servidor de monitoreo, los valores de uso de CPU, memoria y almacenamiento disminuyeron de manera significativa, demostrando una gestión más eficiente de los recursos y una operación mucho más estable.

Tabla 37

Estadísticos de la prueba U de Mann–Whitney de la dimensión rendimiento de la infraestructura de red entre el pretest y postest según recursos

Estadísticos de prueba[a]	CPU (%)	Memoria (%)	Almacenamiento interno (%)
U de Mann-Whitney	0.000	0.500	0.000
W de Wilcoxon	253.000	253.500	253.000
Z	-5.108	-5.092	-5.115
Sig. asin. (bilateral)	0.000	0.000	0.000
Significación exacta [2*(sig. unilateral)]	,000[b]	,000[b]	,000[b]

a. Variable de agrupación: Etapa

b. No corregido para empates.

Nivel de significancia: 5% ($\alpha = 0.05$)

Uso de CPU: $p < .001$

Uso de memoria: $p < .001$

Almacenamiento interno: $p < .001$

Conclusión: Dado que los valores p obtenidos (0.000) son menores que el nivel de significancia (0.05), se rechaza la hipótesis nula (H_0) y se acepta la hipótesis alterna (H_1).

Esto demuestra que existen diferencias estadísticamente significativas entre los valores de pretest y postest en los tres recursos de red analizados.

Hipótesis específica 4

Tabla 38

Rangos de la dimensión rendimiento de la infraestructura del servidor en el pretest y postest

	Etapa	N	Rango promedio	Suma de rangos
Uso de CPU	Pretest	40	54.98	2199.00
	Postest	35	18.60	651.00
	Total	**75**		
Uso de Memoria RAM	Pretest	40	52.18	2087.00
	Postest	35	21.80	763.00
	Total	**75**		
Uso de Almacenamiento	Pretest	40	54.55	2182.00
	Postest	35	19.09	668.00
	Total	**75**		
Temperatura de CPU (°C)	Pretest	40	55.50	2220.00
	Postest	35	18.00	630.00
	Total	**75**		

Análisis e interpretación:

En la tabla de rangos se observan diferencias consistentes entre el pretest y el postest para todos los indicadores que conforman el rendimiento de la infraestructura del servidor: uso de CPU, uso de memoria RAM, uso de almacenamiento y temperatura del CPU.

En el pretest, los rangos promedio son notablemente altos (CPU: 54.98; RAM: 52.18; almacenamiento: 54.55; temperatura: 55.50), lo que indica mayores niveles de consumo de recursos, saturación del sistema y temperaturas más elevadas durante el funcionamiento del servidor.

En contraste, los rangos promedio del postest son considerablemente menores (CPU: 18.60; RAM: 21.80; almacenamiento: 19.09; temperatura: 18.00), lo que refleja una mejora clara en la gestión de recursos y una reducción en la carga operativa del servidor. Esta diferencia preliminar sugiere que, tras la implementación del servidor de monitoreo, la infraestructura del servidor opera de forma más eficiente, estable y con menor estrés térmico y computacional.

Tabla 39

Estadísticos de la prueba U de Mann–Whitney de la dimensión rendimiento de la infraestructura del servidor entre el pretest y postest

Estadísticos de prueba[a]	Uso de CPU	Uso de Memoria RAM	Uso de Almacenamiento	Temperatura de CPU (°C)
U de Mann-Whitney	21.000	133.000	38.000	0.000
W de Wilcoxon	651.000	763.000	668.000	630.000
Z	-7.217	-6.030	-7.038	-7.447
Sig. asin. (bilateral)	0.000	0.000	0.000	0.000

a. Variable de agrupación: Etapa

Análisis e interpretación:

Hipótesis nula (H_0): La implementación del servidor de monitoreo no optimiza el rendimiento de la infraestructura del servidor en la empresa EGEMSA S.A. Cusco, 2025.

Hipótesis alterna (H_1): La implementación del servidor de monitoreo sí optimiza el rendimiento de la infraestructura del servidor en la empresa EGEMSA S.A. Cusco, 2025.

Nivel de significancia: 5% ($\alpha = 0.05$)

Todos los valores p son menores que 0.05.

Conclusión: Dado que en todos los indicadores evaluados el valor de significancia ($p < .001$) es menor que 0.05, se rechaza la hipótesis nula (H_0) y se acepta la hipótesis alterna (H_1). Esto indica que existen diferencias estadísticamente significativas entre el pretest y el

postest, evidenciando mejoras sustanciales en el rendimiento de la infraestructura del servidor después de la implementación del servidor de monitoreo.

Las mejoras se manifiestan en una reducción significativa del uso de CPU, la memoria RAM, el almacenamiento y la temperatura del procesador, lo que demuestra que el servidor opera bajo mejores condiciones, con menor carga y mayor estabilidad.

Por consiguiente, se concluye que la implementación del servidor de monitoreo optimiza de manera significativa el rendimiento de la infraestructura del servidor en la empresa EGEMSA S.A. Cusco, 2025, cumpliéndose la hipótesis específica.

