

NOMBRE DEL TRABAJO

**Implementación de Software Zabbix com
o Sistema de Monitoreo para Equipos en
la Red Local de la Empr**

AUTOR

**KATHERINE GLADYS ZAMBRANO BERR
OCAL**

RECUENTO DE PALABRAS

13003 Words

RECUENTO DE CARACTERES

75185 Characters

RECUENTO DE PÁGINAS

90 Pages

TAMAÑO DEL ARCHIVO

4.2MB

FECHA DE ENTREGA

Mar 26, 2024 8:03 AM GMT-5

FECHA DEL INFORME

Mar 26, 2024 8:04 AM GMT-5

● 6% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos.

- 6% Base de datos de Internet
- Base de datos de Crossref
- 0% Base de datos de trabajos entregados
- 1% Base de datos de publicaciones
- Base de datos de contenido publicado de Crossref

● Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Material citado
- Coincidencia baja (menos de 10 palabras)

**FORMULARIO DE AUTORIZACIÓN PARA LA
PUBLICACIÓN DE TRABAJOS DE INVESTIGACIÓN EN
EL REPOSITORIO INSTITUCIONAL DE LA UNTELS**
(Art. 45° de la ley N° 30220 – Ley)

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

TIPO DE TRABAJO DE INVESTIGACIÓN

- 1). TESIS () 2). TRABAJO DE SUFICIENCIA PROFESIONAL (X)

DATOS PERSONALES

Apellidos y Nombres: ZAMBRANO BERROLAL KATHERINE GLADYS
D.N.I.: 73958420
Otro Documento:
Nacionalidad: PERUANA
Teléfono: 991882429
e-mail: KATTA9308@GMAIL.COM

DATOS ACADÉMICOS

Pregrado

Facultad: FACULTAD DE INGENIERIA Y GESTIÓN
Programa Académico: TRABAJO DE SUFICIENCIA PROFESIONAL
Título Profesional otorgado: Ingeniero Electrónico y Telecomunicaciones

Postgrado

Universidad de Procedencia:
País:
Grado Académico otorgado:

Datos de trabajo de investigación

Título: "IMPLEMENTACIÓN DE SOFTWARE ZABBIX COMO SISTEMA DE MONITOREO PARA EQUIPOS EN LA RED LOCAL DE LA EMPRESA DESYSWEB S.A.C"
Fecha de Sustentación: 17-12-2023
Calificación: APROBADO
Año de Publicación: 2024

AUTORIZACIÓN DE PUBLICACIÓN EN VERSIÓN ELECTRÓNICA

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

Marcar con una X su elección.

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

Si autorizo No autorizo

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

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

- 3) Si usted dispone de una **PATENTE** puede elegir el tipo de **ACCESO RESTRINGIDO** como derecho de autor y en el marco de confiabilidad dispuesto por los numerales 5.2 y 6.7 de la directiva N° 004-2016-CONCYTEC DEGC que regula el Repositorio Nacional Digital de CONCYTEC (Se colgará únicamente datos del autor y el resumen del trabajo de investigación).

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

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

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

Atribuciones de acceso restringido:

Motivos de la elección del acceso restringido:

ZAMBRANO BERROCAL KATHERINE GLADYS

APELLIDOS Y NOMBRES

73958420

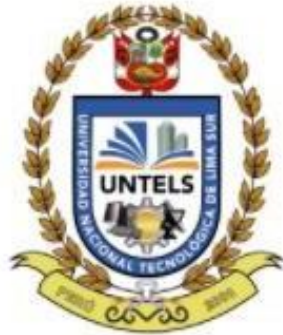
DNI

K. Zambrano
Firma y huella:



Lima, 15 de FEBRERO del 2024

UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR
FACULTAD DE INGENIERÍA Y GESTIÓN
ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA Y
TELECOMUNICACIONES



**"Implementación de Software Zabbix como Sistema de Monitoreo
para Equipos en la Red Local de la Empresa Desysweb S.A.C."**

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de

INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

PRESENTADO POR EL BACHILLER

ZAMBRANO BERROCAL, KATHERINE GLADYS

ORCID: 0009-0007-3302-4665

ASESOR

CASTRO PULCHA, BERNARDO

ORCID: 0000-0001-8578-5940

Villa el Salvador

2023



"Año de la unidad, la paz y el desarrollo"

VI Programa de Titulación por la Modalidad de Trabajo de Suficiencia Profesional
Decanato de la Facultad de Ingeniería y Gestión

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

En Villa El Salvador, siendo las17:30..... horas del día 17 de diciembre de 2023, se reunieron en las instalaciones de la Universidad Nacional Tecnológica de Lima Sur, los miembros del Jurado Evaluador del Trabajo de Suficiencia Profesional integrado por:

Presidente	:	DR. ALEX CARTAGENA GORDILLO	CIP N° 133344
Secretario	:	DR. RICARDO JOHN PALOMARES ORIHUELA	CIP N° 105002
Vocal	:	MG. ENRIQUE MANUEL MORÁN MONTOYA	CIP N° 144807

Designados con Resolución de Decanato de la Facultad de Ingeniería y Gestión N° 984-2023-UNTELS-R-D de fecha 13 de diciembre del 2023.

Se da inició al acto público de sustentación y evaluación del Trabajo de Suficiencia Profesional, para obtener el Título Profesional de Ingeniero Electrónico y Telecomunicaciones, bajo la modalidad de Titulación por Trabajo de Suficiencia Profesional (Resolución de Consejo Universitario N° 065-2023-UNTELS-CU de fecha 08 de agosto del 2023), en la cual se APRUEBA el "Reglamento, Directiva, Cronograma y Presupuesto del VI Programa de Titulación por la Modalidad de Trabajo de Suficiencia Profesional de la Universidad Nacional Tecnológica de Lima Sur"; siendo que el Art. 4º del precitado Reglamento establece que: "La Modalidad de Titulación prevista consiste en la presentación, aprobación y sustentación de un Trabajo de Suficiencia Profesional que dé cuenta de la experiencia profesional y además permita demostrar el logro de las competencias adquiridas en el desarrollo de los estudios de pregrado que califican para el ejercicio de la profesión correspondiente. Quienes participen en esta modalidad no podrán tramitar simultáneamente otras modalidades de titulación. Además, los participantes inscritos en esta modalidad, deberán acreditar un mínimo de dos (02) años de experiencia laboral, de acuerdo a lo establecido en la Resolución N° 174-2019- SUNEDU/CD y al anexo 1 sobre Glosario de Términos en el punto veinte (20)...", en el cual;

La Bachiller KATHERINE GLADYS ZAMBRANO BERROCAL
Sustentó su Trabajo de Suficiencia Profesional: IMPLEMENTACIÓN DE SOFTWARE ZABBIX COMO SISTEMA DE MONITOREO PARA EQUIPOS EN LA RED LOCAL DE LA EMPRESA DESYSWEB S.A.C.

Concluida la Sustentación del Trabajo de Suficiencia Profesional, se procedió a la calificación correspondiente según el siguiente detalle:

CondiciónAprobado.....Equivalencia.....Regular.....de acuerdo al Art. 65º del Reglamento General para el Otorgamiento de Grado Académico y Título Profesional de la UNTELS vigente.

Siendo las18:00..... horas del día 17 de diciembre de 2023 se dio por concluido el acto de sustentación del Trabajo de Suficiencia Profesional, firmando la presente acta los miembros del Jurado.

PRESIDENTE
DR. ALEX CARTAGENA GORDILLO
CIP N° 133344

SECRETARIO
DR. RICARDO JOHN PALOMARES ORIHUELA
CIP N° 105002

VOCAL
MG. ENRIQUE MANUEL MORÁN MONTOYA
CIP N° 144807

DEDICATORIA

Dedico este trabajo a toda mi familia, en especial a mi padre, Alfredo Zambrano Silvera, gracias a sus consejos, amor y apoyo incondicional.

AGRADECIMIENTO

Agradezco a Dios por darme la vida y guiar mis pasos en todo momento.

A mis hermanos Alberth y Inzaghi que me brindan su amor y apoyo incondicional. Agradezco a mi novio Jhair Diaz por su amor, también a mis amigos quienes brindaron ánimos durante este proceso.

A los profesores de la universidad que me brindaron conocimientos sólidos durante mi formación universitaria. De manera muy especial a mi asesor y revisores por su valiosa orientación en todo el proceso del trabajo.

ÍNDICE

DEDICATORIA.....	ii
AGRADECIMIENTO	iii
ÍNDICE	iv
LISTADO DE FIGURAS.....	vi
LISTADOS DE TABLAS.....	viii
RESUMEN.....	ix
INTRODUCCIÓN.....	1
CAPÍTULO I. ASPECTOS GENERALES	2
1.1. Contexto.....	2
1.2. Delimitación temporal y espacial del trabajo.....	2
1.2.1. Temporal	2
1.2.2. Espacial.....	2
1.3. Objetivos	2
1.3.1. Objetivo General.....	2
1.3.2. Objetivos Específicos.....	3
CAPÍTULO II. MARCO TEÓRICO.....	4
2.1. Antecedentes	4
2.1.1. Antecedentes Internacionales.....	4
2.1.2. Antecedentes Nacionales.....	5
2.2. Bases Teóricas	6
2.2.1. Software.....	6
2.2.2. Hardware.....	7
2.2.3. Monitoreo de redes e infraestructura.....	9
2.2.4. SNMP.....	11
2.2.4.2. Base de datos de información de gestión (MIB).....	13
2.2.4.3. Estructura MIB e identificador de objeto (ID de objeto u OID).....	14
2.2.4.4. Versiones de SNMP.....	15
2.2.5. Sistema de monitoreo Zabbix.....	16
2.2.5.1. Arquitectura.....	17

2.2.5.2. Controles pasivos y activos.....	20
2.2.5.3. Flujo de datos.....	21
2.3. Definición de términos básicos.....	23
CAPÍTULO III. DESARROLLO DEL TRABAJO PROFESIONAL	26
3.1. Determinación y análisis del problema.....	26
3.1.1. Encuesta a los usuarios de la red local de la empresa DESYSWEB. ...	26
3.2. Modelos de Solución Propuesto.....	28
3.2.1. Implementación del sistema de monitoreo Zabbix	30
3.2.1.1. Requisitos del sistema de monitoreo.....	30
3.2.1.2. Instalación de la base de datos.....	31
3.2.2. Instalación de la herramienta Zabbix	34
3.2.2.1. Visualización de la interfaz de Zabbix desde un navegador web ...	37
3.2.3. Configuración de los equipos a monitorear en la herramienta Zabbix	41
3.2.4. Comprobación de la funcionalidad de las notificaciones por medio de correo electrónico en Zabbix.....	48
3.3. Resultados	51
3.3.1. Verificación del envío de correo.....	51
3.3.2. Encuestas realizadas.....	52
3.3.2.1. Discusión de los resultados.....	56
CONCLUSIONES.....	57
RECOMENDACIONES	58
REFERENCIAS BIBLIOGRÁFICAS	59
ANEXOS	61

LISTADO DE FIGURAS

Figura 1 <i>Elementos integrantes del protocolo SNMP</i>	13
Figura 2 <i>Comunicación SNMP</i>	14
Figura 3 <i>Estructura jerárquica de una MIB</i>	15
Figura 4 <i>Presentación de Zabbix</i>	17
Figura 5 <i>Arquitectura del sistema de monitoreo Zabbix</i>	18
Figura 6 <i>Mecanismo de sondeo pasivo y activo de Zabbix</i>	21
Figura 7 <i>Flujo de datos de monitoreo de Zabbix</i>	21
Figura 8 <i>Modelo activo del flujo de datos de Zabbix</i>	22
Figura 9 <i>Modelo pasivo del flujo de datos de Zabbix</i>	23
Figura 10 <i>Gráfica comparativa de tiempo de resolución de interrupciones</i>	27
Figura 11 <i>Gráfico de tiempo de localización de dispositivo fallido</i>	28
Figura 12 <i>Flujograma de desarrollo del trabajo</i>	29
Figura 13 <i>SELinux habilitado</i>	31
Figura 14 <i>Proceso de deshabilitar SELinux</i>	31
Figura 15 <i>Flujograma de la instalación de la base de datos</i>	32
Figura 16 <i>Instalación de base de datos MariaDB. Se activa y habilita la base de datos para el funcionamiento</i>	32
Figura 17 <i>Ejecución de gestor de base de datos MariaDB</i>	32
Figura 18 <i>Conexión a base de datos</i>	33
Figura 19 <i>Creación del esquema interno de la base de datos</i>	33
Figura 20 <i>Configurar la base de datos para el servidor Zabbix en el fichero /etc/zabbix/zabbix_server.conf</i>	34
Figura 21 <i>Fichero de configuración del servidor Zabbix</i>	34
Figura 22 <i>Flujograma de la instalación de Zabbix</i>	35
Figura 23 <i>Página principal del proyecto Zabbix</i>	36
Figura 24 <i>Descarga e instalación completada de paquete Zabbix</i>	36
Figura 25 <i>Instalación de paquetes y dependencias requeridas</i>	37
Figura 26 <i>Interfaz web de Zabbix</i>	37
Figura 27 <i>Prerrequisitos del sistema a través de interfaz web</i>	38
Figura 28 <i>Configuración de conexión a base de datos</i>	38
Figura 29 <i>Detalles de la configuración de conexión a base de datos</i>	39
Figura 30 <i>Resumen de parámetros de configuración</i>	39

Figura 31 <i>Conclusión de instalación.</i>	40
Figura 32 <i>Interfaz web de inicio de sesión.</i>	40
Figura 33 <i>Flujograma del proceso de creación de hosts a Zabbix.</i>	42
Figura 34 <i>Creación de grupos de usuarios</i>	43
Figura 35 <i>Creación de plantilla.</i>	44
Figura 36 <i>Configuración del host SNMP Firewall.</i>	45
Figura 37 <i>Configuración de la comunidad.</i>	46
Figura 38 <i>Visualización de los equipos monitoreados.</i>	46
Figura 39 <i>Resumen de alertas que muestra la plataforma Zabbix.</i>	47
Figura 40 <i>Colores asignados para cada tipo de alerta en Zabbix.</i>	47
Figura 41 <i>Configuración tipo de medio en Zabbix para la notificación mediante correo electrónico</i>	50
Figura 42 <i>Reporte de notificación mediante correo electrónico desde el Zabbix.</i>	51
Figura 43 <i>Reporte de notificación mediante correo electrónico desde el Zabbix.</i>	52
Figura 44 <i>Gráfica de tiempo de resolución de incidentes posterior a instalación de Zabbix.</i> .	52
Figura 45 <i>Gráfico de tiempo de localización de dispositivo fallido posterior a instalación de Zabbix.</i>	53
Figura 46 <i>Gráfico de opinión sobre el modelo actual de monitoreo de la empresa.</i>	54
Figura 47 <i>Gráfica sobre la sensación de seguridad sobre sistema de monitoreo de la empresa.</i>	55
Figura 48 <i>Tiempo que se tarda en resolver los incidentes.</i>	55
Figura 49 <i>Tiempo promedio que se demora en encontrar el dispositivo.</i>	56

LISTADOS DE TABLAS

Tabla 1 <i>Tiempo de falla vs tiempo de resolución.</i>	27
Tabla 2 <i>Tiempo de falla vs tiempo de resolución.</i>	28
Tabla 3 <i>Recursos de la máquina virtual.</i>	30
Tabla 4 <i>Detalle de equipos monitoreados en Zabbix.</i>	41
Tabla 5 <i>Tiempo de falla vs tiempo de resolución.</i>	52
Tabla 6 <i>Tiempo de localización del fallo</i>	53
Tabla 7 <i>Evaluación del modelo actual de monitoreo de la empresa</i>	54
Tabla 8 <i>Sensación de seguridad sobre sistema de monitoreo de la empresa</i>	54

RESUMEN

El presente trabajo de titulación hace referencia a la implementación de un software Zabbix como sistema de monitoreo. Esta herramienta de supervisión tiene como principales objetivos detectar de manera oportuna fallas en la red local de la empresa DESYSWEB S.A.C donde es importante asegurar el alto nivel de disponibilidad de la red.

La problemática principal nace mediante la necesidad de detectar de manera oportuna fallas de la red, siendo el problema la falta de seguimiento de cada alarma, al no tener una herramienta de monitoreo que analice, diagnostique y notifique de la pérdida de gestión, provocaba que ciertas áreas se queden sin conectividad, ocasionando un impacto negativo dentro de la empresa.

La solución ante tal problemática es implementar un sistema de monitoreo mediante el software Zabbix permitiendo mejorar la supervisión y gestión de la red en tiempo real.

Como resultado, se obtuvo que la implementación del software mejoró el nivel de actividad del personal de monitoreo, permitiendo supervisar los enlaces en tiempo real, mostrando interfaces de análisis para un mejor entendimiento del incidente acompañado de envío automático de notificación de alerta al personal de monitoreo.

Finalmente, se corrigió que los enlaces sean analizados y diagnosticados de manera más oportuna.

INTRODUCCIÓN

El presente trabajo de suficiencia profesional denominado “Implementación de Software Zabbix como Sistema de Monitoreo para Equipos en la Red Local de la Empresa DESYSWEB S.A.C”, dicha implementación pretende ser una solución ante la necesidad de diagnosticar de manera rápida el motivo de la pérdida de gestión de los equipos para brindar atención o soporte técnico de manera oportuna.

En la actualidad, los sistemas de telecomunicaciones se establecen como una herramienta esencial para la conectividad de equipos permitiendo el envío y recepción de la información en todos los niveles, alcanzando una alta demanda en servicios que sean eficientes y con mayor disponibilidad. Tomando en cuenta la importancia de la conectividad de equipos, las interrupciones de los servicios representan un estado crítico y de alto impacto donde se requiere de una atención proactiva y con tiempo de respuesta de solución lo más rápida posible, desde la solicitud del reclamo por avería. Dado el caso, es importante garantizar la operatividad de los enlaces, mucho más al tratarse de servidores, switch, cámara de seguridad de una empresa de telecomunicaciones por tener un impacto significativo, cuando el enlace no se encuentra operativo.

Bajo ese escenario, la solución comprende la implementación de un software Zabbix que cumpla la función del monitoreo constante de los equipos conectados a la red local con el objetivo de optimizar el desempeño de esta conectividad.

CAPÍTULO I. ASPECTOS GENERALES

1.1. Contexto

DESYSWEB es una empresa peruana dedicada al rubro de Telecomunicaciones y tecnologías de la Información (TI), su experiencia en el mercado de las telecomunicaciones es alrededor de los 13 años gracias a su enfoque de brindar servicios, infraestructura, conectividad a nivel nacional. Brinda soluciones flexibles y de alta calidad, comprenden las etapas de diseño, provisión, implementación, monitoreo, gestión, operación y soporte, incluido el servicio de subcontratación de infraestructura de TI, el desarrollo de proyectos integrales y la venta de soluciones a medida.

Tiene como misión aumentar la productividad empresarial de los clientes, promover el desarrollo de tecnologías dentro de las necesidades del sector corporativo, impulsando el desarrollo de nuevas tecnologías. Su visión es, ser reconocidos como una de las empresas líderes en Perú en cuanto a soluciones innovadoras de telecomunicaciones y tecnología de la información. Gracias por el apoyo de sus asociados y el éxito de sus clientes.

1.2. Delimitación temporal y espacial del trabajo

1.2.1. Temporal

Comprende el periodo abril - agosto del año 2023.

1.2.2. Espacial

El trabajo se ejecutó en la empresa Desysweb S.A.C ubicado en el distrito de San Martín de Porres, Lima- Perú.

1.3. Objetivos

1.3.1. Objetivo General

Implementar el Software Zabbix como sistema de monitoreo para equipos en la red local de la empresa Desysweb S.A.C.

1.3.2. *Objetivos Específicos*

O1: Implementar el software Zabbix, en la red local de Desysweb y establecer un sistema de alertas para notificar cualquier evento imprevisto.

O2: Configurar los dispositivos que comprenden la infraestructura interna de la empresa Desysweb para el correcto monitoreo.

O3: Validar la funcionalidad del sistema de monitoreo mediante notificaciones proactivas a través de correo electrónico con la finalidad de asegurar la gestión eficiente.

CAPÍTULO II. MARCO TEÓRICO

2.1. Antecedentes

Los trabajos de investigación desarrollados por otros autores tanto a nivel internacional como nacional permiten conocer de mejor manera los recursos y herramientas para llevar a cabo el presente trabajo, considerando los resultados alcanzados en cada uno de ellos para realizar una implementación óptima y efectiva que permita alcanzar los objetivos propuestos.

2.1.1. *Antecedentes Internacionales.*

León (2019) en la tesis titulada “La implementación de un servidor Zabbix en el consorcio educativo continental, para el análisis y monitoreo de equipos en la red” que se desarrolló en la ciudad de Cuenca (Ecuador), inicia con el levantamiento de inventario de las particularidades de cada equipo de cómputo y de red para conocer sus características en el consorcio corporativo continental mediante la recopilación de información, con el fin de identificar vulnerabilidades y elementos críticos de supervisión para el mantenimiento de los procesos de negocio. En base a lo anterior, plantea la implementación de un servidor central Zabbix y el uso de agentes para analizar y controlar los equipos informáticos. Este servidor de código abierto permite optimizar el tiempo y los recursos financieros de la institución monitoreando las distintas áreas administrativas y laboratorios, tomando así el control de los equipos y logrando resultados efectivos. Al crear informes en tiempo real con Zabbix, los resultados se obtienen en forma gráfica, lo que permite una mejor comprensión para el usuario.

La tesis indicada comprende una referencia para trazar el inicio del presente trabajo debido a las pautas en la implementación efectiva del software Zabbix, como una herramienta de monitoreo que analiza, controla y reporta el estado del equipo en tiempo real.

Benavides (2023), en el proyecto de investigación “Implementación de la herramienta Zabbix de monitoreo para el núcleo de la red de la empresa Airmaxtelecom Soluciones Tecnológicas S.A. gratuita y de código abierto”

desarrollada en la ciudad de Ibarra (Ecuador), habla sobre la localización de desperfectos, la medida de consumo de recursos y la notificación de alertas programadas vía Telegram. La comprobación de la herramienta implementada se llevó a cabo mediante el modelo DeLone y McLean, el cual comprende parámetros medibles como la calidad del sistema, de la información, del servicio, la satisfacción del usuario, intención de uso y beneficios netos, obteniendo una preferencia promedio superior al 95%. La iniciativa tecnológica contribuye a aumentar la eficacia de los servicios de infraestructura de red. La vigilancia de posibles incidencias por averías en los equipos se trata con una alta prioridad y los niveles de contrato de servicio se cumplen en un menor tiempo según el contrato celebrado en base a tablas históricas de consumo. La composición de diversos recursos tecnológicos, como es el programa de código abierto y las APIS gratuitas, permitió mejorar el servicio web de la empresa sin incidir en altos costos de implementación y lograr una inversión factible para mantener un monitoreo permanente las 24 horas al día, los 7 días de la semana, durante todo el año. De la presente investigación se puede tomar la experiencia del uso y configuración de los parámetros y utilización del protocolo SNMP que ayuda a obtener información de los recursos de *hardware* y la entrega de una notificación a través de mensajería, característica que resulta provechosa para la investigación actual.

