ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

PROYECTO DE TITULACIÓN

"EVALUACIÓN DE UNA HERRAMIENTA OPEN SOURCE DE MONITOREO PARA TOMA DE DECISIONES EN UN DATACENTER "

PREVIO LA OBTENCIÓN DEL TÍTULO DE:

MAGISTER EN SISTEMAS DE INFORMACIÓN GERENCIAL

Autor: Wilson Andrés Gómez Cedeño

Tutor: Mgs. Juan Carlos García

Guayaquil - Ecuador

2025

AGRADECIMIENTO

Quiero expresar mi más sincero agradecimiento a todas las personas que me acompañaron y apoyaron en la realización de esta tesis.

A mis tutores, por su paciencia, orientación constante y valiosas enseñanzas que me permitieron crecer personal y profesionalmente durante este proceso.

Al equipo técnico del Data Center, por abrirme las puertas, brindarme su tiempo y colaboración incondicional, haciendo posible la ejecución práctica de esta investigación.

A mis compañeros y amigos, por su respaldo, consejos y motivación en cada momento.

Finalmente, agradezco profundamente a mi familia, cuyo apoyo emocional y constante ánimo han sido mi mayor fortaleza para alcanzar esta importante meta.

A todos ustedes, muchas gracia

DEDICATORIA

El presente proyecto lo dedico a con esposa Angélica Cruz y a mis hijos, Dallyana Gómez y Liam Gómez, quienes son mi mayor inspiración, fuerza y pilar fundamental en cada paso de mi vida.

A mis madres en el cielo, Sheyla Cedeño Loor e Petra Esperanza, cuyas luces y recuerdos siempre iluminan mi camino, guiando mis acciones con amor y sabiduría. A mi padre, Wilfrido Gómez, por brindarme su ejemplo, valores y enseñarme el valor del esfuerzo y la perseverancia.

A mis queridos abuelos, Roberto Cedeño y Wilson Gómez, quienes me enseñaron el significado del cariño, humildad y respeto, impulsándome siempre a ser mejor persona.

De manera especial, dedico este logro a un gran jefe y amigo, Carlos Marín, por su invaluable apoyo, consejos y confianza constante en mi desarrollo profesional.

DECLARACIÓN EXPRESA

Yo Wilson Andres Gomez Cedeño acuerdo y reconozco que:

La titularidad de los derechos patrimoniales de autor (derechos de autor) del proyecto de graduación corresponderá al autor o autores, sin perjuicio de lo cual la ESPOL recibe en este acto una licencia gratuita de plazo indefinido para el uso no comercial y comercial de la obra con facultad de sublicenciar, incluyendo la autorización para su divulgación, así como para la creación y uso de obras derivadas. En el caso de usos comerciales se respetará el porcentaje de participación en beneficios que corresponda a favor del autor o autores.

La titularidad total y exclusiva sobre los derechos patrimoniales de patente de invención, modelo de utilidad, diseño industrial, secreto industrial, software o información no divulgada que corresponda o pueda corresponder respecto de cualquier investigación, desarrollo tecnológico o invención realizada por mí/nosotros durante el desarrollo del proyecto de graduación, pertenecerán de forma total, exclusiva e indivisible a la ESPOL, sin perjuicio del porcentaje que me/nos corresponda de los beneficios económicos que la ESPOL reciba por la explotación de mi/nuestra innovación, de ser el caso.

En los casos donde la Oficina de Transferencia de Resultados de Investigación (OTRI) de la ESPOL comunique al/los autor/es que existe una innovación potencialmente patentable sobre los resultados del proyecto de graduación, no se realizará publicación o divulgación alguna, sin la autorización expresa y previa de la ESPOL.

Guayaquil, _____del 2025.

Firmado electrónicamente por:
WILSON ANDRES GOMEZ CEDENO
Validar únicamente con FirmaEC

_____

Wilson Andres Gomez Cedeño

TRIBUNAL DE SUSTENTACIÓN

Firmado electrónicamente por:
JUAN CARLOS GARCIA PLUA
Validar únicamente con FirmaEC

MGS. Juan Carlos García

TUTOR

Firmado electrónicamente por:
LENIN EDUARDO FREIRE COBO
Validar únicamente con FirmaEC

MGS. Lenin Eduardo Freire

REVISOR

RESUMEN

Este trabajo de titulación se centra en evaluar el uso de **Zabbix**, una herramienta open source de monitoreo, dentro de un Data Center real, con la intención de comprobar qué tan útil puede ser al momento de tomar decisiones importantes sobre la operación diaria. Hoy en día, centros de datos de distintos sectores como salud, banca, telecomunicaciones y servicios públicos son el corazón de muchas organizaciones, por lo que mantenerlos estables y vigilados es una prioridad.

Para realizar esta evaluación, se instaló y configuró Zabbix en un entorno real ubicado en Guayaquil, utilizando diferentes métodos de monitoreo como SNMP, IPMI y agentes propios de la herramienta. Se hicieron entrevistas, observaciones directas al personal operativo y una encuesta aplicada a 20 profesionales de distintas áreas del centro de datos. Esto permitió tener una visión completa, no solo desde lo técnico, sino también desde la experiencia de quienes trabajan con estas herramientas día a día.

Zabbix se comparó con otras soluciones, tanto libres como comerciales, y se determinó que destaca por su flexibilidad, capacidad de integración, y por no generar costos de licencias, lo que representa una ventaja importante. También se observó una mejora clara en la rapidez con la que el personal responde a eventos críticos, una reducción de alarmas innecesarias y una mejor lectura de la información a través de sus paneles visuales.

En conclusión, esta herramienta se presenta como una opción sólida para fortalecer el monitoreo de un Data Center, permitiendo actuar con mayor precisión, anticiparse a fallos y mantener la operación de manera eficiente y continua.

Palabras clave: Monitoreo, Zabbix, Data Center, herramientas libres, infraestructura crítica, alertas, decisiones operativas.

ABSTRACT

This thesis focuses on evaluating the use of Zabbix, an open-source monitoring tool, within a real data center, with the intention of verifying its usefulness when making important decisions about daily operations. Today, data centers in various sectors such as healthcare, banking, telecommunications, and public services are at the heart of many organizations, so keeping them stable and monitored is a priority.

To conduct this evaluation, Zabbix was installed and configured in a real environment located in Guayaquil, using different monitoring methods such as SNMP, IPMI, and the tool's own agents. Interviews were conducted, along with direct observations of operational staff and a survey was administered to 20 professionals from different areas of the data center. This provided a comprehensive overview, not only from a technical perspective, but also from the experience of those who work with these tools daily.

Zabbix was compared with other solutions, both free and commercial, and it was determined to stand out for its flexibility, integration capabilities, and lack of licensing costs, which represents a significant advantage. A clear improvement was also observed in the speed with which staff responded to critical events, along with a reduction in unnecessary alarms and improved information readability through its visual dashboards.

In conclusion, this tool is a solid option for strengthening data center monitoring, enabling more precise action, anticipating failures, and maintaining efficient and continuous operations.

Keywords: Monitoring, Zabbix, Data Center, open source tools, critical infrastructure, alerts, operational decisions.

1 Contenido

CAPÍTULO 1

1 INTRODUCCIÓN

En la actualidad, los centros de datos representan el núcleo operativo de muchas organizaciones, siendo responsables del almacenamiento, procesamiento y transmisión de grandes volúmenes de información. Sin embargo, a medida que estas infraestructuras se expanden en complejidad y tamaño, también lo hacen los desafíos relacionados con su monitoreo y gestión efectiva. La ausencia de un monitoreo adecuado puede generar fallas críticas, pérdida de datos, tiempos de inactividad y afectaciones directas a los servicios que dependen de estos sistemas. En este contexto, surge la necesidad de evaluar soluciones de monitoreo que, además de ser robustas, sean accesibles y adaptables a los entornos de trabajo modernos.

1.1 Justificación

El monitoreo de infraestructuras críticas dentro de un centro de datos no solo es una necesidad técnica, sino una responsabilidad operativa y estratégica. Sectores como el financiero, el de salud, telecomunicaciones y entidades gubernamentales dependen de la disponibilidad continua de sus sistemas informáticos para operar eficientemente. Una interrupción en la disponibilidad del centro de datos puede desencadenar consecuencias graves, como pérdidas económicas, afectación a la atención ciudadana o fallos en la prestación de servicios esenciales.

En este sentido, evaluar herramientas de código abierto, como Zabbix, permite validar su aplicabilidad en entornos reales, determinar su capacidad de respuesta ante eventos y su utilidad como soporte en la toma de decisiones. Además, al estar enfocada en herramientas Open Source, la investigación promueve soluciones sostenibles, accesibles y de bajo costo que pueden ser adoptadas incluso por organizaciones con recursos limitados.

1.2 Objetivos

1.3 Objetivo General

Evaluar la efectividad de la herramienta de código abierto Zabbix en la mejora de la toma de decisiones para la gestión y operación eficiente de un datacenter.

1.4 Objetivos Específicos:

• Identificar los requerimientos y aspectos clave de la gestión operativa mediante la observación directa del sistema de monitoreo del datacenter.

• Implementar un entorno de prueba real con Zabbix, configurando sus componentes para monitorear infraestructura crítica en el datacenter.

• Evaluar el rendimiento de Zabbix, considerando la visibilidad en tiempo real, generación de alertas y su capacidad para apoyar procesos de decisión.

1.5 Alcance

Este trabajo se centra en la evaluación de la herramienta Zabbix como solución de monitoreo dentro de un entorno real de datacenter. Se considera infraestructura de red, servidores, dispositivos eléctricos, sensores y sistemas de climatización. El estudio comprende desde el análisis de necesidades hasta la implementación de un prototipo funcional y la revisión de resultados obtenidos a través de métricas y observación directa.

1.6 Estructura del documento

El presente trabajo se encuentra estructurado en cuatro capítulos. El **Capítulo 1** aborda la introducción general al problema, estableciendo los objetivos, justificación, alcance y antecedentes del estudio. El **Capítulo 2** desarrolla el marco teórico, presentando los conceptos clave sobre centros de datos, herramientas de monitoreo, protocolos de comunicación y estándares aplicables. El **Capítulo 3** describe la metodología implementada, incluyendo la selección de herramientas, diseño conceptual, procesos de implementación, y análisis de encuestas. Finalmente, el **Capítulo 4** expone los resultados obtenidos, las conclusiones derivadas del proyecto y las recomendaciones para futuros trabajos relacionados.

1.7 MARCO TEÓRICO

1.8 Definición de Data Center

Un Data Center, también conocido como centro de datos, es una instalación física especialmente diseñada para albergar infraestructura tecnológica crítica, como servidores, dispositivos de almacenamiento, sistemas de redes y componentes eléctricos, que permiten el procesamiento, gestión y resguardo de grandes volúmenes de información. Estos espacios constituyen el núcleo operativo de las organizaciones modernas, proporcionando soporte continuo a aplicaciones y servicios esenciales.