Adicionalmente para determinar el tamaño del efecto para cada indicador se calculó la r de Rosenthal, según la formula $r = |Z| / \sqrt{N}$, lo cual nos indica el tamaño del efecto, puede tomar valores entre 1 y 0 tomando de 0.10 – 0.29 efecto pequeño, de 0.30 – 0.49 efecto mediano, y ≥ 0.50 efecto grande obteniendo los siguientes valores:

Tabla 40

Tamaño del efecto según r de Rosenthal

Hipótesis	Indicador	Z	N	r	Magnitud
H.E.1	Tiempo de respuesta	−7.217	68	0.875	Grande
H.E.2	Tiempo de respuesta	−6.904	59	0.899	Grande
H.E.3	Duración	−5.165	36	0.861	Grande
H.E.3	Disponibilidad estimada	−5.179	36	0.863	Grande
H.E.3	CPU (%)	−5.108	37	0.84	Grande
H.E.3	Memoria (%)	−5.092	37	0.837	Grande
H.E.3	Almacenamiento interno (%)	−5.115	37	0.841	Grande
H.E.4	Uso de CPU	−7.217	75	0.833	Grande
H.E.4	Uso de memoria RAM	−6.030	75	0.696	Grande
H.E.4	Uso de almacenamiento	−7.038	75	0.813	Grande
H.E.4	Temperatura de CPU	−7.447	75	0.86	Grande

Los resultados muestran que todos los indicadores evaluados presentan tamaños del efecto superiores a 0.50, el valor más alto corresponde al indicador de tiempo de respuesta

en la dimensión de disponibilidad del servicio, con r = 0.899, mientras que el valor más bajo se registra en el indicador de uso de memoria RAM, con r = 0.696, que aun así se ubica en el rango de efecto grande. Estos resultados indican que las diferencias entre el pretest y el postest no solo son estadísticamente significativas, sino que también poseen relevancia práctica, confirmando que la implementación del servidor de monitoreo produjo mejoras sustanciales y de magnitud considerable en todas las dimensiones de los servicios TI evaluados.

5.2. Discusión

La presente investigación tuvo como propósito determinar si la implementación de un servidor de monitoreo optimiza los servicios TI en la empresa EGEMSA S.A. Cusco, los resultados obtenidos confirmaron la hipótesis general y las cuatro hipótesis específicas, evidenciando mejoras estadísticamente significativas en las dimensiones de eficiencia operativa, disponibilidad del servicio, rendimiento de la infraestructura de red y rendimiento de la infraestructura del servidor. A continuación, se discuten estos hallazgos en relación con los antecedentes de investigación y los fundamentos teóricos que sustentan el estudio.

El hallazgo principal de esta dimensión revela que el tiempo promedio de resolución de incidentes se redujo de 01:40:09 horas en el pretest a 00:16:08 minutos en el postest, lo que representa una disminución superior al 80 %. Además, la fuente de detección pasó de depender mayoritariamente del reporte de usuarios, con un 66.7 % en el pretest, a la alerta automática del sistema de monitoreo, con un 82.9 % en el postest. La prueba U de Mann–Whitney arrojó un valor de $p < .001$ con un tamaño del efecto r = 0.875, clasificado como grande lo que confirma tanto la significancia estadística como la relevancia práctica de la mejora.

Este resultado es consistente con los hallazgos de Montero (2022), quien reportó que, tras la implementación de Zabbix en la empresa avícola POFASA de Ecuador, los tiempos

de atención de incidentes pasaron de más de 4 horas en el 69 % de los casos a 30 minutos en el 89 %, lo cual evidencia una tendencia convergente con los resultados del presente estudio. No obstante, la presente investigación registra una reducción proporcionalmente mayor, posiblemente atribuible a la integración de Grafana como complemento visual que facilita la interpretación inmediata de las alertas, aspecto que no fue considerado en el estudio de Montero. En la misma línea, Robledo (2023) demostró que, en la Gobernación de Risaralda en Colombia, la implementación de un servidor de monitoreo con Cacti sobre Ubuntu Server permitió detectar dispositivos conectados en un promedio de 48 segundos, frente a los 3 a 5 minutos que requería Windows, lo que refuerza la evidencia de que las herramientas de monitoreo contribuyen significativamente a la detección temprana de fallas, tal como se observó en esta investigación.

A nivel nacional, Lizarraga y Ponce (2021) reportaron que el nivel de atención de incidencias de dispositivos de red mejoró de 52.27 % a 93.18 % tras la implementación de un servidor de monitoreo con Nagios y Cacti en la empresa Precisa, un incremento del 40.91 % que coincide con la tendencia de mejora observada en el presente estudio. De igual manera, Casas y Sempértegui (2018) evidenciaron tiempos de detección de caídas de infraestructura de 70 segundos y de servicios de red de 42 segundos tras la implementación de un sistema de monitoreo en la Universidad Nacional Pedro Ruiz Gallo, lo cual es comparable con los tiempos de detección automatizada registrados en la presente investigación.

Desde el fundamento teórico, Serrano et al. (2021) destacan que la eficiencia operativa está directamente relacionada con la capacidad de los sistemas de monitoreo para detectar fallos y responder proactivamente, minimizando los impactos negativos sobre las operaciones de la organización. Esta afirmación se confirma con los datos obtenidos, donde la detección automatizada permitió una respuesta casi inmediata. De manera

complementaria, Ahmad et al. (2020) definen el tiempo promedio de resolución de incidentes como el período transcurrido desde la detección hasta la implementación de una acción de mitigación, y señalan que un menor tiempo de respuesta resulta crucial para limitar el impacto sobre la disponibilidad de los servicios, aspecto que se materializó en la reducción observada de más de 80 minutos en el tiempo promedio de atención. Por su parte, Laudon y Laudon (2019) señalan que un servidor de monitoreo no solo recoge datos de rendimiento, sino que también analiza patrones y tendencias, permitiendo a las organizaciones predecir y prevenir problemas, mejorando así la eficiencia operativa; esta capacidad predictiva se evidenció en la transición de un modelo reactivo a uno proactivo en la gestión de incidentes de EGEMSA.

