ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO Y CONTROL DE LA INFRAESTRUCTURA DE TI PARA LA GESTIÓN DE INCIDENCIAS EN LA RED INTERNA DE LA EMPRESA AVÍCOLA POLLO FAVORITO S.A. (POFASA)

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

HUGO DAVID MONTERO CADENA

hugo.montero@epn.edu.ec

DIRECTOR: MSc. Rodrigo Fabian Chancusig Chuquilla

rodrigo.chancusig@epn.edu.ec

CODIRECTOR: MSc. William Humberto Andrade Hinojosa

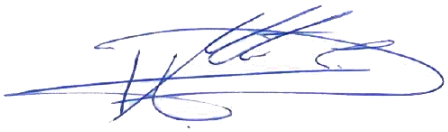
william.andrade@epn.edu.ec

Quito, 2022

DECLARACIÓN

Yo Hugo David Montero Cadena, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.



Hugo David Montero Cadena

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Hugo David Montero Cadena, bajo mi supervisión.

MSc. Rodrigo Chancusig

DIRECTOR DEL PROYECTO

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Hugo David Montero Cadena, bajo mi supervisión.

MSc. William Andrade

DIRECTOR DEL PROYECTO

DEDICATORIA

El presente trabajo de investigación se lo dedico a mi familia y amigos por su apoyo incondicional y su cariño demostrado en todo momento.

Hugo David Montero Cadena.

AGRADECIMIENTOS

A mis padres, quienes me brindaron todo su apoyo y cariño durante esta etapa de mi vida; motivándome siempre a seguir adelante y cumplir con mis metas. Gracias, por su infinita bondad.

A mis hermanos que siempre estuvieron en los momentos más difíciles, por la confianza y sus consejos que me ayudaron a avanzar y lograr mis objetivos.

A mi director MSc. Rodrigo Chancusig y codirector MSc. William Andrade por la paciencia que tuvieron y por compartirme sus conocimientos y todo el apoyo brindado durante la ejecución de este proyecto.

A Estefany Ronquillo, por su cariño y apoyo demostrado en todos estos años.

Hugo David Montero Cadena.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente proyecto integrador se llevó a cabo en la empresa Pollo Favorito SA (POFASA), el principal objetivo fue realizar un análisis de los sistemas de monitoreo más representativos del mercado actual. El sistema de código abierto que obtuvo el mejor rendimiento y se ajustó a las necesidades de la empresa, fue implementado dentro de su infraestructura. Sus principales necesidades fueron: tener un monitoreo permanente y recibir alertas de eventos ocurridos en su infraestructura de TI. Con la notificación inmediata de los eventos relevantes, el área de TI pudo resolver de manera precisa y oportuna los problemas que ocurrieron mucho antes de que afectaran las operaciones del negocio, evitando pérdidas económicas. Se concluye que la implementación de sistemas de monitoreo de TI tiene un impacto positivo en la gestión de incidentes de la red interna de la empresa, al reducir el tiempo de respuesta de 4 horas a 30 minutos para la atención de incidentes y el tiempo para encontrar los dispositivos y servicios afectados se redujo de 2 horas a 30 minutos. Además, se mejoró la calidad de servicio con el personal, de tener una calificación pésima en la satisfacción de los usuarios se obtuvo una calificación excelente después de la implementación. Demostrando que un sistema de monitoreo es necesario para todo tipo de organizaciones porque brinda detalles en tiempo real de toda la infraestructura de TI, lo que le ofrece un mejor control sobre sus operaciones y reporte a tiempo real.

Palabras clave: código abierto, incidente, infraestructura de TI y monitoreo.

ABSTRACT

This project was implemented in the company Pollo Favorito SA (POFASA), the main objective was to perform an analysis of the most representative monitoring systems in the current market. The open-source system that obtained the best performance and adjusted to the needs of the company, was implemented within its infrastructure. Their main needs were to have permanent monitoring and to receive alerts of the events occurring in their IT infrastructure. With an immediate notification of relevant events, the IT area was able to solve in an accurate and timely manner the problems that occurred long before and that have affected the business operations, avoiding economic losses. It is concluded that the implementation of IT monitoring systems has a positive impact on incident management of the company's internal network, by reducing the response time from 4 hours to 30 minutes for incident attention and the time to find the affected devices and services was reduced from 2 hours to 30 minutes. In addition, the service quality was improved with the staff. Thereby, from having a very poor rating in user satisfaction, an excellent rating was acquired after the implementation. Thus, proving that a monitoring system is necessary for all types of organizations because it provides real-time details of the entire IT infrastructure, granting you a better control over your operations and real-time reporting.

Keywords: incident, IT infrastructure, monitoring and open source.

1 INTRODUCCIÓN

El monitoreo de dispositivos y servicios de Tecnologías de la Información (TI) es un proceso de supervisión y control; que evalúa y mide el correcto funcionamiento de la infraestructura de TI de una empresa. El objetivo principal es entender el funcionamiento de los diferentes recursos conectados a una misma red dentro de una organización; para optimizar su rendimiento y actuar de una manera rápida y eficiente ante un error inesperado [1].

En la actualidad las empresas tienen un ilimitado número de dispositivos y servicios que interactúan entre si dentro su red de datos, los cuales, al no ser monitoreados frecuentemente pueden ocasionar fallas de comunicación, disponibilidad y rendimiento con los principales servicios, por ejemplo, el sistema contable o de facturación de una empresa. El proceso debe ser realizado con la ayuda de una herramienta porque es poco factible para el área de TI o personal encargado, realizar la verificación constante del estado de cada uno de los diferentes dispositivos y servicios dentro de la infraestructura interna de la empresa [2].

Por lo que es necesario que el personal encargado del área de TI de la empresa realice el monitoreo de los riesgos identificados en su área, de manera continua, teniendo en cuenta que éstos no dejan de representar una amenaza para la misma. La etapa de monitoreo es esencial para asegurar que las acciones se están llevando a cabo y ayuda a evaluar la eficiencia en su implementación, adelantando revisiones sobre la ejecución de servicios para evidenciar todas las situaciones o factores que pueden estar influyendo en la aplicación de las acciones preventivas [3].

El objetivo del presente trabajo de titulación consistió en realizar un análisis de las herramientas más representativas que existen en el mercado actual; con la herramienta que obtenga el mejor rendimiento y se ajuste a las necesidades de la empresa Pollo Favorito SA (POFASA), facilitando al personal encargado de TI estar actualizado de todos los eventos relevantes a través de diferentes medios como correo electrónico, mensajes o pantallas informativas dentro un tablero virtual. El área de TI al obtener la información de eventos relevantes con alertas inmediatas puede actuar de manera precisa y oportuna en la resolución de problemas encontrados, mucho antes de que afecte a la operación del núcleo del negocio, evitando pérdidas económicas por tiempos muertos en operaciones o transacciones de la empresa POFASA.

1.1 CARACTERÍSTICAS DE LA EMPRESA

La red de datos de la empresa POFASA fue diseñada para conectar sus 4 diferentes sucursales dentro del cantón Quito, con el objetivo de tener una comunicación con sus servidores que funcionan como directorio activo de Microsoft y conectividad de red interna con los 48 puntos de conexión alámbrica que maneja cada sucursal. Además, conectar su sistema contable y de producción diaria con los 80 usuarios administrativos que están laborando en cada sucursal [4].

Las aplicaciones y servicios que tiene dentro de su infraestructura de TI la empresa POFASA son de tipo web y se encuentran alojadas dentro de un servidor externo a su centro datos, por lo cual se debe monitorear la conexión que permite la comunicación con el servidor externo. Esta conexión es administrada por su proveedor de internet (PUNTO NET) a través de una conexión VPN. Además, tiene un servicio de directorio activo que maneja las políticas en cada equipo y el servicio de DNS para navegación por internet por este motivo si el servidor pierde su conexión los usuarios dentro de la red interna no podrían navegar a internet a pesar de tener servicio activo [4].

Para ofrecer los servicios y aplicaciones en la red interna de la empresa tienen los siguientes dispositivos en su infraestructura: 4 corta fuegos de marca FORTINET, 100 computadoras (laptops – desktops) de marca LENOVO, 3 servidores con máquinas virtuales, 6 puntos de acceso wifi de marca UBIQUITI, 2 switch cisco catalyst encargados de administrar VLAN, 6 switch de marca HP y 8 impresoras en red. Dicha red interna tiene medios de comunicación guiados y no guiados; los medios guiados constan de: fibra óptica y cable UTP categoría 6A blindado. En cambio, los no guiados constan de sistemas WIFI con estándar IEEE 802.11n y un sistema de protección WPA versión 2 a través de un controlador remoto manejan la configuración de los equipos inalámbricos. La figura 1 representa los equipos de comunicación dentro de la red de la empresa POFASA y la conexión con sus sucursales [4].