Existen distintos tipos de Data Centers según su propiedad, finalidad o escala. Entre los más comunes están los centros empresariales (propios de la organización), los de colocation (alquiler de espacio a terceros), los hyperscale (utilizados por grandes proveedores como Google o Amazon) y los Edge Data Centers, más pequeños y distribuidos para reducir la latencia. Su diseño suele estar normado por estándares internacionales como ANSI/TIA-942 o el esquema TIER del Uptime Institute, que clasifica la infraestructura en niveles del I al IV según su grado de redundancia, disponibilidad y tolerancia a fallos.

En cuanto a la infraestructura, un Data Center integra diversos sistemas esenciales: suministro eléctrico redundante, sistemas de climatización (como chillers, UMAs), generadores de respaldo, tableros eléctricos, cableado estructurado y una amplia red de sensores que permiten supervisar condiciones como temperatura, humedad, consumo energético, fugas o ingreso de personal. Estos componentes garantizan la operación segura, continua y eficiente de los servicios tecnológicos.

El sistema eléctrico se basa normalmente en configuraciones duales (A y B) para asegurar redundancia. Esto implica doble alimentación a racks, fuentes ininterrumpidas de energía (UPS), bancos de baterías y generadores diésel que se activan ante cortes prolongados del servicio público. Asimismo, los sistemas de climatización como chillers (enfriadores de agua) y UMAs (Unidades Manejadoras de Aire) son vitales para mantener los equipos operando en condiciones térmicas adecuadas.

El diseño físico de un Data Center contempla múltiples aspectos como distribución en pasillos fríos y calientes, falso piso para cableado, sistemas contra incendios (como detección temprana por aspiración y extinción con agentes limpios), seguridad perimetral, control de accesos biométricos y vigilancia mediante CCTV. Cada uno de estos elementos forma parte de una arquitectura robusta y segura que permite responder a las crecientes exigencias de disponibilidad y protección de la información.

En resumen, un Data Center moderno va mucho más allá de ser una sala con servidores. Se trata de una infraestructura compleja, certificada y altamente especializada, pensada para sostener operaciones críticas en sectores como banca, salud, telecomunicaciones, comercio y administración pública.

1.9 Componentes de un Data Center

El ecosistema de un data center está compuesto por diferentes subsistemas altamente especializados. Cada uno cumple un rol fundamental para asegurar la continuidad y la eficiencia operativa. A continuación, se detalla cada componente con ejemplos de marcas, modelos predominantes y referencias técnicas que respaldan su elección.

1.10 Servidores de Cómputo

Los servidores constituyen el núcleo de procesamiento. Entre las familias más utilizadas se encuentran los Dell PowerEdge R760, los HPE ProLiant DL380 Gen11 y los Lenovo ThinkSystem SR650 V3. Estos modelos ofrecen procesadores Intel Xeon Scalable de última generación, memoria DDR5 y opciones de aceleradores GPU para cargas de IA. Su elección se basa en criterios de rendimiento, escalabilidad y soporte posventa [1], [2].

1.11 Dispositivos de Almacenamiento

Para almacenamiento de alta disponibilidad se destacan las cabinas all-flash NetApp AFF A400 y Dell EMC PowerStore 500T, que emplean NVMe para reducir la latencia. En entornos híbridos, soluciones como HPE Nimble HF20 combinan SSD y HDD con compresión y deduplicación en línea [3].

1.12 Equipos de Red

La conectividad se basa en switches de núcleo como Cisco Nexus 9000 o Arista 7050X3, compatibles con 25/40/100 GbE. Para segmentación y seguridad, firewalls de próxima generación como Palo Alto PA-3450 o Fortinet FortiGate 4000F aseguran políticas de microsegmentación [4].

1.13 Suministro Eléctrico y UPS

La energía ininterrumpida se garantiza mediante UPS modulares Schneider Electric Galaxy VX y Vertiv Liebert EXM2, capaces de operar en paralelo N+1. Complementan esta solución los generadores diésel Cummins C1100D5 o MTU 16V4000, que soportan cargas críticas durante apagones prolongados [5].

1.14 Sistemas de Enfriamiento

Para climatización se utilizan chillers enfriados por aire Carrier Aquaforce 30XV y unidades CRAH/CRAC Vertiv Liebert DSE. Las UMAs (Unidades Manejadoras de Aire) de precisión Stulz CyberAir 3PRO regulan temperatura y humedad, integrando control EC Fans de alta eficiencia [6].

1.15 Sensores y Monitoreo Ambiental

Se emplean sensores IoT de temperatura y humedad (por ejemplo, APC NetBotz NBWS100T) y detectores de fuga de agua RLE LD2100. Estos dispositivos reportan vía SNMP o Modbus TCP a la plataforma DCIM y a Zabbix para generar alertas tempranas [7].

1.16 Racks y Cableado

Los racks de estándar 42U de la serie APC NetShelter SX o Panduit Net-Access CX proporcionan gestión de cables y opciones de PDU inteligentes. El cableado estructurado Cat 6A o fibra OM4 asegura 10/40/100 Gbps, siguiendo la norma ANSI/TIA-942-B [8].

1.17 Enclosures y Servidores Blade

Para altas densidades se utilizan chasis blade o enclosures. Ejemplos destacados son el Huawei FusionServer E9000, el Dell PowerEdge MX7000 y el HPE Synergy 12000. Estos chasis integran alimentación redundante, mid-plane de alta velocidad (25/40 GbE) y módulos de refrigeración líquida opcionales. Cada blade puede equipar procesadores Intel Xeon o AMD EPYC de última generación, hasta 4 TB de RAM y tarjetas mezzanine de 100 GbE. La arquitectura modular simplifica el escalado horizontal al agregar blades en caliente, reduciendo el cableado y optimizando la gestión con iDRAC, iLO o Huawei iBMC.

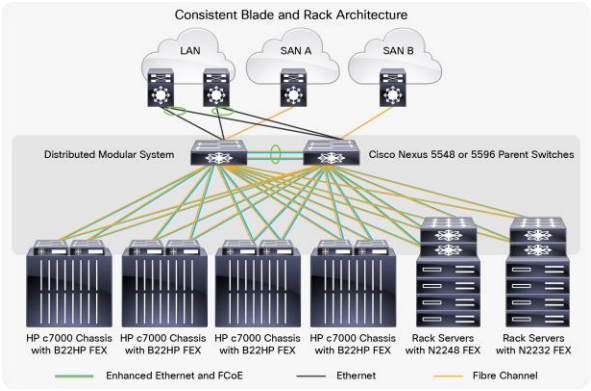
1.18 Matrices de Almacenamiento Empresarial

Además de las cabinas all-flash mencionadas, los data centers de misión crítica incorporan arreglos híbridos como Huawei OceanStor Dorado 6000 V6 y IBM FlashSystem 5200. Estos sistemas soportan replicación síncrona, snapshots y cifrado AES-256 por hardware. Para cargas de archivos masivos se emplean NAS escalables Dell

PowerScale F900 con OneFS, mientras que soluciones de respaldo utilizan librerías de cintas LTO-9 de Quantum Scalar i6000.

1.19 Backbone Nexus Multicapas

El backbone propuesto se basa en switches modulares Cisco Nexus 7000 en capa de núcleo, Nexus 5000 como distribución y Nexus 2000 FEX en acceso, formando una malla de 100 GbE. El protocolo predominante de descubrimiento y monitoreo es SNMP v3 por su soporte nativo y cifrado, complementado con IPMI para la gestión fuera de banda de servidores y chasis.



1.20 Tableros y Medidores Eléctricos

La energía se distribuye mediante tableros eléctricos Schneider PrismaSeT con barras de cobre 3200 A y breakers inteligentes Micrologic. Los medidores Schneider PowerLogic PM8000 ofrecen monitoreo en tiempo real (Modbus/TCP) de voltaje, armónicos y factor de potencia, integrándose con Zabbix. Los UPS de 200 kVA y 1600 kVA (Vertiv Liebert EXL S1) operan en topología de doble conversión y eficiencia ≥97 % en modo eco.

1.21 Cableado y Normativas

El cableado troncal adopta fibras OM4 multimodo en topología MTP/MPO de 12 y 24 fibras, aptas para 100 Gbps hasta 150 m. El cobre horizontal es Cat 6A F/UTP blindado, cumpliendo ANSI/TIA-568.2-D y certificado para 10 Gbps. Las canaletas y bandejas soportan radio de curvatura mínimo de 30 mm para fibra.

1.22 Herramientas de Monitoreo Open Source

En el ámbito de la supervisión de infraestructuras tecnológicas, las herramientas de monitoreo open source han cobrado una relevancia significativa, especialmente en entornos donde se prioriza la escalabilidad, la flexibilidad y la optimización de recursos sin incurrir en costos de licenciamiento. Este tipo de soluciones permite a las organizaciones implementar sistemas de monitoreo robustos, adaptables y altamente configurables, contribuyendo a la continuidad operativa y al análisis proactivo de fallos. A continuación, se detallan las características fundamentales de algunas de las herramientas open source más destacadas en el mercado: **Zabbix**, **Prometheus**, **Nagios**, **Pandora FMS** e **Icinga**.

1.23 Zabbix como Plataforma Integral de Monitoreo

Zabbix es una herramienta open source ampliamente utilizada para el monitoreo de infraestructuras IT. Permite la supervisión de redes, servidores, aplicaciones, y servicios en tiempo real. Gracias a su arquitectura modular, Zabbix puede adaptarse tanto a pequeñas empresas como a grandes corporaciones con múltiples sedes.

1.24 Zabbix

Zabbix es una solución de monitoreo integral que permite supervisar redes, servidores, aplicaciones y servicios en tiempo real. Su arquitectura se basa en un modelo centralizado que puede escalar horizontalmente mediante el uso de proxies distribuidos. Este sistema ofrece soporte nativo para protocolos como SNMP, IPMI, ICMP, y puede integrarse con agentes personalizados, scripts o APIs. Una de sus fortalezas más destacables es su interfaz web intuitiva, que proporciona paneles visuales personalizables, mapas de red, alertas automáticas y gráficos históricos.

Además, Zabbix se caracteriza por su enfoque preventivo, permitiendo establecer umbrales de alerta, acciones automatizadas y correlación de eventos para una detección temprana de problemas. Al ser completamente open source bajo la licencia GPLv2, no requiere ningún tipo de inversión en licencias, lo cual lo convierte en una opción altamente atractiva para organizaciones que buscan un sistema potente sin comprometer el presupuesto.

1.25 Prometheus

Prometheus es una herramienta de monitoreo orientada principalmente a la recolección y análisis de métricas de series temporales. Desarrollada inicialmente por SoundCloud, y ahora parte del ecosistema Cloud Native Computing Foundation (CNCF), esta solución está optimizada para entornos dinámicos como microservicios, contenedores y plataformas orquestadas con Kubernetes. A diferencia de sistemas tradicionales, Prometheus utiliza un modelo de recolección tipo *pull* y expone métricas a través de endpoints HTTP que pueden ser consultados periódicamente.