En relación con la disponibilidad del servicio, los resultados evidencian que el tiempo promedio de recuperación de servicios críticos se redujo de 01:43:36 horas en el pretest a 00:17:30 minutos en el postest, lo que constituye una disminución superior al 83 %. Asimismo, el 82.4 % de los incidentes en el postest fueron atendidos en un máximo de 15 minutos, cuando en el pretest el rango más frecuente era de 1:50:00 horas, que concentraba el 20.0 % de los casos. La prueba U de Mann–Whitney confirmó la significancia de esta diferencia con $p < .001$ y un tamaño del efecto $r = 0.899$, el más alto registrado en todas las dimensiones evaluadas, lo que indica que la mejora en la disponibilidad del servicio fue no solo significativa sino de magnitud muy elevada.

Estos resultados coinciden con los hallazgos de Casas y Sempértegui (2018), quienes reportaron que, tras la implementación de un sistema de monitoreo en la Universidad Nacional Pedro Ruiz Gallo, los tiempos de detección y notificación de incidentes se redujeron significativamente, con registros de caídas de infraestructura en 70 segundos y de servicios de red en 42 segundos, con notificaciones enviadas en menos de dos minutos. Esta convergencia sugiere que los sistemas de monitoreo, independientemente del entorno

organizacional, logran reducir de manera consistente los tiempos de inactividad. Asimismo, Guevara (2023) reportó que, en la Universidad Nacional de Cajamarca, la implementación de Zabbix generó una mejora del 10 % en el nivel de operatividad de los recursos de TI y una reducción del 99.99 % en los tiempos de detección de incidencias, resultados que, aunque obtenidos en un contexto universitario, respaldan la tendencia observada en la presente investigación respecto a la mejora de la continuidad operativa.

El estudio de Montero (2022) también ofrece evidencia convergente, al reportar que la satisfacción de los usuarios alcanzó un 95 % de valoraciones entre bueno y excelente, y que la confianza en el sistema aumentó de un 11 % a un 95 %, lo cual puede interpretarse como un indicador indirecto de la mejora en la disponibilidad percibida por los usuarios finales. Aunque la presente investigación no midió la satisfacción del usuario de manera directa, la reducción sustancial en los tiempos de recuperación de servicios sugiere un efecto positivo sobre la experiencia del usuario, tal como lo señalan González et al. (2021) al afirmar que las estrategias de redundancia y recuperación ante desastres son cruciales para mantener la continuidad del servicio.

Desde la perspectiva teórica, Serrano et al. (2021) enfatizan que una alta disponibilidad es fundamental para las operaciones de carácter crítico, ya que cualquier interrupción puede resultar en pérdidas significativas. Esta afirmación cobra especial relevancia en el contexto de EGEMSA, empresa del sector energético donde la continuidad de los servicios tecnológicos resulta estratégica para la operación de sus procesos de generación y distribución eléctrica. Kumar et al. (2023) complementan esta perspectiva al indicar que el monitoreo continuo de los servicios TI facilita datos valiosos para identificar y corregir vulnerabilidades que afectan la disponibilidad, aspecto que se confirmó cuando el sistema de alertas automáticas permitió detectar caídas, lentitudes y fallas intermitentes de forma inmediata, reduciendo significativamente el tiempo entre el inicio de un incidente y

su identificación. Además, Stallings (2017) señala que los servidores de monitoreo son esenciales para mantener la disponibilidad y el rendimiento de los servicios de TI, ya que proporcionan una vigilancia constante y alertan a los administradores sobre problemas potenciales antes de que se conviertan en fallos críticos, lo cual se verificó empíricamente al observar que la detección pasó de ser predominantemente manual y reactiva a automatizada y oportuna.

En la dimensión de rendimiento de la infraestructura de red, los resultados muestran mejoras significativas en todos los indicadores evaluados. La disponibilidad estimada de los equipos de red aumentó de un promedio de 99.11 % en el pretest a 99.79 % en el postest, con incrementos entre 0.61 % y 0.75 % en todos los dispositivos. Si bien esta diferencia puede parecer reducida en términos absolutos, en el contexto de infraestructura crítica cada fracción porcentual representa horas de operación recuperadas. La duración promedio de las incidencias de red se redujo de 40:20 minutos a 10:17 minutos, lo que equivale a una disminución de más de 30 minutos por evento. En cuanto al uso de recursos, el consumo promedio de CPU en equipos de red disminuyó de 89 % a 72 %, la memoria de 80 % a 64 % y el almacenamiento interno de 71 % a 58 %, representando reducciones de 17, 16 y 13 puntos porcentuales, respectivamente. Todas las pruebas U de Mann–Whitney arrojaron valores de $p < .001$ con tamaños del efecto entre $r = 0.837$ y $r = 0.863$, todos clasificados como efecto grande.