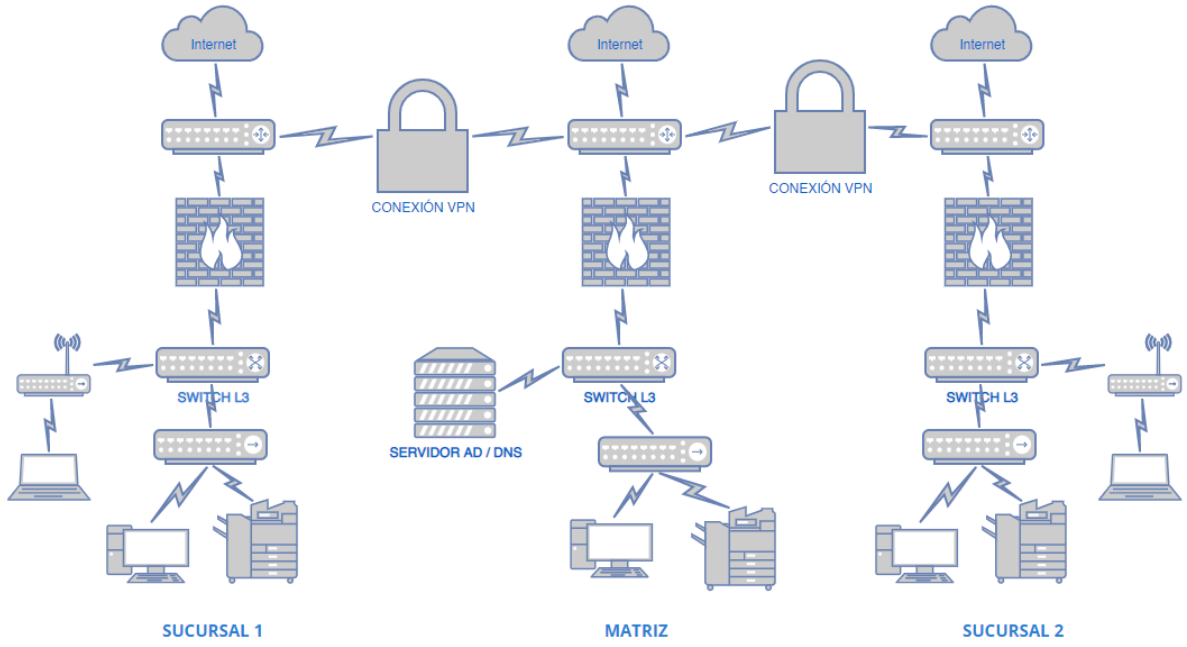


Figura 1. Diagrama representativo de la red POFASA

1.2 FORMULACIÓN DEL PROBLEMA

Actualmente, las pequeñas, medianas y grandes empresas del país tienen un constante crecimiento tecnológico, lo que implica la gestión de una mayor cantidad de información a través de su red. También cuentan con servicios de TI con diferentes componentes en hardware, software, bases de datos y sistemas operativos con distintos fabricantes. Cada componente consta de un sistema de monitoreo de funcionamiento en plataformas de software propietarios de cada marca y consolas diferentes por el tipo de hardware.

Los administradores y supervisores de TI deben observar y monitorear continuamente las fallas de la infraestructura de los cuartos de datos que están afectando la eficiencia de los procesos internos y externos. Actualmente, Ecuador no cuenta con una cultura por el servicio de monitoreo, debido a la dificultad en la instalación y mantenimiento de dicho sistema. Por otro lado, el traslado del personal de TI, cuyo fin es recolectar continuamente la información de manera presencial por cada dispositivo, en las diferentes oficinas o sedes que tienen dentro y fuera de la ciudad de residencia; genera grandes pérdidas de tiempo y dinero. Además, dicha movilización se convierte en una de las mayores dificultades que las empresas enfrentan en la actualidad.

La empresa POFASA no cuenta con un sistema de monitoreo automatizado, este proceso se realiza de manera manual a través de mantenimientos preventivos presenciales, en los cuales se constata el estado actual de la infraestructura. En situaciones de fallos de disponibilidad, estos son reportados por el personal operativo que se encuentra utilizando el servicio o dispositivo. Sin embargo, el proceso para monitorear la infraestructura puede ser costoso y complejo, ya que la empresa debe contar con varias pantallas y personal que se movilice para verificar cada una de las consolas de los componentes de hardware ubicados en los diferentes sitios dentro de la provincia de Pichincha.

En este contexto, la empresa POFASA requiere que sus servicios sean monitoreados en línea para detectar posibles caídas o alteraciones adicionales que puedan estar experimentando la infraestructura de TI. Si las posibles causas no se controlan de manera efectiva, pueden provocar graves problemas de conectividad y disponibilidad de servicios.

Dados estos problemas como lo son: el monitoreo de manera presencial en las diferentes sucursales de la empresa POFASA, el no contar con alertas preventivas en condiciones de pérdidas de disponibilidad de uno o varios dispositivos o servicios de TI y especialmente tener un monitoreo proactivo en lugar de preventivo para la infraestructura de TI.

Por esta razón, se implementará un sistema de monitoreo y control que conecte los dispositivos y servicios críticos de la infraestructura de TI de la empresa, el cual será un soporte para los administradores o encargados de los diferentes tipos de infraestructura.

1.3 JUSTIFICACIÓN

La empresa POFASA y probablemente en todas las pequeñas, medianas y grandes compañías, surge la necesidad de tener un cuarto de datos. POFASA también requiere un correcto control y gestión de sus componentes lógicos y físicos; por tal motivo, tener un área de TI que administre estos servicios es fundamental. Así mismo, es necesario contar con un sistema encargado del monitoreo de servicios alojados en el cuarto de datos como son equipos de comunicación y enlaces de red hacia las diferentes sedes u oficinas que tiene la empresa en relación con su negocio.

En la infraestructura de TI de las empresas es necesario utilizar herramientas automatizadas para monitorear el uso de sus dispositivos y servicios críticos de TI. Con el objetivo de identificar problemas o situaciones anormales en su funcionamiento. La variedad de recursos,

la cantidad de usuarios y su demanda ocasiona el aumento de vulnerabilidad de la infraestructura de TI, por lo que es necesario implementar herramientas automatizadas para apoyar la gestión de monitoreo remoto.

Actualmente, existen varias herramientas disponibles para monitoreo remoto, como lo son: Windows Management Instrumentation (WMI), Remote Procedure Calls (RPC), Remote Method Invocation (RMI), Internet Control Message Protocol (ICMP), Simple Network Management Protocol (SNMP), entre otros. Existen dos tipos de comunicación remota como la comunicación remota directa, se refiere al uso de los componentes de monitoreo local del equipo, como ICMP, Traceroute o Tracert y SNMP y la comunicación remota indirecta, que requiere la instalación local de programas denominados agentes que tiene la tarea de establecer la comunicación entre el equipo y el sistema de monitoreo [5].

Cada herramienta de monitoreo ofrece funciones específicas, por lo que es importante comprender sus características y limitaciones a la hora de elegir una solución que soporte la gestión de la infraestructura de TI, teniendo en cuenta que estas características deben coincidir con los objetivos de la empresa. A la hora de seleccionar un sistema de seguimiento, además del cumplimiento de las funcionalidades técnicas, se debe tener en cuenta la relación costo-beneficio examinando los ahorros mediante la reducción de los tiempos de inactividad, la reducción del esfuerzo de seguimiento y la mejora de la calidad de los servicios para llevar a cabo su adquisición, implementación y mantenimiento.

La empresa POFASA busca flexibilidad y varios métodos de notificación de eventos, lo cuales pueden ser, de advertencia o fallos en la disponibilidad del servicio. Herramientas de monitorio con licencia pública general (GPL), como son: Nagios, Sensu, Icinga y Zabbix; que permiten aprovechar sus funcionalidades sin ningún costo [6].

El sistema que se implementó en el presente proyecto otorgará un beneficio directo para los administradores de TI ya que permitirá tener un control preventivo y correctivo del estado de salud de los diferentes equipos y software dentro del cuarto de datos. De igual manera, implica una reducción de los tiempos de servicios que se realizaban periódicamente para la verificación individual de cada equipo a su cargo.

1.4 OBJETIVOS

1.4.1 OBJETIVO GENERAL

Implementar un sistema de monitoreo y control de la infraestructura de TI para la gestión de incidencias en la red interna de la empresa avícola Pollo Favorito S.A. (POFASA) a través del análisis de los servicios y dispositivos críticos.

1.4.2 OBJETIVOS ESPECÍFICOS

- Realizar una comparativa de los diferentes sistemas más reconocidos y representativos en el monitoreo de TI en base a su rendimiento.
- Establecer los parámetros críticos de monitoreo en los diferentes sistemas y dispositivos de TI, de acuerdo con la importancia y objetivos de la infraestructura tecnológica.
- Implementar y configurar el sistema de monitoreo en la infraestructura interna de la empresa.
- Realizar pruebas de conexión y monitoreo de los diferentes sistemas y dispositivos conectados en una sola consola.
- Generar notificaciones y alertas por fallos en comunicación y energía eléctrica en diferentes plataformas de correo electrónico, Microsoft Teams y Telegram.
- Evaluar los resultados obtenidos por el sistema implementado y la satisfacción de los usuarios que administran la infraestructura de TI.

1.5 MARCO TEÓRICO

1.5.1 DEFINICIÓN DE TÉRMINOS

1.5.1.1 MONITOREO DE TI

El monitoreo se refiere a la actividad de observar una situación para detectar cambios que ocurren con el tiempo. Hay diferentes tipos de herramientas de monitoreo y diferentes situaciones en las que se utilizará cada una. A continuación, vamos a ver los diferentes tipos de monitoreo que se pueden realizar [7]:

- La monitorización activa se refiere al "interrogatorio" continuo de un dispositivo o sistema para determinar su estado. Este tipo de monitoreo puede requerir muchos

recursos y generalmente se reserva para monitorear de manera proactiva la disponibilidad de dispositivos o sistemas críticos; o como paso de diagnóstico al intentar resolver un incidente o diagnosticar un problema [7].

- El monitoreo pasivo es más común y se refiere a la generación y transmisión de eventos a un "dispositivo de escucha" o agente de monitoreo. El monitoreo pasivo depende de la definición exitosa de los eventos y la instrumentación del sistema que se está monitoreando [7].

En la actualidad, existen tres tipos de herramientas para el monitoreo de infraestructura TIC: software propietario, software de código de abierto y software como servicio (SaaS).

1.5.1.2 INFRAESTRUCTURA DE TI

El término infraestructura de TI se define según la guía de buenas prácticas para la gestión de servicios de tecnologías de la información ITIL [8], como un conjunto combinado de hardware, software, redes, instalaciones, etc. (incluidos todos los equipos relacionados con la tecnología de la información) utilizados para desarrollar, probar, entregar, monitorear, controlar o respaldar servicios de TI. El personal, la documentación y los procesos no son parte de la infraestructura de TI. Sin embargo, sin personal competente y bien calificado a cargo de ejecutar y mantener su infraestructura, limitará involuntariamente las capacidades de su organización [7].