2.1.2. Antecedentes Nacionales.

Casas y Sempértegui (2018) en el proyecto de investigación titulado “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” plantean como objetivo examinar e implementar un sistema que supervise de forma continua los dispositivos conectados en la infraestructura y servicios de la red para así mejorar la administración de la red de dicha universidad. Para empezar, analizan las principales preocupaciones del ámbito de la investigación en relación con el control y la administración de recursos inherentes al sistema de redes de información. Se analizaron las principales herramientas de seguimiento por medio de un cuadro comparativo y una valoración de acuerdo con los requerimientos del área encargada de la Administración de la Red Telemática. El sistema se instaló y configuró para cumplir con los requisitos del departamento de la universidad para verificar y

demostrar la efectividad de la propuesta. Finalmente se consiguió que el administrador de red pueda acceder a información en línea y obtener actualizaciones precisas sobre los servicios destacados e infraestructura de la red, reduciendo el tiempo de falla de estos mediante el uso de un sistema de notificación inmediata. Además, el sistema produce informes que ayudan a los administradores a tomar decisiones y optimizar las operaciones de la red. Se pueden utilizar estas pautas como guía para la adquisición de activos y la creación de un inventario efectivo para el posterior seguimiento de la plataforma informática.

Trujillo (2020) en su trabajo denominado “Influencia de la aplicación del software Zabbix en el monitoreo de la red de área local de la Superintendencia Nacional de los Registros Públicos zona registral N.º V - sede Trujillo”, propone como objetivo establecer la influencia al utilizar el software Zabbix para monitorear la red de área local de la SUNARP. Se realizó la elaboración de un modelo de diseño para la implementación del prototipo que fue probado de forma estadística mediante la prueba T de Student donde obtuvo un error del 5% y un 95% de confianza. Tras la implementación del prototipo, se desarrolló un modelo de diseño y luego se llevó a cabo la aplicación piloto del software, mejorando la eficiencia de la gestión y la emisión de mensajes de notificación temprana de alertas y eventos de la red. El software Zabbix también optimizó los informes de incidentes y facilitó la resolución de problemas durante la planificación y compra de activos. De esta investigación se puede establecer la utilidad e influencia del Software Zabbix en el proceso de monitoreo de redes, así como un análisis estadístico de la efectividad de la propuesta en base a los resultados.

2.2. Bases Teóricas

2.2.1. Software.

Se conoce como “*software*” al grupo de instrucciones, datos o programas que utilizan las computadoras para operarlas y ejecutar tareas específicas, en contraste con el término *hardware* se utiliza para describir los componentes no esenciales de una computadora. El software de un dispositivo es un conjunto de programas, scripts y aplicaciones que se ejecutan en él. Si bien el *hardware* no es fijo, puede considerarse

el elemento variable de una computadora (Awati & Rosencrance, 2021).

Las dos categorías principales en las que se puede dividir el software son de aplicación y de sistema. Una aplicación comprende un software que realiza tareas o satisface necesidades específicas. Mientras que un sistema sirve para operar el *hardware* de la computadora y proporciona una plataforma en la que pueden ejecutarse las aplicaciones.

El software que ofrece a los programadores los recursos de programación necesarios son el middleware, que conecta el software del sistema y las aplicaciones; y el software de controlador, que maneja *hardware* y periféricos de computadora (Awati & Rosencrance, 2021).

2.2.1.1. Software Libre y Software Privativo.

En general, el software puede comercializarse como libre o como propietario. En la categoría de tipo libre se encuentran aquellos que se distribuyen por medio de una licencia que autoriza su utilización, copia, estudio, modificación y redistribución de muchas maneras diferentes (Universidad Politécnica de Valencia, 2023).

Por otro lado, el de tipo propietario constituye una persona natural o jurídica (empresa, empresa, universidad, etc.) que tiene en su poder los derechos de uso de este software y posee la capacidad de controlar y limitar su uso y distribución. Las condiciones en las que los usuarios pueden usar el software se establecen por medio de un Acuerdo de licencia de usuario final (EULA) (Software libre y Software privativo, 2023).

2.2.2. Hardware.

El término “*hardware*” se refiere a cualquier componente físico de una computadora analógica o digital. Este distingue los aspectos tangibles de un dispositivo informático del software, que consiste en instrucciones o programas escritos y legibles por máquina que indican a los componentes físicos qué hacer y cuándo hacerlo. El *software* y el *hardware* son complementarios.

El *hardware* de una computadora se puede dividir en partes internas o externas. Por lo general, los componentes internos constituyen también parte del externo ya que

es necesario para que la computadora funcione correctamente y no se pueden monitorear físicamente (Software libre y Software privativo, 2023).

2.2.2.1. Componentes internos.

Los componentes internos procesan o almacenan colectivamente las instrucciones entregadas por el programa o sistema operativo (SO). Estos incluyen lo siguiente:

Tarjeta madre: se constituye por una placa de circuito impreso que contiene la unidad central de procesamiento (CPU) y otro *hardware* interno esencial cuya función es ser el eje central por el que transitan todos los demás componentes de *hardware*.

CPU: se lo considera como el cerebro de la computadora puesto que en él se procesan y ejecutan las instrucciones digitales de los programas; su velocidad de reloj establece el rendimiento y la eficiencia en el procesamiento de los datos (Awati & Rosencrance, 2021).

RAM: comprende un almacenamiento de memoria temporal que permite gestionar información que sea accesible de forma rápida para los programas; la RAM se considera volátil ya que los datos almacenados son borrados cuando la computadora se apaga.

Disco duro: las unidades de disco duro son módulos de almacenamiento físico que acumulan datos de forma permanente o temporal en diversos formatos como son programas, sistemas operativos, archivos de dispositivos, fotografías, entre otros.

Unidad óptica: las unidades ópticas normalmente residen en un compartimiento para unidades en el dispositivo; permiten que la computadora lea e interactúe con medios externos no magnéticos, como discos compactos de memoria de sólo lectura o discos de video digitales (Awati & Rosencrance, 2021).

Unidad de procesamiento gráfico: este elemento está basado en un chip para procesar datos gráficos y, comúnmente, trabaja como una ramificación de la CPU principal.

Tarjeta de interfaz de red (NIC): es una placa de circuito o chip que permite conectar la computadora a una red; también se denomina adaptador de red y generalmente admite la conexión a una red llamada Ethernet.

2.2.3. Monitoreo de redes e infraestructura.

El monitoreo de red suministra información en tiempo real que los administradores de red requieren para comprobar si una red funciona de forma correcta. Para identificar brechas y mejorar la eficiencia, los administradores emplean herramientas de *software* que facilitan la supervisión de red (Cisco, 2023).

Monitoreo de servidores: su función principal es monitorear el rendimiento del equipo y mostrar la disponibilidad del mismo. Esto puede ocurrir en la nube o en un entorno físico (Cisco, 2023).

Monitoreo de Redes: hoy en día, el monitoreo de red es responsable de supervisar el tráfico en curso y garantizar la seguridad de la red, lo que es crucial para garantizar que la red esté siempre disponible (Cisco, 2023).

Monitoreo de aplicaciones: se utiliza principalmente para monitorear de manera más exhaustiva los mecanismos que la componen, como servidores web, bases de datos, etc. Por otro lado, también permiten identificar problemas con la disponibilidad y el rendimiento.

Se encuentran disponibles varios componentes de los sistemas de monitoreo de red, incluidas herramientas que monitorean el flujo de información, el ancho de banda utilizado y el rendimiento de la red. Además de facilitar actualizaciones de estado, estos sistemas también pueden verificar los dispositivos y unidades que están conectados a la red (Cisco, 2023).

Los administradores emplean los sistemas de monitoreo para detectar errores en equipos, nodos o también identificar los cuellos de botella que restringen el flujo de datos. Estos sistemas pueden ejecutar un análisis de red para enviar informes de error a través de notificaciones mediante correo electrónico o mensajería a los administradores.

2.2.3.1. Tipos de protocolos de monitoreo de red.

a) SNMP.

El Protocolo Simple de Administración de Redes es un protocolo de capa 7, y emplea un sistema de solicitud y contestación para comprobar los estados de varios dispositivos de infraestructura (Walton, 2018).

b) ICMP.

Mediante el uso del Protocolo de Mensajes de Control de Internet, los dispositivos de red, como enrutadores y servidores, pueden transmitir información de operación mediante IP, así como emitir alertas de error en caso de falla del dispositivo (Walton, 2018).

c) Protocolos Proprietarios.

Existen algunos protocolos propietarios, como Cisco Discovery Protocol, que simplifican la gestión de dispositivos Cisco a través de la detección y configuración de sistemas que reciben información entre sí, gracias a diversos protocolos de capa de red (Walton, 2018).

2.2.3.2. Importancia del monitoreo de redes.

a) Visibilidad clara de la red.

Los administradores al monitorear la red pueden identificar todos los dispositivos conectados y observar el flujo de datos, permitiendo solucionar rápidamente cualquier problema que genere fallas o altere el rendimiento (Cisco, 2023).

b) Mejor uso de los recursos de Tecnologías de Información (TI).

Las herramientas de *hardware* y *software* que permiten la supervisión de red ayudan a los equipos de TI a reducir las tareas manuales, garantizando más tiempo al personal de TI para ocuparse en proyectos fundamentales para la organización (Cisco, 2023).

c) Análisis temprano de las necesidades de infraestructura futuras.

Los sistemas de supervisión tienen capacidad de generar informes acerca del rendimiento de los mecanismos de la red en un período de tiempo establecido. Los administradores se basan en estos informes para poder establecer requisitos de la organización que permitan actualizar o implementar una nueva o mejor infraestructura de TI (Cisco, 2023).

d) La capacidad para identificar amenazas de seguridad más rápido.

Las organizaciones se apoyan en la supervisión de las operaciones de la red para determinar el rendimiento promedio de sus redes. La identificación de problemas y detección de posibles riesgos de seguridad es una función de los administradores al observar un aumento inesperado en los niveles de tráfico de la red (Cisco, 2023).

2.2.4. SNMP.

El protocolo de capa de aplicación SNMP (*Simple Network Management Protocol*) incluye el conjunto de protocolos TCP/IP¹, mismo que se estableció por la Junta de Arquitectura de Internet (IAB) en el RFC1157. Su principal función es facilitar el intercambio de datos informáticos y de administración entre dispositivos de la red, permitiendo así la gestión y el monitoreo de los recursos (ManageEngine, 2020).

SNMP es muy utilizado en la supervisión y administración de dispositivos de red puesto que, en general, todo dispositivo de red profesional cuenta con un agente SNMP, que debe ser configurado y habilitado para establecer comunicación con el Sistema de Administración de Red (NMS) (ManageEngine, 2020).

2.2.4.1. Elementos integrantes del SNMP.

a) Administrador de SNMP.

El administrador es un ente independiente que cumple la función de interactuar con los dispositivos de red que utilizan agentes SNMP. Por lo general, se compone de una computadora que permite correr uno o varios sistemas de gestión de red. Las

¹ TCP/IP (Protocolo de control de transmisión/Protocolo de Internet) es un conjunto de protocolos de comunicación que permiten interconectar dispositivos de red en Internet.

principales funciones del administrador SNMP son:

- Agente de consultas.
- Obtener una respuesta desde el agente.
- Establecer variables en el agente.
- Identificar eventos asincrónicos del agente.

b) Dispositivo administrado.

Un dispositivo de la red gestionado o administrado es una unidad que requiere alguna forma de monitoreo y control, como *routers*, *switches*, servidores, *desktops*, impresoras, UPS, entre otros (ManageEngine, 2020).

c) Agente SNMP.

Los agentes son programas que están encapsulados en elementos de red, cuando se habilitan admiten la recopilación de información sobre la administración de dispositivos conectados a nivel local y facilitan la entrega al administrador SNMP cuando lo solicite. Estos agentes pueden ser estándar (p. ej., Net-SNMP) o definidos por el proveedor, por ejemplo, *HP Insight Agent* (ManageEngine, 2020).

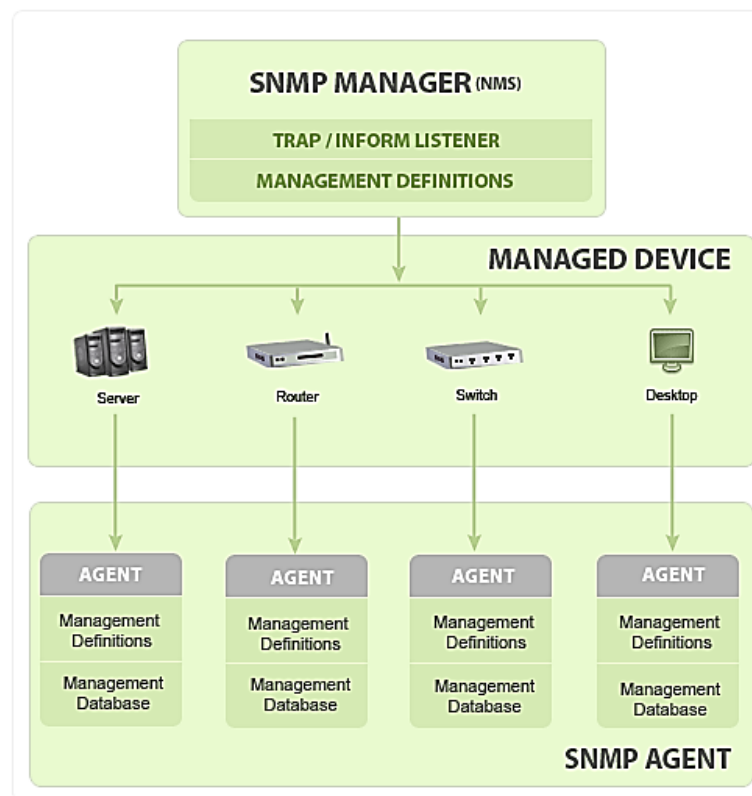
Las funciones principales del agente SNMP son:

- Recopilar información administrativa del entorno local.
- Almacenar y recuperar información administrativa o de gestión definida en la Base de datos de información de gestión (MIB).
- Reportar el incidente a un administrador.
- Cumple la función de Proxy para ciertos nodos administrados que no son SNMP.

En la Figura 1 se ilustran los elementos que componen este protocolo en cada dispositivo y muestra cómo funciona el agente SNMP en cada uno de ellos para la administración de bases de datos y procesamiento de la información.

Figura 1

Elementos integrantes del protocolo SNMP.



Nota: Tomado de “*What is SNMP?*”, por ManageEngine, (2020).

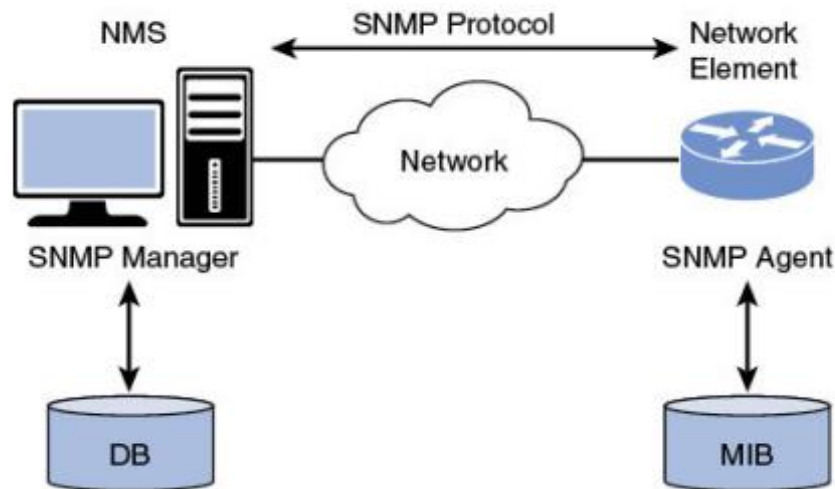
2.2.4.2. Base de datos de información de gestión (MIB).

Un agente SNMP contiene una base de datos donde se establecen los parámetros de los equipos administrados. El administrador de SNMP usa esta información para realizar consultas específicas al agente e interpretar aún más los datos que necesita el sistema de administración de red (NMS). Esta base de datos, que por lo general es compartida entre agentes y administradores, se denomina Base de Información de Administración (MIB) (ManageEngine, 2020).

Las MIB, en general, almacenan un conjunto de estadísticas estándar y valores de control definidos para cada dispositivo. SNMP también permite que estos valores predeterminados se amplíen a valores específicos del agente utilizando MIB privados, la Figura 2 ilustra el proceso de comunicación mediante el protocolo SNMP de las bases de datos.

Figura 2

Comunicación SNMP.



Nota: Un archivo MIB, a modo de resumen, se compone de un grupo de consultas que un administrador puede realizar a un agente. Tomado de “*What is SNMP?*”, por ManageEngine, (2020), <https://www.manageengine.com/network-monitoring/what-is-snmp.html>.

2.2.4.3. Estructura MIB e identificador de objeto (ID de objeto u OID).

Una base de información de administración (MIB) se compone de objetos administrados y reconocidos por identificadores de objetos con nombre (ID de objeto u OID). El identificador es único para cada objeto y establece una propiedad específica de la entidad gestionada. Cuando se ejecuta una consulta, el valor que retorna cada ID puede ser diferente, como texto, número, tipo, entre otros. Hay dos tipos de ID de objeto: escalar y tabla (Walton, 2018).

Escalar: Define una sola instancia del objeto (por ejemplo, el nombre de la entidad proveedora) cuyo resultado se limita a ser sólo uno.

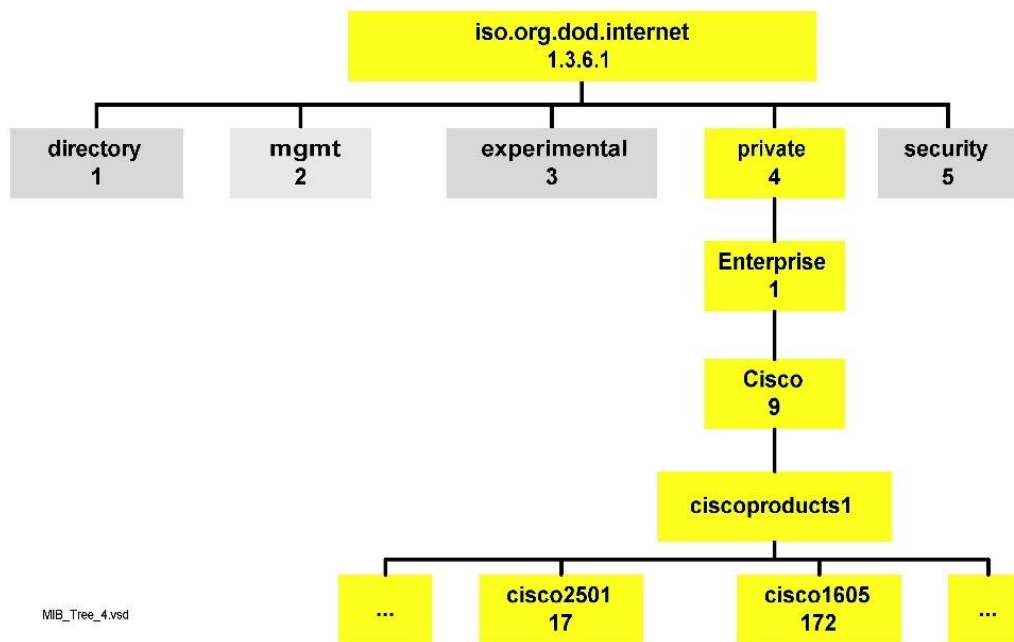
Tabla: Esto devolverá un resultado para cada variable de forma individual, es decir, varios resultados para un mismo ID de objeto.

La MIB está organizada jerárquicamente mediante el ID de objeto, misma que puede representarse como una distribución en forma de árbol con un único

identificador de variable como se puede apreciar en la Figura 3 para un equipamiento Cisco.

Figura 3

Estructura jerárquica de una MIB.



Nota: Árbol jerárquico de una MIB de equipamiento Cisco. Tomado de SNMP: funcionamiento y configuración – CCNA, por Walton A., (2018).

2.2.4.4. Versiones de SNMP.

Desde sus inicios, SNMP se ha actualizado significativamente. Sin embargo, SNMP v1 y v2c se consideran las versiones más utilizadas. El soporte para el protocolo SNMP v3 aún no es tan popular en el mercado a pesar de ser más seguro que las anteriores (Walton, 2018).

a) SNMP v1.

Es la primera adaptación y se estableció en los RFC 1155 y 1157.

b) SNMP v2c.

Es una revisión de la SNMPv1, que mejora los aspectos relacionados al tipo de paquetes, mapas de transporte y objetos estructurales MIB, sin dejar de lado el marco

de gestión de SNMPv1 existente. Se estableció en RFC 1901, RFC 1905, RFC 1906, RFC 2578 (Walton, 2018).

c) *SNMPv3*.

Constituye la versión más segura y también facilita la configuración remota de dispositivos SNMP. Fue definido en los RFC 1905, RFC 1906, RFC 3411, RFC 3412, RFC 3414, RFC 3415. A pesar de que cada lanzamiento avanza hacia una funcionalidad mayor, el enfoque especial se da a ciertos aspectos de seguridad de cada actualización. Entre ellos:

- Seguridad comunitaria SNMP v1.
- Seguridad comunitaria SNMP v2c.
- Seguridad basada en el usuario de SNMP v2u.
- Seguridad de grupo SNMP v2.
- Seguridad basada en el usuario SNMP v3.

2.2.5. Sistema de monitoreo Zabbix.

Zabbix fue creado por Alexei Vladishev en el año 2001, y en la actualidad se desarrolla y respalda por Zabbix SIA como una alternativa para realizar el monitoreo bajo la condición de distribución con código abierto de clase empresarial.