Estos hallazgos son consistentes con los reportados por Lizarraga y Ponce (2021), quienes evidenciaron un aumento del 45.53 % en el nivel de control de saturación del tráfico de red, pasando de 42.35 % a 87.88 % tras la implementación de un servidor de monitoreo en la empresa Precisa. Aunque las métricas empleadas difieren, puesto que en la presente investigación se midió directamente el uso de CPU, memoria y almacenamiento de los equipos de red, mientras que Lizarraga y Ponce evaluaron el control general de la saturación,

ambos estudios convergen en demostrar que el monitoreo permite reducir los niveles de sobrecarga en la infraestructura. De igual forma, Fernández (2019) evidenció que la implementación de un servidor de monitoreo en la UGEL Huamanga permitió una supervisión más eficiente de la infraestructura al identificar los principales patrones de tráfico, aunque su enfoque fue observacional y no incluyó mediciones de pretest y postest como la presente investigación.

El estudio de Robledo (2023) aporta evidencia complementaria al demostrar que Ubuntu Server superó ampliamente a Windows en la detección de eventos de red, con tiempos de detección entre 27 y 51 segundos frente a fallas eléctricas, desconexiones de patch cord y desconexiones masivas. La presente investigación, que también utilizó Ubuntu Server como sistema operativo base, confirma la eficacia de esta plataforma para la detección rápida de anomalías en la red, reflejada en la reducción de la duración promedio de incidencias de más de 40 minutos a aproximadamente 10 minutos.

Teóricamente, Serrano et al. (2021) afirman que el rendimiento de la infraestructura de red incluye la capacidad de manejar cargas de tráfico de manera efectiva, minimizar la pérdida de datos y garantizar la disponibilidad continua. Los resultados del presente estudio confirman esta premisa, ya que la reducción en el uso de recursos evidencia una gestión más eficiente de las cargas de trabajo. Ahmad et al. (2020) complementan esta perspectiva al indicar que una infraestructura de red bien gestionada no solo optimiza el flujo de información, sino que también reduce el tiempo de respuesta en la resolución de problemas, aspecto que se materializó en la disminución de la duración de incidencias. Asimismo, Kumar et al. (2023) señalan que las herramientas de monitoreo activo son esenciales para obtener datos en tiempo real sobre la salud de la red, facilitando la toma de decisiones informadas; esta capacidad fue clave para que los administradores de EGEMSA pudieran identificar cuellos de botella y optimizar la distribución de recursos antes de que los equipos

alcanzaran niveles de saturación. Por su parte, IBM (2023a) destaca que el monitoreo efectivo ayuda a los equipos de TI a mantener operaciones confiables y evitar que los problemas escalen sin ser detectados, lo que se evidenció en la mejora de la disponibilidad de la red de 99.11 % a 99.79 %.

Respecto al rendimiento de la infraestructura del servidor, los resultados revelan mejoras consistentes en todos los indicadores evaluados. El uso promedio de CPU se redujo de 81.50 % a 60.11 %, lo que representa una disminución de 21.4 puntos porcentuales; la memoria RAM descendió de 76.18 % a 65.26 %, con una reducción de 10.9 puntos porcentuales; el almacenamiento bajó de 76.65 % a 62.49 %, equivalente a una reducción de 14.2 puntos porcentuales; y la temperatura promedio de CPU disminuyó de 80.25 °C a 62.00 °C, registrando una reducción de 18.25 °C. Todos los valores de p fueron menores a .001 y los tamaños del efecto oscilaron entre r = 0.696 y r = 0.860, todos clasificados como efecto grande, siendo la temperatura de CPU el indicador con mayor magnitud de efecto, con r = 0.860, y el uso de memoria RAM el de menor magnitud relativa, con r = 0.696, que aun así supera ampliamente el umbral de efecto grande.

Estos resultados encuentran respaldo en la investigación de Guevara (2023), quien reportó un incremento del 13 % en el nivel de funcionalidad y del 10 % en la operatividad de los recursos de TI tras la implementación de Zabbix en la Universidad Nacional de Cajamarca. Aunque Guevara evaluó estos indicadores desde una perspectiva funcional y no mediante mediciones directas de recursos del servidor, ambos estudios coinciden en evidenciar que los sistemas de monitoreo contribuyen a una gestión más eficiente de la infraestructura. De manera similar, Garay (2018) demostró que la herramienta Centreon proporcionó una visibilidad mejorada y mayor control sobre el hardware y software en América Móvil Perú S.A.C., lo cual es consistente con la capacidad del sistema

implementado en EGEMSA para identificar eventos anómalos y optimizar el uso de recursos en los servidores.

Lizarraga y Ponce (2021) aportan evidencia convergente al reportar que el nivel de control de servicios caídos mejoró de 60.61 % a 90.91 %, un aumento del 30.3 %, tras la implementación del servidor de monitoreo, resultado que se relaciona directamente con la capacidad de los sistemas de supervisión para prevenir fallas en los servidores mediante la detección temprana de sobrecargas, tal como se observó en la presente investigación. Además, Montero (2022) reportó que las quejas relacionadas con el servicio se redujeron de un promedio de tres por semana a una por semana en el 78 % de los casos, lo cual sugiere que la mejora en el rendimiento del servidor, al reducir la frecuencia de interrupciones, tiene un efecto positivo indirecto sobre la percepción del servicio por parte de los usuarios.