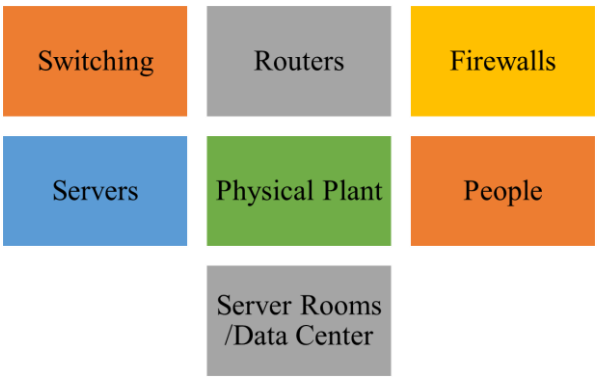


Figura 2. Elementos de la infraestructura de TI

1.5.1.3 SERVICIO DE TI

Es un medio para entregar valor a los clientes facilitando resultados que los clientes desean lograr sin asumir costos y riesgos específicos. El término 'servicio' a veces se usa como sinónimo de servicio central, servicio de TI o paquete de servicios. Un servicio de TI se

compone de una combinación de personas, procesos y tecnología, y podrían definirse en un Acuerdo de Nivel de Servicio (SLA) [7].

1.5.1.4 MODELO PDCA O CICLO DE DEMING

En un proceso central, los resultados reales de una acción se comparan con un objetivo o un punto de referencia; se menciona la diferencia entre ambos y se adoptan medidas correctoras si la disparidad es grande. La naturaleza repetida y continua de la mejora continua sigue esta definición habitual de control y está representada por el ciclo PDCA (Plan, Do, Check, Act). En español el ciclo tiene el nombre PHVA (Planificar, Hacer, Verificar, Actuar). También se conoce como el círculo de Deming, llamado así por W. E. Deming [9].

Las etapas del ciclo PDCA consisten en:

- Planificar: establece metas de mejora, incluido el análisis de la brecha, la definición de pasos de acción para cerrar la brecha y el establecimiento e implementación de medidas para asegurar que la brecha se haya cerrado y se hayan logrado los beneficios. Para desarrollar esta fase es importante tener claro qué tipo de resultados se desean en el sistema de monitoreo; de esta forma, la fase se puede orientar en torno al logro de los objetivos planteados por la empresa POFASA.
- Hacer: desarrollo e implementación de un proyecto para cerrar la brecha. Implementación o mejora de procesos y establecimiento del buen funcionamiento del proceso. Esto implica no solo realizar el cambio para completar la fase de implementación del sistema de monitoreo, también surge la necesidad de supervisar todo el proceso mientras se realiza y registrar la mayor cantidad de datos con el objetivo de determinar si el sistema implementado realmente funciona de la manera adecuada para la empresa.
- Verificar: comparación del entorno implementado con las medidas de éxito establecidas en la fase de planificar. La comparación determina si todavía existe una brecha entre los objetivos de mejora del proceso y el estado del proceso operativo. Las brechas no necesariamente requieren un cierre. Una brecha puede considerarse tolerable si el desempeño real está dentro de los límites de desempeño permitidos por la empresa.
- Actuar: el proceso de decisión para determinar si se requiere más trabajo para cerrar las brechas restantes, la asignación de recursos necesarios para respaldar otra vuelta al ciclo de mejora. Si es necesario, el ciclo debe repetirse una y otra vez hasta encontrar

una mejora constante; esto ayudará a promover la cultura de mejora continua con el personal de TI.

Los beneficios de implementar esta metodología incluyen brindar soluciones efectivas y rápidas a varios problemas; documentando los procesos antes y después de la solución en el ciclo. Esta información se podrá utilizar en el siguiente ciclo de mejora continua. Además, se ha comprobado que la aplicación del ciclo PDCA es mucho más eficaz que la adopción de un enfoque "correcto a la primera". El ciclo permite dos tipos de acción correctiva: temporal y permanente. La acción temporal tiene por objetivo obtener resultados abordando y solucionando prácticamente el problema. La acción permanente, en cambio, consiste en investigar y eliminar las causas de fondo y, por tanto, tiene como objetivo la sostenibilidad del proceso mejorado [9]. La empresa puede extender su aplicación a otros departamentos, con la confianza que brindará los beneficios esperados.

1.5.2 HERRAMIENTAS DE MONITORIZACIÓN REMOTA

Las herramientas de monitoreo remota ayudan a los administradores de red a identificar dónde radica el problema a través del acceso remoto. Actualmente existen dos tipos de comunicación remota:

- Directa, se utilizan componentes de comunicación locales del equipo, ejemplo: SNMP, ICMP, Tracert y Traceroute.
- Indirecta, se requiere la instalación de un programa llamado agente en el equipo a monitorear, este agente realiza la comunicación entre el equipo y la herramienta de monitoreo.

A continuación, se definirán algunos elementos de monitoreo remoto utilizados por personal del área de TI para verificar el estado de los dispositivos y servicios de la infraestructura.

1.5.2.1 WINDOWS MANAGEMENT INSTRUMENTATION

WMI está presente en todos los sistemas operativos Windows, forma parte de un potente conjunto de herramientas utilizadas para gestionar los sistemas Windows tanto local como remotamente. WMI ha sido bien conocido y utilizado en gran medida por los administradores de sistemas desde sus inicios. WMI es un servicio instalado en todos los sistemas operativos de Microsoft. Así que puede escribir libremente scripts o aplicaciones para automatizar las tareas

administrativas en los sistemas basados en Windows. Además, actúa como un medio para adquirir información sobre el funcionamiento de un sistema operativo [10].

Ayuda a los administradores a obtener información sobre todos los aspectos de un sistema operativo. WMI es una herramienta útil para la administración de sistemas y la gestión de ordenadores. Sin embargo, la capacidad y características de WMI son también herramientas potenciales para la distribución de amenazas. Así que la herramienta WMI puede ser más útil o perjudicial según el incidente. El uso de WMI puede reunir información sobre los servicios de un sistema, el procesador, el disco y todos los objetos información. También WMI puede automatizar la recopilación de datos de hardware y software y puede ser utilizado para automatizar las actividades maliciosas. Windows PowerShell es la forma más potente de interactuar con WMI y que permite una multitud de opciones de formato de resultados [10].

1.5.2.2 SIMPLE NETWORK MANAGEMENT PROTOCOL

El protocolo SNMP se introdujo en 1988 para para satisfacer la creciente necesidad de un estándar para la gestión de dispositivos del Protocolo de Internet (IP). SNMP ofrece a sus usuarios un conjunto "sencillo" de operaciones que permite gestionar estos dispositivos de forma remota. El núcleo de SNMP es un simple conjunto de operaciones (y la información que estas operaciones recogen) que da a los administradores la capacidad de cambiar el estado de algún dispositivo basado en SNMP. Por ejemplo, puede utilizar SNMP para apagar una interfaz en su router o comprobar la velocidad a la que funciona su interfaz Ethernet. Incluso supervisar la temperatura de su conmutador y avisarle cuando es demasiado alta. Suele asociarse a la gestión de routers, pero es importante entender que puede utilizarse para gestionar muchos tipos de dispositivos. Mientras que el predecesor de SNMP, Simple Gateway Management Protocol (SGMP), fue desarrollado para gestionar routers de Internet de Internet, SNMP puede utilizarse para gestionar sistemas Unix, sistemas Windows, impresoras, racks de módem, fuentes de alimentación, etc. Cualquier dispositivo que ejecute un software que permita la recuperación de información SNMP puede ser gestionado. Esto incluye no sólo dispositivos físicos, sino también el software, como los servidores web y las bases de datos [11].

Otro aspecto de la gestión de la red es la supervisión de la misma, es decir, la supervisión de una red completa en lugar de routers individuales, hosts y otros dispositivos remotos. La monitorización remota de la red se desarrolló para ayudarnos a entender cómo está funcionando la red en sí, así como cómo los dispositivos individuales de la red afectan en conjunto a la red.

Puede utilizarse para supervisar no sólo el tráfico local (LAN), también las interfaces Wide Area Network (WAN) [11].

Dentro SNMP hay dos tipos de entidades: los gestores y los agentes. Un gestor es un servidor que ejecuta algún tipo de sistema de software que puede manejar las tareas de gestión de una red. Los gestores suelen denominarse estaciones de gestión de red (NMS, sus acrónimos en ingles significan Network Management System). Un NMS es responsable de sondear y recibir capturas de los agentes en la red. Un sondeo, en el contexto de la gestión de la red, es el acto de consultar un agente (enrutador, conmutador, servidor Unix, etc.) para obtener algún tipo de información. Esta información puede ser usada más tarde para determinar si ha ocurrido algún tipo de evento catastrófico. Una captura es una forma de que el agente le diga al NMS que ha ocurrido algo. Las capturas se envían de forma asíncrona, no en respuesta a las consultas del NMS. Por ejemplo, cuando su infraestructura a internet se cae, su router puede enviar una captura a su NMS y este a su vez puede llevar a cabo alguna acción, por ejemplo, notificar que ha ocurrido algo [11].

La segunda entidad, el agente, es una pieza de software que se ejecuta en los dispositivos de red que están gestionando. Puede ser un programa independiente (un demonio, en lenguaje Unix), o puede estar incorporado en el sistema operativo (por ejemplo, el IOS de Cisco en un router, o el sistema operativo de bajo nivel). Hoy en día, la mayoría de los dispositivos IP vienen con algún tipo de agente SNMP incorporado. El hecho de que los proveedores estén dispuestos a implementar agentes en muchos de sus productos facilita el trabajo del equipo de TI. El agente proporciona información de gestión al NMS, manteniendo un seguimiento de varios aspectos operativos del dispositivo. Por ejemplo, el agente de un router es capaz de mantener un registro del estado de cada una de sus interfaces: cuáles están activas, cuáles están caídos, etc. El NMS puede consultar el estado de cada interfaz y tomar acción apropiada si alguna de ellas está caída. Cuando el agente se da cuenta de que algo malo ha sucedido, puede enviar una captura al NMS. Esta captura se origina en el agente y se envía al NMS, donde se gestiona adecuadamente [11].