Constituye una herramienta de *software* que supervisa diversos parámetros de la red y el bienestar de servidores, aplicaciones, servicios, máquinas virtuales, bases de datos, sitios *web*, la nube y otros componentes. Proporciona seguimiento para estos parámetros. Un sistema de notificación fácil de usar permite la creación de alertas de cualquier evento mediante correo electrónico. Esto garantiza una resolución oportuna de los problemas que presenta el servidor. Además, ofrece funciones destacadas para la visualización de datos y generación de informes con base en los datos almacenados. Convirtiendo a Zabbix en una opción ideal en la planificación de capacidad (Zabbix, 2023).

Este programa proporciona funciones para el sondeo y la captura, es decir, realiza la monitorización usando SNMP en sus dos formas *polling* o *trapping*. Una interfaz basada en web proporciona acceso a todos los informes, estadísticas y

parámetros de configuración, para supervisar el estado de su red y servidores de forma remota. Zabbix puede ser un componente crucial de la infraestructura de TI para su monitoreo, siempre que esté configurado correctamente. Las implicaciones son igualmente aplicables a las pequeñas empresas con servidores limitados y a las grandes empresas con una cantidad significativa de servidores. No hay cargos por usar el *software*, ya que cuenta con una Licencia Pública General (GPL) versión 2. Su código fuente está disponible gratuitamente y abierto al público, la Figura 4 presenta la pantalla de inicio del sitio web oficial de Zabbix donde se puede obtener sus manuales y ficheros de instalación (Zabbix, 2023).

Figura 4

Presentación de Zabbix.



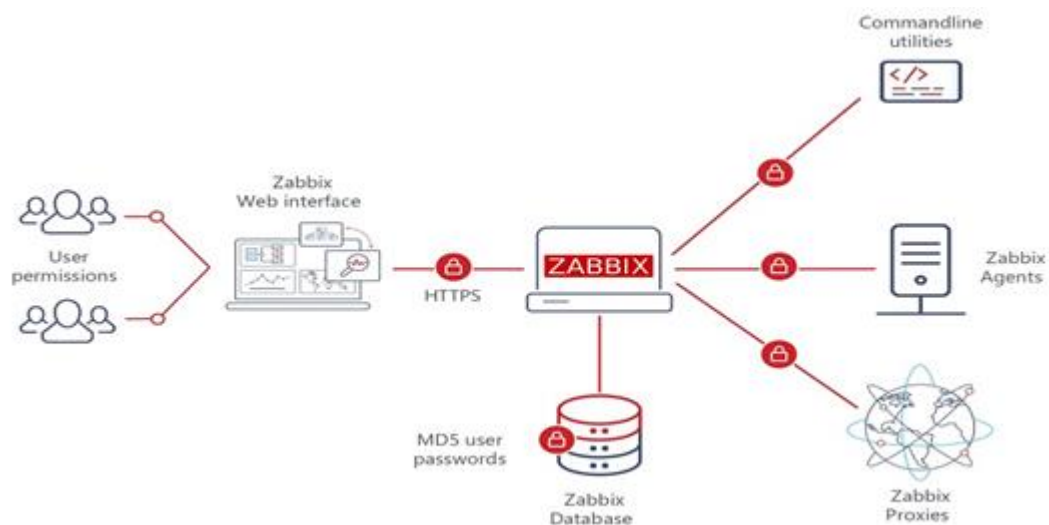
Nota: Captura de la página de inicio del software. Tomado de Zabbix Features Overview, (2023).

2.2.5.1. Arquitectura.

Varios componentes de *software* importantes componen a Zabbix, como se ilustra en la Figura 5, cada uno cumple con funciones específicas que se describen a continuación.

Figura 5

Arquitectura del sistema de monitoreo Zabbix.



Nota: Tomado de Zabbix Features Overview, (2023).

a) Servidor Zabbix.

Los agentes brindan información crucial en torno a la disponibilidad, integridad y datos estadísticos del uso del servidor Zabbix como componente central, ya que en este se almacenan todos los datos relacionados con la configuración, operatividad y de estado que también sirve como sistema de alerta para los administradores cuando los sistemas experimentan problemas inesperados.

Recopila datos, calcula activadores y envía notificaciones a los usuarios a través de la contaminación del servidor. El factor principal que impulsa los informes de los agentes y proxies de Zabbix sobre la disponibilidad e integridad del sistema es este aspecto. Se pueden utilizar comprobaciones de servicio simples para inspeccionar de forma remota los servicios de red, como servidores web y servidores de correo (Zabbix, 2023).

Un servidor Zabbix básico para su operatividad requiere tres componentes distintos como son servidor, interfaz web y almacenamiento de bases de datos. Tanto el servidor como la interfaz interactúan con la base de datos, en la que se almacena la información concerniente a la configuración de Zabbix.

La creación de un nuevo artículo a través de la interfaz *web* (o API) da como resultado su inclusión en una tabla de artículos en la base de datos. Se recuperará una lista de elementos activos del caché del servidor Zabbix una vez por minuto y se almacenará en la tabla de elementos. Por este motivo, la interfaz de Zabbix puede tardar hasta dos minutos en aparecer en la sección de datos más recientes (Zabbix, 2023).

b) Almacenamiento de base de datos.

Contiene toda la información de configuración y datos recopilados por Zabbix.

c) Interfaz web.

Accesible desde cualquier ubicación al ser basada en *web* que simplifica el proceso. Normalmente, la interfaz está ubicada en la máquina física del servidor y no se ejecuta por separado.

d) Proxy.

Ayuda a recolectar los datos de utilidad y disponibilidad en nombre del servidor. Se considera como una parte opcional en el proceso de implementación de Zabbix, pero aporta con grandes beneficios en funciones como distribuir la carga de un único servidor (Zabbix, 2023).

e) Agente.

El monitoreo activo de recursos y aplicaciones locales implica la implementación de agentes Zabbix que reportan datos al servidor. La versión 4.4 ha introducido dos tipos de agentes: el agente Zabbix, que es liviano y se puede usar en varias plataformas con código C, y el agente Zabbix 2, que ofrece flexibilidad y compatibilidad de complementos con Go (Zabbix, 2023).

El agente Zabbix lleva a cabo la supervisión activa de los recursos y aplicaciones locales, incluidos los discos duros, la memoria y las estadísticas del procesador, cuando se implementa en un objetivo de supervisión. Este recupera información operativa del servidor para enviarla a la base de datos central que se encarga de su posterior procesamiento. Cuando el servidor experimenta fallas, como un disco duro completamente operativo o un proceso de servicio defectuoso, puede

alertar a los administradores de la máquina afectada. El uso de llamadas al sistema nativo para recopilar información estadística hace que los agentes de Zabbix sean altamente eficientes (Zabbix, 2023).

2.2.5.2. Controles pasivos y activos.

Las comprobaciones que realizan los agentes de Zabbix pueden ser pasivas y activas seleccionando el tipo de elemento durante el monitoreo.

Durante una solicitud de datos en una verificación pasiva, los datos, como la carga de la CPU, se solicitan al servidor Zabbix (o proxy) y el agente designado devuelve el resultado. El procesamiento es más complejo para los controles activos. Para que el agente procese una lista de elementos de forma independiente, es necesario obtener su lista del servidor Zabbix. Una vez concluido el proceso, envía periódicamente nuevos números al servidor (Zabbix, 2023).

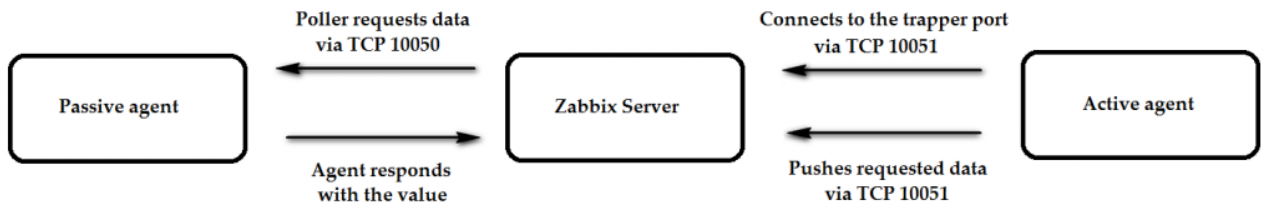
El agente en modo pasivo significa que el sondeador (proceso interno del servidor) se conecta al agente en el puerto 10050/TCP y sondea un determinado valor (por ejemplo, carga de la CPU del *host*). El sondeador espera hasta que el agente del *host* responda con el valor. Luego, el servidor recupera el valor y la conexión se cierra (Zabbix, 2023).

En el modo activo, todo el procesamiento de datos se realiza en el agente, sin la interferencia de los encuestadores. Sin embargo, el agente debe saber qué métricas deben monitorearse y por esta razón el agente se conecta al puerto denominado Trapper 10051/TCP del servidor una vez cada dos minutos (de forma predeterminada). El agente solicita información sobre los elementos y luego realiza la supervisión en el *host* y envía los datos al servidor a través del mismo puerto TCP (Zabbix, 2023).

El funcionamiento del servidor con el agente en modo pasivo y activo de Zabbix se puede apreciar de manera gráfica en la Figura 6.

Figura 6

Mecanismo de sondeo pasivo y activo de Zabbix.



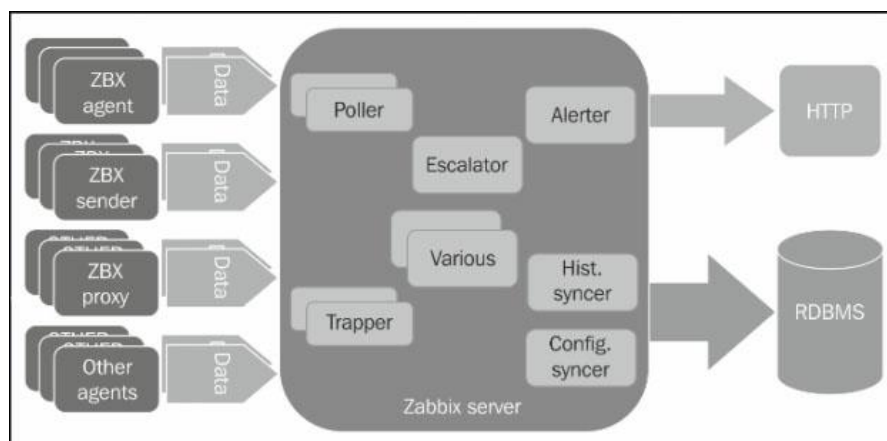
Nota: Ilustración de la conexión del agente en modo pasivo y activo. Tomado de Zabbix Agent: Active vs. Passive, por D. Lambert, (2020).

2.2.5.3. Flujo de datos

Para capturar los datos en Zabbix, se requiere un *host* que se debe crear primero. Dentro del entorno de Zabbix, debes tener algo que crear si lo deseas. Crear una acción requiere un desencadenante, ya que los datos fluyen a través del servidor como se aprecia en la Figura 7, por ejemplo, en caso de que la carga de su CPU sea demasiado alta, se activa la notificación a través del servidor y luego se recibe una notificación por correo electrónico. Puede parecer un proceso largo, pero el uso de plantillas los hace destacar. Este diseño permite la creación de una configuración altamente adaptable (Lambert, 2020).

Figura 7

Flujo de datos de monitoreo de Zabbix.

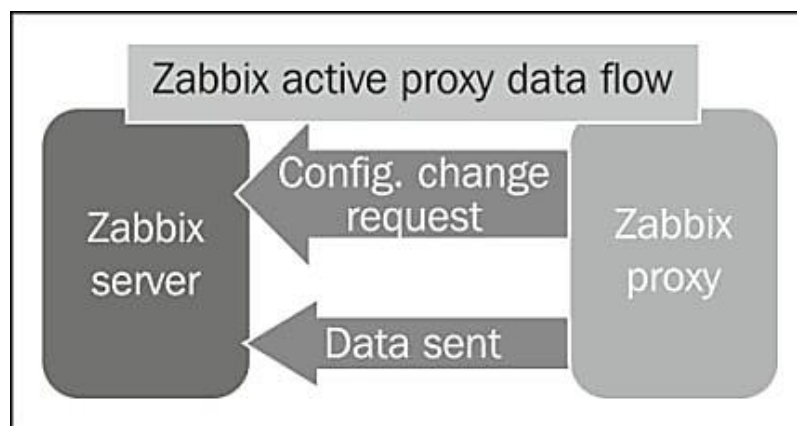


Nota: Tomado de Zabbix Agent: Active vs. Passive, por D. Lambert, (2020).

Los proxies de Zabbix pueden operar en dos modos diferentes, activo y pasivo. La configuración predeterminada es el proxy activo. En esta configuración, el proxy inicia todas las conexiones al servidor Zabbix, mismo que se utiliza en el proceso de restablecimiento de información relacionada a la configuración de los objetos monitoreados y la conexión para enviar mediciones al servidor (Zabbix, 2023).

Figura 8

Modelo activo del flujo de datos de Zabbix.



Nota: Tomado de Zabbix Agent: Active vs. Passive, por D. Lambert, (2020).

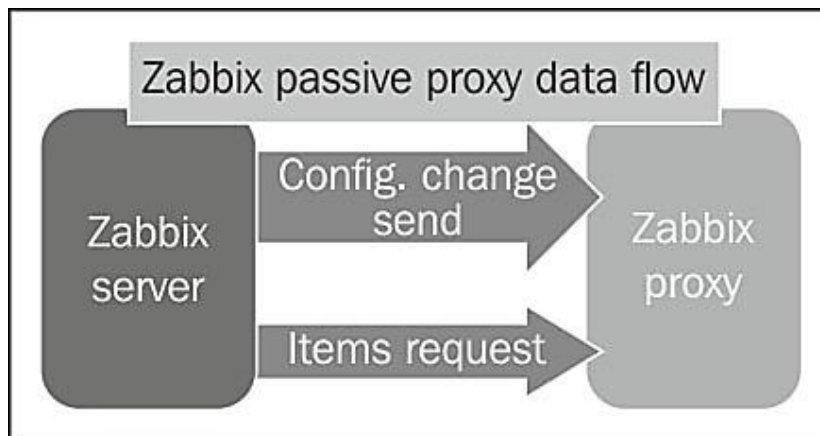
Como puede ver en la Figura 8, el servidor esperará recibir solicitudes del proxy y nada más. El proxy activo es la forma más eficaz de descargar tareas del servidor. De hecho, el servidor simplemente permanecerá esperando que se le pregunte sobre cambios en la configuración o recibir nuevos datos de monitoreo (Lambert, 2020).

Por otro lado, los servidores proxy generalmente se implementan para monitorear segmentos de red seguros con políticas estrictas de tráfico saliente y generalmente se instalan en DMZ (red perimetral). En este tipo de escenarios, normalmente es muy difícil obtener permiso para que el proxy inicie la comunicación con el servidor. Desafortunadamente, no se debe sólo a las políticas. Las DMZ están lo más aisladas posible de las redes internas, ya que deben ser lo más seguras posible. En torno al aspecto de seguridad, por lo general, suele ser más fácil y aceptado iniciar una conexión desde la red interna a una DMZ. En este tipo de

escenario, el proxy pasivo resulta muy útil. El proxy pasivo es casi una imagen reflejada de la configuración del proxy activo, como puede ver en la Figura 9.

Figura 9

Modelo pasivo del flujo de datos de Zabbix.



Nota: Tomado de Zabbix Agent: Active vs. Passive, por D. Lambert, (2020).

2.3. Definición de términos básicos

API (*Application Programming Interface*): Una interfaz de programación de aplicaciones se resume como un conjunto de características y protocolos utilizados para diseñar y componer el *software* de las aplicaciones (IBM, 2023).

CPU: Elemento del sistema informático encargado de controlar la interpretación y ejecución de las instrucciones (Walton, 2018).

DMZ: Una red perimetral o subred apantallada que separa una red interna que es más confiable de una red externa que es menos confiable. Una red creada conectando dos *firewalls*. Aquellos sistemas con acceso remoto exterior que requieren de ciertas protecciones son las que generalmente se establecen en redes DMZ (Stouffer, Pillitteri, Lightman, Abrams, & Hahn, 2023).

HTTP: Se ubica en la capa de aplicación y es conocido como Protocolo de transferencia de hipertexto (HTTP) para transferir documentos hipermedia, incluido HTML. La finalidad de su diseño es facilitar la comunicación entre servidores *web* y navegadores, pero también puede utilizarse para otros fines (Cloudfare, 2023).

ICMP: Sus siglas significan Protocolo de Mensajes de Control de Internet (ICMP) y sirve para identificar problemas de comunicación de red. Su principal objetivo en la capa de red es garantizar la entrega oportuna de datos (Cloudfare, 2023).

IP: Consiste en un identificador que habilita el envío de información entre los dispositivos conectados en una red, este se compone de datos de ubicación y permite que los equipos accedan a la comunicación (Walton, 2018).

ITIL V4: El marco ITIL se ha reestructurado fundamentalmente para dar más peso a los valores, costos y riesgos, ya que incorpora conocimientos y conceptos actualizados, el nuevo marco aún mantiene muchos de los mismos elementos que ITIL V3, con un enfoque en la prestación de servicios de TI basados en valor (Ivanti, 2023).

NOC: Un centro de operaciones de red, es una ubicación que se concentra en la gestión de redes de comunicación, ya sea a nivel local o nacional. Su función principal es la de monitorizar las redes y estar pendientes de cualquier avería que se presente, sea cual sea el motivo, para actuar de inmediato y desviar las cargas de tráfico según convenga en cada momento (Servicenow, 2023).

NTP: El Protocolo de Hora de Red se utiliza para sincronizar las fuentes de hora del reloj de la computadora en una red al ser un protocolo de Internet (Walton, 2018).

Protocolo: Consiste en un conjunto estandarizado de normativas que especifican la manera de llevar a cabo una conversación, incluyendo el formato, tiempo, secuenciación y/o verificación de errores (Cloudfare, 2023).

SLA: Sus siglas se traducen como Acuerdo de Nivel de Servicio (SLA) y comprende un acuerdo celebrado entre un proveedor de servicios y sus clientes a través de un documento que detalla lo contratado y establece las pautas de servicio que debe cumplir el proveedor. Una forma más amplia y generalizada de un SLA es un compromiso de nivel de servicio denominado por sus siglas SLA (Rouse, 2018).

SMTP: El Protocolo Simple de Transferencia de Correo consiste en un protocolo de comunicación que permite intercambiar mensajes de correo electrónico a través de Internet (AWS, 2023).

SNMP (*Simple Network Management Protocol*): Se considera un protocolo estándar de tipo solicitud-respuesta que recopila información de gestión de los equipos de red, proporcionando un medio para monitorear el tráfico y establecer parámetros de configuración (Walton, 2018).

SPSS (*Statistical Package for the Social Sciences*): Es un *software* muy útil para el análisis de datos estadísticos utilizando una interfaz intuitiva que provee de varias funciones para llevar a cabo la extracción de información procesable de los datos de forma rápida. Esta herramienta contribuye en el proceso de toma de decisiones respecto a la calidad gracias a su gran precisión (IBM, 2023).

TCP: Se considera como un protocolo principal de las redes y se compone de dos partes. El protocolo IP es el encargado únicamente de los paquetes mientras que TCP se ocupa de que dos *hosts* puedan establecer una conexión para intercambiar flujos de datos y garantiza a más de la entrega de los paquetes también que el orden de entrega sea el mismo en que fueron enviados (Stouffer, Pillitteri, Lightman, Abrams, & Hahn, 2023).

UDP: El Protocolo de Datagramas de Usuario se utiliza en internet para transmisiones categorizadas de urgentes, como la reproducción de video o búsquedas de DNS. Al ser un protocolo de comunicación contrario a TCP, acelera las comunicaciones, pero no está orientado la conexión antes de iniciar la transferencia de información (Stouffer, Pillitteri, Lightman, Abrams, & Hahn, 2023).

VLAN: Una Red de Área Local Virtual consiste en una red incorporada de forma lógica que congrega un subconjunto de equipos que comparten una LAN (Red de Área Local) física, seccionando el tráfico de cada grupo (Walton, 2018).

CAPÍTULO III. DESARROLLO DEL TRABAJO PROFESIONAL

3.1. Determinación y análisis del problema

DESYSWEB S.A.C. es una empresa dedicada a brindar soluciones tecnológicas integrales a distintos clientes tanto del sector corporativo como de gobierno dentro del rubro de las telecomunicaciones.

Dentro de las gestiones de identificación de averías se estableció que existía una gran necesidad de conocer e identificar cuando los equipos perdían conexión y más aún identificar las causas, tiempos de desconexión y generar una notificación en tiempo real que permita identificar dichas desconexiones. Para actuar proactivamente ante reclamos, así como establecer con precisión la criticidad de las averías.

En primer lugar, no se contaba con una herramienta dentro del área local que permita el monitoreo de los distintos equipos que componen la infraestructura de TI. Esto ocasionó que, al no tener una herramienta de monitoreo que detecte equipos desconectados o averiados, no se dé el tratamiento oportuno, quedando inclusive sin funcionamiento por mucho tiempo.

Por lo tanto, algunas de las áreas se veían perjudicadas al no poder realizar de manera oportuna pagos a proveedores, a causa de la no operatividad del equipo de la base de datos, retrasando la entrega de los materiales en los plazos establecidos. En el primer trimestre del año la empresa se vio perjudicada económicamente al incumplir el SLA de entrega, no se podrá detallar la cifra por confidencialidad de la empresa.

Por lo expuesto, el presente trabajo profesional busca solventar o reducir los tiempos de desconexión de los equipos de la red local de la empresa a través de la implementación del *software* Zabbix como herramienta de monitoreo para la gestión correctiva.

La necesidad de sustentar la implementación de un sistema de monitoreo que permita optimizar los tiempos de atención es en base a la siguiente encuesta de diagnóstico situacional antes de desarrollar este trabajo.

3.1.1. Encuesta a los usuarios de la red local de la empresa DESYSWEB.

La encuesta está dirigida a los empleados que utilizan dispositivos o recursos que parecen requerir conectividad y acceso a base de datos todos los días. El formato de encuesta se presenta en el ANEXO 4.

Se tiene como objetivo determinar los efectos positivos y negativos de la implementación del *software* Zabbix como herramienta de monitoreo de la red local de la empresa DESYSWEB.

A partir de la Figura 10 se puede decir que, el 50% de los usuarios indican que antes de la implementación del Zabbix aproximadamente se tardaban una hora en resolver los incidentes de infraestructura de TI. Por otro lado, a partir de la Tabla 1 se puede decir que, el 85.7% de los usuarios indican que antes de la implementación del Zabbix como máximo se tardaban dos horas aproximadamente en resolver los incidentes de infraestructura de TI.