Desde la fundamentación teórica, González et al. (2021) explican que un servidor bien gestionado debe manejar eficazmente las demandas de procesamiento, almacenamiento y disponibilidad de las aplicaciones críticas, lo cual se cumple en el postest, donde los niveles de uso de recursos se mantuvieron dentro de rangos aceptables. Ahmad et al. (2020) complementan esta perspectiva al señalar que una infraestructura del servidor con un rendimiento óptimo contribuye a la estabilidad y escalabilidad de los servicios tecnológicos, aspecto que se materializó en la reducción de la carga operativa y la temperatura del procesador, indicadores de un funcionamiento más estable. Serrano et al. (2021) afirman que las herramientas avanzadas de supervisión pueden proporcionar datos en tiempo real sobre el estado del hardware y software, facilitando la detección temprana de problemas; esta capacidad fue determinante para que los administradores de EGEMSA pudieran anticipar fallas y redistribuir cargas de trabajo antes de que los servidores alcanzaran condiciones críticas. En lo referente a la temperatura de CPU, Serrano et al. (2021) explican que el monitoreo constante es fundamental para prevenir sobrecalentamientos, y González

et al. (2021) destacan que una temperatura elevada puede ser resultado de una carga excesiva de trabajo; la reducción de 18.25 °C registrada en el postest confirma que el monitoreo permitió gestionar adecuadamente la carga computacional, prolongando la vida útil del hardware. Finalmente, IBM (2023b) señala que solo las arquitecturas más robustas logran niveles de disponibilidad cercanos al 99.99 %, lo cual requiere la eliminación de puntos únicos de falla y la automatización del failover; aunque la presente investigación no alcanzó ese estándar de forma directa, los resultados demuestran un avance significativo hacia un modelo de gestión proactiva que sienta las bases para la mejora continua de la infraestructura del servidor.

A pesar de los resultados favorables obtenidos, es necesario señalar algunas limitaciones que deben considerarse en la interpretación de los hallazgos, en primer lugar, el diseño preexperimental de pretest y postest con un solo grupo no permite el control estricto de variables extrañas, lo cual limita la capacidad de atribuir la totalidad de las mejoras exclusivamente a la implementación del servidor de monitoreo, ya que factores como cambios en el personal técnico, variaciones estacionales en la demanda de servicios o actualizaciones paralelas de infraestructura podrían haber influido en los resultados. En segundo lugar, la investigación se centró en indicadores técnicos de desempeño, sin incorporar medidas de percepción o satisfacción del usuario final, variable que fue considerada en estudios como el de Montero (2022) y Guevara (2023), y que podría enriquecer la comprensión integral del impacto de la implementación.

Desde el punto de vista de la generalización y escalabilidad los resultados corresponden a una empresa específica del sector energético ubicada en la ciudad de Cusco, con una infraestructura compuesta por seis equipos de red, nueve servidores y un conjunto acotado de servicios críticos, lo cual limita la extrapolación directa de los hallazgos a organizaciones de mayor escala, diferente sector productivo o mayor complejidad

tecnológica. Sin embargo, la convergencia de los resultados con los reportados por Lizarraga y Ponce (2021) en una empresa privada de Lima, Guevara (2023) en una institución universitaria de Cajamarca y Montero (2022) en una empresa agroindustrial de Ecuador sugiere que las mejoras observadas responden a principios generales del monitoreo de infraestructura que trascienden el contexto específico de EGEMSA, lo que fortalece la validez externa del estudio dentro de los límites propios de un diseño preexperimental.

En cuanto a las posibilidades de escalabilidad de la solución implementada, la arquitectura basada en contenedores Docker con Zabbix, Grafana y MySQL sobre Ubuntu Server presenta características que favorecen su crecimiento progresivo. Al tratarse de una solución modular y de código abierto, es técnicamente viable ampliar la cobertura de supervisión hacia nuevas sedes operativas de EGEMSA, incorporar dispositivos adicionales mediante el protocolo SNMP sin requerir licenciamiento por nodo, integrar nuevos tipos de alertas o canales de notificación, y habilitar módulos de análisis predictivo basados en el histórico de métricas almacenado en la base de datos. Adicionalmente, IBM (2023c) señala que la tendencia actual en gestión de infraestructura avanza hacia el concepto de observabilidad, que no solo detecta cuándo algo falla, sino que permite identificar la causa raíz y anticipar comportamientos anómalos; en esa dirección, la plataforma implementada constituye una base técnica sólida sobre la cual es posible incorporar capacidades de análisis avanzado, inteligencia operacional y automatización de respuestas, lo que amplía significativamente el horizonte de aplicación de esta solución más allá del contexto inicial de la presente investigación.

Finalmente, los resultados corresponden a una empresa específica del sector energético en la ciudad de Cusco, lo cual limita la generalización de los hallazgos a organizaciones de diferentes sectores, tamaños o ubicaciones geográficas. No obstante, la convergencia de los resultados con los reportados en contextos organizacionales diversos,

como el sector avícola, telecomunicaciones gubernamentales, instituciones educativas y empresas tecnológicas, sugiere una tendencia consistente que fortalece la validez externa del estudio.

A partir de las limitaciones identificadas y los hallazgos obtenidos, se sugiere que futuras investigaciones consideren el empleo de diseños cuasiexperimentales con grupo de control para fortalecer la validez interna de los resultados. Asimismo, se recomienda ampliar el periodo de observación del postest para evaluar la sostenibilidad de las mejoras a lo largo del tiempo. La incorporación de variables cualitativas, como la satisfacción del usuario y la percepción del personal técnico, permitiría una comprensión más integral del impacto de los sistemas de monitoreo. Finalmente, se sugiere replicar este tipo de estudios en organizaciones de sectores estratégicos similares al energético, con el fin de generar evidencia acumulativa que permita establecer estándares de implementación y buenas prácticas sectoriales.