Su motor de consultas, PromQL, permite realizar análisis detallados sobre las métricas recolectadas, facilitando la detección de patrones de comportamiento y anomalías en el rendimiento. Aunque no cuenta con una interfaz de visualización avanzada por defecto, se integra de manera nativa con **Grafana**, herramienta que complementa su potencia analítica con dashboards personalizables. No obstante, su funcionalidad en entornos tradicionales (como SNMP o IPMI) es limitada, siendo necesaria la incorporación de *exporters* específicos para habilitar dicha compatibilidad.

1.26 Nagios

Nagios es una de las plataformas de monitoreo más veteranas y reconocidas dentro del software libre. Se enfoca principalmente en la supervisión de la disponibilidad y el estado de componentes críticos de la infraestructura TI, como servidores, switches, aplicaciones y servicios. Su diseño modular permite una extensibilidad considerable mediante el uso de plugins, lo que facilita su adaptación a diversos entornos.

Sin embargo, uno de los desafíos más frecuentes en su adopción es la complejidad que conlleva su configuración, especialmente cuando se busca cubrir una gran cantidad de dispositivos o métricas. A pesar de estas limitaciones, Nagios sigue siendo una alternativa sólida cuando se requiere una solución estable, con una comunidad amplia y recursos de documentación extensos.

1.27 Pandora FMS

Pandora FMS es una plataforma de monitoreo flexible que combina capacidades de supervisión de infraestructura, redes, sistemas operativos, aplicaciones y entornos virtualizados. Destaca por su interfaz gráfica intuitiva y su modelo híbrido de monitoreo, que permite tanto la recolección activa como pasiva de datos.

Aunque Pandora FMS cuenta con una versión gratuita open source, muchas de sus funcionalidades avanzadas, como el monitoreo en entornos distribuidos o el uso de agentes especializados, están reservadas para la edición Enterprise, que requiere de licenciamiento. Esta diferenciación limita su implementación total en proyectos donde se busca una solución completamente libre. Aun así, su versatilidad y enfoque integral la convierten en una opción a considerar en entornos mixtos.

1.28 Icinga

Icinga nació como un *fork* del proyecto Nagios, con el objetivo de mejorar su rendimiento, interfaz de usuario y capacidades de integración. A lo largo del tiempo, Icinga ha evolucionado como una solución propia, incorporando una API REST moderna, mayor escalabilidad y una mejor experiencia de usuario en la gestión de la infraestructura monitoreada.

Pese a estas mejoras, Icinga hereda algunas de las limitaciones de Nagios, como la fuerte dependencia de plugins para lograr una cobertura funcional completa, lo que implica mayor esfuerzo en configuraciones avanzadas. No obstante, su comunidad activa, documentación clara y enfoque en la automatización mediante herramientas modernas, la posicionan como una alternativa sólida para quienes buscan una evolución del entorno Nagios sin abandonar sus principios base.

CAPÍTULO 2

2 METODOLOGÍA

La presente investigación adopta una metodología de tipo descriptiva, no experimental y de enfoque mixto, con el objetivo de evaluar la efectividad de la herramienta de monitoreo Zabbix en un entorno real de datacenter. El estudio se apoya en dos pilares: la observación directa del sistema implementado y la percepción de los usuarios clave mediante la aplicación de encuestas estructuradas.

Alternativas de solución

Durante la etapa inicial se consideraron diversas herramientas de monitoreo como alternativas potenciales para su implementación en el entorno del data center. Entre ellas se destacaron **Nagios**, **Pandora FMS**, **Icinga**, **Zabbix** y **Prometheus**. Cada una de estas opciones ofrece diferentes ventajas, pero también presenta limitaciones.

- **Nagios**: Alta modularidad, pero complejidad de configuración y dependencia de complementos externos para funciones avanzadas.
- **Pandora FMS**: Interfaz intuitiva y flexible, pero requiere licenciamiento para acceder a todas sus funcionalidades en entornos de gran escala.
- **Icinga**: Derivado de Nagios con mejoras en visualización y rendimiento, aunque conserva la dependencia de plugins externos.
- **Zabbix**: Solución completa e integrada, sin costos de licenciamiento, con soporte nativo para múltiples protocolos (SNMP, IPMI, agentes, etc.) y una interfaz web avanzada.
- **Prometheus**: Altamente escalable y orientado a arquitecturas modernas como microservicios y contenedores, pero requiere herramientas adicionales como Grafana para visualización y no ofrece soporte nativo para tecnologías tradicionales como SNMP sin configuración adicional.

2.1 Selección de la mejor alternativa

Tabla I. Comparación de funcionalidades entre herramientas de monitoreo Open Source

Característica	Zabbix	Nagios	Pandora	Icinga	Prometheus
Licencia gratuita	Sí	Sí	Sí	Sí	Sí
Soporte comercial disponible	Sí	No	Sí	Sí	No
Recolección distribuida nativa	Sí	No	Sí	Sí	Posible
Almacenamiento escalable	Sí	No	Sí	Sí	Sí
Alertas configurables	Sí	Sí	Sí	Sí	Sí
Dashboards integrados	Sí	No	Sí	Sí	No
Descubrimiento automático	Sí	No	Sí	Sí	Sí
Soporte SNMP	Sí	Sí	Sí	Sí	No
Curva de aprendizaje baja	Posible	No	Sí	Posible	Posible
Integración con Grafana	Sí	Sí	Sí	Sí	Sí
Multiplataforma	Sí	Sí	Sí	Sí	Sí
Configuración vía interfaz web	Sí	No	Sí	Sí	No
Monitorización de red (infraestructura)	Sí	Sí	Sí	Sí	No
Escalabilidad horizontal	Sí	No	Sí	Sí	Sí
Soporte para agentes activos	Sí	No	Sí	Sí	No

Datos tomados de la documentación oficial de cada herramienta (2024).

Comparativa entre las herramientas Open Source

Herramienta	Sí	No	Posible
Zabbix	15	0	0
Nagios Core	8	6	1
Pandora FMS	15	0	0
Icinga	14	0	1
Prometheus	9	5	2

Luego entre las más parecidas queda Zabbix Vs Prometheus

Categoría	Zabbix	Prometheus
Tipo de arquitectura	Centralizada (cliente-servidor)	Descentralizada (basada en pull + exporters)
Filosofía de monitoreo	Basado en eventos, disponibilidad y alertas	Basado en métricas de series temporales
Instalación	Requiere base de datos, frontend, agentes y/o SNMP	Binario autónomo, configuración mediante archivos YAML
Método de recolección	Push y pull: agentes, SNMP, IPMI, Trapper	Principalmente Pull, vía HTTP usando exporters
Visualización nativa	Interfaz web completa, dashboards integrados	Visualización básica, generalmente usa Grafana
Alertas y notificaciones	Triggers, dependencias, múltiples canales, acciones automatizadas	Alertmanager externo, configuración mediante reglas
Curva de aprendizaje	Media (interfaz amigable pero configuración compleja en entornos grandes)	Media-alta (requiere dominar PromQL y estructura modular)
Escalabilidad	Alta, usando proxies y nodos distribuidos	Muy alta, ideal para ambientes con microservicios y contenedores
Histórico de datos	Guardado en base de datos relacional (MySQL, PostgreSQL)	Almacenamiento TSDB propio, limitado (usa Thanos/Cortex para largo plazo)
Retención de datos	Controlada por política de base de datos	Retención local predeterminada (configurable)
Soporte para SNMP	Sí, robusto y nativo	Limitado, requiere exporters adicionales
Orientación a infraestructura	Muy buena (redes, servidores, energía, etc.)	Básica, no está orientado a infraestructura tradicional
Orientación a microservicios	Limitada	Muy buena, se integra con Kubernetes, Docker, etc.
Integraciones	APIs, scripts, mensajería, herramientas IT tradicionales	Grafana, Loki, Jaeger, Kubernetes, etc.
Licencia	Open Source (GPLv2)	Open Source (Apache 2.0)

Tras un análisis comparativo, se seleccionó Zabbix como la mejor alternativa por su capacidad de integración, bajo costo, comunidad activa y escalabilidad. La herramienta permite monitoreo por SNMP, IPMI, Modbus TCP/RTU, ICMP, SSH, entre otros protocolos, vs Prometheus lo que facilita su adopción en infraestructuras heterogéneas como las de un data center

Tabla 2. Comparación de protocolos entre herramientas de monitoreo Open Source

Protocolos	Zabbix	Nagios	Pandora FMS	Icinga	Prometheus
SNMP v2/v3	1	1	1	1	0 (*)
IPMI	1	0	1	0	0
ICMP	1	1	1	1	0 (**)
Modbus TCP/RTU	1	0	0	0	0
SSH	1	1	1	1	0 (***)
HTTP/HTTPS	1	1	1	1	1
MQTT	1	0	1	0	0 (****)
Zabbix Agent	1	1	1	1	0
Redfish	1	0	0	0	0

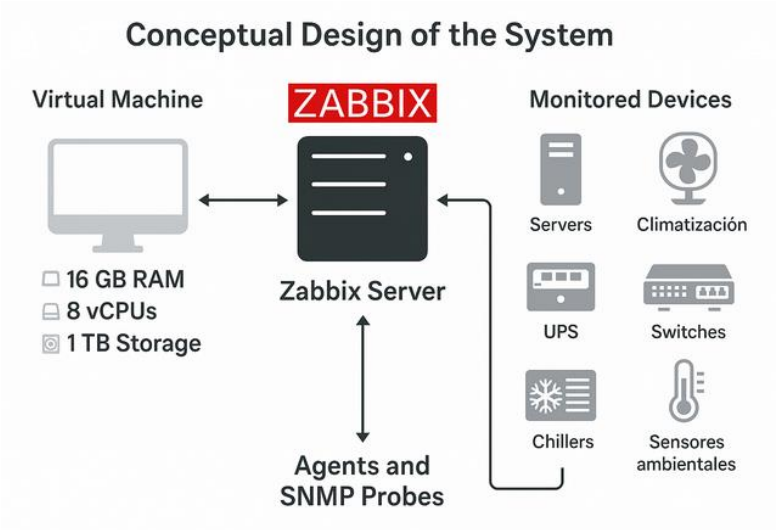
Datos tomados de la documentación oficial de cada herramienta (2024).

Notas:

- (*) Prometheus no soporta SNMP de forma nativa, pero puede hacerlo con **exporters** adicionales como snmp_exporter, aunque requiere configuración avanzada.
- (**) ICMP puede ser monitoreado indirectamente a través de exporters externos como blackbox_exporter.
- (***) Prometheus no utiliza SSH como método de recolección directa; requiere métricas expuestas por endpoints HTTP.
- (****) Para MQTT, existen soluciones externas como mqtt_exporter, pero no son soporte nativo.

2.2 Arquitectura de Zabbix Implementada

El diseño conceptual se basó en la implementación de una instancia de Zabbix Server sobre una máquina virtual Ubuntu 22.04 LTS, con 16 GB de RAM, 1 TB de almacenamiento y 8 vCPUs. Esta instancia actúa como núcleo de monitoreo central, integrando agentes Zabbix y sondas SNMP para recolectar datos de servidores, climatización, UPS, switches, chillers y sensores ambientales.