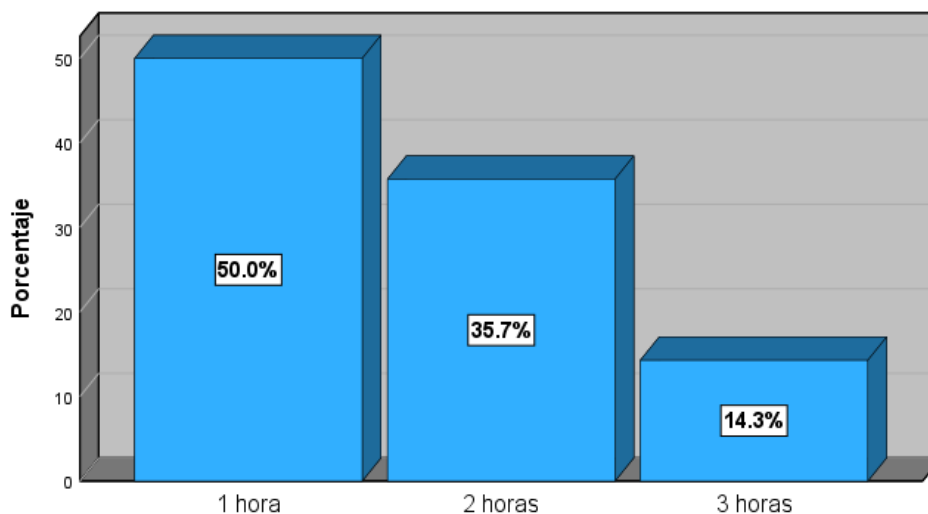
Tabla 1

Tiempo de falla vs tiempo de resolución.

Opciones	Frecuencia	Porcentaje	Porcentaje acumulado
1 hora	7	50,0	50,0
2 horas	5	35,7	85,7
3 horas	2	14,3	100,0
Total	14	100,0	

Figura 10

Gráfica comparativa de tiempo de resolución de interrupciones.



Los resultados que se presentan en la Figura 11 indican que el 64.3% de los usuarios señalan que antes de la implementación en promedio se tardaba una hora en encontrar el dispositivo o servicio de TI que causaba el incidente. Por otro lado, a partir de la Tabla 2 se puede decir que, el 92.9% de los usuarios revelan que antes de la implementación requerían como máximo una hora para encontrar el dispositivo o servicio de TI que causaba el incidente.

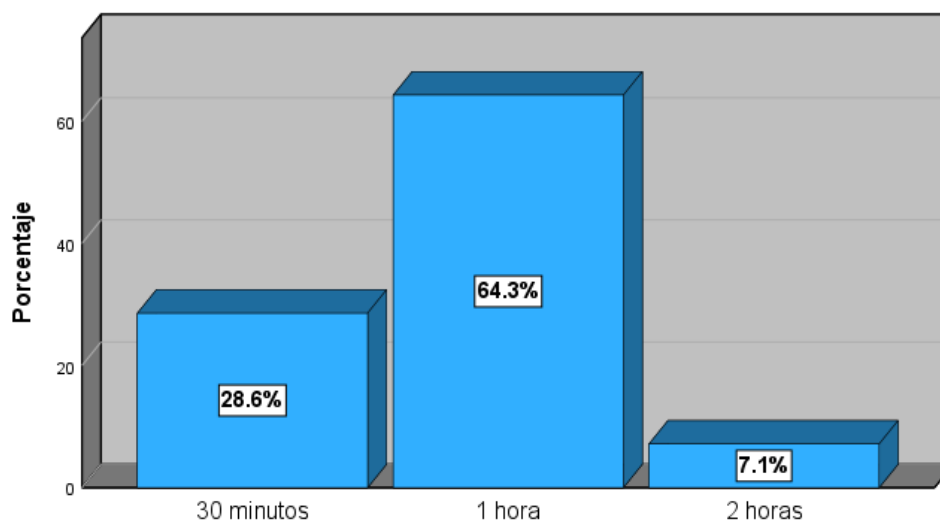
Tabla 2

Tiempo de falla vs tiempo de resolución.

Opciones	Frecuencia	Porcentaje	Porcentaje acumulado
30 minutos	4	28,6	28,6
1 hora	9	64,3	92,9
2 horas	1	7,1	100,0
Total	14	100,0	

Figura 11

Gráfico de tiempo de localización de dispositivo fallido.



3.2. Modelos de Solución Propuesto

Ante la problemática expuesta, se desarrolla la implementación del *software* Zabbix para disponer de una herramienta integrada que permita agilizar la acción de monitoreo. La implementación ha permitido una rápida corrección de incidentes dentro

de la organización, además, detectar posible aparición de eventos y tomar acción de manera más oportuna y no incurrir en penalidades.

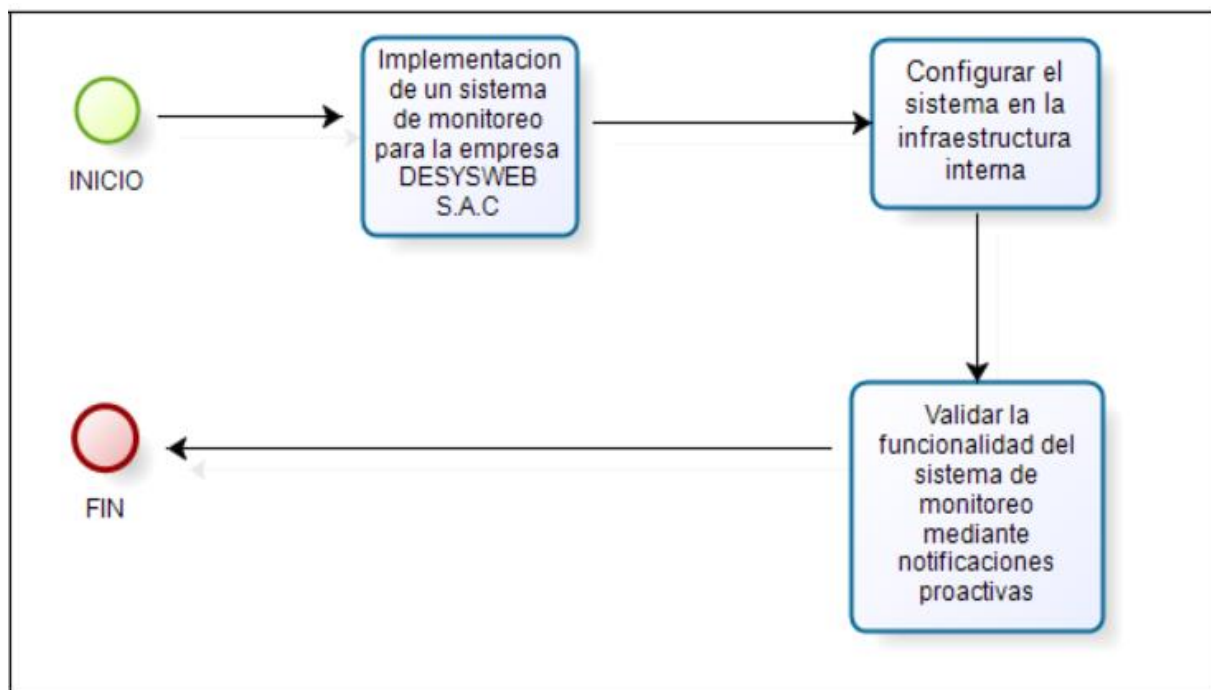
La implementación de plataforma Zabbix ha garantizado verificar de manera constante el estado de los equipos configurados, permite visualizar los cambios o anomalías detectados en intervalos de tiempo breves.

Las diversas asignaturas que se ha desarrollado durante la formación universitaria han contribuido significativamente a la consolidación de conocimientos teóricos y prácticos en materias como: teorías de redes, arquitectura de redes y protocolos, transmisión de datos, telecomunicaciones I, entre otras. Además, fuera del entorno universitario se ha alcanzado una certificación en ITIL V4, llevar cursos y diplomados en Ciberseguridad que han permitido ejecutar el presente trabajo de manera adecuada, lo que ha ayudado a resolver problemas dentro de la organización.

En la Figura 12 se muestra el diagrama de flujo del desarrollo de este trabajo.

Figura 12

Flujograma de desarrollo del trabajo.



3.2.1. Implementación del sistema de monitoreo Zabbix

Se describe a continuación los requerimientos y consideraciones que se establecieron para realizar la instalación del *software* Zabbix de versión 6.0. Así mismo, se explica mediante diagramas las instalaciones tanto de las bases de datos como la instalación del instrumento Zabbix, su configuración y validación del sistema de monitoreo.

3.2.1.1. Requisitos del sistema de monitoreo

Realizar la instalación del sistema de monitoreo Zabbix, se puede realizar tanto en un servidor virtualizado como físico, importante considerar los recursos del servidor, cantidad de almacenamiento, memoria etc. para que sea más eficiente la cantidad de *hosts* que deseamos.

La implementación se llevó a cabo en una máquina virtual con sistema operativo CentOS Stream 8. En la Tabla 3 se muestra el detalle de las especificaciones del sistema.

Tabla 3

Recursos de la máquina virtual.

Sistema Operativo	CentOS 8 Stream
Almacenamiento	500.00 GB
Memoria RAM (GB)	8 GB
Disco Duro Aprox. (GB)	8 GB

Para garantizar que el servidor Zabbix funcione correctamente, es necesario deshabilitar SELinux durante el proceso de configuración de la máquina virtual. Además, preparar el sistema operativo correctamente es esencial. Dado que es importante tener una fecha precisa en el sistema, el cliente NTP debe configurarse. Se recomienda encarecidamente que todos los sistemas Zabbix mantengan la fecha del sistema sincronizada.

Se evidencia en la Figura 13 mediante el comando **sestatus** que por defecto SELinux se encuentra habilitado, es importante deshabilitarlo antes de instalar Zabbix.

Figura 13

SELinux habilitado.

```
[root@localhost ~]# sestatus
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:      /etc/selinux
Loaded policy name:          targeted
Current mode:                 enforcing
Mode from config file:       enforcing
Policy MLS status:           enabled
Policy deny_unknown status:  allowed
Memory protection checking:   actual (secure)
Max kernel policy version:   33
[root@localhost ~]#
```

Se detalla en la Figura 14 el proceso de deshabilitar SELinux, para ello se ingresa al fichero de configuración utilizando el comando **vi/etc/selinux/config**.

Figura 14

Proceso de deshabilitar SELinux.

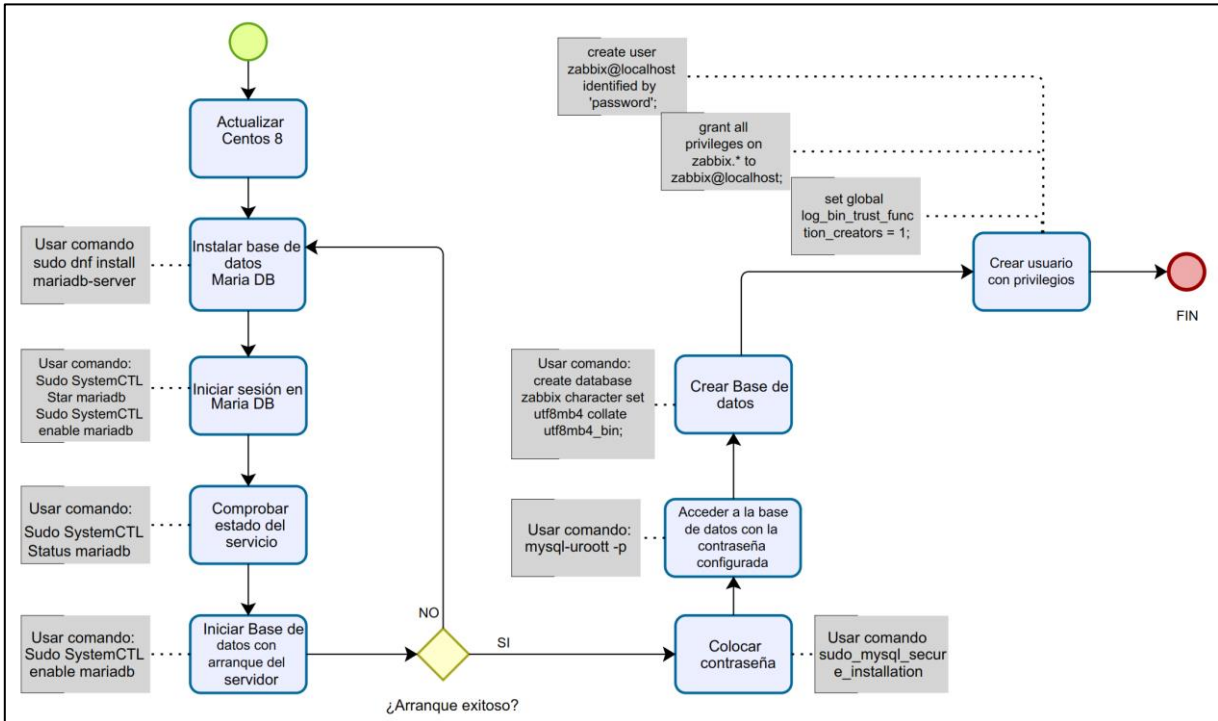
```
2. 192.168.134.228
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of these three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

3.2.1.2. Instalación de la base de datos

Mediante un diagrama de flujo, como se muestra en la Figura 15, se indican los pasos que se requieren para instalar la base de datos MariaDB 10.6. Se debe considerar que este procedimiento se realizó con usuario Root.

Figura 15

Flujograma de la instalación de la base de datos.



Se detalla en los siguientes pasos los comandos de instalación de la base de datos MariaDB 10.6.

Paso 1.

La ejecución de comandos en la máquina virtual se evidencia a través de capturas de pantalla. Se muestra en la Figura 16 los comandos para el proceso de instalación y en la Figura 17 la ejecución para la gestión.

Figura 16

Instalación de base de datos MariaDB. Se activa y habilita la base de datos para el funcionamiento.

```
[root@localhost ~]# sudo dnf install mariadb-server
```

Figura 17

Ejecución de gestor de base de datos MariaDB.

```
[root@localhost ~]# sudo systemctl start mariadb  
[root@localhost ~]# sudo systemctl enable mariadb
```

Paso 2.

A continuación, se evidencia en la Figura 18 la lista del esquema de base de datos Zabbix, y en la Figura 19 el proceso de creación de las tablas y el inicio de sesión en el motor de base de datos para crear la instancia inicial.

Figura 18

Conexión a base de datos.

```
[root@localhost ~]# mysql -uroot -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 16
Server version: 10.3.28-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MariaDB [(none)]>
```

Figura 19

Creación del esquema interno de la base de datos.

```
MariaDB [(none)]> create database zabbix character set utf8mb4 collate utf8mb4_bin;
Query OK, 1 row affected (0.001 sec)

MariaDB [(none)]> create user zabbix@localhost identified by 'p4ssw0rd';
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> grant all privileges on zabbix.* to zabbix@localhost;
Query OK, 0 rows affected (0.000 sec)

MariaDB [(none)]> set global log_bin_trust_function_creators = 1;
Query OK, 0 rows affected (0.000 sec)

MariaDB [(none)]> quit;
```

Paso 3.

El detalle de las configuraciones se presenta en la Figura 20, mientras que la Figura 21 muestra el importe del esquema y los datos iniciales de Zabbix respecto con la base de datos previamente creada.

Figura 20

Configurar la base de datos para el servidor Zabbix en el fichero `/etc/zabbix/zabbix_server.conf`.

```
[root@localhost ~]# zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz |
mysql --default-character-set=utf8mb4 -uzabbix -p zabbix
Enter password:
[root@localhost ~]#
```

Figura 21

Fichero de configuración del servidor Zabbix.

```
### Option: DBPassword
# Database password.
# Comment this line if no password is used.
#
# Mandatory: no
# Default:
```

Finalmente, se realiza la activación de los puertos para ingresar al Zabbix y efectuar la configuración de la *web*.

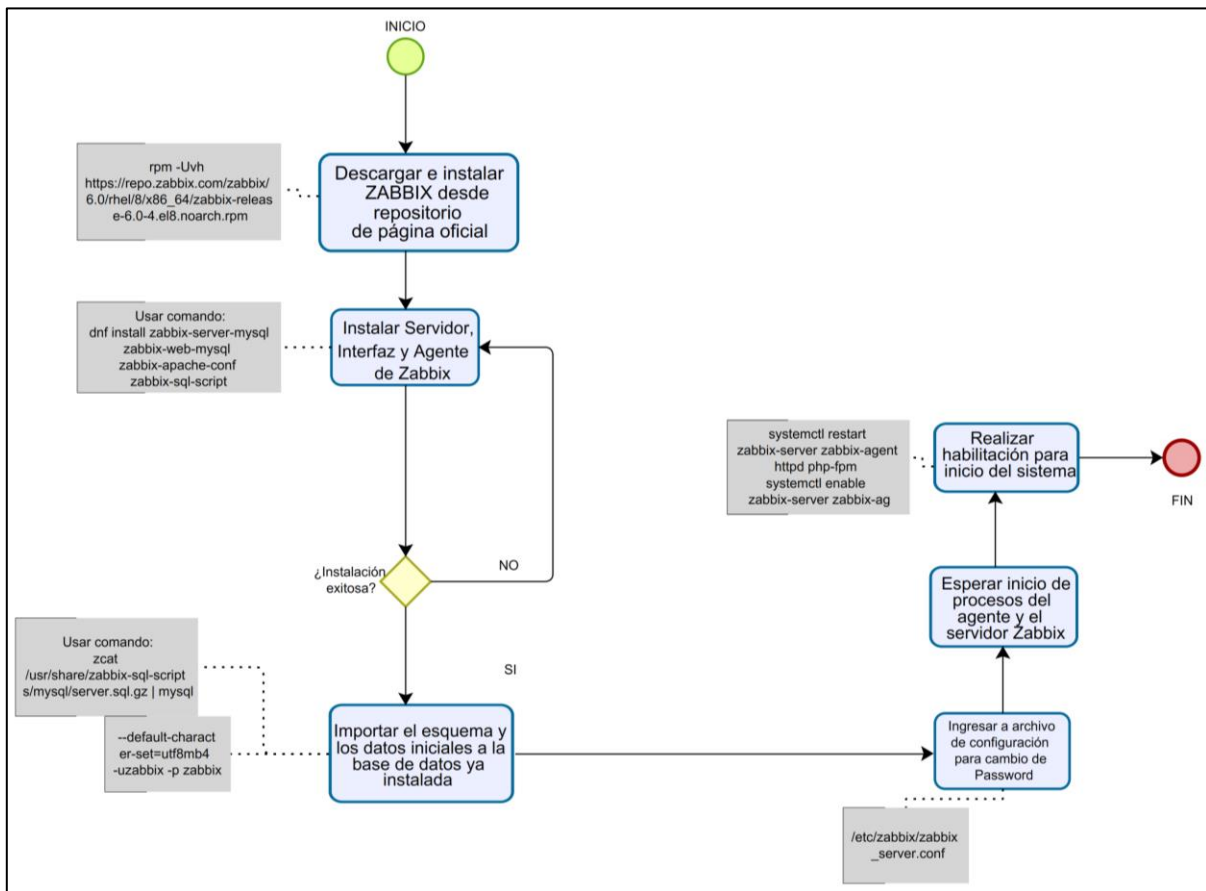
3.2.2. Instalación de la herramienta Zabbix

Se realiza la descarga para ejecutar los comandos necesarios para la instalación, estos se obtienen desde la página oficial de Zabbix, herramienta *Open Source*, y detalla las fases de la implementación del *software* Zabbix.

A continuación, se presenta en la Figura 22 los pasos para efectuar la instalación de la herramienta.

Figura 22

Flujograma de la instalación de Zabbix.

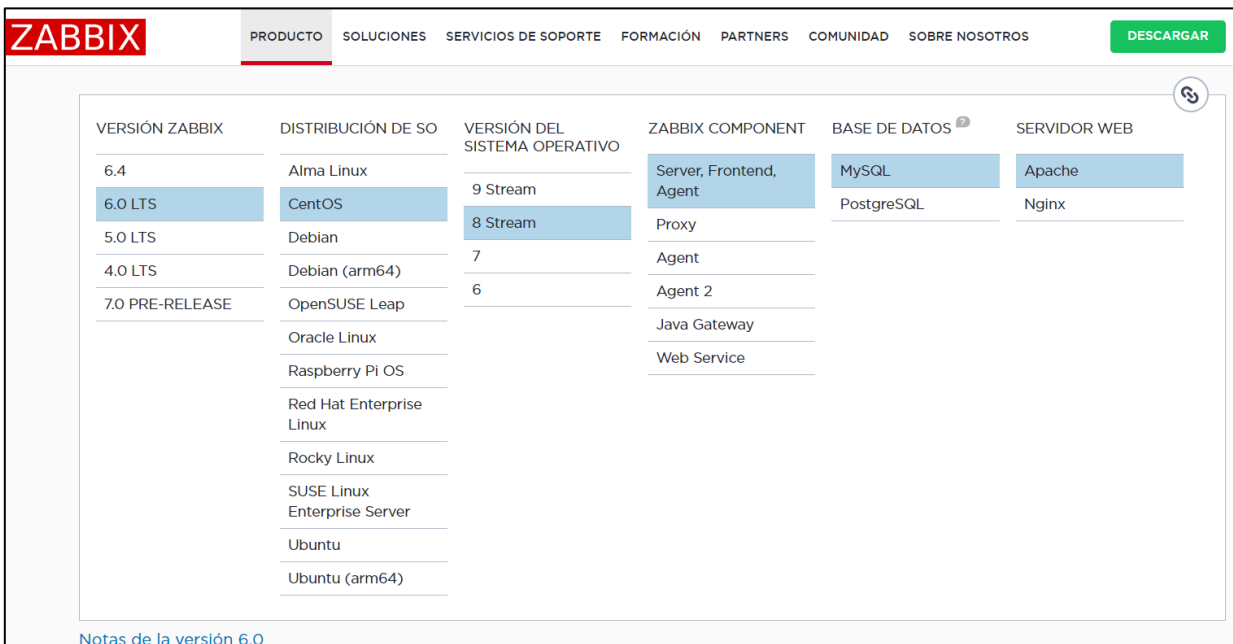


Paso 1.

Se ingresa a la página oficial del Zabbix para buscar el repositorio, como se ilustra en la Figura 23, y obtener los comandos para realizar la instalación de Zabbix Versión 6.0 para el sistema operativo CentOS 8 Stream dentro del componente *server*, *frontend Agent* con la base de datos MySQL en el Servidor Web Apache.

Figura 23

Página principal del proyecto Zabbix.



Nota: Tomado de Zabbix Features Overview, (2023).

Paso 2.

Instalación del servidor desde paquetes obtenidos del repositorio Zabbix como se indica en la Figura 24. La instalación se completa garantizando que los tres servicios se han instalado correctamente, esto son: Instalación del servidor, interfaz web asociado a MySQL y el agente de Zabbix. Se detalla en la Figura 25.

Figura 24

Descarga e instalación completada de paquete Zabbix.



Figura 25

Instalación de paquetes y dependencias requeridas.