VI. Conclusiones

1. Los resultados obtenidos en el análisis estadístico permiten concluir que la implementación del servidor de monitoreo optimiza de manera significativa los servicios TI en la empresa EGEMSA S.A. Cusco, 2025. Las dimensiones evaluadas presentaron valores de significancia $p < .001$, lo que evidencia diferencias estadísticamente significativas entre el pretest y el postest. Asimismo, los rangos promedio muestran mejoras consistentes en cada aspecto analizado, reflejando reducciones importantes en los tiempos de respuesta, disminución en la duración de los incidentes, mayor disponibilidad de los servicios, y un uso más eficiente de los recursos de red y del servidor. Estos resultados confirman que la intervención tuvo un impacto positivo en el funcionamiento de los servicios TI, validando la hipótesis general.
2. Los resultados permiten concluir que la implementación del servidor de monitoreo optimizó de manera significativa la eficiencia operativa de los servicios TI en EGEMSA S.A. La diminución de los tiempos de respuesta y la transición hacia una detección automática de incidentes, respaldada por un valor de significancia $p < .001$, confirman mejoras sustanciales en la atención, resolución y gestión de eventos.
3. Los resultados estadísticos evidencian que la disponibilidad del servicio mejoró de forma considerable después de la implementación del servidor de monitoreo. La disminución del tiempo de afectación ante interrupciones, junto con el valor $p < .001$, demuestra una diferencia significativa entre el pretest y el postest. Estos hallazgos confirman que el sistema permitió responder con mayor rapidez a fallas y mantener los servicios operativos durante más tiempo.
4. La comparación entre el pretest y el postest muestra mejoras estadísticamente significativas en la duración de los incidentes de red y en la disponibilidad efectiva

de la infraestructura. La reducción del tiempo de indisponibilidad y el incremento de la estabilidad de la red, corroborados por un valor $p < .001$, indican que el servidor de monitoreo mejoró la gestión del tráfico y la detección temprana de fallas.

5. Los resultados obtenidos permiten concluir que el rendimiento del servidor mejoró significativamente con la implementación del sistema de monitoreo. Los análisis estadísticos reflejan disminuciones importantes en el uso de CPU, memoria RAM, almacenamiento y temperatura del procesador, lo que evidencia una operación más eficiente y estable del servidor. Con un valor $p < .001$ en todos los indicadores, se confirma una diferencia significativa entre el pretest y el postest.

VII. Recomendaciones

1. Se recomienda que la empresa EGEMSA S.A. considere el uso del servidor de monitoreo como parte fundamental de su estrategia de gestión de servicios TI. Esto implica integrar formalmente el sistema en los procesos de operación diaria, establecer un centro de alertas unificado, capacitar al personal técnico en análisis de métricas y asegurar la revisión continua de los indicadores clave de desempeño. La adopción sostenida del monitoreo permitirá mantener la optimización alcanzada, prevenir fallas, tomar decisiones basadas en datos y garantizar la continuidad operativa de los servicios TI en la organización.
2. Se recomienda que la empresa EGEMSA S.A. consolide el uso del servidor de monitoreo como herramienta principal para la detección temprana de incidentes, mejorando los mecanismos de alerta automática y estandarizando los procedimientos de atención. Dado que el sistema permitió reducir de manera significativa los tiempos de respuesta, es pertinente establecer protocolos formales que integren las alertas del monitoreo dentro del flujo operativo del personal TI, garantizando que cada evento sea atendido oportunamente. Asimismo, se sugiere realizar capacitaciones periódicas al equipo técnico para asegurar el uso eficiente de las funciones avanzadas del monitoreo, reduciendo aún más los tiempos de resolución.
3. Se recomienda mantener una supervisión continua a través del servidor de monitoreo, especialmente en los componentes críticos cuya caída afecta directamente la operatividad institucional. Es aconsejable que EGEMSA implemente políticas de mantenimiento preventivo basadas en la información histórica proporcionada por el sistema, priorizando aquellos servicios que presentaron mayor frecuencia de interrupciones en el pretest. Asimismo, se sugiere configurar accesos más estrictos de alerta con el fin de anticipar fallas y prevenir interrupciones futuras.

4. Se recomienda que la empresa realice un monitoreo más detallado del tráfico y la saturación en enlaces críticos, aprovechando las métricas proporcionadas por el servidor. Es importante establecer alertas tempranas para detectar patrones de congestión o deterioro del rendimiento. Asimismo, se sugiere complementar este monitoreo con auditorías periódicas del estado de los equipos de red y la verificación del uso adecuado de ancho de banda, garantizando que el sistema siga operando de forma estable y eficiente.
5. Se recomienda que EGEMSA continúe utilizando el servidor de monitoreo para supervisar de manera constante la carga del sistema y el funcionamiento de sus servicios internos. Además, se sugiere programar mantenimientos preventivos basados en las métricas recolectadas, ajustando parámetros de rendimiento, limpiando procesos innecesarios y optimizando los servicios ejecutados en el servidor. También es recomendable evaluar periódicamente la capacidad del hardware para anticipar necesidades de actualización y evitar futuros puntos de saturación.