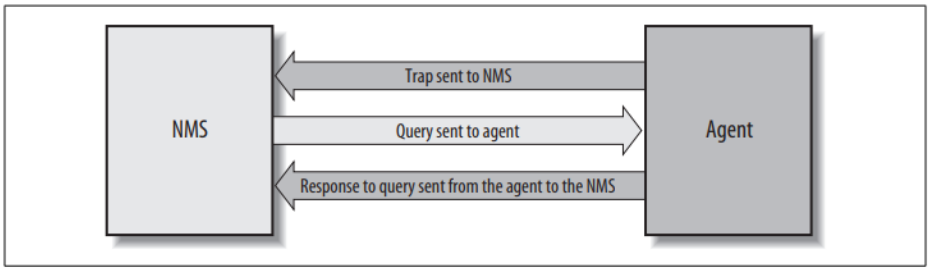


Figura 3. Muestra la relación entre el NMS y un agente.

1.5.2.3 INTERNET CONTROL MESSAGE PROTOCOL

ICMP es parte de la capa de internet (the open systems interconnection: OSI model) y se transporta dentro de datagramas IP. Es un protocolo de control de internet, su función es apoyar y detectar daños en diversas situaciones atípicas durante el trabajo de las direcciones IP. Las tareas del protocolo son [12]:

- Controlar el flujo de datos; cuando la computadora de destino de la transmisión IP no logra procesar los datagramas IP entrantes, el ICMP envía un Source Quench (mecanismo que informa al remitente de datos que los paquetes no se pueden reenviar debido a la sobrecarga) después de lo cual el remitente debe detener temporalmente la transmisión.
- Informar la falta de posibilidad de entrega de datos; si la computadora de destino no responde, el sistema que encontró el problema envía "Destino Inalcanzable" al remitente, si este mensaje es enviado por el enrutador, significa que el enrutador no puede enviar paquetes a un equipo determinado. Puede ocurrir en dos casos: la dirección IP de destino no existe (por ejemplo, la computadora de destino está apagada, su red esta apagada, la máscara está configurada incorrectamente); luego esta host inamovible, el enrutador no puede entregar el datagrama a esta red; luego esta red inalcanzable, cuando el host envía el mensaje, puede significar que el equipo no tiene ningún soporte para ningún protocolo de capas superiores.
- Redirigir las rutas, si la computadora (router) a la que llegó el datagrama decide que otro dispositivo de la misma red será mejor puerta de enlace, envía redirigir mostrando a otro equipo (debe estar en la misma red). Después de recibir dicho mensaje, el receptor debe actualizar su tabla de enrutamiento.
- Probar la disponibilidad del host remoto, tiene lugar durante el comando ping, se envía el mensaje "Solicitud" y después de recibirlo, la computadora de destino debe responder con "Respuesta". Si no lo hace y el dispositivo que trasmite no obtiene la respuesta en un tiempo determinado, el host de destino se considera inalcanzable.
- Si un datagrama alcanza el límite cero de tiempo de vida en su camino a través del enrutador, se elimina. El mensaje ICMP de tiempo excedido se envía a la computadora de origen de un datagrama dado. Este protocolo es muy importante para el control en internet. Soporta la mayoría de las emergencias e informa a los anfitriones interesados sobre dichas emergencias. Se utiliza muy a menudo para resolver cualquier tipo de problema mediante el uso del popular comando "ping" y "traceroute" implementados

en la mayoría de los sistemas operativos de red. Una de las desventajas de estos comandos es que existen muchas posibilidades de dañar la red de dispositivos por esta razón los administradores desactivan dicho protocolo [12].

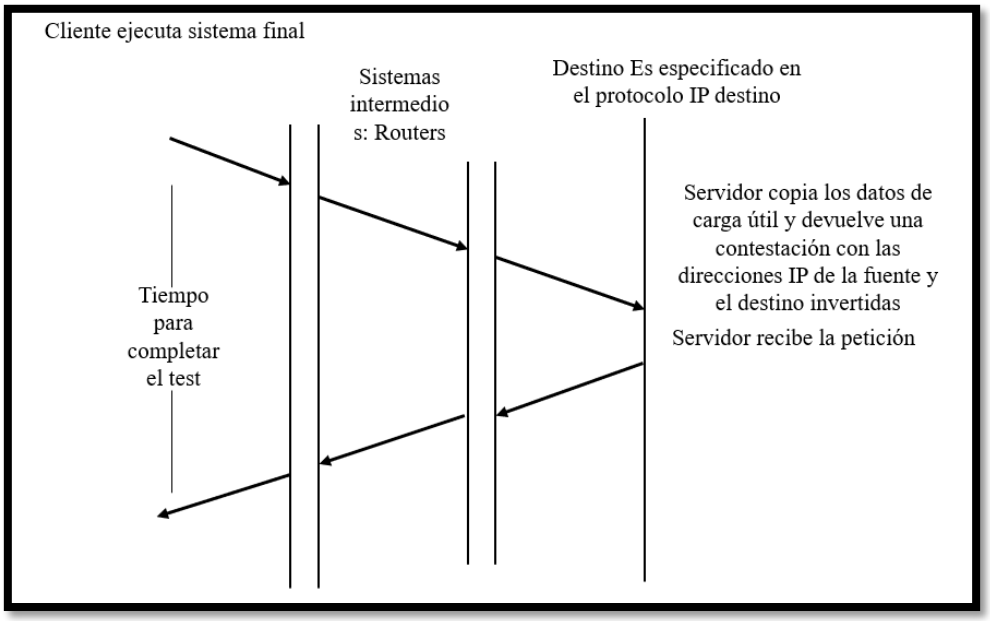


Figura 4. Ejemplo de envío y recepción de un ping.

1.5.3 PARÁMETROS DE MONITOREO

Los parámetros de medición o variables de monitoreo del hardware y software que son parte de la infraestructura de TI, al momento de cambiar su estado pueden impactar de manera negativa a las actividades esenciales de la empresa; es fundamental identificar y medir estos parámetros ya que son importantes para el cumplimiento de los objetivos de la empresa. Existen parámetros comunes entre los diferentes dispositivos y servicios de la infraestructura de TI que ayudan a su monitoreo, por ejemplo, utilización del procesador – GPU, utilización de espacio en disco duro, temperatura y estado operativo. Dichos parámetros tienen un rango de aceptación para su correcto funcionamiento, al momento de salir del rango mencionado altera su funcionamiento y desempeño.

Técnicamente, se consideran parámetros críticos todas las variables de hardware que, al cambiar negativamente, afectan el rendimiento de un servicio de TI. Estos parámetros deben ser medibles para ser integrados en el monitoreo de infraestructura de TI. Como resultado, el personal encargado de TI podrá establecer buenos umbrales de rendimiento, dependiendo de las necesidades normales de los recursos y servicios utilizados por la empresa. El objetivo de detectar un valor fuera de rango es generar alertas para notificar la ocurrencia de cualquier

problema. Además, identificar los dispositivos afectados para que se puedan tomar las acciones correctivas necesarias [5].

En el instructivo de mejores prácticas para el monitoreo a través de herramienta propietaria, se proponen recomendaciones sobre la supervisión básica del estado de los dispositivos de esta marca, entre las cuales clasifican parámetros de sistema y de entorno. El primer parámetro de sistema describe al uso del procesador y la memoria del dispositivo junto con el estado de las interfaces del dispositivo. El segundo parámetro de entorno describe al estado del ventilador, al sensor de temperatura, voltaje y el suministro de energía del dispositivo. Cabe mencionar que el instructivo está dedicado a dispositivos de la marca CISCO, pero es válido para dispositivos de otras marcas ya que son parámetros generales que comparten [13].

Parámetros	**Descripción**
Sistema	Uso de procesador
	Uso del almacenamiento (disco duro)
	Uso de memoria RAM
Entorno	Estado del ventilador
	Estado del sensor de temperatura
	Estado del suministro de energía
Red	Disponibilidad de las interfaces
	Uso de interfaces de red
	Tiempo de respuesta

Tabla 1. Parámetros básicos de monitoreo [13]

El objetivo del presente trabajo es estandarizar los parámetros básicos y comunes entre los diversos dispositivos IP de la infraestructura de TI (servidores, corta fuegos, switch, computadores y puntos de acceso) que son utilizados para configurar las métricas en un sistema de monitoreo.

1.6 ANÁLISIS DE SISTEMA DE MONITOREO

Cada herramienta de monitoreo proporciona funciones específicas, por lo que es importante conocer sus características y limitaciones a la hora de elegir una solución que soporte la gestión de la infraestructura de TI, teniendo en cuenta que estas características deben cumplir con los objetivos de la empresa. Para la selección del sistema de monitoreo, además de respetar las

funciones técnicas, se debe tener en cuenta la relación costo/beneficio, mediante el ahorro generado por la reducción del tiempo de inactividad, la reducción del esfuerzo de monitoreo y la mejora de la calidad de servicios y mantenimientos [14].

Para el presente proyecto se realizó un análisis de las herramientas de código abierto por el motivo que no se disponía de un presupuesto asignado para el monitoreo de la infraestructura de TI. Además, se utilizó la página oficial de Gartner, una de las empresas consultoras y de investigación de TI más importantes a nivel mundial. Esta empresa se dedica al análisis e investigación de las tendencias tecnológicas del mercado mundial [15].

Gartner indica que las herramientas de monitoreo son las encargadas de capturar el estado y la utilización de recursos de los componentes de la infraestructura de TI sin importar dónde residan, por ejemplo en un centro de datos, infraestructura como servicio (IaaS) o plataforma como servicio (PaaS). Esto permite al personal de TI monitorear y recopilar las métricas de disponibilidad y utilización de recursos de entidades físicas y virtuales, incluidos servidores, contenedores, dispositivos de red, instancias de bases de datos, hipervisores y almacenamiento. En particular, estas herramientas recopilan datos en tiempo real y realizan análisis de datos históricos o tendencias de los elementos que monitorean [15].

Basado en el listado en su página web, se contó con herramientas propietarias y de código abierto, por lo cual se tomaron las 3 herramientas de código abierto mejor ranqueades en su página; las cuales son: Zabbix, Nagios XI y Pandora FMS. A continuación, se detalla un análisis de cada una de estas herramientas [16].