```
[root@localhost ~]# dnf install zabbix-server-mysql zabbix-web-mysql zabbix-apache-conf zabbix-sql-scripts zabbix-agent
Last metadata expiration check: 0:02:24 ago on Sun 22 Oct 2023 10:37:17 PM EDT.
Package zabbix-server-mysql-6.0.22-release1.el8.x86_64 is already installed.
Package zabbix-web-mysql-6.0.22-release1.el8.noarch is already installed.
Package zabbix-apache-conf-6.0.22-release1.el8.noarch is already installed.
Package zabbix-sql-scripts-6.0.22-release1.el8.noarch is already installed.
Package zabbix-agent-6.0.22-release1.el8.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@localhost ~]#
```

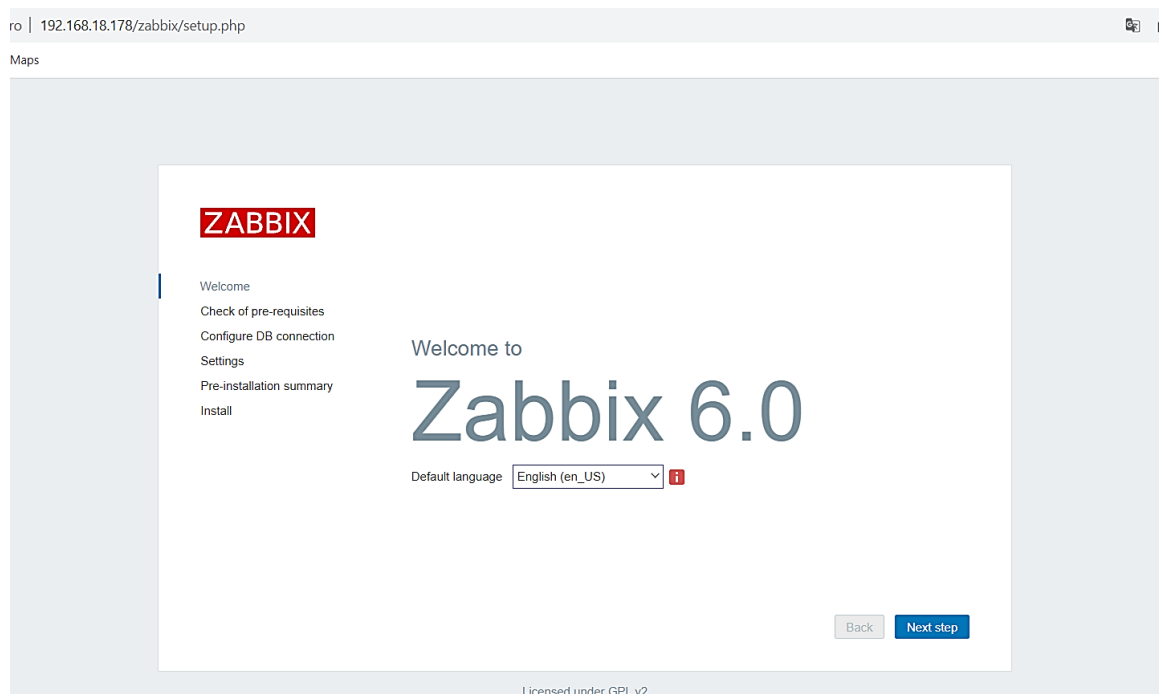
3.2.2.1. Visualización de la interfaz de Zabbix desde un navegador web

Se procede a digitar la dirección IP de la máquina virtual para verificar el funcionamiento de la herramienta, como se observa en la Figura 26 mostrando la interfaz web.

La Interfaz web de Zabbix (*Dashboard*) es donde se elige el idioma de Zabbix, la fecha y se debe tomar en cuenta que la última versión 6.0 no cuenta con el idioma en español para Zabbix.

Figura 26

Interfaz web de Zabbix.



Los prerequisites del sistema a través de interfaz *web* se muestran en un listado donde cada uno deben estar “OK”, en caso de que se muestre “Fail”, se debe revisar la configuración del requisito como se muestra en la Figura 27.

Figura 27

Prerrequisitos del sistema a través de interfaz web.

	Current value	Required	
PHP version	7.2.24	7.2.5	OK
PHP option "memory_limit"	128M	128M	OK
PHP option "post_max_size"	16M	16M	OK
PHP option "upload_max_filesize"	2M	2M	OK
PHP option "max_execution_time"	300	300	OK
PHP option "max_input_time"	300	300	OK
PHP databases support	MySQL		OK
PHP bcmath	on		OK
PHP mbstring	on		OK
PHP option "mbstring.func_overload"	off	off	OK

En la Figura 28 se ilustra la configuración para conectar la base de datos con la interface *web*, para llegar a este punto los prerequisites deben estar “OK”. En la Figura 29 se detalla la configuración de la base de datos, nombre de Zabbix a nivel de interface web y la zona horaria.

Figura 28

Configuración de conexión a base de datos.

Please create database manually, and set the configuration parameters for connection to this database. Press "Next step" button when done.

Database type:

Database host:

Database port: 0 - use default port

Database name:

Store credentials in: Plain text HashiCorp Vault

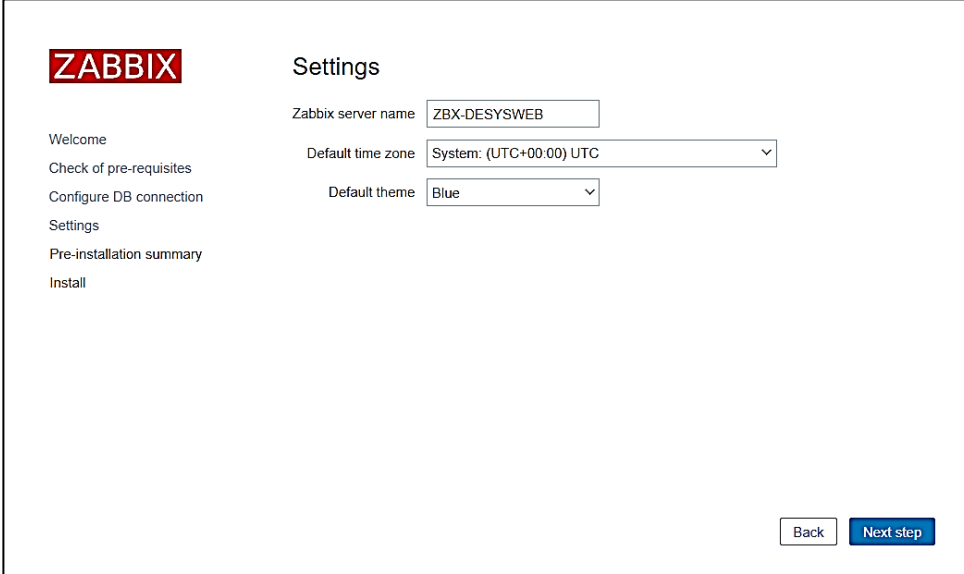
User:

Password:

Database TLS encryption: Connection will not be encrypted because it uses a socket file (on Unix) or shared memory (Windows).

Figura 29

Detalles de la configuración de conexión a base de datos.

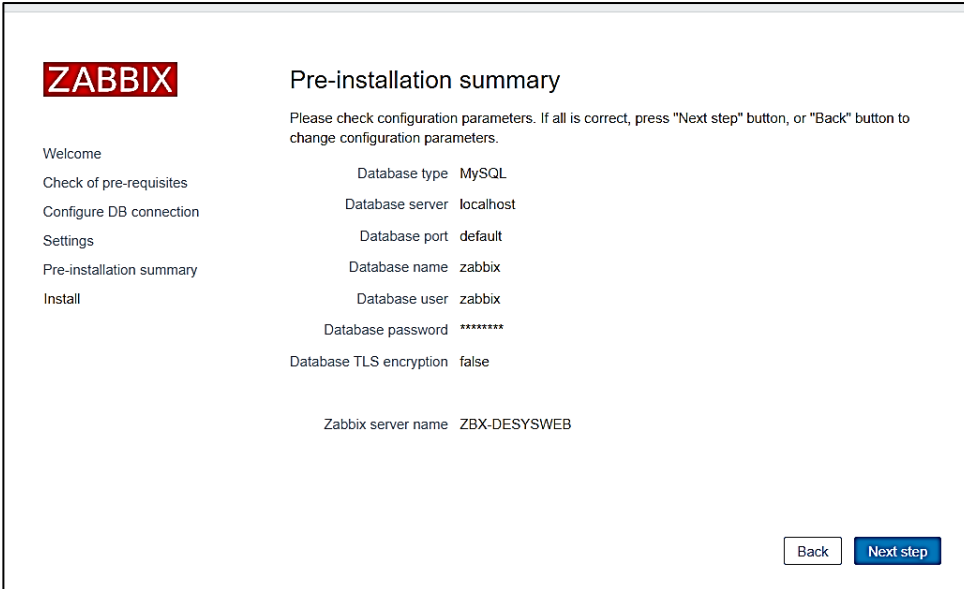


The screenshot shows the Zabbix installation settings page. On the left is a navigation menu with the ZABBIX logo and steps: Welcome, Check of pre-requisites, Configure DB connection, Settings, Pre-installation summary, and Install. The 'Settings' step is active. The main content area is titled 'Settings' and contains three configuration fields: 'Zabbix server name' with the value 'ZBX-DESYSWEB', 'Default time zone' with a dropdown menu showing 'System: (UTC+00:00) UTC', and 'Default theme' with a dropdown menu showing 'Blue'. At the bottom right, there are two buttons: 'Back' and 'Next step'.

En la Figura 30, se detalla el resumen de parámetros de configuración, una vez culminados todos los pasos se brinda un resumen indicando que todo está conforme.

Figura 30

Resumen de parámetros de configuración.

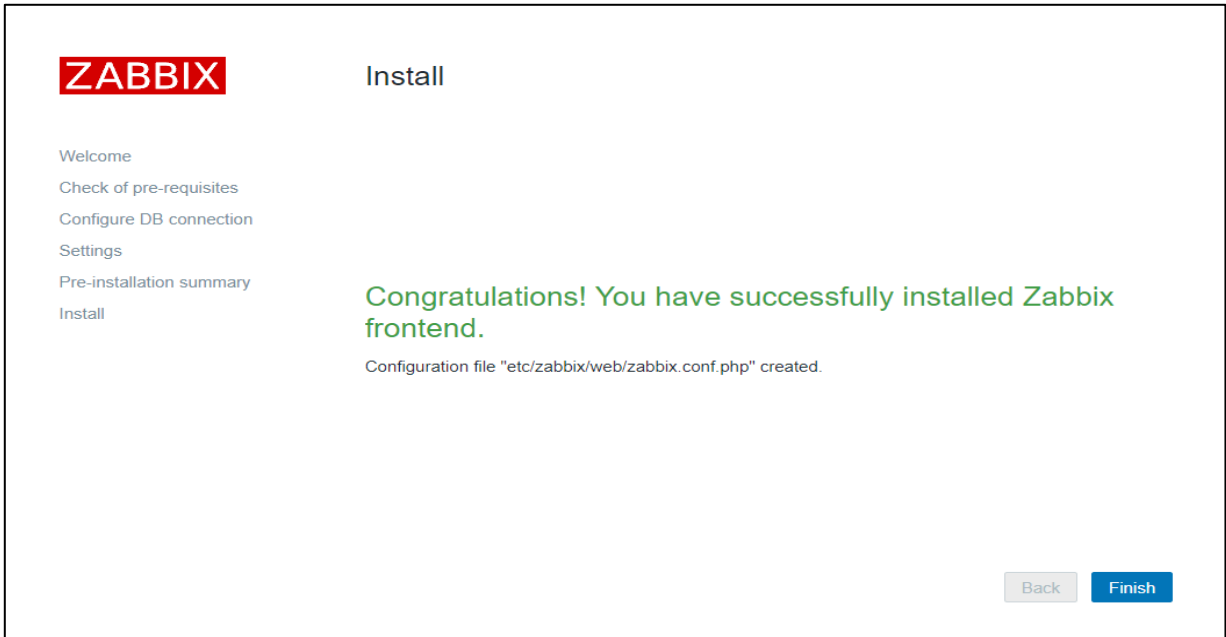


The screenshot shows the Zabbix pre-installation summary page. On the left is a navigation menu with the ZABBIX logo and steps: Welcome, Check of pre-requisites, Configure DB connection, Settings, Pre-installation summary, and Install. The 'Pre-installation summary' step is active. The main content area is titled 'Pre-installation summary' and contains a message: 'Please check configuration parameters. If all is correct, press "Next step" button, or "Back" button to change configuration parameters.' Below this message is a list of configuration parameters: Database type MySQL, Database server localhost, Database port default, Database name zabbix, Database user zabbix, Database password ***** (masked), Database TLS encryption false, and Zabbix server name ZBX-DESYSWEB. At the bottom right, there are two buttons: 'Back' and 'Next step'.

Se informa que se culminó con la configuración de la interface web mediante el detalle de conclusión de instalación, como se indica en la Figura 31.

Figura 31

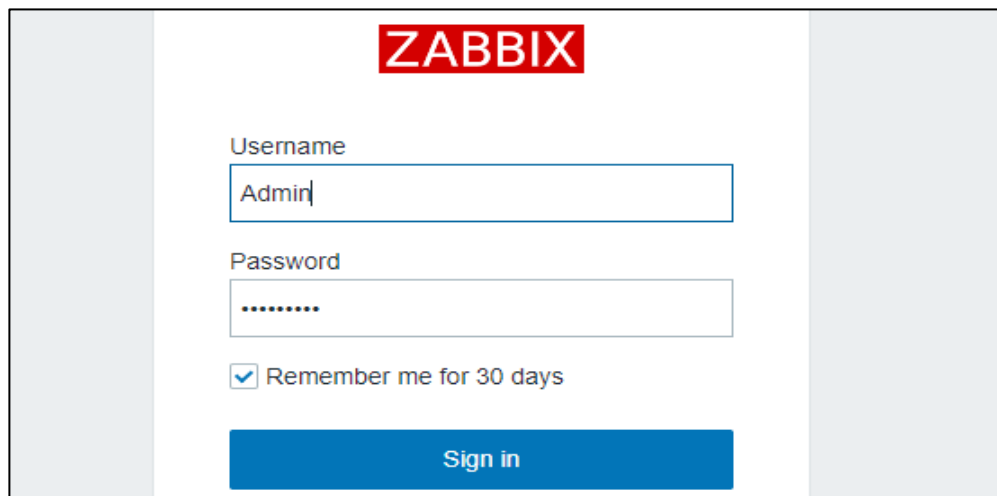
Conclusión de instalación.



Finalmente, se muestra el inicio de la interfaz web para iniciar con el acceso a la plataforma colocando los parámetros de configuración como indica la Figura 32.

Figura 32

Interfaz web de inicio de sesión.



Nota: En ANEXO 1 se presenta el dashboard del software Zabbix ya implementado.

3.2.3. Configuración de los equipos a monitorear en la herramienta Zabbix

Para agregar los equipos de interés de supervisión, se hace uso de la Tabla 4, donde se muestra los equipos a monitorear dentro de la red local. Estos equipos se encuentran físicamente en el *Data Center* de DESYSWEB S.A.C.

Tabla 4

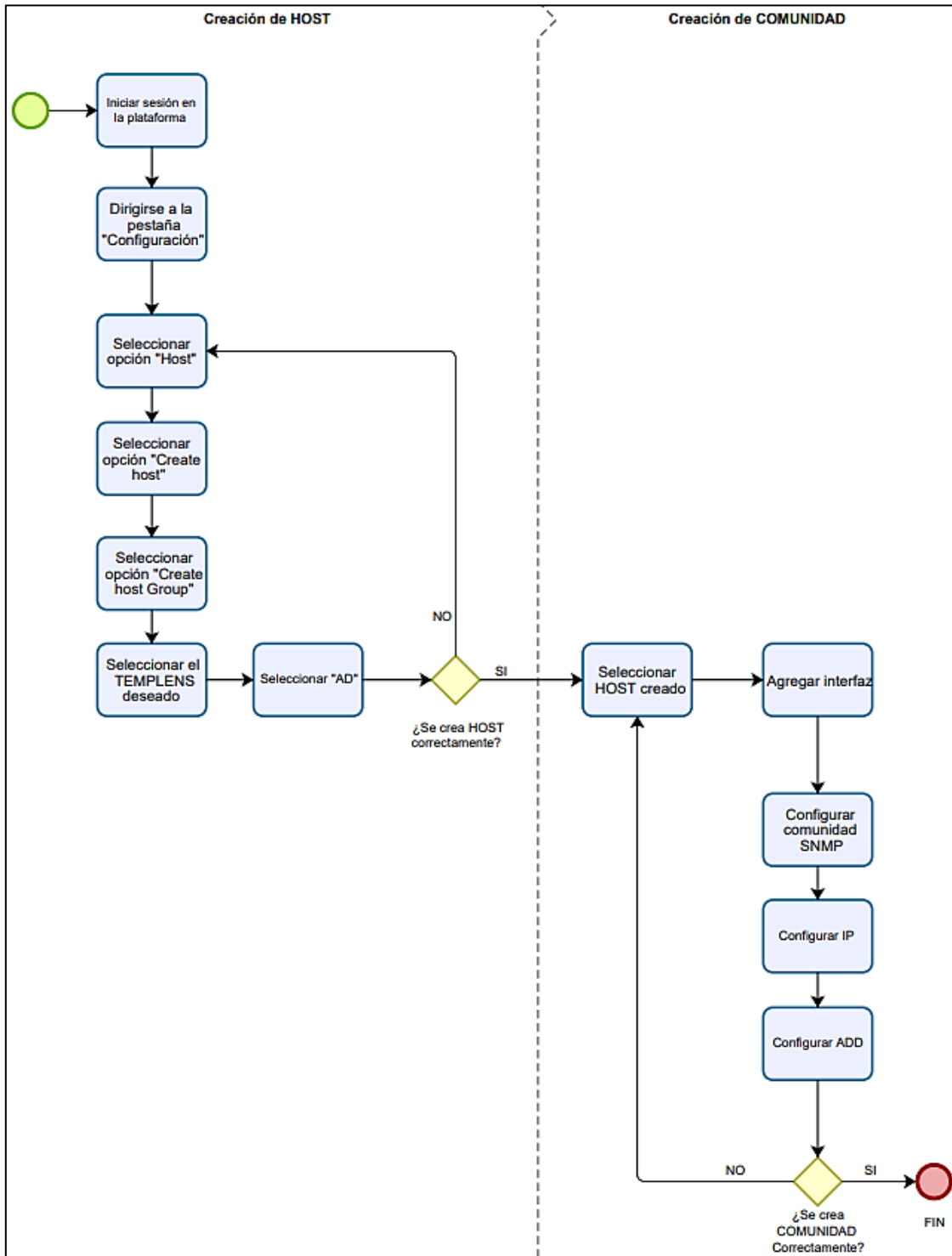
Detalle de equipos monitoreados en Zabbix.

Nombre del equipo	Marca	Descripción
Firewall	Fortinet	Área de TI
Switch Core P1	Cisco	Manejo de Vlans
Servidor P2	Cisco	Servidor virtualizado
Servidor P3	Cisco	Servidor de base de datos

El proceso de la configuración del *host* se detalla en el flujograma de la Figura 33, señalando todo el desarrollo que se requiere para la creación del *host* dentro de la plataforma Zabbix.

Figura 33

Flujograma del proceso de creación de hosts a Zabbix

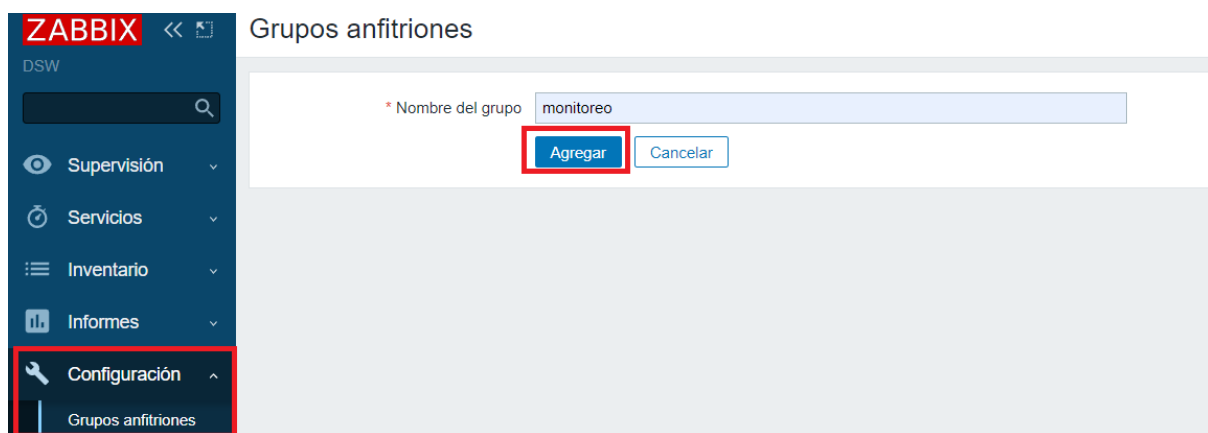


A partir de la Tabla 4, se procede a agregar los diferentes usuarios a la plataforma de gestión de Zabbix. Se realiza el registro de los equipos que se necesitan monitorear, agregando un total de 4 equipos, como se detalla en la Figura 38, también se muestran las opciones de configuración de usuarios en Zabbix, plantillas preconfiguradas (*templates*), la agrupación de dichos usuarios en esquemas lógicos llamados *hostgroups*, una IP y un puerto de escucha SNMP (161 UDP).

A continuación, se evidencia la configuración que se emplea en el sistema de monitoreo Zabbix. El primer paso comprende la creación de grupos, facilitando la identificación y agrupación de dispositivos como se muestra en la Figura 34.

Figura 34

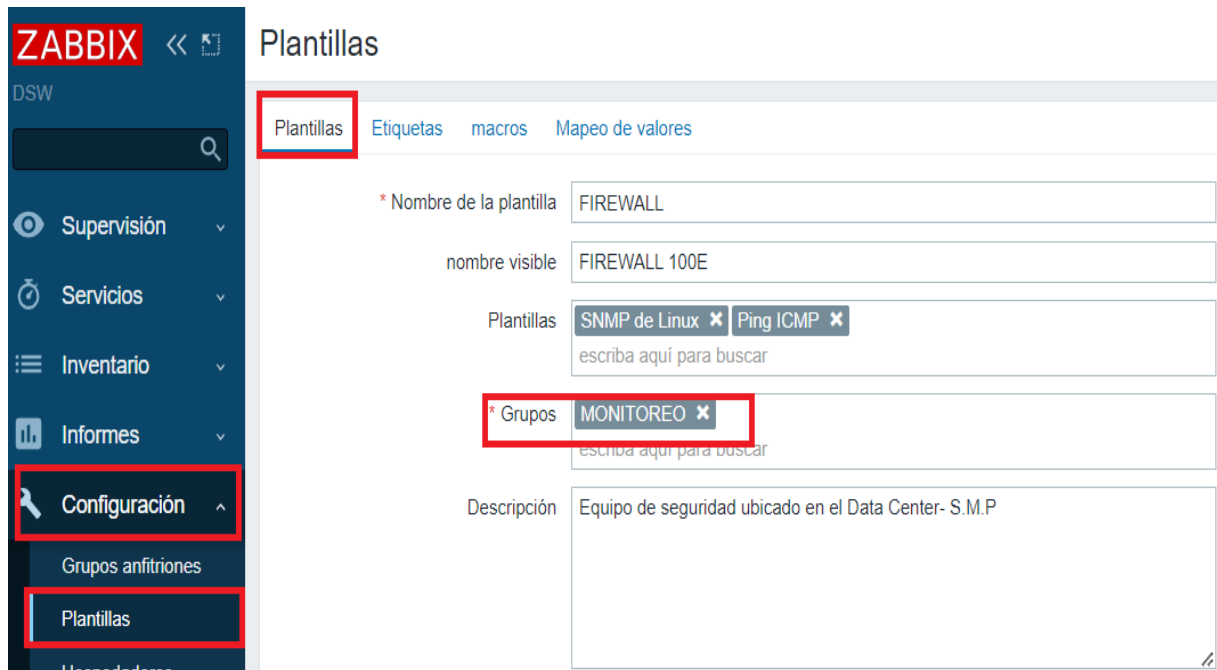
Creación de grupos de usuarios



Es importante indicar que la generación de plantillas tiene como objetivo servir como agentes para el tipo de conexión. En este caso, se crea un sistema operativo Windows como muestra la Figura 35. Se detalla que, para organizar las plantillas y *hosts*, es fundamental agregar al grupo que se formó en el paso anterior.

Figura 35

Creación de plantilla.



Es importante considerar que llevar a cabo la configuración del protocolo SNMP facilita el envío y recepción de información de dispositivos en Zabbix. La conexión del agente se configuró en el lado del *host*. En este ejemplo, se utiliza un dispositivo *firewall*.

En la Figura 36 se conforma la cadena de comunidad en el agente Zabbix y en la configuración SNMP del *host*. Dentro de la configuración en el equipo firewall, es importante detallar que el equipo de seguridad cuenta con una interfaz amigable y herramientas de configuración intuitivas.

Figura 36

Configuración del host SNMP Firewall.

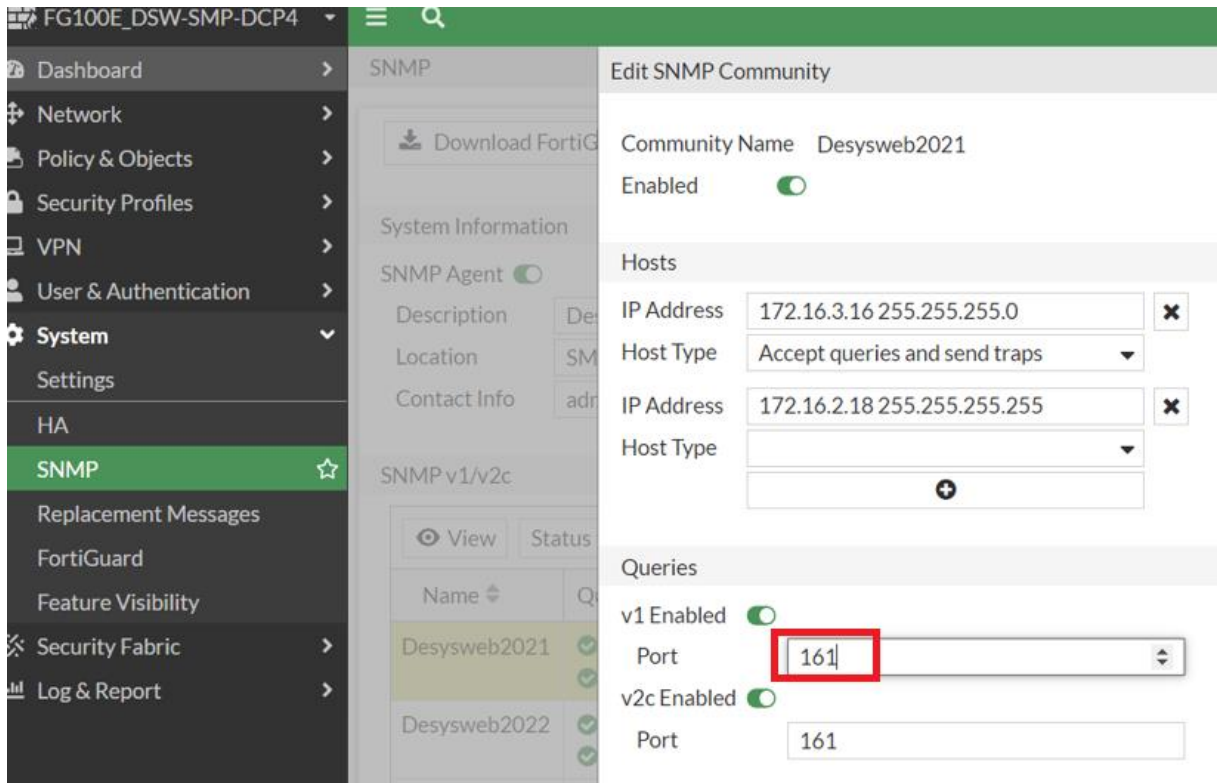
The screenshot displays the FortiGate web interface for the device 'FG100E_DSW-SMP-DCP4'. The left sidebar shows the navigation menu with 'System' and 'SNMP' highlighted. The main content area is titled 'SNMP' and includes two download buttons: 'Download FortiGate MIB File' and 'Download Fortinet Core MIB File'. Below these is the 'System Information' section, which includes a toggle for 'SNMP Agent' (turned on), and input fields for 'Description' (Desysweb S.A.C.), 'Location' (SMP), and 'Contact Info'. The 'SNMP v1/v2c' section contains a table with columns for Name, Queries, Traps, Events, and Status. The table lists three community strings: Desysweb2021, Desysweb2022, and dsw, all of which are enabled for both v1 and v2 queries and traps, with 40 events and an 'Enable' status.

Name	Queries	Traps	Events	Status
Desysweb2021	✓ v1 Enable ✓ v2 Enable	✓ v1 Enable ✓ v2 Enable	40	✓ Enable
Desysweb2022	✓ v1 Enable ✓ v2 Enable	✓ v1 Enable ✓ v2 Enable	40	✓ Enable
dsw	✓ v1 Enable ✓ v2 Enable	✓ v1 Enable ✓ v2 Enable	40	✓ Enable

Dentro del equipo *firewall*, en la pestaña 'Sistemas', se encuentra la opción SNMP. Dentro de esta sección, se realiza la configuración de la comunidad, ingresando las direcciones IP correspondientes junto con el puerto de escucha SNMP (161 UDP), tal como se detalla en la Figura 37.

Figura 37

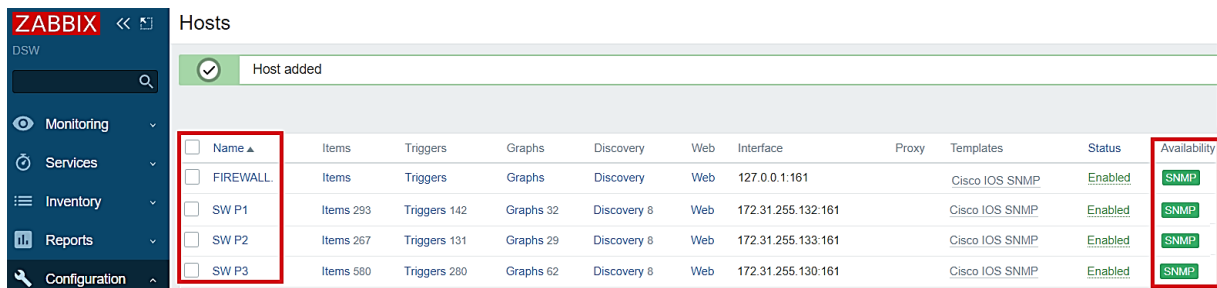
Configuración de la comunidad.



Finalmente, se puede observar en la Figura 38 los equipos que están siendo monitoreados dentro de la plataforma Zabbix.

Figura 38

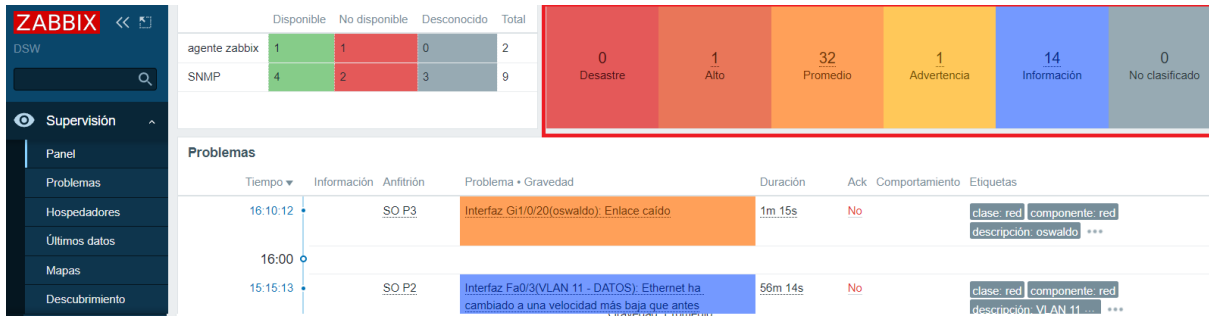
Visualización de los equipos monitoreados.



En la Figura 39 se presenta un resumen de las alertas que indican posibles problemas detectados por Zabbix, en la parte superior derecha de la imagen se muestran las seis categorías de alarmas, cada una se identifica con un color distinto.

Figura 39

Resumen de alertas que muestra la plataforma Zabbix.



En ANEXO 2 se detalla el tipo de problema, la duración de alarma, además se muestra el historial de caída y restablecimiento de cada una. Cada etiqueta de alerta representa un problema distinto que se ha detectado como se ilustra en la Figura 40.

Figura 40

Colores asignados para cada tipo de alerta en Zabbix.

Desastre	Alto	Promedio	Advertencia	Información	No clasificado
<ul style="list-style-type: none"> Desconexión de IP de gestión 	<ul style="list-style-type: none"> Ha ocurrido algo importante 	<ul style="list-style-type: none"> Problema promedio 	<ul style="list-style-type: none"> Tener en cuenta un posible fallo 	<ul style="list-style-type: none"> A título informativo 	<ul style="list-style-type: none"> Gravedad desconocida

El grupo de alerta revela el nivel de gravedad del problema detectado y la prioridad con que debe atenderse, como se explica a continuación:

Desastre (nivel 5): por lo general indican una desconexión del equipo de gestión de Zabbix que puede corregirse mediante un reinicio del puerto de la interfaz para reestablecer el servicio, y a continuación ejecutar el comando PING con la dirección IP del dispositivo para comprobar que el problema se ha solucionado.

Alto (nivel 4): señala un consumo de memoria excesivo o un elevado procesamiento de CPU que pueden ser causados por ataques o fallas en los equipos y deben ser atendidas para evitar intermitencias en los servicios para los usuarios de la red.

Promedio (nivel 3): se generan cuando el tiempo de respuesta es alto (supera los 350 milisegundos) o existe una pérdida de paquetes en la red, si estas advertencias son frecuentes los equipos de tipo cliente experimentarán lentitud en los servicios o a su vez pérdidas de datos al compartir información.

Advertencia (nivel 2): indican una mala configuración en el equipo y que debido a ello no se recibe una respuesta SNMP, por lo general esta alerta puede corregirse sin necesidad de informar al cliente.

Información (nivel 1): comprenden aquellas actividades que han ocurrido en los equipos como reinicios del dispositivo cliente o que no se está utilizando el servicio de red por al menos dos días consecutivos.

No clasificado (nivel 0): agrupa las alertas cuyo nivel de gravedad no es posible categorizar en ninguna de las etiquetas antes mencionadas y que no representan un riesgo elevado para la infraestructura TI.

3.2.4. Comprobación de la funcionalidad de las notificaciones por medio de correo electrónico en Zabbix

Una vez se agregados todos los elementos de red de la infraestructura en el sistema de monitoreo, resulta primordial la configuración de notificaciones para una alerta temprana de eventos anómalos, Para ello, en el panel de "Administración" se selecciona "Tipos de medios" y se especifica el correo electrónico creado previamente, o "Crear tipo de medio", como se detalla en los siguientes pasos:

Paso 1

Para la configuración de tipos de medio:

- Se define el nombre.
- En tipo se elige correo electrónico.