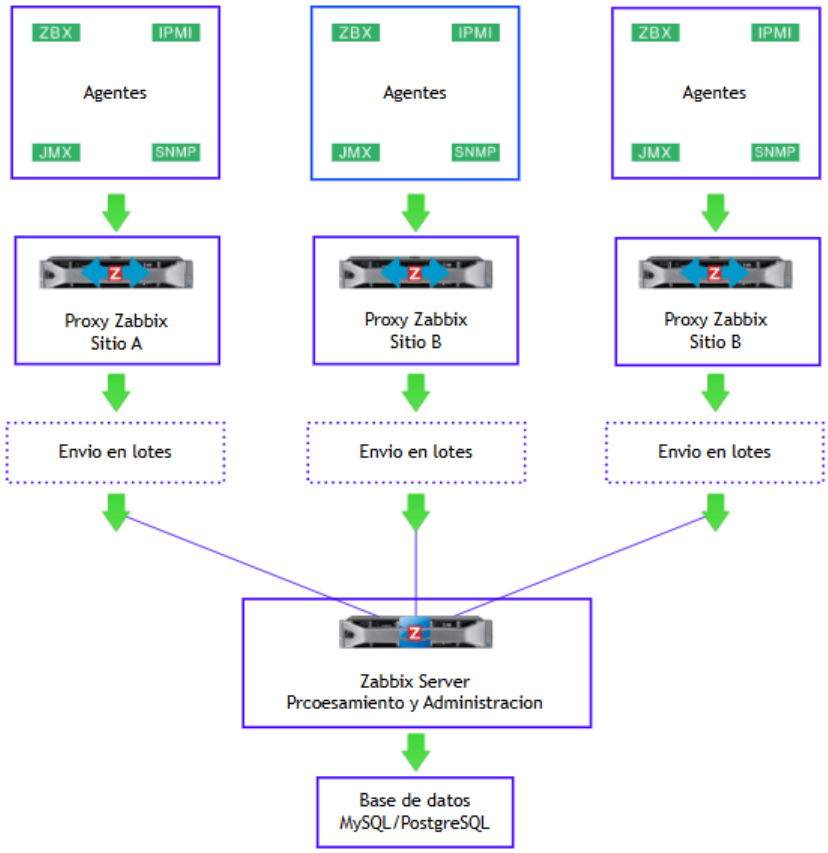
En entornos de centros de datos a gran escala, se adoptó una arquitectura descentralizada mediante la implementación de proxies Zabbix. Estos elementos funcionaron como nodos intermedios encargados de recolectar métricas localmente desde distintos segmentos de la infraestructura. Posteriormente, los datos fueron enviados en bloques hacia el servidor principal, lo cual permitió disminuir considerablemente la carga directa sobre el Zabbix Server y optimizar el uso del ancho de banda en redes distribuidas del datacenter.

Información del sistema

Parámetro	Valor	Detalles
El servidor Zabbix se está ejecutando	Sí	.10051
Versión del servidor Zabbix	7.0.12	
Versión de interfaz de Zabbix	7.0.16	
Número de equipos (habilitados/deshabilitados)	1107	1001 / 106
Número de plantillas	408	
Número de métricas (habilitadas/deshabilitadas/no soportadas)	414794	339536 / 63849 / 11409
Número de iniciadores (habilitados/deshabilitados [problema/ok])	180456	168765 / 11691 [88 / 168677]
Número de usuarios (en línea)	67	10
Rendimiento de servidor requerido, nuevos valores por segundo	2953.12	
Clúster de alta disponibilidad	Desactivado	

La arquitectura típica del sistema implementado en el centro de datos estuvo compuesta por varios elementos fundamentales que permitieron su operación eficiente:

- **Servidor Zabbix**: actuó como el núcleo central del sistema, encargado del almacenamiento histórico, procesamiento de eventos, administración general de la plataforma, generación de reportes y coordinación del sistema de alertas.
- **Proxies Zabbix**: desempeñaron el papel de intermediarios estratégicos en entornos distribuidos. Estos proxies recolectaron métricas desde dispositivos locales dentro de distintas zonas del datacenter, minimizando el tráfico directo al servidor principal y asegurando una entrega eficiente y estructurada de los datos.
- **Bases de Datos**: se utilizó PostgreSQL, optimizada para soportar altos volúmenes de escritura y consultas concurrentes, garantizando el rendimiento necesario para almacenar y recuperar información en tiempo real sin comprometer la estabilidad del sistema.



2.3 Flujo de Datos y Comunicación

En el entorno del centro de datos, el flujo de datos entre los componentes del sistema de monitoreo resultó determinante para garantizar la eficiencia operativa y la detección temprana de incidentes críticos. La comunicación se estructuró de la siguiente manera:

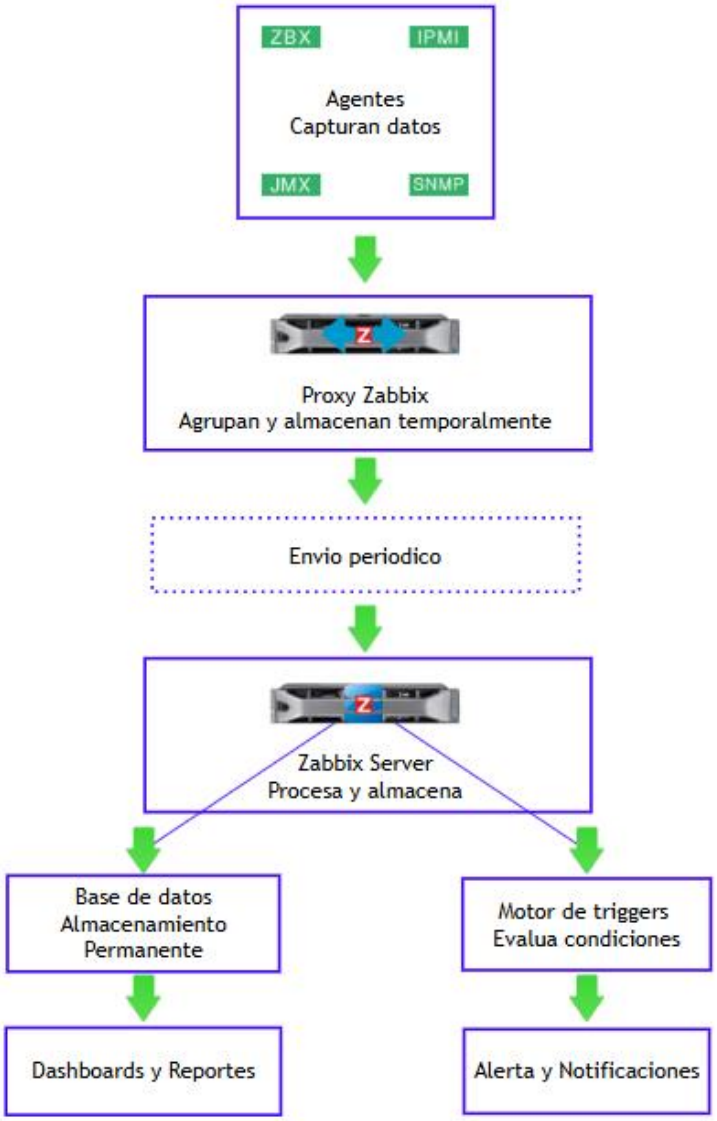
- **Agentes Zabbix y sondas SNMP**: fueron desplegados en servidores, switches, sistemas de almacenamiento y otros dispositivos clave, permitiendo la captura constante de métricas como uso de CPU, temperatura, voltaje, estado de servicios y conectividad. Esto facilitó una supervisión precisa y en tiempo real de la infraestructura física y lógica del datacenter.

- **Proxies Zabbix**: operaron como nodos descentralizados encargados de recolectar, almacenar temporalmente y organizar los datos generados localmente. Su implementación permitió reducir la latencia de red y descongestionar la comunicación directa con el servidor central. Periódicamente, estos proxies se sincronizaban con el servidor principal, enviando los lotes de información estructurada para su análisis.

- **Servidor Zabbix**: fue el punto de procesamiento central, donde se recibieron y almacenaron de forma permanente todas las métricas en una base de datos PostgreSQL. En este servidor se ejecutaron los *triggers*, encargados de detectar condiciones anómalas en tiempo real. Además, se aplicaron reglas de correlación, análisis históricos y modelos predictivos para anticiparse a posibles fallos.

- **Visualización y alertas**: se diseñaron *dashboards* personalizados para cada equipo operativo (energía, climatización, conectividad, virtualización, etc.), permitiendo una visualización clara de los indicadores clave. Las alertas fueron configuradas para ser enviadas automáticamente a través de múltiples canales, incluyendo correo electrónico, Telegram y plataformas colaborativas como Slack. Asimismo, se integraron con herramientas de gestión de eventos empresariales como IBM OMNIbus, fortaleciendo la respuesta inmediata ante incidentes críticos.

Esta arquitectura de flujo garantizó un monitoreo continuo, eficaz y adaptable a las necesidades específicas del centro de datos.

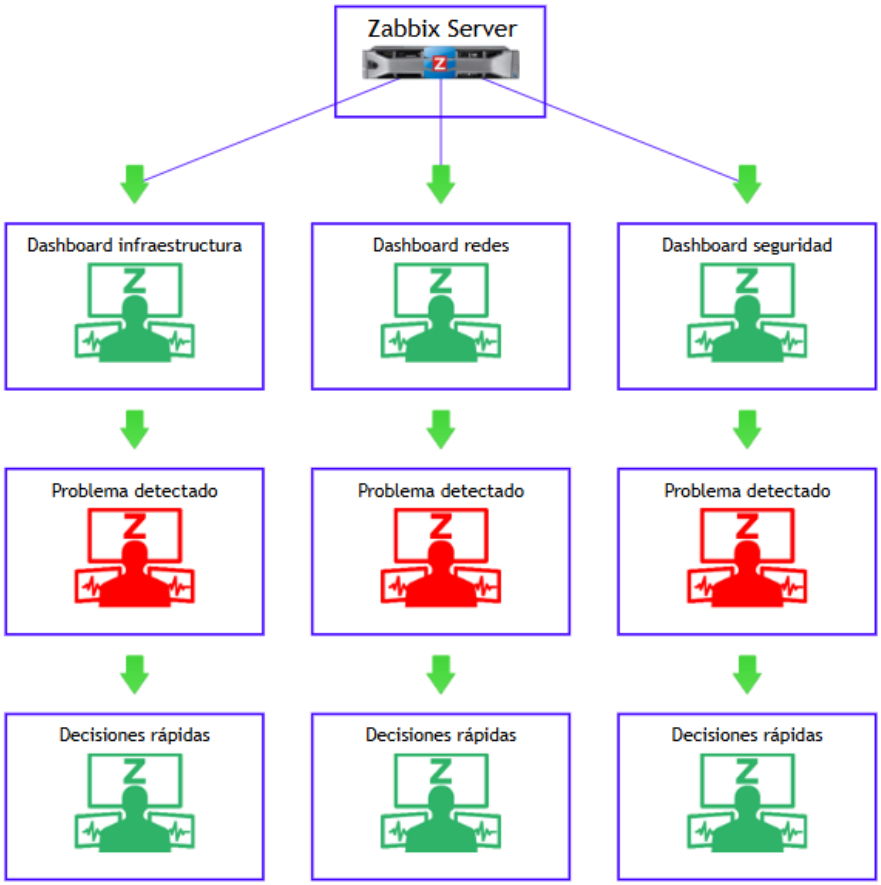


2.4 Dashboards efectivos por rol o área

Durante la implementación del sistema de monitoreo, se diseñaron *dashboards* personalizados dirigidos a cada equipo operativo del centro de datos, tales como infraestructura, aplicaciones, redes y seguridad. Esta segmentación permitió que cada grupo visualizara exclusivamente los indicadores relevantes a su función, lo que facilitó una interpretación rápida y una toma de decisiones más precisa y eficiente.