VIII. Referencias bibliográficas

Ahmad, A., Maynard, S., Desouza, K., Kotsias, J., Whitty, M., & Baskerville, R. (2020). Cybersecurity Incident Response in Organizations: An Exploratory Case Study and Process Model of Situation Awareness. *Computers & Security*, 102122. https://doi.org/10.1016/j.cose.2020.102122

Arnarson, H., Mahdi, H., Solvang, B., & Bremdal, B. (2022). Towards automatic configuration and programming of a manufacturing cell. *Journal of Manufacturing Systems, 64*, 225-235. https://doi.org/10.1016/j.jmsy.2022.06.005

Bessen, J. (2020). Industry concentration and information technology. *Journal of Law & Economics, 63*(3), 531 - 556. https://scholarship.law.bu.edu/faculty_scholarship/267

Bringhenti, D., Marchetto, G., Sisto, R., & Valenza, F. (2023). Automation for Network Security Configuration: State of the Art and Research Trends. *ACM Computing Surveys, 56*(3), 1-37. https://doi.org/10.1145/3616401

Cacti.net. (s.f.). *Cacti*. http://www.cacti.net/

Canonical. (2023). *Ubuntu Server Monitoring and Best Practices*. Canonical Documentation. https://ubuntu.com/server/docs/

Casas, R., & Sempértegui, M. (2018). *Implementación de un sistema de monitoreo y supervisión de la infraestructura y servicios de red para optimizar la gestión de TI en la Universidad Nacional Pedro Ruiz Gallo*. [Tesis de pregrado, Universidad Nacional Pedro Ruiz Gallo]. https://repositorio.unprg.edu.pe/handle/20.500.12893/1576

Center for Internet Security. (2022). *CIS Benchmarks – Guías de configuración segura.* Center for Internet Security, Inc. https://www.cisecurity.org/cis-benchmarks-overview

Choudhury, S. (2024). Intelligent Network Optimization: Revolutionizing Network Management through AI and ML. *International Journal of Computer Engineering & Technology, 15*(6), 2075–2084. https://iaeme.com/Home/article_id/IJCET_15_06_178

Corado, R. (2022). Sistemas de información y monitoreo en negocios. *Realidad Empresarial*(13), 56-62. https://doi.org/10.51378/reuca.v1i13.7051

EezIT. (2024). *Overheating Nightmares: How Temperature Affects Your Computer's Performance.* https://eezit.ca/how-temperature-affects-computer-performance/

EGEMSA. (2022). *Plan de Gobierno Digital. Plan de Gestión TIC.* Comité de Gobierno Digital - EGEMSA. https://transparencia.egemsa.com.pe/static/archivos/bPlan_de_Gobierno_Digital_2022.pdf

Fernández, O. (2019). *Implementación de un servidor como gestión y monitoreo de servicios para la red de datos en la UGEL Huamanga, 2018.* [Tesis de pregrado, Universidad Nacional de San Cristóbal de Huamanga]. https://repositorio.unsch.edu.pe/handle/UNSCH/3612

Field, T. (2024). *Unpatched Vulnerabilities Cause 60% of Cyber Compromises.* BankInfoSecurity – ISMG: https://www.bankinfosecurity.com/unpatched-vulnerabilities-cause-60-cyber-compromises-a-26051

Garay, D. (2018). *Implementación de la herramienta Centreon para el monitoreo de la infraestructura de T.I. en la empresa América Móvil Perú S.A.C.* [Tesis de pregrado, Universidad Autónoma del Perú]. https://repositorio.autonoma.edu.pe/handle/20.500.13067/678

Geetha, M., Kingsy, R., Manju, S., & Krishna, V. (2020). PTCWA: Performance Testing of Cloud Based Web Applications. *Computational Vision and Bio-inspired Computing*, 345–356. https://doi.org/10.1007/978-3-030-41862-5_32

González, G., González, S., & Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors, 21*(14), 4759. https://doi.org/10.3390/s21144759

Govindappa, G. V. y Singh, A. (2024). CIS Benchmarks: Enhancing security configurations in multi-cloud infrastructures. *Iconic Research and Engineering Journals*, 8(5), 234–248. https://www.irejournals.com/paper-details/1706503

Guevara, N. (2023). *Sistema de monitoreo de infraestructura de TI para soporte a la gestión de recursos de la oficina de tecnologías de la información de la Universidad Nacional de Cajamarca.* [Tesis de pregrado, Universidad Nacional de Cajamarca]. https://repositorio.unc.edu.pe/handle/20.500.14074/6712

Gunawan, H., Pradipta, A., & Prima, J. (2024). Implementation of sustainable service improvement in organizations using framework information technology infrastructure library (ITIL). *Procedia Computer Science, 234*, 748 - 755. https://doi.org/10.1016/j.procs.2024.03.061

Hatt, M. (2025). *Server Hardening Standards for Security and Compliance.* Down to Earth Technology Blog: https://downtoearthtech.net/hardening-standards/

Hernández, R., & Mendoza, C. (2018). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta.* McGraw Hill. https://virtual.cuautitlan.unam.mx/rudics/?p=2612

IBM. (2021). *¿Qué es el monitoreo de red?* IBM Think Blog. https://www.ibm.com/mx-es/think/topics/network-

monitoring#:~:text=Un%20sistema%20de%20monitoreo%20de,parte%20de%20un%20ecosistema%20h%C3%ADbrido.