- Servidor SMTP, se coloca el servidor SMTP que es utilizado por la compañía.
- Se configura el puerto del servidor SMTP.
- Se configura el saludo SMTP y el correo electrónico SMTP de la compañía.
- En seguridad de conexión indicar SSL/TLS.
- Nombre y contraseña de una cuenta configurada en el servidor de correo.
- Finalmente agregar.

Paso 2

Para la administración de usuarios se configura el usuario administrador para que envíe los correos, este usuario tiene los privilegios de visualización y escritura sobre el resto que enviarán las alertas.

- Se ingresa al usuario y se elige la opción media.
- Se agrega la media colocando agregar.
- En tipo se elige el tipo de medio creado.
- Se agrega la lista de correos en enviar.
- Se mantiene activo el envío de correo 24/07 en cuanto al activo.
- Finalmente agregar.

Paso 3

Localizar el menú Configuración -> Acciones -> Acciones desencadenantes:

- Iniciar la creación en Crear acción.
- Se define el nombre.
- Agregar en condiciones los usuarios para el envío de correos de alerta.
- Seleccionar la pestaña operaciones para continuar con la configuración.
- Se agrega una operación.
- Seleccionar el usuario antes creado.
- Indicar los tipos de medios creados.
- Para finalizar se coloca agregar.

Tomando en cuenta estos pasos, se procede a realizar las configuraciones de notificación del sistema como indica la Figura 41.

Figura 41

Configuración tipo de medio en Zabbix para la notificación mediante correo electrónico

The screenshot displays the Zabbix web interface for configuring a media type. On the left is a dark blue sidebar with the Zabbix logo and a search bar. Below the search bar are menu items: Monitoring, Services, Inventory, Reports, Configuration, Administration (expanded), Support, and Integrations. The Administration menu includes General, Proxies, Authentication, User groups, User roles, Users, Media types (highlighted with a red box), Scripts, and Queue. The main content area is titled 'Media types' and has three tabs: 'Media type' (selected), 'Message templates', and 'Options'. The configuration form includes the following fields and options:

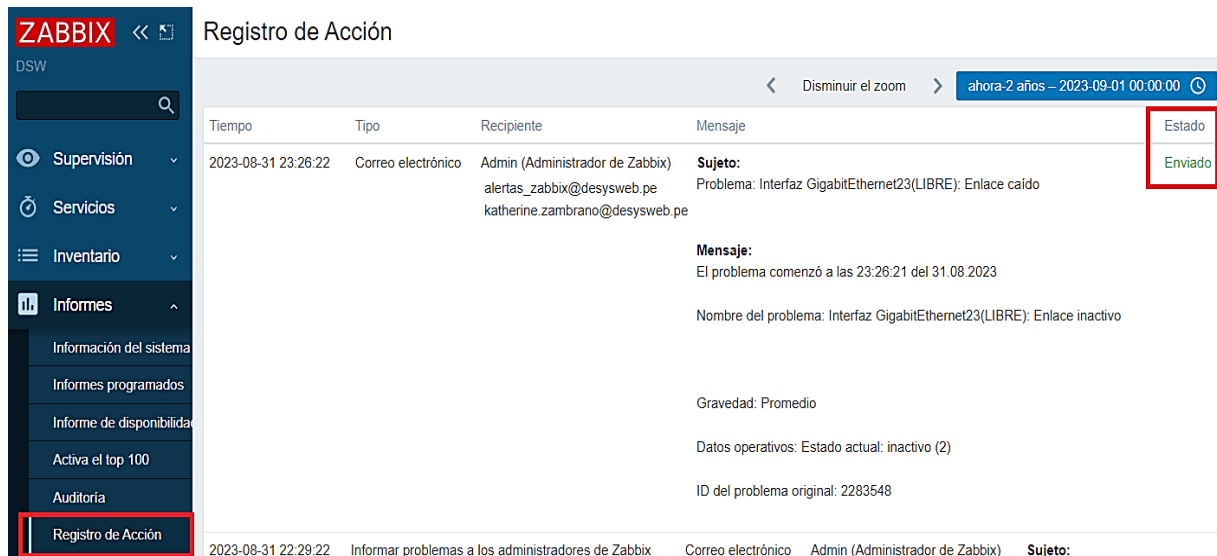
- Name: monitoreo
- Type: Email
- * SMTP server: alerta_monitoreo@desysweb.pe
- SMTP server port: 587
- * SMTP helo: example.com
- * SMTP email: alerta_monitoreo@desysweb.pe
- Connection security: None, STARTTLS, SSL/TLS (selected)
- SSL verify peer:
- SSL verify host:
- Authentication: None, Username and password (selected)
- Username: katherine.zambrano@des
- Password: Change password
- Message format: HTML, Plain text (selected)
- Description: Notificación de alerta desde el Zabbix
- Enabled:

At the bottom of the form are buttons for Update, Clone, Delete, and Cancel.

Al realizar el registro del correo electrónico al que se notificará cuando ocurra algún problema con un equipo ya monitoreado en Zabbix, este emitirá la alerta de notificación al correo electrónico configurado. El registro de la acción se puede ubicar en la pestaña reportes, al seleccionar el grupo 'Registro de acción' donde se visualizan las notificaciones que se han enviado desde Zabbix, de este modo se conoce si la notificación se ha realizado con éxito al observar en estatus la descripción enviada (texto en color verde resaltado como muestra la Figura 42).

Figura 42

Reporte de notificación mediante correo electrónico desde el Zabbix.



De tal forma se lleva a cabo el proceso de las notificaciones enviadas por Zabbix vía *Email*, si se llega a presentar un evento que necesite soporte. Es necesario contar con este recurso para una mejor administración y evitar incidencias futuras que puedan llegar a generar consecuencias debido a la pérdida de comunicación quebrantando así el SLA de atención.

La notificación oportuna busca anticipar incidentes, observando el proceder de los equipos en tiempo real y las 24 horas del día, los 7 días de la semana como se indica en el ANEXO 3.

3.3. Resultados

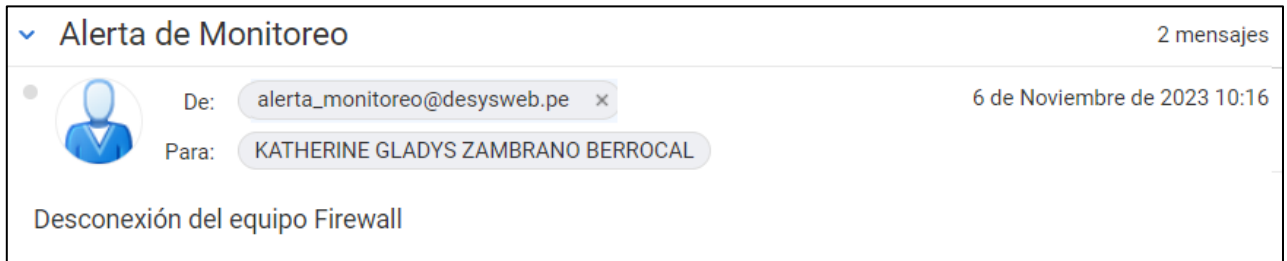
Al realizar la implementación del *software* como sistema de monitoreo, permitió prevenir y resolver incidencias de manera más ágil. Al mismo tiempo, contribuyó que el área de monitoreo fuera notificada de manera oportuna, cumpliendo con los tiempos de respuesta y no caer en penalidades. Los beneficios que se ha obtenido han sido significativos, desde la finalización de la implementación.

3.3.1. Verificación del envío de correo

Los resultados obtenidos son que respecto a cada alerta el personal de monitoreo es notificado como se detalla en la Figura 43.

Figura 43

Reporte de notificación mediante correo electrónico desde el Zabbix



3.3.2. Encuestas realizadas

La encuesta se llevó a cabo entre el personal usuario y es importante detallar previamente la utilización del *software* SPSS para los cálculos estadísticos.

Los resultados obtenidos para la métrica del tiempo de falla con respecto al tiempo de resolución se muestran en la Figura 44 y en la Tabla 5, donde, más del 75% de los usuarios encuestados perciben que, luego de la implementación, el tiempo de solvencia es aproximadamente 10 minutos.

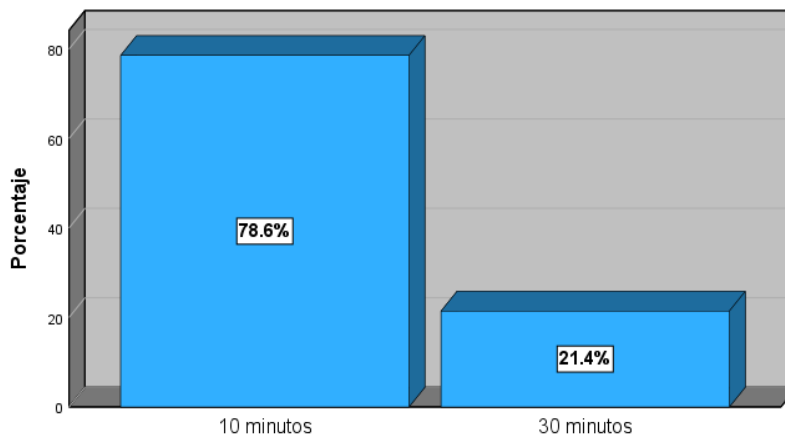
Tabla 5

Tiempo de falla vs tiempo de resolución.

Opciones	Frecuencia	Porcentaje	Porcentaje acumulado
10 minutos	11	78,6	78,6
30 minutos	3	21,4	100,0
Total	14	100,0	

Figura 44

Gráfica de tiempo de resolución de incidentes posterior a instalación de Zabbix.



Con respecto a la Tabla 6, y la interpretación que nos muestra la gráfica en la Figura 45, se deduce que la mayor parte de los usuarios encuestados indicaron que el tiempo promedio para la detección de la falla después de la implementación es de 5 minutos, con una métrica de 57,1% y al añadirse el 14,3% de usuarios que perciben 1 minuto, se alcanza una satisfacción de 71,4% del total de encuestados. Cabe destacar que sólo un 28,6% ha señalado un promedio de 10 minutos en llevar a cabo esta actividad.

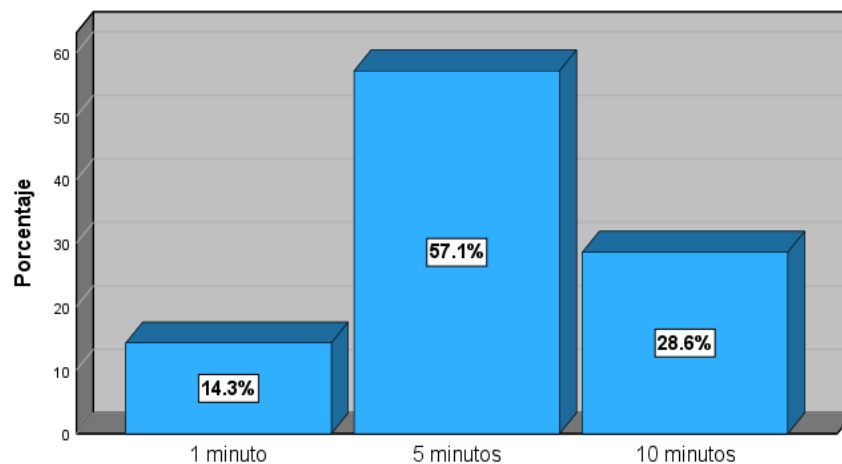
Tabla 6

Tiempo de localización del fallo.

Opciones	Frecuencia	Porcentaje	Porcentaje acumulado
1 minuto	2	14,3	14,3
5 minutos	8	57,1	71,4
10 minutos	4	28,6	100,0
Total	14	100,0	

Figura 45

Gráfico de tiempo de localización de dispositivo fallido posterior a instalación de Zabbix.



Se puede decir que, el 64.3% de los usuarios indican que el actual monitoreo de la infraestructura de TI de la empresa es excelente, evidenciado en la Tabla 7. Por otro lado, como se observa en la Figura 46, se interpreta que el 92.9% de los usuarios indican que el actual monitoreo de la infraestructura de TI de la empresa es entre bueno y excelente.

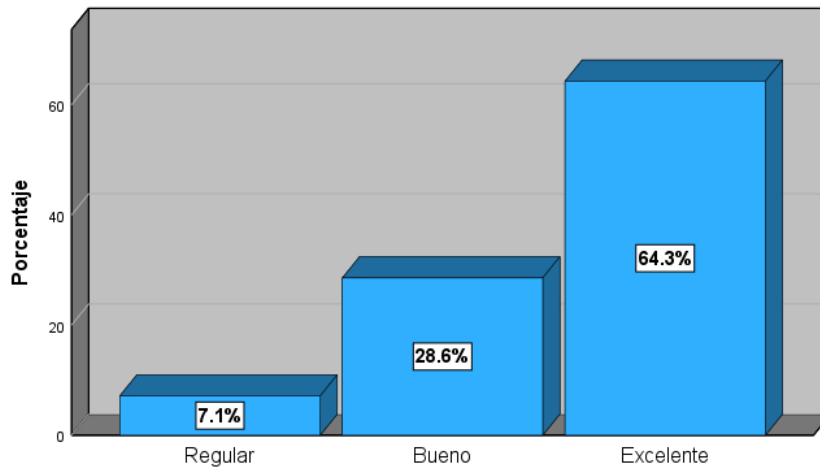
Tabla 7

Evaluación del modelo actual de monitoreo de la empresa.

Opciones	Frecuencia	Porcentaje	Porcentaje acumulado
Regular	1	7,1	7,1
Bueno	4	28,6	35,7
Excelente	9	64,3	100,0
Total	14	100,0	

Figura 46

Gráfico de Opinión sobre el modelo actual de monitoreo de la empresa.



Los resultados que se detallan en la Tabla 8, y se ilustran en la Figura 47, revelan que el 100% de los usuarios que participaron en la encuesta perciben que actualmente se sienten seguros con la forma en que se realiza el monitoreo de la infraestructura de TI de la empresa.

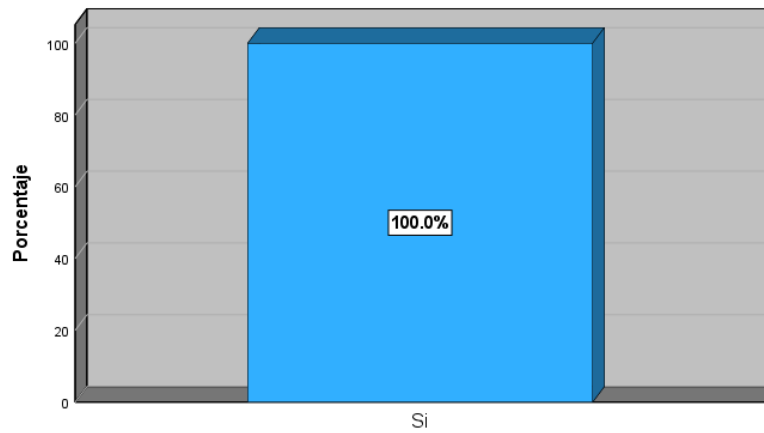
Tabla 8

Sensación de seguridad sobre sistema de monitoreo de la empresa.

Opciones	Frecuencia	Porcentaje	Porcentaje acumulado
No	0	0,0	0,0
Si	14	100,0	100,0
Total	14	100,0	

Figura 47

Gráfica sobre la sensación de seguridad sobre sistema de monitoreo de la empresa.

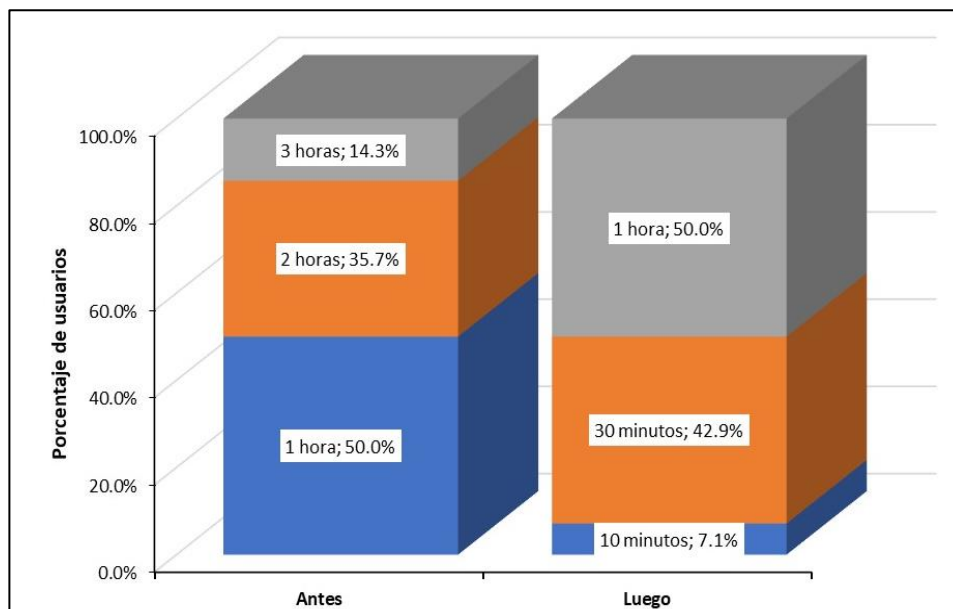


Para contrastar, se presentan a continuación gráficos comparativos ejecutados en el *software* SPSS. Estos muestran de manera más clara la reducción en los tiempos de resolución de incidentes, incluyendo el tiempo promedio para localizar dispositivos dentro de la red local de la empresa DESYSWEB.

En la Figura 48 se puede observar que, antes de la implementación, el 50% de los usuarios requerían de una hora para resolver los incidentes de infraestructura de TI, mientras que, luego de la implementación, el 50% de los usuarios tardaron entre 30 a 10 minutos en resolver los incidentes de infraestructura de TI.

Figura 48

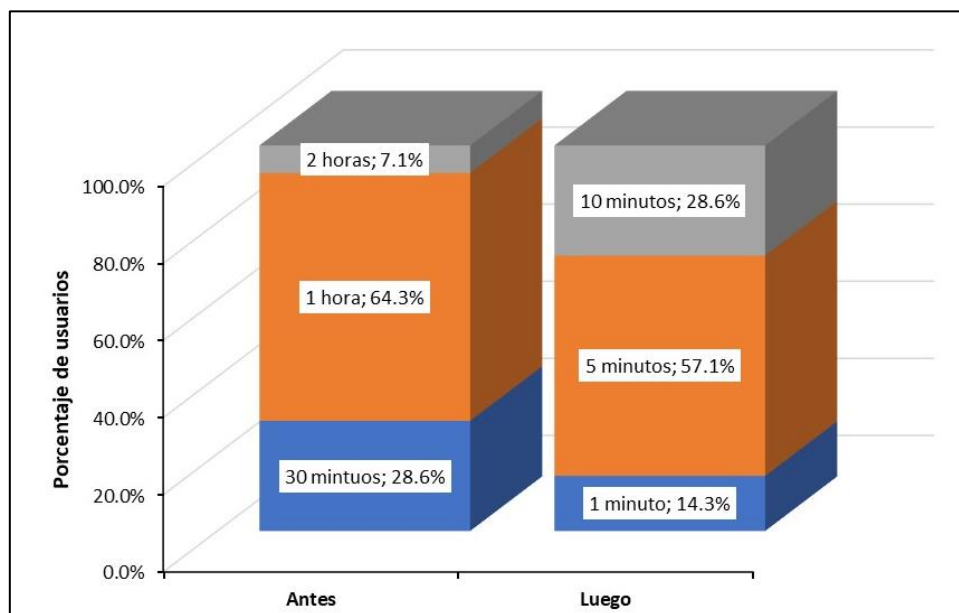
Tiempo que se tarda en resolver los incidentes.



A partir del gráfico mostrado en la Figura 49 se observa que antes de la implementación el 64.3% de los usuarios tardaban en promedio una hora en encontrar el dispositivo o servicio de TI que causó el incidente, mientras que, luego de la implementación el 57.1% de los usuarios requirió un promedio de 5 minutos para encontrar el dispositivo o servicio de TI que causó el incidente.

Figura 49

Tiempo promedio que se demora en encontrar el dispositivo.



3.3.2.1. Discusión de los resultados

Con base en los resultados arrojados por la encuesta se puede concluir que gran parte de los usuarios percibieron un cambio con la implementación del servidor Zabbix que cumpla la función de monitoreo de la red. En el orden de las preguntas se puede constatar que el tiempo de resolución promedio percibido es de 10 minutos mientras que para detectar el origen de la falla se requiere de un tiempo entre 1 y 5 minutos. Las preguntas de carácter cualitativo demostraron que el enfoque actual del monitoreo realizado por la empresa es considerado como bueno y excelente para la gran mayoría y que todos los usuarios de la muestra poblacional perciben mayor seguridad en el servicio.

La reducción de los tiempos de atención y solución que se alcanzó con la implementación del servidor Zabbix para monitorear la infraestructura de TI de la empresa han mejorado la aceptación del servicio que perciben los clientes.

CONCLUSIONES

- Se logró realizar la implementación sistema de monitoreo en DESYSWEB S.A.C sobre una máquina virtual en Linux dentro de un servidor localizado en el Data Center. El resultado ha permitido contar con una herramienta que se ajusta a las necesidades dentro del área de TI de la empresa.
- La configuración se llevó a cabo satisfactoriamente desde la instalación dentro de la base de datos y posterior a ello, se ha realizado la implementación gracias a las distintas configuraciones dentro de la plataforma Zabbix de acuerdo con los equipos monitoreados.
- La validación de notificaciones de alertas por medio de correo electrónico ha permitido la mejora continua de la infraestructura TI al ser notificado al personal encargado para la toma de acción ante la presencia de un incidente o avería dentro de la red local de la empresa. Esto permitió que el personal atiende de una manera más ágil y evitar tiempos elevados de indisponibilidad del servicio, como se evidencia en la medición de satisfacción de los usuarios en el apartado de resultados.
- Se analizó los resultados de la encuesta realizada al personal usuario concluyendo que la implementación del software Zabbix ha generado gran satisfacción ya que los tiempos de resolución de inconvenientes y detección de origen de errores se han reducido a 10 minutos y 5 minutos respectivamente. Las respuestas brindadas demuestran que el enfoque actual del monitoreo realizado por la empresa alcanza mayoritariamente una calificación entre bueno y excelente, todos los encuestados perciben mayor seguridad en el servicio que brinda la empresa.

RECOMENDACIONES

- Se recomienda implementar sistemas de monitoreo en diferentes organizaciones con la finalidad de mejorar la eficiencia y rapidez para el tratamiento oportuno de sus gestiones.
- Al instalar el sistema de código abierto es necesario entender el funcionamiento del sistema operativo Linux comprender la funcionalidad de los comandos que se necesita aplicar previamente para no tener inconvenientes al momento de implementar el Zabbix.
- En el momento de la instalación previos a la implementación del sistema es importante estar atentos que todos los comando y librerías este debidamente instaladas sino el sistema no iniciará correctamente, lo cual, no nos permitirá llevar con éxito la configuración.
- Es crucial revisar continuamente las alertas y notificaciones para adaptarlas a la evolución de la infraestructura y las prioridades de la empresa. Esto garantizará que el sistema continúe funcionando.
- Para mantener y mejorar la eficacia del sistema de monitoreo implementado con Zabbix, se sugiere establecer un plan de capacitación continua para el personal encargado del monitoreo y la gestión de alarmas.

REFERENCIAS BIBLIOGRÁFICAS

- Awati, R., & Rosencrance, L. (2021). *Computer hardware*. Obtenido de TechTarget - Networking: <https://www.techtarget.com/searchnetworking/definition/hardware>