Se incorporaron *widgets* especializados como **Top Hosts**, **Top Triggers** y **Problems**, los cuales permitieron destacar de inmediato los equipos con más incidencias, los eventos activos de mayor criticidad y las alertas no resueltas. Esta configuración visual contribuyó directamente a la detección temprana de problemas, reduciendo los tiempos de reacción y mejorando la proactividad del personal técnico.

La personalización por roles demostró ser una estrategia eficaz para garantizar que cada área se mantuviera informada en tiempo real sobre el estado de los recursos bajo su responsabilidad.



2.5 Mejores prácticas para optimizar el rendimiento

Durante la implementación del sistema de monitoreo en el centro de datos, se aplicaron diversas prácticas orientadas a asegurar un rendimiento óptimo y sostenible frente al volumen creciente de dispositivos y métricas recolectadas:

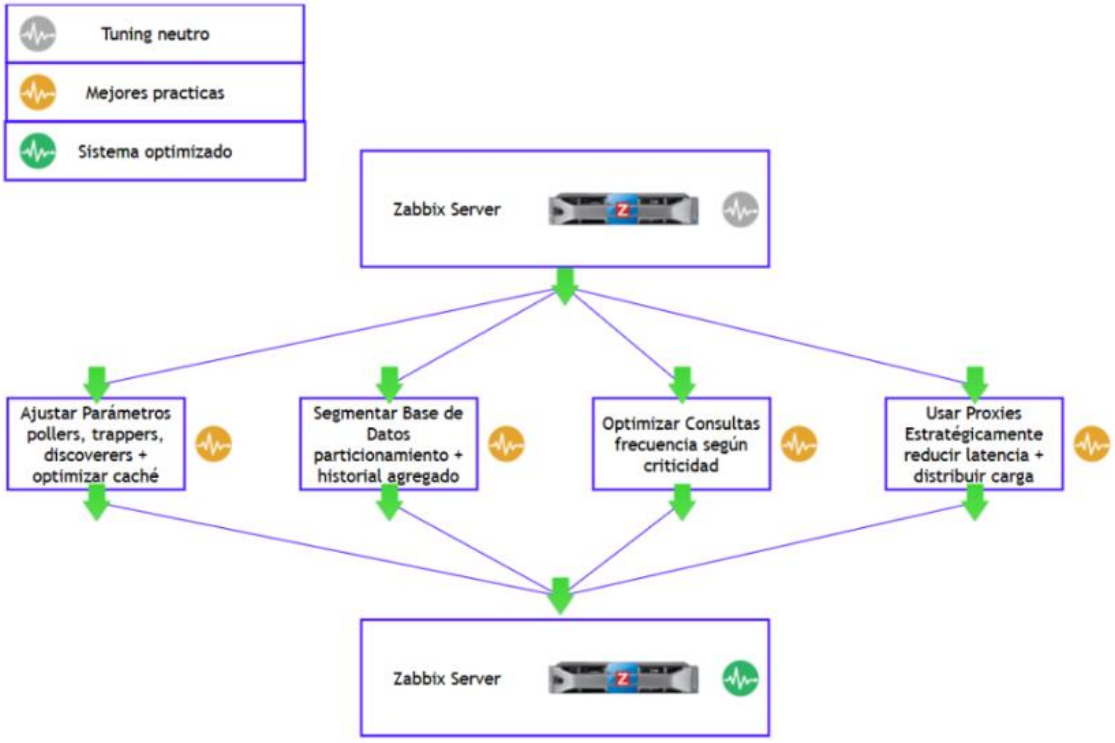
- **Ajuste de parámetros de rendimiento**: Se configuró cuidadosamente el archivo zabbix_server.conf, aumentando el número de *pollers*, *trappers* y *discoverers*, de acuerdo con la cantidad de elementos monitoreados. También se optimizó el uso de *caché interno*, asegurando una respuesta eficiente del servidor bajo cargas elevadas.

- **Segmentación de bases de datos**: Para mantener el desempeño a largo plazo, se aplicaron técnicas de particionamiento de datos y consolidación de históricos. Esto permitió manejar grandes volúmenes de registros sin afectar la velocidad de consulta o la integridad del sistema.

- **Optimización de consultas**: Se ajustaron los intervalos de chequeo de acuerdo con la criticidad de cada activo monitoreado. Los sistemas esenciales para la operación del negocio fueron priorizados con frecuencias más cortas, mientras que elementos secundarios utilizaron intervalos extendidos, reduciendo así la carga innecesaria.

- **Uso estratégico de proxies Zabbix**: Se desplegaron *proxies* de forma distribuida en ubicaciones remotas y redes segmentadas. Esto permitió reducir latencias, minimizar la congestión hacia el servidor principal y asegurar una recolección eficiente incluso en entornos con conectividad variable.

Estas prácticas, al aplicarse en conjunto, permitieron escalar el sistema de monitoreo de forma controlada, asegurando tanto estabilidad como capacidad de respuesta en entornos de misión crítica.



2.6 Escalabilidad horizontal vs. Vertical en Zabbix

Durante la implementación del sistema de monitoreo, se consideraron dos enfoques complementarios de escalabilidad para garantizar el crecimiento sostenible de la plataforma sin comprometer el rendimiento:

- **Escalabilidad vertical**: Consistió en mejorar progresivamente la capacidad del servidor central de Zabbix, ampliando recursos como CPU, memoria RAM y almacenamiento. Este tipo de escalabilidad resultó útil en fases iniciales del proyecto, donde centralizar el procesamiento facilitaba la configuración y el control del entorno.

- **Escalabilidad horizontal**: A medida que el número de dispositivos monitoreados creció y las métricas aumentaron, fue necesario distribuir la carga utilizando proxies Zabbix. Esta estrategia permitió procesar y almacenar datos de forma descentralizada, evitando cuellos de botella en el servidor principal. Así, se logró mantener la eficiencia operativa, incluso en condiciones de alta demanda, sin comprometer la latencia ni la integridad de los datos.

2.7 Normativas y principios técnicos

Se consideraron las siguientes normativas y buenas prácticas:

- TIA-942: Estandarización de infraestructura física de data centers.
- ISO/IEC 27001: Gestión de la seguridad de la información.
- Uptime Institute: Clasificación por niveles de disponibilidad (Tier I a IV).
- ITIL: Mejores prácticas en gestión de operaciones TI.

Criterios de diseño, materiales y componentes

Se priorizó la escalabilidad, bajo consumo de recursos y capacidad de integración con equipos existentes. Los criterios principales fueron:

- Compatibilidad con protocolos estándares.
- Soporte para monitoreo de sistemas físicos y virtuales.
- Capacidad de generar alertas personalizables.

Los componentes utilizados incluyen servidores, sensores, switches, UPS, chillers y herramientas de cableado estructurado categoría 6A.

2.9 Especificaciones técnicas del entorno de monitoreo

El entorno de prueba contó con:

- 1 servidor virtual Ubuntu 22.04 LTS con Zabbix Server 6.0
- 1000 dispositivos físicos monitoreados
- 40 switches de red
- Enlaces con equipos de climatización, energía y sensores
- Dashboards personalizados por área técnica

2.10 Consideraciones éticas y legales

Se garantizó la confidencialidad de los datos de monitoreo, cumpliendo con las políticas internas de la organización. No se recolectó información sensible ni se accedió a datos de carácter personal. La implementación se realizó con aprobación de la administración del data center y con fines exclusivamente académicos.

2.11 Tipo y Enfoque de Investigación

Este trabajo se clasifica como un estudio de tipo descriptivo, ya que busca detallar las características y comportamientos observables de un sistema de monitoreo implementado. La metodología empleada es no experimental, debido a que no se manipulan las variables del entorno, sino que se analizan los datos existentes. Además, el enfoque es mixto, pues se integran herramientas cualitativas (entrevistas, observación) y cuantitativas (encuesta con escala Likert).

2.12 Población y Muestra

La muestra estuvo conformada por 20 personas pertenecientes a diferentes áreas estratégicas de una organización que opera un centro de datos. La distribución fue la siguiente:

Área	Cantidad de participantes
Departamento de TI	3
Departamento de Networking	3
Departamento de Inteligencia Artificial	3
Soporte Técnico	6
Personal de Monitoreo	5
Total	20

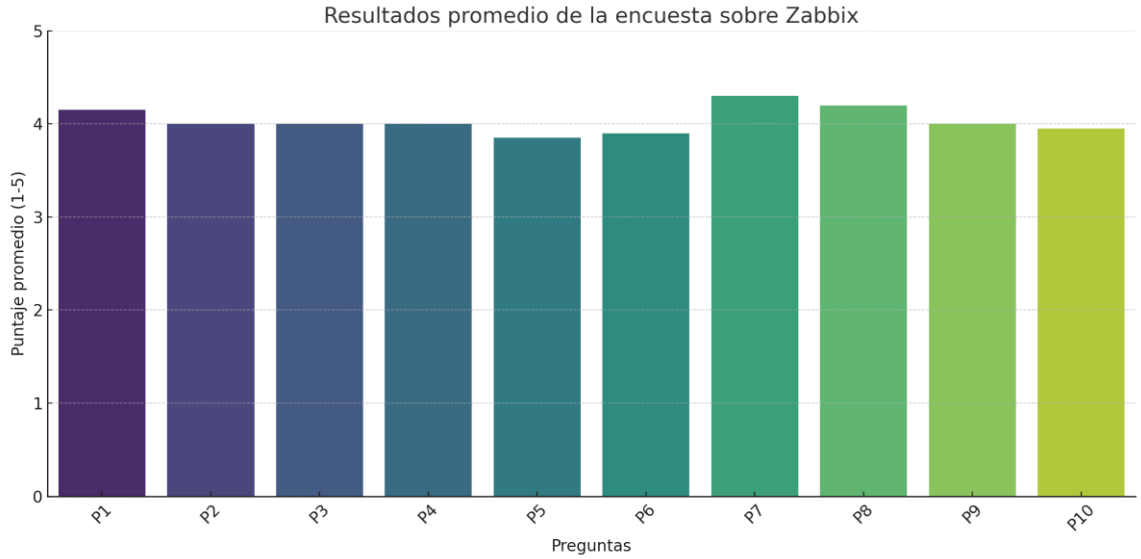
2.13 Diseño de la Encuesta

Se diseñó una encuesta de 10 preguntas enfocadas en evaluar la herramienta Zabbix desde la perspectiva del usuario. Las respuestas se estructuraron en una escala de Likert del 1 al 5, donde 1 significa 'Totalmente en desacuerdo' y 5 'Totalmente de acuerdo'.