1.6.1 ZABBIX

Zabbix es una solución de monitoreo distribuido de código abierto de clase empresarial. Es un software que monitorea numerosos parámetros de una red y la salud e integridad de servidores, máquinas virtuales, aplicaciones, servicios, bases de datos, sitios web, la nube y más. Permite a los usuarios configurar diferentes tipos de alertas a través de un mecanismo flexible basado en correo electrónico para cualquier evento reportado. Esto permite una reacción rápida a los problemas del servidor. Además, ofrece excelentes funciones de generación de informes y visualización de datos basadas en los datos almacenados. Esto hace que Zabbix sea ideal para la planificación de la capacidad de crecimiento de dispositivos y puede desempeñar un papel importante en la supervisión de la infraestructura de TI. Esto es aplicable para organizaciones pequeñas con pocos servidores y para grandes empresas con muchos servidores. Está escrito y

distribuido bajo la licencia al público general (GPL). Significa que su código fuente se distribuye libremente y está disponible para el público en general [17]. Las características son:

Recopilación de datos

- Comprobaciones de disponibilidad y rendimiento
- Soporte para VMware, snmp, jmx e icmp
- Comprobaciones personalizadas
- Recopilación de datos deseados a intervalos personalizados

Definiciones de umbral flexibles

- Puede definir umbrales de problemas muy flexibles, denominados desencadenadores, que hacen referencia a valores de la base de datos.

Alertas altamente configurables

- El envío de notificaciones se puede personalizar para el programa de escalamiento, el destinatario y el tipo de medio.
- Las acciones automáticas incluyen comandos remotos

Gráficos en tiempo real

- Los elementos supervisados se grafican inmediatamente mediante la funcionalidad de gráfico integrada

Capacidades de monitoreo web

- Comprueba la funcionalidad y tiempo de repuesta a través de la simulación de la ruta de clics de un ratón

Almacenamiento de datos históricos

- Datos almacenados en una base de datos
- Historial configurable
- Procedimiento de limpieza incorporado

Detección de redes

- Detección automática de dispositivos de red
- Auto registro del agente
- Descubrimiento de sistemas de archivos e interfaces de red

Interfaz web rápida

- Frontend basado en web en PHP
- Accesible desde cualquier lugar

- Tiene registros de auditoría

Agente con todas las funciones y fácilmente extensible

- Desplegado en objetivos de supervisión
- Puede ser implementar tanto en Linux como en Windows

1.6.2 PANDORA FMS

Pandora FMS es un software de monitorización que recoge los datos de cualquier sistema, genera alertas en base a esos datos y muestra gráficos, informes y mapas de nuestro entorno. Tendremos la posibilidad de monitorizar sistemas, servidores, aplicaciones, redes, eventos y una larga lista de dispositivos. Pandora FMS recoge la información que queremos monitorizar, la recopila y la guarda para representarla visualmente, con el objetivo de realizar acciones que requieran nuestros sistemas. Esta herramienta puede correr en distintos sistemas operativos, entre ellos Windows y Linux, siendo este último el sistema operativo recomendado.

La consola de Pandora FMS permite administrar y operar con la herramienta a diferentes usuarios con distintos perfiles. Con esta herramienta web podemos controlar el estado de la monitorización actual, ver información estadística mediante gráficas o informes y controlar las incidencias generadas por la monitorización [18]. Las características son:

- Detección automática de la topología de red y autodescubrimiento.
- Supervisión de errores y advertencias
- Agentes multiplataforma para Windows, HP-UX, Solaris, BSD, AIX y Linux.
- Monitorización de disponibilidad y rendimiento.
- Consola visual personalizable.
- Agentes para Android y dispositivos empotrados.
- Monitoreo de red en diferentes protocolos SNMP, WMI, TCP, ICMP, Ipv4 e Iv6.
- Monitorización de servicios en red interna
- Niveles de acceso personalizados con interfaz web
- Monitorización personalizada en mapas de topología
- Conexión SSH/Telent a dispositivos desde el interfaz web.
- SLA y Elaboración de Informes, con ITIL v3 métricas.

1.6.3 NAGIOS

Nagios XI es una aplicación de monitoreo de infraestructura de TI completa y fácil de usar capaz de monitorear sus servidores críticos, equipos de red, servicios y aplicaciones y notificarle cuando ocurren problemas. Es capaz de monitorear cientos de diferentes tipos de aplicaciones, servicios, protocolos y hardware informático mediante el uso de capacidades integradas y extensiones y complementos de terceros [19]. Sus características son:

- Motor de monitoreo Nagios Core 4, proporciona a los usuarios una supervisión eficiente y escalable.
- Panel de control, proporciona una descripción general de alto nivel personalizable de hosts, servicios y dispositivos de red.
- Los administradores pueden ver fácilmente los incidentes de la red y resolverlos antes de que se transformen en grandes desastres.
- Los gráficos automatizados e integrados de tendencias y capacidad permiten a las organizaciones planificar actualizaciones.
- Guarda sus configuraciones más recientes. Así podrá archivar y revertir cambios cuando lo desee, evitando perder la configuración actual.
- Configura y administre fácilmente cuentas de usuario con solo unos pocos clics y luego asigne roles personalizados para garantizar un entorno seguro.

1.7 METODOLOGÍA PDCA

Para el desarrollo de este proyecto se utilizó la metodología PDCA. La metodología mencionada sirvió de guía para el análisis, implementación, comprobación y optimización de la calidad del proceso de monitoreo de la infraestructura de TI de la empresa POFASA; para que el mecanismo de monitoreo se mantenga en su lugar y consistente con los objetivos de la empresa, considerando que los servicios tecnológicos están respaldando operativamente al Core de la empresa. Con el fin de orientar al administrador de la red, en la ejecución de un proceso de monitoreo ordenado y constante, asegurando el correcto uso de los recursos disponibles de la red. El desarrollo del proyecto constó de las siguientes fases:

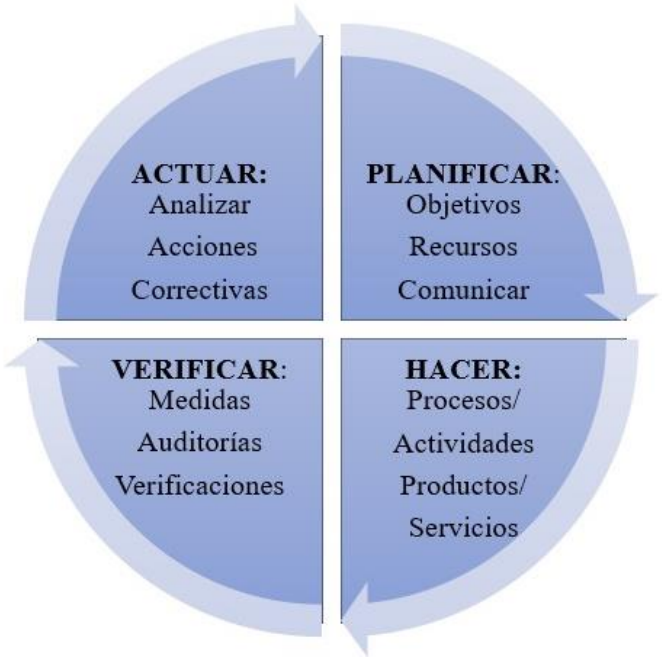


Figura 5. Fases del ciclo de vida de la Metodología PDCA

La fase de planificar se describe con el proceso de análisis de los objetivos, la importancia y el nivel de criticidad con la infraestructura de TI, que ayudan a cumplir labores esenciales dentro y fuera de la empresa. Esta infraestructura se desglosa en los siguientes componentes: dispositivos y servicios críticos de TI. Además de identificar el mecanismo actual de monitoreo utilizado, el cual debe estar correlacionado con los objetivos principales de la empresa. Este análisis se lo debe realizar periódicamente por los cambios que pueden existir en la infraestructura de TI. En dicha fase, se utilizan encuestas detalladas para recopilar datos sobre el estado actual del monitoreo de la infraestructura de TI, los datos obtenidos se registran y tabulan para generar gráficos entendibles para el usuario.

La fase de hacer consiste en la implementación de un sistema de monitoreo de la infraestructura de TI de acuerdo con los objetivos establecidos en la fase anterior. Además, se realiza un análisis de las características de los distintos sistemas de monitoreo de código abierto, con el fin de seleccionar un sistema que se adapte a los objetivos de la empresa. A continuación, se instalan y configuran los servicios de monitoreo; se generan las alertas correspondientes en sus servicios críticos.

La fase de verificar, en esta fase se comprobó que la implementación del sistema ha sido efectiva, de acuerdo con las expectativas establecidas en la fase de análisis. Cada alteración

detectada se documenta para que pueda tratarse en la fase de optimización o proponerse a la siguiente iteración del ciclo.

La fase de actuar, en esta fase se analizarán y gestionarán las desviaciones detectadas en la fase anterior de la siguiente manera:

- Aceptación: la implementación fue un éxito; no existe errores en las conexiones de red y alarmas implementadas para la infraestructura de TI. Además de cumplir con los objetivos planteados por la empresa.
- Evasión: no se realiza el proceso o implementación que generó la inconformidad en el análisis final. Todo esto queda documentado para que posteriormente la empresa genere un nuevo ciclo para las correcciones necesarias.

La ejecución de las cuatro fases mencionadas se llevó a cabo con el objetivo de incorporar mejoras y actualizaciones al proceso de monitoreo de infraestructura de TI, manteniéndolo actualizado y optimo en el tiempo y con ellos, lograr un estándar alto de disponibilidad en los dispositivos y servicios de la infraestructura de TI.

Para la evaluación del sistema implementado, se realizaron pruebas de carga en la red con el objetivo de medir el rendimiento en el servidor asignado por la empresa POFASA. Estas pruebas van a ser a nivel de CPU, memoria, ancho de banda, SNMP, ICMP y WMI. Además, se constató con un Check List, el cumplimiento de los objetivos establecidos por la empresa referente a los dispositivos y servicios críticos que tienen dentro de su infraestructura; realizando la desconexión involuntaria y provocando pérdida de disponibilidad en cada servicio critico dentro de las diferentes sucursales que tiene la empresa.