- AWS. (2023). *¿Qué es SMTP? Explicación del servidor SMTP - AWS*. Obtenido de Amazon Web Services, Inc.: <https://aws.amazon.com/es/what-is/smtp/#:~:text=SMTP%20significa%20protocolo%20simple%20de,electr%C3%B3nico%20a%20trav%C3%A9s%20de%20Internet>.
- Benavides Sánchez, C. A. (2023). *Implantación de la herramienta Zabbix de monitoreo para el núcleo de red de la empresa Airmaxtelecom Soluciones Tecnológicas S.A. gratuita y de código abierto*. Ibarra, Ecuador: [Tesis de grado, Universidad Técnica del Norte]. Obtenido de <http://repositorio.utn.edu.ec/bitstream/123456789/13878/2/04%20ISC%20674%20TRABAJO%20GRADO.pdf>
- Casas, R. M., & Sempértegui, M. L. (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*. Lambayeque: [Tesis de grado, Universidad Nacional Pedro Ruiz Gallo]. Obtenido de <https://repositorio.unprg.edu.pe/handle/20.500.12893/1576>
- Cisco. (2023). *¿Qué es el monitoreo de red?* Obtenido de https://www.cisco.com/c/es_mx/solutions/automation/what-is-network-monitoring.html
- Cloudflare. (2023). *¿Qué es HTTP?* Obtenido de Cloudflare: <https://www.cloudflare.com/es-es/learning/ddos/glossary/hypertext-transfer-protocol-http/>
- IBM. (2023). *¿Qué es una interfaz de programación de aplicaciones (API)?* Obtenido de IBM: <https://www.ibm.com/mx-es/topics/api>
- Ivanti. (2023). *What is ITIL 4?* Obtenido de <https://www.ivanti.com/glossary/itil-4#:~:text=ITIL%204%20represents%20a%20fundamental,focus%20to%20IT%20service%20delivery>
- Lambert, D. (2020). *Zabbix Agent: Active vs. Passive*. Obtenido de Zabbix Blog: <https://blog.zabbix.com/zabbix-agent-active-vs-passive/9207/>

León, J. F. (2019). *Implementación de un servidor Zabbix en el consorcio educativo continental, para el análisis y monitoreo de equipos en la red*. Cuenca, Ecuador: [Tesis de grado, Instituto Sudamericano Cuenca]. Obtenido de <https://repositorio.sudamericano.edu.ec/handle/123456789/57?mode=full>

ManageEngine. (2020). *What is SNMP?* Obtenido de <https://www.manageengine.com/network-monitoring/what-is-snmp.html>

Rouse, M. (28 de Septiembre de 2018). *Acuerdo de Nivel de Servicio o SLA*. Obtenido de ComputerWeekly.es: <https://www.computerweekly.com/es/definicion/Acuerdo-de-nivel-de-servicio-o-SLA>

Servicenow. (2023). *¿Qué es un centro de operaciones de red (NOC)?* Obtenido de <https://www.servicenow.com/es/products/it-operations-management/what-is-network-operations-center.html>

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (28 de Septiembre de 2023). *Guide to Industrial Control Systems (ICS) Security*. Obtenido de NIST: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>

Trujillo Silva, M. T. (2020). *Influencia de la aplicación del software Zabbix en el monitoreo de la red de área local de la Superintendencia Nacional de los Registros Públicos zona registral N° V - sede Trujillo*. Trujillo: [Tesis de maestría, Universidad Privada Antenor Orrego]. Obtenido de https://repositorio.upao.edu.pe/bitstream/20.500.12759/6085/1/REP_MAEST.INGE_MARCO.TRUJILLO_INFLUENCIA.APLICACION.SOFTWARE.ZABBIX.MONITOREO.RED.%c3%81REA.LOCAL.SUPERINTENDENCIA.NACIONAL.REGISTROS.P%c3%9aBLICOS.ZONA.REGISTRAL.V.TRUJILLO.pdf

Universidad Politécnica de Valencia. (2023). *Software libre y Software privativo*. Obtenido de <https://www.upv.es/entidades/I2T/info/890613normalc.html>

Walton, A. (15 de Febrero de 2018). *SNMP: funcionamiento y configuración - CCNA desde cero*. Obtenido de CCNA desde Cero: <https://ccnadesdecero.es/snmp-funcionamiento-configuracion/>

Zabbix. (2023). *Producto Zabbix*. Obtenido de <https://www.zabbix.com/la/features>

ANEXOS

ANEXO 1. DASHBOARD PRINCIPAL DE ZABBIX

The screenshot displays the Zabbix web interface. On the left is a navigation sidebar with categories like Supervisión, Servicios, and Configuración. The main content area is divided into several sections:


- Información del sistema:** A table listing system parameters such as 'El servidor Zabbix se está ejecutando', 'Número de hosts', and 'Número de elementos'.
- Status Bar:** A horizontal bar with colored segments representing different severity levels: Desastre (0), Alto (1), Promedio (32), Advertencia (1), Información (14), and No clasificado (0).
- Problemas:** A table listing active issues, including details like 'Interfaz Gi1/0/20(oswald): Enlace caído' and 'Interfaz Fa0/3(VLAN 11 - DATOS): Ethernet ha cambiado a una velocidad más baja que antes'.

ANEXO 2. HISTORIAL DE CAIDA

Tiempo ▼	Tiempo de recuperación	Estado	Duración	Ack	Etiquetas
15:15:13		PROBLEMA	1h 5m 6s	No	clase: red componente: red descripción: VLAN 11 ...
15:00					
14:25:13	14:55:13	RESUELTO	30m	No	clase: red componente: red descripción: VLAN 11 ...
14:00					
12:50:13	13:05:13	RESUELTO	15m	No	clase: red componente: red descripción: VLAN 11 ...
12:00					
10:40:13	10:50:13	RESUELTO	10m	No	clase: red componente: red descripción: VLAN 11 ...
Hoy					
2023-12-01 20:15:13	09:15:13	RESUELTO	2d 13h	No	clase: red componente: red descripción: VLAN 11 ...
2023-12-01 19:25:13	2023-12-01 20:05:13	RESUELTO	40m	No	clase: red componente: red descripción: VLAN 11 ...
2023-12-01 18:15:13	2023-12-01 18:25:13	RESUELTO	10m	No	clase: red componente: red descripción: VLAN 11 ...
2023-12-01 15:30:13	2023-12-01 16:50:13	RESUELTO	1h 20m	No	clase: red componente: red descripción: VLAN 11 ...
2023-12-01 14:00:13	2023-12-01 14:10:13	RESUELTO	10m	No	clase: red componente: red descripción: VLAN 11 ...
2023-12-01 12:00:13	2023-12-01 12:10:13	RESUELTO	10m	No	clase: red componente: red descripción: VLAN 11 ...
Diciembre					
2023-11-30 17:55:13	2023-11-30 18:15:14	RESUELTO	20m 1s	No	clase: red componente: red descripción: VLAN 11 ...
2023-11-30 15:10:13	2023-11-30 16:10:13	RESUELTO	1 hora	No	clase: red componente: red descripción: VLAN 11 ...
2023-11-30 13:00:13	2023-11-30 13:25:13	RESUELTO	25m	No	clase: red componente: red descripción: VLAN 11 ...
2023-11-30 11:50:13	2023-11-30 12:00:13	RESUELTO	10m	No	clase: red componente: red descripción: VLAN 11 ...

ANEXO 3. NOTIFICACION DE ALERTA POR CORREO ELECTRÓNICO

▼ alerta_monitoreo@desysweb.pe 3 mensajes

 De: alerta_monitoreo@desysweb.pe 6 de Noviembre de 2023 10:25
Para: KATHERINE GLADYS ZAMBRANO BERROCAL

Desconexión del Firewall ubicado en el cuarto de comunicaciones. Piso 4 Data Center S.M.P

[Responder](#) - [Responder a todos](#) - [Reenviar](#) - [Más acciones](#)

ANEXO 4. FORMATO DE ENCUESTA

FORMATO DE ENCUESTA

1. ¿Cuánto tiempo aproximadamente se tardaba en resolver los incidentes de infraestructura de TI antes de la implementación del Zabbix?
 - a. 30 minutos
 - b. 1 hora
 - c. 2 horas
 - d. 3 horas

2. ¿En promedio, cuánto tiempo lleva encontrar el dispositivo o servicio de TI que causó el incidente antes de la implementación?
 - a. 30 minutos
 - b. 1 hora
 - c. 2 horas
 - d. 3 horas

3. Luego de la implementación, ¿Cuánto tiempo aproximadamente se tarda en resolver los incidentes de infraestructura de TI?
 - a. 30 minutos
 - b. 1 hora
 - c. 2 horas
 - d. 3 horas

4. Luego de la implementación, ¿En promedio, cuánto tiempo lleva encontrar el dispositivo o servicio de TI que causó el incidente después de la implementación?
 - a. 1 minuto
 - b. 5 minutos
 - c. 10 minutos
 - d. 15 minutos

5. ¿Cómo evaluaría el enfoque actual de monitoreo de la infraestructura de TI de la empresa?
 - a. Pésimo
 - b. Malo
 - c. Regular
 - d. Bueno
 - e. Excelente

6. ¿Se siente seguro actualmente como se lleva el monitoreo de la infraestructura de TI de la empresa?
 - a. Si
 - b. No

ANEXO 5. ENCUESTA REALIZADA AL PERSONAL USUARIO

ENCUESTA SOBRE LA IMPLEMENTACIÓN DE SOFTWARE ZABBIX COMO SISTEMA DE MONITOREO

Apellidos y Nombres: Yini Rodríguez

1. ¿Cuánto tiempo aproximadamente se tardaba en resolver los incidentes de infraestructura de TI antes de la implementación del Zabbix?
 30 minutos
 1 hora
 2 horas
 3 horas
2. ¿En promedio, cuánto tiempo lleva encontrar el dispositivo o servicio de TI que causó el incidente antes de la implementación?
 30 minutos
 1 hora
 2 horas
 3 horas
3. Luego de la implementación, ¿Cuánto tiempo aproximadamente se tarda en resolver los incidentes de infraestructura de TI?
 10 minutos
 30 minutos
 1 hora
 2 horas
4. Luego de la implementación, ¿En promedio, cuánto tiempo lleva encontrar el dispositivo o servicio de TI que causó el incidente después de la implementación?
 1 minuto
 5 minutos
 10 minutos
 15 minutos
5. ¿Cómo evaluaría el enfoque actual de monitoreo de la infraestructura de TI de la empresa?
 Pésimo
 Malo
 Regular
 Bueno
 Excelente
6. ¿Se siente seguro actualmente como se lleva el monitoreo de la infraestructura de TI de la empresa?
 Sí
 No

ANEXO 6. ENCUESTA REALIZADA AL PERSONAL USUARIO

ENCUESTA SOBRE LA IMPLEMENTACIÓN DE SOFTWARE ZABBIX COMO SISTEMA DE MONITOREO

Apellidos y Nombres: Olivero Olivero Mayken

1. ¿Cuánto tiempo aproximadamente se tardaba en resolver los incidentes de infraestructura de TI antes de la implementación del Zabbix?
 30 minutos
 1 hora
 2 horas
 3 horas
2. ¿En promedio, cuanto tiempo lleva encontrar el dispositivo o servicio de TI que causó el incidente antes de la implementación?
 30 minutos
 1 hora
 2 horas
 3 horas
3. Luego de la implementación, ¿Cuánto tiempo aproximadamente se tarda en resolver los incidentes de infraestructura de TI?
 10 minutos
 30 minutos
 1 hora
 2 horas
4. Luego de la implementación, ¿En promedio, cuánto tiempo lleva encontrar el dispositivo o servicio de TI que causó el incidente después de la implementación?
 1 minuto
 5 minutos
 10 minutos
 15 minutos
5. ¿Cómo evaluaría el enfoque actual de monitoreo de la infraestructura de TI de la empresa?
 Pésimo
 Malo
 Regular
 Bueno
 Excelente
6. ¿Se siente seguro actualmente como se lleva el monitoreo de la infraestructura de TI de la empresa?
 Sí
 No

ANEXO 7. ENCUESTA REALIZADA AL PERSONAL USUARIO

ENCUESTA SOBRE LA IMPLEMENTACIÓN DE SOFTWARE ZABBIX COMO SISTEMA DE MONITOREO

Apellidos y Nombres: R. Lozano, Stacy

1. ¿Cuánto tiempo aproximadamente se tardaba en resolver los incidentes de infraestructura de TI antes de la implementación del Zabbix?
 30 minutos
 1 hora
 2 horas
 3 horas
2. ¿En promedio, cuanto tiempo lleva encontrar el dispositivo o servicio de TI que causó el incidente antes de la implementación?
 30 minutos
 1 hora
 2 horas
 3 horas
3. Luego de la implementación, ¿Cuánto tiempo aproximadamente se tarda en resolver los incidentes de infraestructura de TI?
 10 minutos
 30 minutos
 1 hora
 2 horas
4. Luego de la implementación, ¿En promedio, cuánto tiempo lleva encontrar el dispositivo o servicio de TI que causó el incidente después de la implementación?
 1 minuto
 5 minutos
 10 minutos
 15 minutos
5. ¿Cómo evaluaría el enfoque actual de monitoreo de la infraestructura de TI de la empresa?
 Pésimo
 Malo
 Regular
 Bueno
 Excelente
6. ¿Se siente seguro actualmente como se lleva el monitoreo de la infraestructura de TI de la empresa?
 Sí
 No

ANEXO 8. ENCUESTA REALIZADA AL PERSONAL USUARIO

ENCUESTA SOBRE LA IMPLEMENTACIÓN DE SOFTWARE ZABBIX COMO SISTEMA DE MONITOREO

Apellidos y Nombres: Gonzales Quipe Giorgio Alejandro

1. ¿Cuánto tiempo aproximadamente se tardaba en resolver los incidentes de infraestructura de TI antes de la implementación del Zabbix?
 30 minutos
 1 hora
 2 horas
 3 horas
2. ¿En promedio, cuanto tiempo lleva encontrar el dispositivo o servicio de TI que causó el incidente antes de la implementación?
 30 minutos
 1 hora
 2 horas
 3 horas
3. Luego de la implementación, ¿Cuánto tiempo aproximadamente se tarda en resolver los incidentes de infraestructura de TI?
 10 minutos
 30 minutos
 1 hora
 2 horas
4. Luego de la implementación, ¿En promedio, cuánto tiempo lleva encontrar el dispositivo o servicio de TI que causó el incidente después de la implementación?
 1 minuto
 5 minutos
 10 minutos
 15 minutos
5. ¿Cómo evaluaría el enfoque actual de monitoreo de la infraestructura de TI de la empresa?
 Pésimo
 Malo
 Regular
 Bueno
 Excelente
6. ¿Se siente seguro actualmente como se lleva el monitoreo de la infraestructura de TI de la empresa?
 Sí
 No

ANEXO 9. ENCUESTA REALIZADA AL PERSONAL USUARIO

ENCUESTA SOBRE LA IMPLEMENTACIÓN DE SOFTWARE ZABBIX COMO SISTEMA DE MONITOREO

Apellidos y Nombres: Alvarado Chira Hilagros

1. ¿Cuánto tiempo aproximadamente se tardaba en resolver los incidentes de infraestructura de TI antes de la implementación del Zabbix?
 30 minutos
 1 hora
 2 horas
 3 horas
2. ¿En promedio, cuanto tiempo lleva encontrar el dispositivo o servicio de TI que causó el incidente antes de la implementación?
 30 minutos
 1 hora
 2 horas
 3 horas