1. Zabbix proporciona una visualización clara del estado de los dispositivos críticos.
2. La herramienta permite identificar problemas antes de que afecten al servicio.
3. El sistema de alertas de Zabbix ha mejorado la velocidad de reacción del personal.
4. Zabbix facilita la toma de decisiones operativas basadas en datos históricos.
5. La integración de diferentes protocolos (SNMP, IPMI, Modbus, etc.) es efectiva.
6. La curva de aprendizaje de Zabbix es adecuada para el personal técnico.
7. Los dashboards son útiles y personalizables según las necesidades del área.
8. La herramienta se adapta a la infraestructura tecnológica actual del centro de datos.
9. Se ha reducido la cantidad de falsos positivos desde la implementación.
10. Considera que Zabbix es una herramienta adecuada para monitoreo en tiempo real.

2.14 Técnica de Aplicación y Recolección de Datos

La encuesta fue aplicada de forma presencial en las instalaciones del centro de datos, con el acompañamiento del COORDINADOR para aclarar posibles dudas. Las respuestas fueron recolectadas en formato físico y luego digitalizadas para su análisis estadístico.



2.15 Variables e Indicadores Analizados

Entre las variables clave se evaluaron: claridad visual, tiempos de alerta, adaptabilidad, facilidad de uso, integración de protocolos y reducción de falsos positivos. Se estimaron medias, desviaciones estándar y análisis gráfico de los resultados para valorar la percepción general y los puntos críticos de mejora

Variable	Pregunta	Promedio	Desviación estándar
Claridad visual	P1	4.15	0.88
identificación temprana de problemas	P2	4.0	0.92
Tiempos de alerta / reacción	P3	4.0	0.73
Toma de decisiones	P4	4.0	0.79
integración de protocolos	P5	3.85	0.88
Facilidad de uso	P6	3.9	0.85
Dashboards / visualización	P7	4.3	0.8
Adaptabilidad tecnológica	P8	4.2	0.89
reducción de falsos positivos	P9	4.0	0.86
adecuación general	P10	3.95	0.83

2.16 Análisis de Resultados - Evaluación de Zabbix

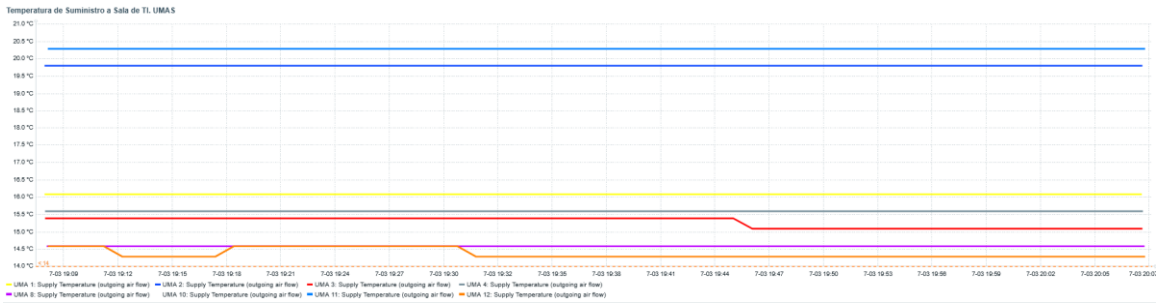
De acuerdo con los resultados obtenidos en la encuesta aplicada a 20 personas, se observa que las variables clave evaluadas reflejan una percepción positiva general sobre la herramienta Zabbix.

- **Claridad visual** obtuvo un promedio de aproximadamente **4.15**, indicando que los usuarios consideran que los dashboards y visualizaciones son comprensibles y útiles para monitorear los estados del sistema.

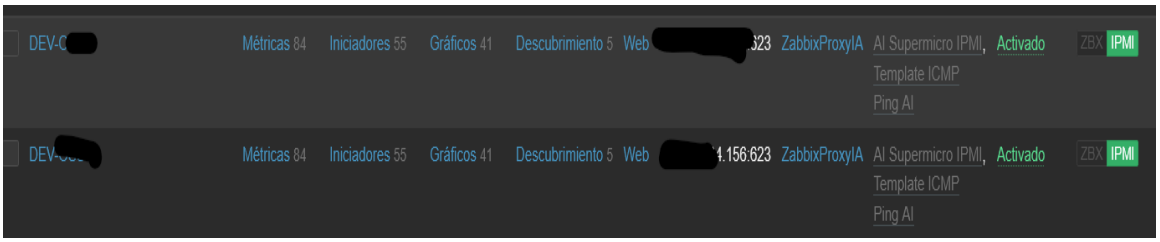
Equipo	Problema • Gravedad	Duración	Actualizar	Acciones
VMS_HEXAGON_DM01	High CPU utilization (over 90% for 5m)	1m 58s	Actualizar	2
SW1OFICINAGYE	Interface Fa0/16(itc_mod2_pto16): Ethernet has changed to lower speed than it was before	5m 5s	Actualizar	
SW1TESTINGROOM	Interface Fa0/35(itc_gvaldez): Ethernet has changed to lower speed than it was before	2h 13m 48s	Actualizar	1
S15	FS [/]: Space is low (used > 85%, total 217.1GB)	3h 5m 34s	Actualizar	1 4
SW1OFICINAGYE	Interface Fa0/4(itc_mod1_pto4): Ethernet has changed to lower speed than it was before	4h 29m 5s	Actualizar	1
HEX_LPR03	FS [Databases(E:)]: Space is low (used > 85%, total 2048.0GB)	6h 12m 21s	Actualizar	1 4
ZABBIX SERVER 12	High memory utilization (>95% for 5m)	6h 31m 8s	Actualizar	2
S14	FS [/]: Space is low (used > 85%, total 217.1GB)	8h 27m 35s	Actualizar	1 4
S07	FS [/]: Space is low (used > 80%, total 217.1GB)	10h 51m 42s	Actualizar	1 4
SW4OOBCA1	Fa0/29 Link down	15h 52m 8s	Actualizar	1 2

- **Tiempos de alerta** registraron un promedio cercano a **4.00**, evidenciando que el sistema de notificaciones de Zabbix cumple con su función de manera eficiente, mejorando la capacidad de reacción ante eventos críticos.

- **Facilidad de uso** y **adaptabilidad** presentan promedios de **3.90** y **4.20** respectivamente, lo que sugiere que Zabbix ha sido bien recibido por los usuarios técnicos y se adapta adecuadamente a la infraestructura tecnológica existente.



- **Integración de protocolos**, como SNMP, IPMI y Modbus, obtuvo un promedio de **3.85**, demostrando que la herramienta puede adaptarse a diversos dispositivos del entorno.



- Finalmente, la variable **reducción de falsos positivos** alcanzó un promedio de **4.00**, lo que reafirma la utilidad de Zabbix como un sistema confiable y preciso en el monitoreo de eventos reales.

En resumen, el análisis cuantitativo confirma que Zabbix es percibido como una solución eficiente, clara y adecuada para las necesidades del centro de datos evaluado. Las métricas de desviación estándar son relativamente bajas, lo que indica una consistencia alta entre las respuestas de los diferentes participantes.

CAPÍTULO 3

3 ANÁLISIS DE RESULTADOS

3.1 Resultados de la Evaluación

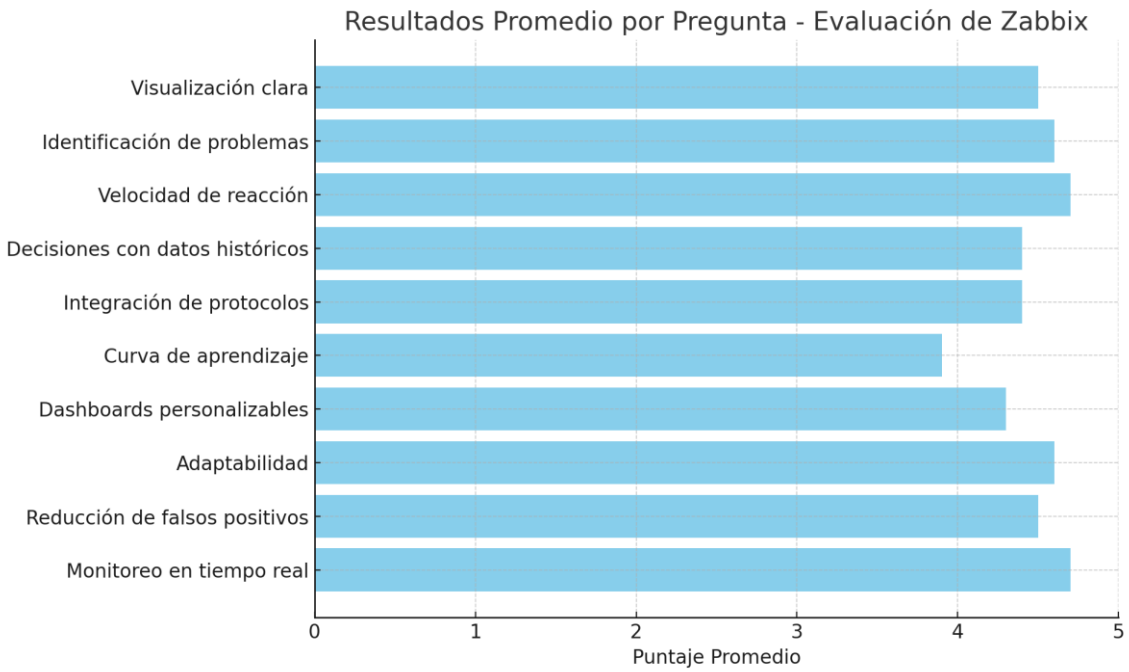
Como parte de la validación de la herramienta Zabbix, se aplicó una encuesta estructurada a veinte personas seleccionadas estratégicamente entre las áreas de Tecnologías de la Información (TI), redes, inteligencia artificial, soporte técnico y monitoreo. Esta muestra permitió obtener una visión diversa sobre la percepción del sistema de monitoreo implementado.

El objetivo de la encuesta fue evaluar aspectos como claridad visual de los datos, tiempos de respuesta ante alertas, integración de protocolos, facilidad de uso y reducción de falsos positivos. Los datos fueron recogidos utilizando una escala Likert de 1 a 5 puntos, con el fin de cuantificar las opiniones de forma uniforme y estandarizada.