2 METODOLOGÍA

2.1 FASE DE PLANIFICAR

La importancia de la infraestructura de TI se mencionó en el capítulo anterior, los cuales son relevantes porque permiten a los usuarios de la empresa el cumplimiento de sus labores cotidianas y el alcance de sus objetivos. La infraestructura está compuesta de dispositivos de hardware y software. Además, la infraestructura critica de TI que es importante para el propósito de este proyecto se clasifica en dos niveles. En el primer nivel, encontramos los servicios y dispositivos que proveen comunicación y acceso al personal de la empresa. En cambio, en el segundo nivel encontramos los servicios críticos de TI, que son la base de los procesos de la empresa; estos servicios son dependientes de los dispositivos del primer nivel en su operación para garantizar su funcionamiento y disponibilidad. Los servicios críticos que presenta la empresa POFASA son: correo electrónico, antivirus, dominio, DHCP, internet corporativo e impresión.

Con el propósito de implementar el sistema de monitoreo en este trabajo de titulación, se han identificado y descrito los siguientes objetivos de la empresa POFASA:

- Identificar la infraestructura critica que debe ser monitorizada en base a los procesos que maneja la empresa como su prioridad.
- Establecer las responsabilidades del personal a cargo de los dispositivos y servicios, eliminando la duplicidad de funciones e incertidumbre sobre el estado de la infraestructura.
- Mantener la disponibilidad e integridad de los servicios utilizados por el personal que labora en la empresa.
- Establecer notificaciones en diferentes plataformas para los dispositivos de la infraestructura de TI.

2.1.1 SERVICIOS CRÍTICOS EN LA INFRAESTRUCTURA DE TI

Esta fase del análisis es responsable de identificar los servicios críticos, donde se incluyen los servicios comunes de la infraestructura de TI que maneja la empresa POFASA. Los servicios comunes son:

- Correo electrónico: Microsoft Office 365 en la nube.
- Impresión: Servicio Ricoh en red.

- Internet: Servicio de fibra óptica de Punto Net

Los servicios críticos son los siguientes:

- Base de Datos: MySql versión 5.6
- Servicio de DHCP: Windows Server 2016
- Dominio activo (Active Directory): Windows Server 2016
- Antivirus: Servicio Eset Endpoint Security

Todos estos servicios están relacionados con los objetivos establecidos por el jefe del área de TI de la empresa POFASA. Además, la empresa no tiene acuerdos de niveles de servicio (SLA) por lo que no existe un monitoreo de la calidad de servicio que es entregado por parte de sus proveedores, por ejemplo, el servicio de internet por parte de su proveedor Punto Net. Esto es importante ya que se debe supervisar el cumplimiento de los acuerdos de servicio con todos los proveedores involucrados en la infraestructura de TI.

2.1.2 DISPOSITIVOS CRÍTICOS EN LA INFRAESTRUCTURA DE TI

De igual manera se identificaron los diferentes dispositivos de la infraestructura de TI, estos dispositivos son considerados críticos para los procesos que maneja la empresa POFASA. Estos dispositivos son:

- Firewall: Cada oficina y planta tiene 1 de marca Fortinet.
- Switch Core L3: Capa 3, marca Cisco que maneja 4 VLANs
- Switch o Hub L2: Capa 2, marca HP.
- Servidor DNS, DHCP: Servidor virtualizado con Windows Server 2016.
- Servidor de Base de Datos: Servidor virtualizado con Ubuntu Server.
- Servidor NAS: Servidor de respaldo de información, marca Wester Digital.

Los dispositivos de TI se encuentran creciendo exponencialmente conforme avanza el tiempo, por este motivo la herramienta seleccionada debe tener compatibilidad con los protocolos de comunicación creados o estandarizados por los fabricantes de los diferentes dispositivos, con el objetivo de tener una consola general para el correcto monitoreo.

2.1.3 PARÁMETROS CRÍTICOS

Los parámetros críticos utilizados fueron tomados de la tabla 1 y se adaptaron a cada dispositivo y servicio de la infraestructura de TI. A continuación, se describe el dispositivo y parámetro monitoreado en base a la plantilla establecida por el sistema de monitoreo seleccionado.

- Firewall: Fortigate 60D y 60E

Parámetros	**Descripción**
Sistema	Uso de procesador
	Uso del almacenamiento (disco duro)
	Uso de memoria RAM
Red	Disponibilidad de las interfaces
	Uso de interfaces de red

Tabla 2. Parámetros monitoreo de Firewall

- Switch: HP J9623A - CISCO CATALYST 2960

Parámetros	**Descripción**
Sistema	Uso de procesador
	Uso de memoria RAM
Entorno	Temperatura
	Estado del suministro de energía
Red	Disponibilidad de las interfaces
	Uso de interfaces de red

Tabla 3. Parámetros monitoreo de Switch

- Servidor Windows: Windows Server 2016 - 2012 y Windows 10 Pro

Parámetros	**Descripción**
Sistema	Uso de procesador
	Uso del almacenamiento (disco duro)
	Uso de memoria RAM
Entorno	Temperatura
	Estado del suministro de energía
Red	Uso de interfaces de red

	Tiempo de respuesta

Tabla 4. Parámetros monitoreo de Servidor Windows

- Servidor Linux: Ubuntu Server, CentOS, UNIX Wester Digital

Parámetros	**Descripción**
Sistema	Uso de procesador
	Uso del almacenamiento (disco duro)
	Uso de memoria RAM
Entorno	Temperatura
	Estado del suministro de energía
Red	Uso de interfaces de red
	Tiempo de respuesta

Tabla 5. Parámetros monitoreo de Servidor Linux

- Servidor Base de Datos: MySql v 5.7

Parámetros	**Descripción**
Entorno	Operaciones
	Uso de memoria

Tabla 6. Parámetros monitoreo de base de datos MySql

Los incidentes generados en base a los parámetros críticos mostrados se clasificarán por su gravedad. Tendremos de tipo informativo, advertencia, nivel alto y desastre. El nivel de sensibilidad de estos parámetros críticos lo marca cada fabricante en sus consolas de administración.

2.1.4 MECANISMO ACTUAL DE MONITOREO

Se utilizaron encuestas y cuestionarios estructurados para definir los mecanismos e indicadores del monitoreo manual utilizado, con el objetivo de medir el impacto de implementar un sistema de monitoreo automatizado de la infraestructura de TI para gestionar incidentes en la Local Area Network (LAN) de la empresa POFASA. Las encuestas fueron realizadas al personal a cargo de servicios o dispositivos a pesar de no ser parte del área de TI; obteniendo los siguientes resultados:

- **Tiempo de Respuesta**

  ¿Cuál es el tiempo promedio de atención de incidentes de infraestructura TI?

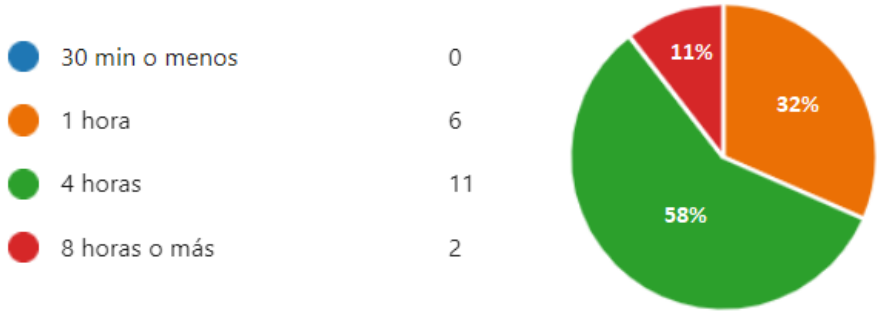


Figura 6. Resultados de encuesta pregunta 1

EL gráfico muestra que un 58% de los encuestados indican que el tiempo promedio de atención es de 4 horas y solo el 11% indica que es 8 horas o más. Si sumamos las dos respuestas, tenemos un índice del 69% que afirma que el servicio tarda más de 4 horas frente al 32% que indica que es 1 hora.

- **Exactitud al encontrar el incidente**

  ¿Cuánto tiempo lleva en promedio identificar el dispositivo o servicio de TI que está causando el incidente?

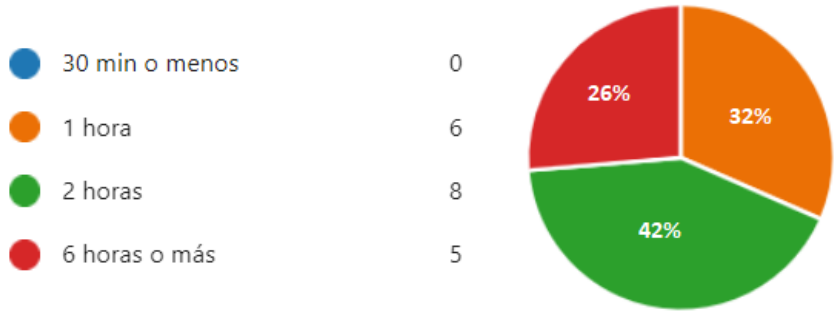


Figura 7. Resultados de encuesta pregunta 2

EL gráfico muestra que un 42% de los encuestados indican que el tiempo que se tarda en identificar el dispositivo o servicio de TI es 2 horas y un 26% indica que es 6 horas o más. Sumando estos dos resultados obtenemos un 68% que afirma que el tiempo promedio es sobre las 2 horas frente al 32% que dice que es 1 hora o menos.

- **Satisfacción del usuario**

  ¿Cómo calificaría el método actual para monitorear la infraestructura de TI de la empresa?

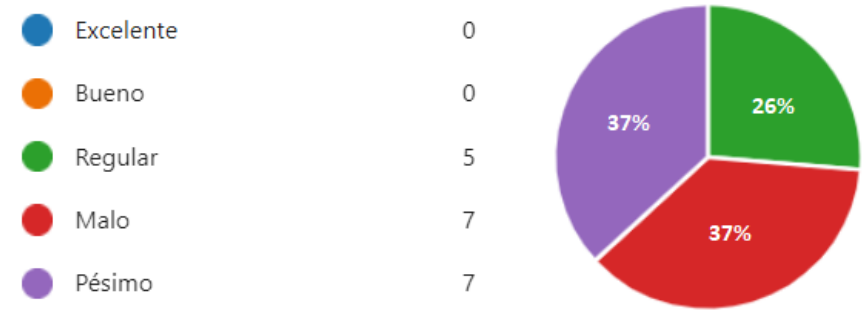


Figura 8. Resultados de encuesta pregunta 3

El gráfico muestra que un 37% de los encuestados indican que el método actual de monitoreo es pésimo y un 37% indica que es malo. Si sumamos estos dos resultados obtenemos un 74% que no está conforme con el método actual de monitoreo frente al 26% que piensa que el método es regular.