3. Luego de la implementación, ¿Cuánto tiempo aproximadamente se tarda en resolver los incidentes de infraestructura de TI?
 10 minutos
 30 minutos
 1 hora
 2 horas
4. Luego de la implementación, ¿En promedio, cuánto tiempo lleva encontrar el dispositivo o servicio de TI que causó el incidente después de la implementación?
 1 minuto
 5 minutos
 10 minutos
 15 minutos
5. ¿Cómo evaluaría el enfoque actual de monitoreo de la infraestructura de TI de la empresa?
 Pésimo
 Malo
 Regular
 Bueno
 Excelente
6. ¿Se siente seguro actualmente como se lleva el monitoreo de la infraestructura de TI de la empresa?
 Sí
 No

ANEXO 10. ENCUESTA REALIZADA AL PERSONAL USUARIO

ENCUESTA SOBRE LA IMPLEMENTACIÓN DE SOFTWARE ZABBIX COMO SISTEMA DE MONITOREO

Apellidos y Nombres: Torres Cordova Alexis Elvis

1. ¿Cuánto tiempo aproximadamente se tardaba en resolver los incidentes de infraestructura de TI antes de la implementación del Zabbix?
 30 minutos
 1 hora
 2 horas
 3 horas
2. ¿En promedio, cuanto tiempo lleva encontrar el dispositivo o servicio de TI que causó el incidente antes de la implementación?
 30 minutos
 1 hora
 2 horas
 3 horas
3. Luego de la implementación, ¿Cuánto tiempo aproximadamente se tarda en resolver los incidentes de infraestructura de TI?
 10 minutos
 30 minutos
 1 hora
 2 horas
4. Luego de la implementación, ¿En promedio, cuánto tiempo lleva encontrar el dispositivo o servicio de TI que causó el incidente después de la implementación?
 1 minuto
 5 minutos
 10 minutos
 15 minutos
5. ¿Cómo evaluaría el enfoque actual de monitoreo de la infraestructura de TI de la empresa?
 Pésimo
 Malo
 Regular
 Bueno
 Excelente
6. ¿Se siente seguro actualmente como se lleva el monitoreo de la infraestructura de TI de la empresa?
 Sí
 No

ANEXO 11. ENCUESTA REALIZADA AL PERSONAL USUARIO

ENCUESTA SOBRE LA IMPLEMENTACIÓN DE SOFTWARE ZABBIX COMO SISTEMA DE MONITOREO

Apellidos y Nombres: López Ramírez Cristhion Alonso

1. ¿Cuánto tiempo aproximadamente se tardaba en resolver los incidentes de infraestructura de TI antes de la implementación del Zabbix?
 30 minutos
 1 hora
 2 horas
 3 horas
2. ¿En promedio, cuánto tiempo lleva encontrar el dispositivo o servicio de TI que causó el incidente antes de la implementación?
 30 minutos
 1 hora
 2 horas
 3 horas
3. Luego de la implementación, ¿Cuánto tiempo aproximadamente se tarda en resolver los incidentes de infraestructura de TI?
 10 minutos
 30 minutos
 1 hora
 2 horas
4. Luego de la implementación, ¿En promedio, cuánto tiempo lleva encontrar el dispositivo o servicio de TI que causó el incidente después de la implementación?
 1 minuto
 5 minutos
 10 minutos
 15 minutos
5. ¿Cómo evaluaría el enfoque actual de monitoreo de la infraestructura de TI de la empresa?
 Pésimo
 Malo
 Regular
 Bueno
 Excelente
6. ¿Se siente seguro actualmente como se lleva el monitoreo de la infraestructura de TI de la empresa?
 Sí
 No

ANEXO 12. ENCUESTA REALIZADA AL PERSONAL USUARIO

ENCUESTA SOBRE LA IMPLEMENTACIÓN DE SOFTWARE ZABBIX COMO SISTEMA DE MONITOREO

Apellidos y Nombres: Anyela Rosmeru Mamani Santos

1. ¿Cuánto tiempo aproximadamente se tardaba en resolver los incidentes de Infraestructura de TI antes de la implementación del Zabbix?
 30 minutos
 1 hora
 2 horas
 3 horas
2. ¿En promedio, cuanto tiempo lleva encontrar el dispositivo o servicio de TI que causó el incidente antes de la implementación?
 30 minutos
 1 hora
 2 horas
 3 horas
3. Luego de la implementación, ¿Cuánto tiempo aproximadamente se tarda en resolver los incidentes de infraestructura de TI?
 10 minutos
 30 minutos
 1 hora
 2 horas
4. Luego de la implementación, ¿En promedio, cuánto tiempo lleva encontrar el dispositivo o servicio de TI que causó el incidente después de la implementación?
 1 minuto
 5 minutos
 10 minutos
 15 minutos
5. ¿Cómo evaluaría el enfoque actual de monitoreo de la infraestructura de TI de la empresa?
 Pésimo
 Malo
 Regular
 Bueno
 Excelente
6. ¿Se siente seguro actualmente como se lleva el monitoreo de la infraestructura de TI de la empresa?
 Sí
 No

ANEXO 13. ENCUESTA REALIZADA AL PERSONAL USUARIO

ENCUESTA SOBRE LA IMPLEMENTACIÓN DE SOFTWARE ZABBIX COMO SISTEMA DE MONITOREO

Apellidos y Nombres: CESAR ESPINO SUENA

1. ¿Cuánto tiempo aproximadamente se tardaba en resolver los incidentes de infraestructura de TI antes de la implementación del Zabbix?
 30 minutos
 1 hora
 2 horas
 3 horas
2. ¿En promedio, cuanto tiempo lleva encontrar el dispositivo o servicio de TI que causó el incidente antes de la implementación?
 30 minutos
 1 hora
 2 horas
 3 horas
3. Luego de la implementación, ¿Cuánto tiempo aproximadamente se tarda en resolver los incidentes de infraestructura de TI?
 10 minutos
 30 minutos
 1 hora
 2 horas
4. Luego de la implementación, ¿En promedio, cuánto tiempo lleva encontrar el dispositivo o servicio de TI que causó el incidente después de la implementación?
 1 minuto
 5 minutos
 10 minutos
 15 minutos
5. ¿Cómo evaluaría el enfoque actual de monitoreo de la infraestructura de TI de la empresa?
 Pésimo
 Malo
 Regular
 Bueno
 Excelente
6. ¿Se siente seguro actualmente como se lleva el monitoreo de la infraestructura de TI de la empresa?
 Sí
 No

ANEXO 14. ENCUESTA REALIZADA AL PERSONAL USUARIO

ENCUESTA SOBRE LA IMPLEMENTACIÓN DE SOFTWARE ZABBIX COMO SISTEMA DE MONITOREO

Apellidos y Nombres: Castillo Guerrero Mauricio Fernando

1. ¿Cuánto tiempo aproximadamente se tardaba en resolver los incidentes de infraestructura de TI antes de la implementación del Zabbix?
 30 minutos
 1 hora
 2 horas
 3 horas
2. ¿En promedio, cuánto tiempo lleva encontrar el dispositivo o servicio de TI que causó el incidente antes de la implementación?
 30 minutos
 1 hora
 2 horas
 3 horas
3. Luego de la implementación, ¿Cuánto tiempo aproximadamente se tarda en resolver los incidentes de infraestructura de TI?
 10 minutos
 30 minutos
 1 hora
 2 horas
4. Luego de la implementación, ¿En promedio, cuánto tiempo lleva encontrar el dispositivo o servicio de TI que causó el incidente después de la implementación?
 1 minuto
 5 minutos
 10 minutos
 15 minutos
5. ¿Cómo evaluaría el enfoque actual de monitoreo de la infraestructura de TI de la empresa?
 Pésimo
 Malo
 Regular
 Bueno
 Excelente
6. ¿Se siente seguro actualmente como se lleva el monitoreo de la infraestructura de TI de la empresa?
 Sí
 No

ANEXO 15. ENCUESTA REALIZADA AL PERSONAL USUARIO

ENCUESTA SOBRE LA IMPLEMENTACIÓN DE SOFTWARE ZABBIX COMO SISTEMA DE MONITOREO

Apellidos y Nombres: Perez Vasquez Carlos Edward

1. ¿Cuánto tiempo aproximadamente se tardaba en resolver los incidentes de infraestructura de TI antes de la implementación del Zabbix?
 30 minutos
 1 hora
 2 horas
 3 horas
2. ¿En promedio, cuánto tiempo lleva encontrar el dispositivo o servicio de TI que causó el incidente antes de la implementación?
 30 minutos
 1 hora
 2 horas
 3 horas
3. Luego de la implementación, ¿Cuánto tiempo aproximadamente se tarda en resolver los incidentes de infraestructura de TI?
 10 minutos
 30 minutos
 1 hora
 2 horas
4. Luego de la implementación, ¿En promedio, cuánto tiempo lleva encontrar el dispositivo o servicio de TI que causó el incidente después de la implementación?
 1 minuto
 5 minutos
 10 minutos
 15 minutos
5. ¿Cómo evaluaría el enfoque actual de monitoreo de la infraestructura de TI de la empresa?
 Pésimo
 Malo
 Regular
 Bueno
 Excelente
6. ¿Se siente seguro actualmente como se lleva el monitoreo de la infraestructura de TI de la empresa?
 Sí
 No

ANEXO 16. ENCUESTA REALIZADA AL PERSONAL USUARIO

ENCUESTA SOBRE LA IMPLEMENTACIÓN DE SOFTWARE ZABBIX COMO SISTEMA DE MONITOREO

Apellidos y Nombres: García Hidalgo Russel

1. ¿Cuánto tiempo aproximadamente se tardaba en resolver los incidentes de infraestructura de TI antes de la implementación del Zabbix?
 30 minutos
 1 hora
 2 horas
 3 horas
2. ¿En promedio, cuánto tiempo lleva encontrar el dispositivo o servicio de TI que causó el incidente antes de la implementación?
 30 minutos
 1 hora
 2 horas
 3 horas
3. Luego de la implementación, ¿Cuánto tiempo aproximadamente se tarda en resolver los incidentes de infraestructura de TI?
 10 minutos
 30 minutos
 1 hora
 2 horas
4. Luego de la implementación, ¿En promedio, cuánto tiempo lleva encontrar el dispositivo o servicio de TI que causó el incidente después de la implementación?
 1 minuto
 5 minutos
 10 minutos
 15 minutos
5. ¿Cómo evaluaría el enfoque actual de monitoreo de la infraestructura de TI de la empresa?
 Pésimo
 Malo
 Regular
 Bueno
 Excelente
6. ¿Se siente seguro actualmente como se lleva el monitoreo de la infraestructura de TI de la empresa?
 Sí
 No

ANEXO 17. ENCUESTA REALIZADA AL PERSONAL USUARIO

ENCUESTA SOBRE LA IMPLEMENTACIÓN DE SOFTWARE ZABBIX COMO SISTEMA DE MONITOREO

Apellidos y Nombres: Itzylke Kenia Requejo Mendoza

1. ¿Cuánto tiempo aproximadamente se tardaba en resolver los incidentes de infraestructura de TI antes de la implementación del Zabbix?
 30 minutos
 1 hora
 2 horas
 3 horas
2. ¿En promedio, cuánto tiempo lleva encontrar el dispositivo o servicio de TI que causó el incidente antes de la implementación?
 30 minutos
 1 hora
 2 horas
 3 horas
3. Luego de la implementación, ¿Cuánto tiempo aproximadamente se tarda en resolver los incidentes de infraestructura de TI?
 10 minutos
 30 minutos
 1 hora
 2 horas
4. Luego de la implementación, ¿En promedio, cuánto tiempo lleva encontrar el dispositivo o servicio de TI que causó el incidente después de la implementación?
 1 minuto
 5 minutos
 10 minutos
 15 minutos
5. ¿Cómo evaluaría el enfoque actual de monitoreo de la infraestructura de TI de la empresa?
 Pésimo
 Malo
 Regular
 Bueno
 Excelente
6. ¿Se siente seguro actualmente como se lleva el monitoreo de la infraestructura de TI de la empresa?
 Sí
 No

ANEXO 18. ENCUESTA REALIZADA AL PERSONAL USUARIO

ENCUESTA SOBRE LA IMPLEMENTACIÓN DE SOFTWARE ZABBIX COMO SISTEMA DE MONITOREO

Apellidos y Nombres: NEXAR SANTOS SIMONZA.

1. ¿Cuánto tiempo aproximadamente se tardaba en resolver los incidentes de infraestructura de TI antes de la implementación del Zabbix?
 30 minutos
 1 hora
 2 horas
 3 horas
2. ¿En promedio, cuánto tiempo lleva encontrar el dispositivo o servicio de TI que causó el incidente antes de la implementación?
 30 minutos
 1 hora
 2 horas
 3 horas
3. Luego de la implementación, ¿Cuánto tiempo aproximadamente se tarda en resolver los incidentes de infraestructura de TI?
 10 minutos
 30 minutos
 1 hora
 2 horas
4. Luego de la implementación, ¿En promedio, cuánto tiempo lleva encontrar el dispositivo o servicio de TI que causó el incidente después de la implementación?
 1 minuto
 5 minutos
 10 minutos
 15 minutos
5. ¿Cómo evaluaría el enfoque actual de monitoreo de la infraestructura de TI de la empresa?
 Pésimo
 Malo
 Regular
 Bueno
 Excelente
6. ¿Se siente seguro actualmente como se lleva el monitoreo de la infraestructura de TI de la empresa?
 Sí
 No

ANEXO 19. CONSTANCIA DE TRABAJO



Lima, 14 de Agosto del 2023

CONSTANCIA DE TRABAJO

DESYSWEB S.A.C identificado con R.U.C 20503795079, deja constancia que la Srta. **ZAMBRANO BERROCAL KATHERINE GLADYS**, identificado con DNI N° 73958420, viene ejerciendo las labores de SUPERVISORA DE NOC en el **Área de Proyecto**. Desde el 20 de Junio de 2022 hasta la actualidad, demostrando compromiso, eficiencia y responsabilidad de sus labores.

Se emite el presente documento para los fines que el interesado estime conveniente.

SOLUCIONES TECNOLÓGICAS INTEGRALES

A handwritten signature in blue ink, appearing to read 'Oswaldo Veas Santa Cruz', is written over a horizontal line.

Oswaldo Veas Santa Cruz
Gerente General
LA EMPRESA

San Martín de Porres, Lima

ANEXO 20. CARTA DE AUTORIZACION PARA USO DE DATOS



SOLUCIONES TECNOLOGICAS INTEGRALES

Lima, 1 de diciembre del 2023

Yo, Oswaldo Veas Santa Cruz, con DNI N° 06780843, representante de la empresa DESYSWEB S.A.C, con ruc N° 20503795079, autorizo a Katherine Gladys Zambrano Berrocal, con DNI N° 73958420, utilizar los datos de la organización necesarios para el desarrollo su informe de suficiencia profesional referidos al proyecto "Implementación de Software Zabbix como Sistema de Monitoreo para Equipos en la Red Local de la Empresa Desysweb S.A.C."

Oswaldo Jesús Veas Santa Cruz
Gerente General

The signature block contains a circular stamp with the text 'DSW DESYSWEB' at the top. Inside the stamp is a handwritten signature in blue ink. Below the stamp, the name 'Oswaldo Veas Santa Cruz' is printed in a smaller font, followed by 'Oswaldo Jesús Veas Santa Cruz' and 'Gerente General' in a larger font.

San Martín de Porres, Lima

ANEXO 21. PRUEBAS DE INTERFAZ DEL MODO USUARIO