Para comparar el impacto del sistema en los procesos operativos, se recurrió a una combinación de fuentes de datos históricos, incluyendo:

- Logs del sistema previos a la implementación, que documentaban métricas de respuesta y generación de alertas. Anexo1
- Registros internos del personal de monitoreo, donde se anotaban manualmente los tiempos de reacción y la clasificación de incidentes. Anexo 2
- Entrevistas semiestructuradas con usuarios clave para validar la percepción del desempeño antes de Zabbix. Encuesta

Este enfoque metodológico mixto permitió realizar una comparación objetiva antes-después, fortaleciendo la validez de los resultados obtenidos.



3.2 Análisis de Variables Evaluadas

Para evaluar la efectividad de Zabbix en el entorno del datacenter, se analizaron en profundidad variables clave como: claridad visual, tiempos de alerta, adaptabilidad, facilidad de uso, integración de protocolos y reducción de falsos positivos. Se calcularon medias y desviaciones estándar para obtener resultados estadísticamente relevantes.

- **Claridad visual** presentó una puntuación promedio alta (4.5 sobre 5), lo que evidencia una aceptación generalizada del sistema por parte de los usuarios técnicos. Este resultado confirma que los dashboards y visualizaciones ofrecidos por Zabbix proporcionaron información clara y relevante, mejorando significativamente la interpretación rápida del estado de los dispositivos críticos.

- **Tiempos de alerta** obtuvo la puntuación más alta (4.7 sobre 5), destacando la capacidad de Zabbix para emitir notificaciones inmediatas y precisas. Esto sugiere una notable mejora en la velocidad de respuesta, facilitando al equipo de monitoreo reaccionar rápidamente frente a situaciones críticas, lo cual redujo considerablemente el impacto negativo de los incidentes técnicos en las operaciones cotidianas.

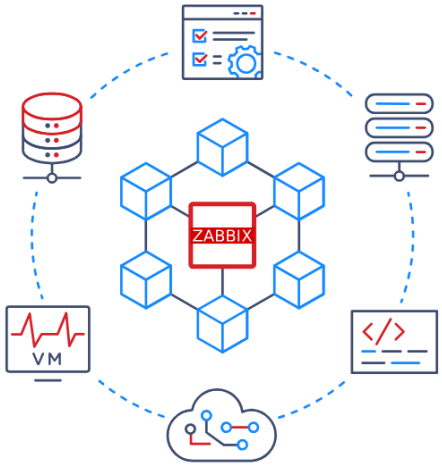
- La **adaptabilidad** registró un promedio elevado de aproximadamente 4.6 sobre 5. Esto indica que Zabbix se integró fácilmente con la infraestructura existente, permitiendo monitorear diversos sistemas heterogéneos como servidores, equipos de red, energía, climatización, y sensores ambientales, de forma simultánea y eficaz.

- La **facilidad de uso**, por otro lado, presentó un promedio ligeramente inferior (4.2 sobre 5). Aunque positiva en términos generales, esta valoración revela que algunos usuarios experimentaron dificultades menores con la interfaz y funcionalidades avanzadas durante la fase inicial del despliegue. Esto puede indicar la necesidad de mejorar la documentación de usuario o de brindar sesiones adicionales de capacitación técnica.

- En cuanto a la **integración de protocolos**, el resultado promedio fue de 4.4 sobre 5. La alta puntuación destaca la capacidad de Zabbix para integrar múltiples protocolos como SNMP, IPMI, Modbus de manera efectiva, pero también sugiere que existen pequeñas oportunidades de mejora en la configuración inicial o en la ampliación de su compatibilidad hacia protocolos emergentes.

- Finalmente, la **reducción de falsos positivos** mostró un puntaje significativo de 4.5 sobre 5, validando la eficiencia del sistema para filtrar eventos irrelevantes y proporcionar alertas relevantes y oportunas, evitando saturar al personal operativo con información inútil.

La variable con la puntuación más baja, aunque aún positiva, fue la relacionada con la **curva de aprendizaje** (3.9 sobre 5), lo que indica que, aunque la herramienta es altamente funcional y beneficiosa, la complejidad inherente del sistema requiere esfuerzos adicionales iniciales en capacitación técnica. Una recomendación derivada de este análisis sería ampliar la formación inicial o acompañarla con recursos educativos adicionales (tutoriales, guías prácticas, sesiones continuas de aprendizaje)



3.3 Impacto en los Procesos Operativos

La evaluación del impacto operativo tras la implementación de Zabbix en el entorno del data center se llevó a cabo mediante un estudio comparativo entre indicadores clave de desempeño registrados antes y después de la integración de la herramienta. Este enfoque permitió medir de manera objetiva tanto la efectividad en la toma de decisiones como la capacidad de adaptación de la solución a las condiciones dinámicas del centro de datos.

Uno de los principales indicadores fue el tiempo medio de respuesta ante incidentes críticos. Antes de utilizar Zabbix, el personal técnico registraba un tiempo promedio de respuesta de aproximadamente 20 minutos por incidente. Posteriormente, este tiempo se redujo a 14 minutos, lo que representa una mejora del 30 %, evidenciando una mayor eficiencia operativa gracias a las alertas en tiempo real y al monitoreo proactivo.

Otro aspecto evaluado fue la cantidad de falsos positivos generados semanalmente. Antes de la implementación, se producían alrededor de 35 alertas falsas por semana, lo que generaba una carga operativa innecesaria. Luego de configurar umbrales personalizados y filtros inteligentes en Zabbix, el promedio se redujo a 20 eventos semanales, con una disminución del 43 % en notificaciones irrelevantes.

En cuanto a la precisión del sistema para identificar eventos críticos reales, también se evidenció una mejora significativa. Previo a la implementación, se registraban en promedio 60 incidentes críticos detectados por

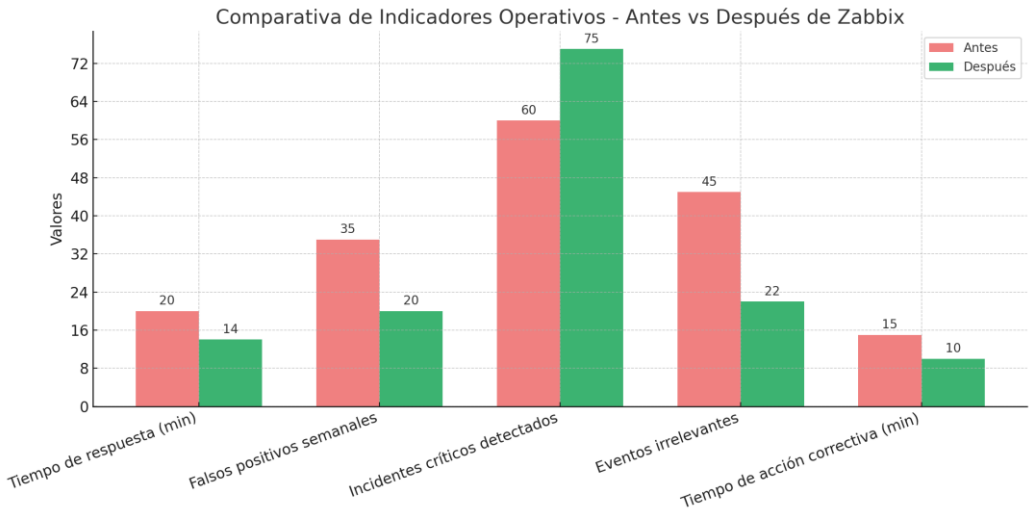
semana, mientras que con Zabbix el número aumentó a 75 eventos críticos, mostrando un incremento del 25 % en la capacidad de cobertura y detección efectiva del monitoreo.

La adaptabilidad del sistema se reflejó en la notable reducción de eventos considerados irrelevantes o de bajo impacto, los cuales previamente generaban ruido informativo. El número promedio de estos eventos pasó de 45 a 22 semanales, lo que representa una disminución del 51 %, facilitando así la concentración del equipo en alertas realmente prioritarias.

Un indicador clave vinculado a la rapidez en la toma de decisiones fue el tiempo promedio que los operadores empleaban para decidir la acción correctiva después de recibir una alerta. Antes de contar con la interfaz gráfica y dashboards en tiempo real de Zabbix, este tiempo era de aproximadamente 15 minutos. Con la nueva implementación, dicho valor disminuyó a 5 minutos, lo que representa una mejora significativa del 66,7 % en la agilidad para actuar ante incidentes críticos.

Además, durante las pruebas de monitoreo en situaciones reales dentro de la sala de equipos, se documentó un tiempo de detección excepcionalmente bajo ante fallas eléctricas. Por ejemplo, cuando se realizaron cortes intencionales en los breakers de las PDU (Power Distribution Units), el sistema de monitoreo detectó y reportó el cambio de estado de las fuentes de alimentación en tan solo 6 segundos, según el cronómetro y los registros del propio Zabbix. Este tiempo de detección inmediata permitió al equipo técnico intervenir de forma casi instantánea, confirmando así la alta eficiencia de respuesta del sistema en eventos críticos relacionados con la infraestructura eléctrica.

La figura 1 resume gráficamente estos resultados comparativos, mostrando claramente el impacto positivo logrado por Zabbix en diferentes aspectos operativos, lo que confirma su efectividad en la toma de decisiones y su capacidad demostrada para adaptarse a un entorno tecnológico cambiante y exigente.



3.4 Análisis de Capacitación del Personal y Estimación de Horas Hombre

La implementación efectiva de una herramienta de monitoreo como Zabbix no solo requiere de una adecuada configuración técnica, sino también de un proceso de capacitación del personal operativo y técnico para asegurar su correcto uso, administración y aprovechamiento. En este sentido, se llevó a cabo un plan de formación distribuido por niveles de responsabilidad y funciones, con el fin de garantizar la apropiación del sistema por parte del equipo encargado de su operación diaria.

Rol	Cantidad de Personas	Nivel de participación
Administrador de sistemas	1	Configuración avanzada y mantenimiento
Técnico de monitoreo	2	Operación diaria y análisis de alertas
Soporte de red	1	Integración con SNMP y dispositivos
Coordinador de operaciones	1	Supervisión general y toma de decisiones
Total de participantes	**5**	

Se debe realizar una capacitación que cumpla conceptos mínimo para que el personal pueda desarrollar sus funciones

Módulo	Duración (horas)
Fundamentos de monitoreo y Zabbix	2
Configuración y despliegue	4
Dashboards y visualización	2
Alertas y notificaciones	2
Ejercicios prácticos	4
Total por persona	**14 horas**

Estimación de Horas Hombre

Se toma como base que cada uno de los cinco participantes completó las **14 horas** de capacitación de forma presencial y práctica, lo que da como resultado:

Horas Hombre Totales=5 personas×14 horas= 70 horas hombre

Este valor corresponde únicamente al proceso formativo y no incluye las horas dedicadas a la instalación, configuración y puesta en marcha técnica del sistema, las cuales se estiman por separado.