- **Integridad**

  ¿Confía en el método actual para monitorear la infraestructura de TI de la empresa?

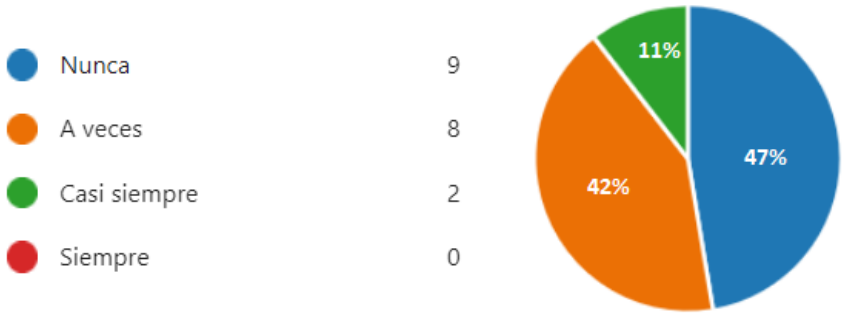


Figura 9. Resultados de encuesta pregunta 4

El gráfico muestra que un 47% de los encuestados indican que nunca confían en el sistema actual de monitoreo y un 42% indica que solo confían a veces. Si sumamos estos dos resultados obtenemos un 89% que no confían en el método actual de monitoreo frente al 11% que indican que casi siempre confían.

- **Calidad de Servicio**

  ¿Cuántas quejas se realizan cada semana sobre disponibilidad del servicio y mal funcionamiento de los dispositivos en la red?

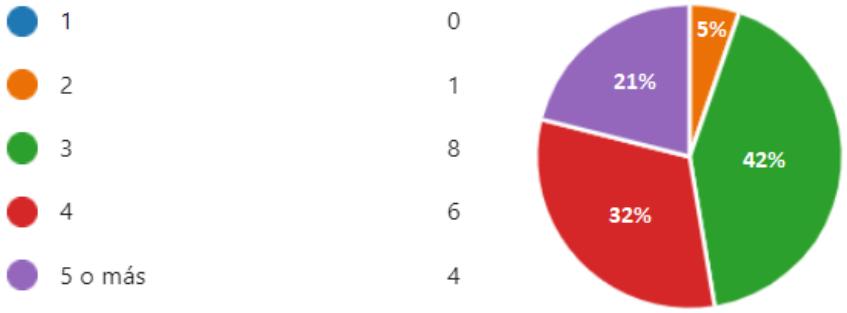


Figura 10. Resultados de encuesta pregunta 5

El gráfico muestra que un 42% de los encuestados indican que existen 3 quejas por semana sobre disponibilidad del servicio y un 32% indica que son 4 quejas de disponibilidad del servicio. Si sumamos estos 3 resultados obtenemos un 95% que afirma que existe más de 3 quejas de disponibilidad del servicio por semana frente al 5% que dice que solo son 2 quejas de disponibilidad.

Como podemos observar el promedio de aceptación por parte de los usuarios es bajo porque el monitoreo actual es de manera manual, es decir una persona está encargada debe revisar cada una de las consolas del fabricante con el objetivo de comprobar el estado actual cada dispositivo y servicio de la infraestructura. En el mayor de los casos los incidentes son reportados por los usuarios que utilizan el dispositivo o servicio, razón por la cual el tiempo de respuesta es relativamente alto.

2.2 FASE DE HACER

En esta fase se requirió analizar las principales herramientas de monitoreo de código abierto, las características fueron detalladas en el capítulo 1 del presente trabajo de titulación. A continuación, se presenta la comparación de las características necesarias por la empresa POFASA entre las 3 herramientas seleccionadas:

CARACTERÍSTICAS	ZABBIX	PANDORA	NAGIOS
Administración			
Centralizada	Si	Si	Si
Interfaz Web	Si	Si	Si
Monitoreo			
Tiempo Real	Si	Si	Si
Servidores	Si	Si	Si
Switch - Router	Si	Si	Si
SNMP-WMI	Si	Si	Si
Agentes externos	Si	Si	No
Monitoreo Base de Datos			
Oracle	Si	Si	Si
MySql	Si	Si	Si
SQL Server	Si	Si	Si
PostgreSQL	Si	Si	No
Instalación y Configuración			
Fácil configuración	No	Si	Si
Auto detección de dispositivos	Si	Si	No
Vista gráfica	Si	Si	Si
Notificaciones			
Visuales	Si	Si	Si
Sonoras	Si	No	Si
Correo Electrónico	Si	Si	Si
Ms Teams - Telegram	Si	No	No
Multiplataforma			
Linux	Si	Si	Si
Windows	Si	Si	Si
Otros	Si	Si	Si
Informes			
Logs de Usuario	Si	Si	Si
Estadísticas	Si	Si	Si
Mapa de red	Si	No	No

Tabla 7. Comparación de herramientas de monitoreo.

En base a las características y recomendaciones investigadas en los diferentes foros de internet, se seleccionó la herramienta ZABBIX, porque existe la suficiente documentación sobre su instalación y configuración, a pesar de tener una dificultad alta cuando no se maneja o se tiene conocimiento de la consola de Linux. Los requerimientos de hardware por parte de Zabbix son:

Tipo	Plataforma	CPU/Memoria	Base de Datos	Host Monitoreados
Pequeño	CentOS	Aplicación Virtual	MySql Inno DB	100
Mediano	CentOS	2 CPU / 2 GB	MySql Inno DB	500

Grande	RedHat E	4 CPU / 8 GB	RAID 10 MySql	>1000
Muy Grande	RedHat E	8 CPU / 16 GB	RAID 10 MySql	>10 000

Tabla 8. Ejemplos de configuración de hardware Zabbix.

La implementación fue realizada sobre una máquina virtual con sistema operativo Linux. La empresa POFASA cuenta con un servidor IBM virtualizado con capacidad de 2 TB de disco duro, 36 GB de RAM y un procesador Intel Xenón 2.10 GHz con 12 procesadores lógicos. El virtualizador ocupado es un VMware ESXi el cual es multiplataforma y de licencia pagada.

2.2.1 INSTALACIÓN

La configuración establecida para la máquina virtual donde se instaló el sistema de monitoreo fue la siguiente:

- SO: Linux distribución CentOS
- Almacenamiento: 100GB
- Memoria RAM: 4GB
- Números de CPU: 2

Estas son las características recomendadas por el fabricante para el correcto funcionamiento de la herramienta de monitoreo, no se tomó en cuenta las recomendaciones mínimas porque la empresa POFASA quería que el sistema de monitoreo se encuentre 100% operativo y no en una etapa de prototipo. Concluido el proceso de configuración e instalación de nuestro sistema operativo Linux, procedimos con la instalación del sistema a través de nuestra consola.

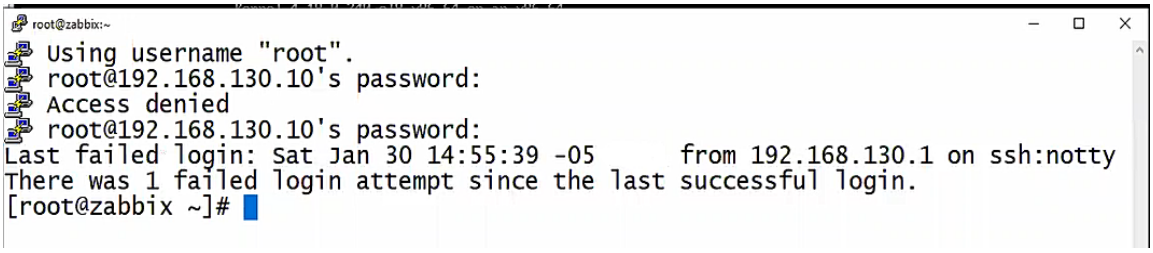


Figura 11. Consola Linux

- Procedimos con la instalación de los paquetes EPEL (paquetes adicionales para Linux empresarial), es un requerimiento por parte de ZABBIX para su funcionamiento.

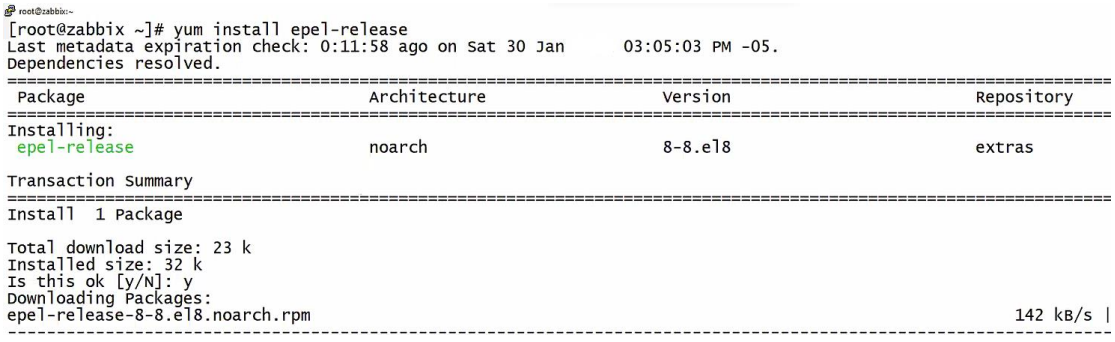


Figura 12. Instalación EPEL

- Instalación de repositorio ZABBIX.