IBM. (2023a). *¿Qué es el monitoreo de servidores? IBM Think.* https://www.ibm.com/mx-es/think/topics/server-monitoring

IBM. (2023b). *What is High Availability?* IBM Think: https://www.ibm.com/think/topics/high-availability

IBM. (2023c). *Observability vs. Monitoring: What's the Difference?* IBM Think: https://www.ibm.com/think/topics/observability-vs-monitoring

IBM. (2025). *Supervisión de infraestructura con Instana Observability.* https://www.ibm.com/es-es/products/instana/infrastructure-monitoring

Junco, G., & Rabelo, S. (2018). Los recursos de red y su monitoreo. *Revista Cubana de Informática Médica, 10*(1), 76-83. https://revinformatica.sld.cu/index.php/rcim/article/view/260

Kumar, S., Ranjan, R., Brupati, Dutt, H., & Misra, Y. (2023). Failure log analytics for reducing electrical machine downtime using deep learning. *WSEAS Transactions on Information Science and Applications, 20*(46), 444-452. https://doi.org/10.37394/23209.2023.20.46

Laudon, C., & Laudon, J. (2019). *Management Information Systems: Managing the Digital Firm.* Pearson. https://books.google.co.cr/books?id=KD8ZZ66PF-gC&printsec=copyright#v=onepage&q&f=false

Lizárraga, E., & Ponce, Y. (2021). *Implementación de un Servidor de Monitoreo para optimizar la Gestión de Servicios TI en la empresa Precisa, 2021.* [Tesis de pregrado, Universidad Cesar Vallejo]. https://repositorio.ucv.edu.pe/handle/20.500.12692/79020

Lozada, J. (2014). Investigación aplicada: Definición, propiedad intelectual e industria. *CIENCIAMÉRICA*(3), 34-39. https://dialnet.unirioja.es/servlet/articulo?codigo=6163749

Montero, H. (2022). *Implementación de un sistema de monitoreo y control de la infraestructura de ti para la gestión de incidencias en la red interna de la empresa avícola Pollo Favorito S.A. (POFASA).* [Tesis de pregrado, Escuela Politécnica Nacional]. https://bibdigital.epn.edu.ec/handle/15000/23196?locale=de

Mora, M. G. (2015). An extensive review of IT service design in seven international ITSM processes frameworks: Part II. *International Journal of Information Technologies and Systems Approach, 8*(1), 69-90. https://doi.org/10.4018/ijitsa.2015010104

Nagios Enterprises. (s.f.). *Nagios.* https://www.nagios.org/

Nessus. (2023). *Nessus User Guide (Versión 10.5).* Tenable™ Network Security. https://docs.tenable.com/nessus/10_5/

OpenVAS / Greenbone Networks. (2023). *OpenVAS Documentation 22.4.* Greenbone/OpenVAS Project. https://www.greenbone.net/en/documents/

Oppenheimer, P. (2010). *Top-Down Network Design.* Cisco Press. https://faculty.kfupm.edu.sa/COE/marwan/richfiles/Cisco.Press.Top-Down.Network.Design.3rd.Edition.Aug.2010.pdf

Red Hat, Inc. (2023). *Securing and Hardening Red Hat Enterprise Linux 8.* Red Hat Official Documentation. https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/8/html/security_hardening/index

Robledo, S. (2023). *Implementación de un servidor de monitoreo de telecomunicaciones en la gobernación de Risaralda.* [Tesis de pregrado, Universidad Católica de Pereira].

https://repositorio.ucp.edu.co/entities/publication/c3a52e6a-63d2-49ab-90af-62e288a9f620

Sasidharan, R. (2022). A case study to implement Windows system hardening using CIS controls. *International Journal of Computer Trends and Technology*, 70(7), 1–7. https://doi.org/10.14445/22312803/IJCTT-V70I7P101

Selector. (2023). *Network Visibility: Components, Challenges, and Best Practices*. https://www.selector.ai/learning-center/network-visibility-components-challenges-and-best-practices/

Serrano, J., Faustino, J., Adriano, D., Pereira, R., & Mira da Silva, M. (2021). An IT Service Management Literature Review: Challenges, Benefits, Opportunities and Implementation Practices. *Information, 12*(3), 111. https://doi.org/10.3390/info12030111

Seun, E., Babajide, G., Taye, F., Aderonke, A., & Olabode, B. (2024). Impact of Information Systems on Operational Efficiency: A Comprehensive Analysis. *Indian Journal of Computer Science and Engineering, 14*(4), 661 - 673. https://www.researchgate.net/publication/373267444_Impact_of_Information_Systems_on_Operational_Efficiency_A_Comprehensive_Analysis

Shrestha, A., Cater-Steel, A., Toleman, M., Behari, S., & Mohammad, R. (2019). Development and evaluation of a software-mediated process assessment. *Information & Management*, *57*(4). https://doi.org/10.1016/j.im.2019.103213

Stallings, W. (2017). *Network Security Essentials: Applications and Standards.* Pearson Education. https://www.emgywomenscollege.ac.in/templateEditor/kcfinder/upload/files/Network-security-essentials.pdf

UptimeRobot. (2023). *The 6 Hidden Costs of Downtime*. https://uptimerobot.com/blog/hidden-costs-of-downtime/

Zabbix LLC. (2023). *Zabbix 6.0 Documentation – Overview and Best Practices.* Zabbix SIA. https://www.zabbix.com/documentation/6.0/en/start

Los anexos, panel fotográficos y otros documentos están resguardados en la oficina de repositorio digital institucional en la Biblioteca Central de la Universidad Tecnológica delos Andes.