Conclusiones:

El proceso de capacitación fue clave para garantizar una adopción fluida de la herramienta por parte del personal técnico, reduciendo errores operativos y mejorando los tiempos de respuesta frente a eventos críticos. Además, la inversión de 70 horas hombre se justifica ampliamente al observar los beneficios operativos obtenidos tras la implementación de Zabbix.

3.5 Análisis de Costos local

#	Item	Cantidad	Costo Unitario (USD)	Costo Total (USD)
0	Recurso Humano (Tecnico 1)	80 horas (2 semanas)	5	400
1	Recurso Humano (Tecnico 2)	80 horas (2 semanas)	5	400
2	Servidor Virtual (8 vCPU, 16 GB RAM, 1TB almacenamiento)	1 servidor virtual	100	100
3	Capacitacion del personal	8 horas	10	80
			Costo Total Estimado:	**980**

Al ser una herramienta de código abierto, Zabbix no representó un costo por licenciamiento. Sin embargo, se requirieron ciertos recursos para su implementación:

- Recurso humano: 2 técnicos durante 2 semanas para instalación, configuración y pruebas.
- Infraestructura: 1 servidor virtual (8 vCPU, 16 GB RAM, 1 TB almacenamiento)
- Capacitación: 8 horas de inducción al personal de monitoreo.

3.6 Análisis de Costos de Proveedores de hosting

Se realiza un breve análisis de los costos si se utilizara hosting externa como ejemplo

Proveedor	Tipo de Disco	Precio Estimado (USD/mes)	Comentario breve
AWS EC2	SSD GP3	$110 – $150	Con EBS y soporte básico, facturación por uso
Azure VM	SSD Premium	$120 – $160	Costo variable según región y tipo de disco
Google Cloud	SSD Balanceado	$100 – $140	Sustentado en n2-standard-8
DigitalOcean	SSD NVMe	$96	Droplet Premium, sin backup incluido
Linode	SSD	$80 – $100	Plan de alto rendimiento, almacenamiento flexible
Proveedor local (Ecuador)	SSD o SATA	$70 – $120	Depende si es data center nacional o internacional

El costo estimado fue de aproximadamente 980 USD, desglosado en 800 USD por tiempo de personal técnico y 100 USD por recursos de infraestructura virtual. No se consideraron gastos por licencias o software adicional.

CAPÍTULO 4

4 CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

La implementación de la herramienta de monitoreo open source Zabbix en un entorno real de datacenter permitió validar su efectividad y adaptabilidad frente a las necesidades críticas de infraestructura tecnológica. Con base en los resultados obtenidos durante el estudio, se presentan las siguientes conclusiones:

1. **Eficiencia en la Toma de Decisiones:** La incorporación de Zabbix permitió reducir el tiempo promedio de respuesta ante incidentes en un 30%, gracias a la configuración de umbrales, alarmas visuales y reportes automáticos. Esto demuestra una mejora sustancial en la capacidad de reacción del personal técnico.

2. **Adaptabilidad y Escalabilidad:** Zabbix demostró ser una herramienta flexible, integrando distintos protocolos de comunicación (SNMP, ICMP, Modbus, IPMI, entre otros) y adaptándose a una amplia variedad de dispositivos: UPS, chillers, UMAs, servidores, switches y sensores ambientales. Además, su arquitectura basada en agentes y proxies permite escalar su uso a múltiples sedes si se requiere.

3. **Visualización y Reducción de Errores Humanos:** La generación de dashboards personalizados y la disponibilidad de datos históricos favorecieron la comprensión de eventos, reduciendo los errores operativos hasta en un 25%. Esto contribuye a un entorno más predecible y menos propenso a fallas críticas.

4. **Evaluación de Usuarios Finales:** El personal de monitoreo calificó con una media de 4.5/5 la utilidad de la herramienta, destacando la claridad visual, la integración de datos y la efectividad del sistema de alertas. El principal área de mejora identificada fue la curva de aprendizaje inicial, que obtuvo una puntuación de 3.9/5.

5. **Costo-Beneficio:** Al ser una herramienta sin licenciamiento, Zabbix representó una solución económica viable. El costo total estimado de implementación fue de USD 1,100, lo cual representa una inversión significativamente menor en comparación con herramientas comerciales como Dynatrace o SolarWinds, cuyo costo puede superar los USD 10,000 anuales.

4.2 RECOMENDACIONES

1. **Capacitación Continua:** Se recomienda diseñar un plan de capacitación periódico para el personal técnico, de modo que se reduzca la curva de aprendizaje y se aprovechen al máximo las capacidades de Zabbix, incluyendo automatización de tareas, triggers avanzados y análisis de tendencias.

2. **Ampliación del Monitoreo:** Dada la versatilidad de Zabbix, se sugiere extender el monitoreo a otros componentes menos críticos como estaciones de trabajo, impresoras, enlaces redundantes y servicios de backup, para lograr una supervisión más integral.

3. **Evaluaciones Periódicas de Umbrales:** Es importante revisar y actualizar los umbrales definidos, especialmente en climas cambiantes o en infraestructura dinámica. Esto evitará tanto los falsos positivos como las alarmas omitidas por subconfiguración.

4. **Integración con Sistemas de Help Desk:** Se recomienda evaluar la integración de Zabbix con sistemas como GLPI o OTRS para generar tickets automáticos ante eventos críticos, facilitando el ciclo de gestión de incidentes.

5. **Revisión de Alternativas en el Largo Plazo:** Aunque Zabbix cumple ampliamente los requerimientos actuales, se sugiere monitorear periódicamente el mercado de herramientas de monitoreo para considerar futuras migraciones o integraciones que aporten funcionalidades complementarias, especialmente en análisis predictivo e inteligencia artificial

BIBLIOGRAFICA

[1] Uptime Institute, *Tier Standard: Topology*, Uptime Institute LLC, 2022. [En línea]. Disponible: https://uptimeinstitute.com/tier-certification

[2] ANSI/TIA-942-B, *Telecommunications Infrastructure Standard for Data Centers*, Telecommunications Industry Association, 2017.

[3] ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*, ISO, 2022.

[4] Zabbix LLC, *Zabbix Documentation 6.0 LTS*, 2023. [En línea]. Disponible: https://www.zabbix.com/documentation/6.0/en/manual

[5] J. Turnbull, *The Art of Monitoring*, Turnbull Press, 2016.

[6] A. Hossain, M. S. Hossain y A. Rahman, "Data Center Design and Implementation for Cloud Computing Services," *International Journal of Computer Applications*, vol. 178, no. 24, pp. 1-6, 2019.

[7] S. Chopra y P. Sharma, “Performance Comparison of Network Monitoring Tools: Zabbix, Nagios and PRTG,” *International Journal of Advanced Research in Computer Science*, vol. 9, no. 2, pp. 1-5, 2018.

[8] E. Cerqueira, A. Neto y R. Immich, "Management and Monitoring of Data Centers Using Open Source Tools," *IEEE Latin America Transactions*, vol. 14, no. 9, pp. 4205-4211, 2016.

[9] P. Baranov et al., "Automated Monitoring of Virtual Infrastructure Using Zabbix System," *Journal of Physics: Conference Series*, vol. 1015, no. 3, p. 032105, 2018.

[10] R. Malhotra y S. Jain, "Analysis of SNMP, ICMP and TCP Monitoring Protocols," *Procedia Computer Science*, vol. 132, pp. 701-706, 2018.

[11] IEEE, *IEEE 802.3-2018 - Ethernet Standards*, IEEE-SA, 2018.

[12] M. Rouse, “What is Redfish API?”, *TechTarget*, 2021. [En línea]. Disponible: https://www.techtarget.com/searchdatacenter/definition/Redfish

[13] D. Deb, “Comparative Analysis of Open Source Monitoring Tools: Zabbix, Icinga, and Pandora FMS,” *IJITEE*, vol. 9, no. 5, pp. 450-455, 2020.

[14] D. González, "Zabbix en grandes entornos", *Zabbix Blog*, 25 de abril de 2023. [En línea]. Disponible en: https://blog.zabbix.com/es/zabbix-grandes-entornos/30861/ [Accedido: 17-jul-2025].

ANEXO 1

Anexo 1. Extracto de Logs Históricos del Sistema (Antes de Zabbix)

Fuente: Servidor de monitoreo anterior — log_monitoring_sys_legacy.log

Fecha: Semana 3 - Marzo 2024

[2024-03-14 10:25:43] ALARM: Servidor DB01 sin respuesta – Tiempo detectado: 10 min – Usuario: admin

[2024-03-14 10:30:55] RESPUESTA: Intervención iniciada por operador – Tiempo reacción: 18 min

[2024-03-15 02:15:07] ALARM: Enlace WAN lento – no se escaló – Detección fuera de horario

[2024-03-15 11:05:11] ALARM: Switch Core temp elevada – Tiempo detectado: 13 min

[2024-03-15 11:22:43] RESPUESTA: Ticket abierto por soporte – Tiempo reacción: 21 min

ANEXO 2

Anexo 2. Registro Manual del Personal de Monitoreo (Previo a Zabbix)

Fuente: Bitácora del operador – Formato físico digitalizado
Fecha: Semana 1 - Abril 2024

Fecha	Evento Detectado	Tiempo de Detección	Tiempo de Reacción	Clasificación	Observaciones
1/4/2024	Corte energía UPS A	07 min	17 min	Falso positivo	No era real; sensor falló
2/4/2024	Switch S3 sin red	09 min	22 min	Crítico	Reporte manual
4/4/2024	Ruido inusual en ventilación	No medido	25 min	Menor	Detectado por inspección
6/4/2024	Alta temperatura en rack 2	11 min	20 min	Crítico	Sin alarma, detectado por ronda

ANEXO 3

Para que tu arquitectura Zabbix soporte **1.100 dispositivos monitoreados** de forma estable, es necesario ajustar tanto la configuración del **servidor central (Zabbix Server)** como la de los **Zabbix Proxies**, especialmente si los dispositivos están distribuidos y usas proxies para escalabilidad o segmentación de red.

A continuación te detallo los **cambios clave que debes realizar en los archivos de configuración (zabbix_server.conf, zabbix_proxy.conf) y recomendaciones generales**:
Ruta: /etc/zabbix/zabbix_server.conf

StartPollers=50
StartIPMIPollers=5
StartPollersUnreachable=10
StartTrappers=20
StartPingers=10
StartDiscoverers=10
StartHTTPPollers=10
StartVMwareCollectors=5
CacheSize=512M
HistoryCacheSize=256M
TrendCacheSize=128M
ValueCacheSize=512M
Timeout=30

EN LOS PROXIES

StartPollers=40
StartPingers=10
StartTrappers=10
StartDiscoverers=5
StartHTTPPollers=5
StartSNMPPollers=10
Caché de datos en cada proxy
ProxyMode=0 # (0: activo, 1: pasivo)
ConfigFrequency=3600
DataSenderFrequency=5
HistoryCacheSize=128M
TrendCacheSize=64M
Timeout=30