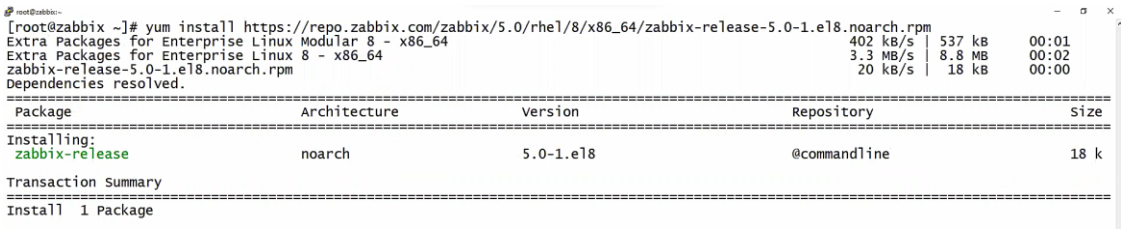


Figura 13. Instalación repositorio ZABBIX

- Instalación de herramientas de diagnóstico de red (telnet, tracert, ping).

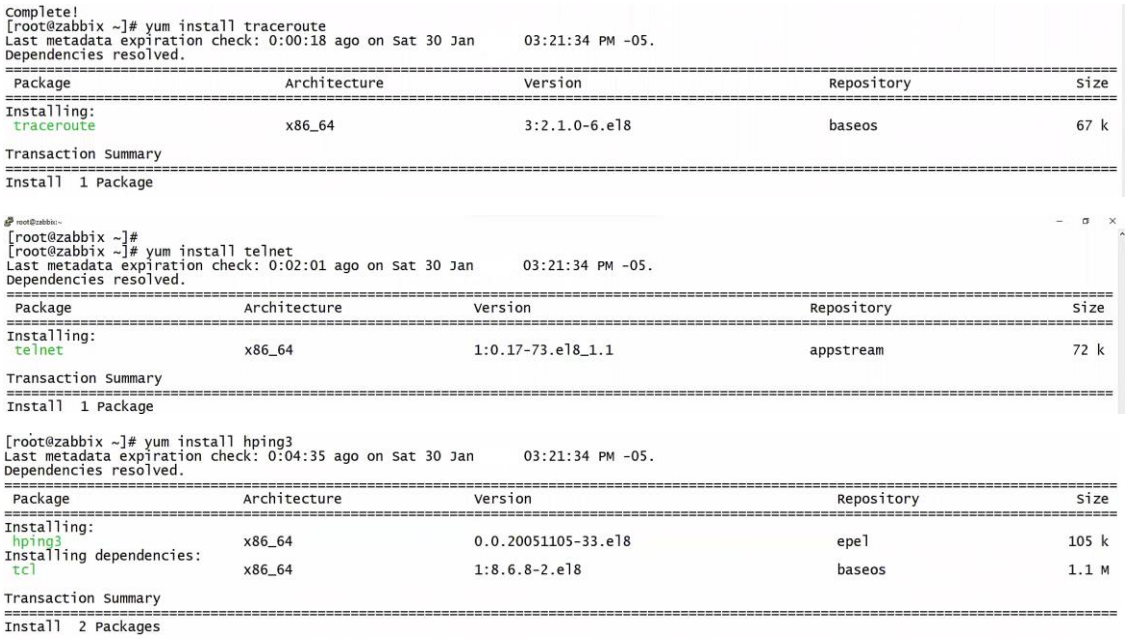


Figura 14. Instalación herramientas de diagnóstico de red.

- Instalación de una pila LAMP (Linux, Apache, MySql y PHP), la unión de estas herramientas permitió ejecutar aplicaciones web de alto rendimiento y de código abierto.

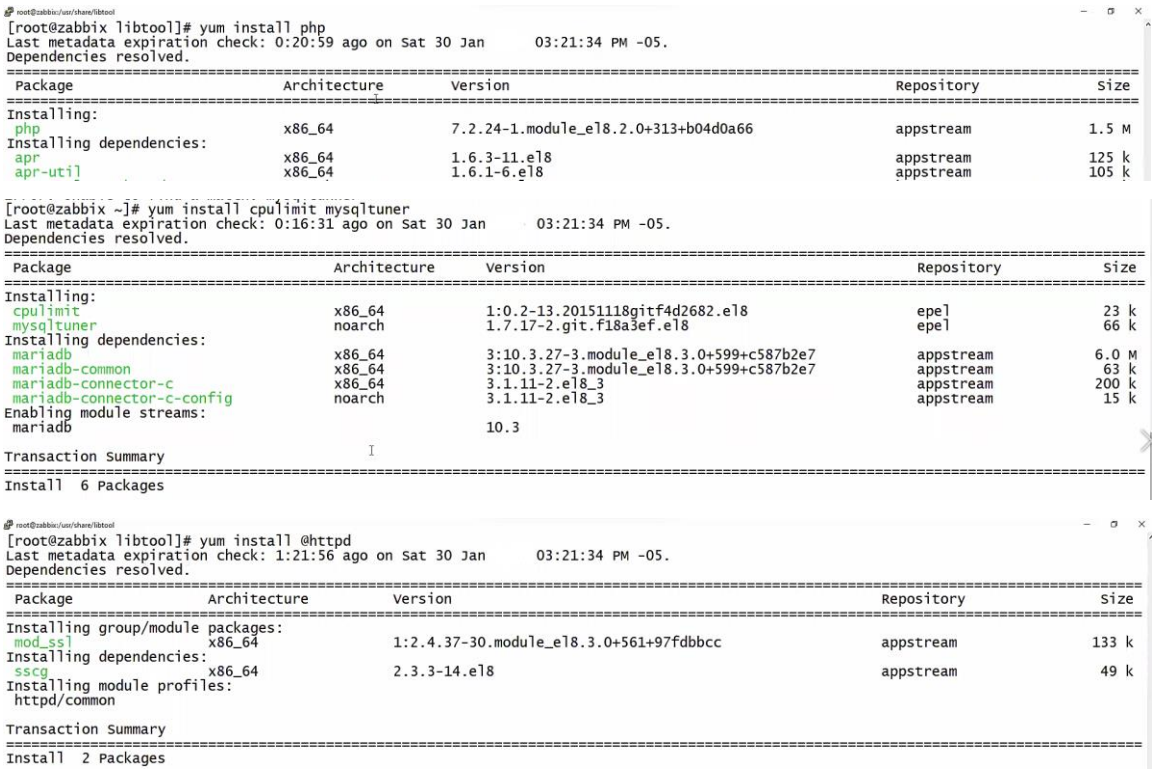


Figura 15. Instalación pila LAMP

- Comprobación de estado del servicio HTTPD Apache (servidor web).

Figura 16. Comprobación estado de servicio Web

- Concluida la instalación de requisitos previos se procedió con la instalación del agente ZABBIX.

```
Complete!
[root@zabbix libtool]# yum install zabbix-agent
Last metadata expiration check: 1:33:47 ago on Sat 30 Jan      03:21:34 PM -05.
Dependencies resolved.
================================================================================================================================
 Package                          Architecture              Version                        Repository                    Size
================================================================================================================================
Installing:
 zabbix-agent                     x86_64                    5.0.8-1.el8                    zabbix                       466 k

Transaction Summary
================================================================================================================================
Install  1 Package
```

Figura 17. Instalación agente ZABBIX

- Importación esquema de base de datos de ZABBIX

```
[root@zabbix libtool]# zcat /usr/share/doc/zabbix-server-mysql/create.sql.gz | mysql -uroot -p zabbix
Enter password:
[root@zabbix libtool]# mysql -uroot -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 21
Server version: 10.3.27-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)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| zabbix             |
+--------------------+
4 rows in set (0.001 sec)
```

Figura 18. Esquema de base de datos ZABBIX

- Se comprobó el funcionamiento de la herramienta, ingresando la dirección IP de la máquina virtual.

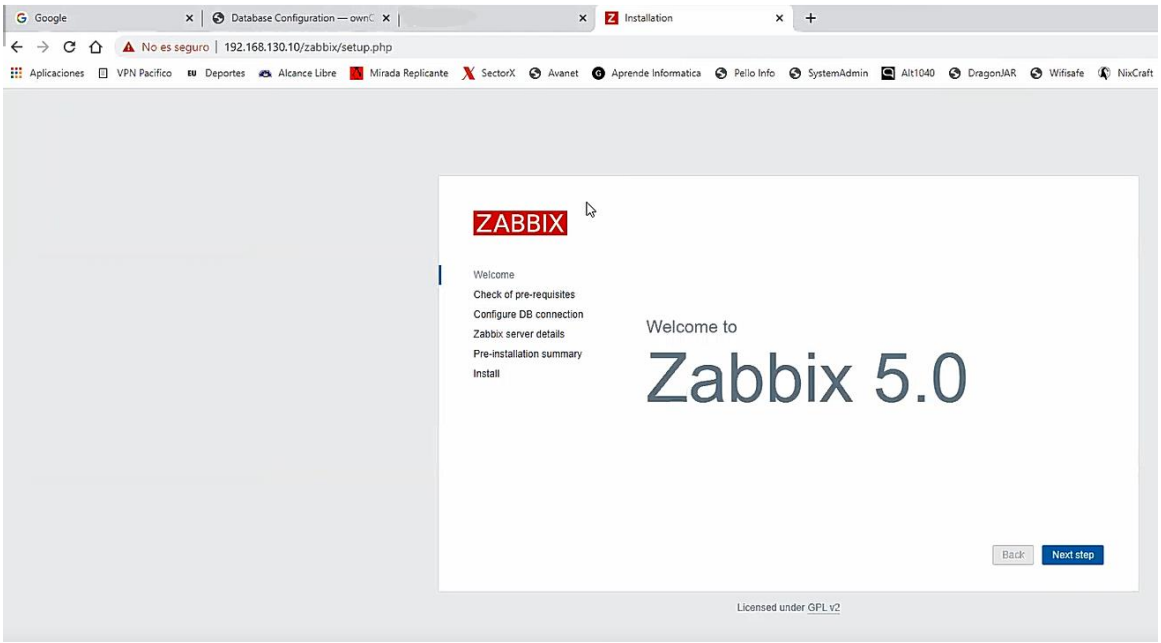


Figura 19. Inicio de consola Web

- Comprobación de requisitos previos por parte de interfaz web.

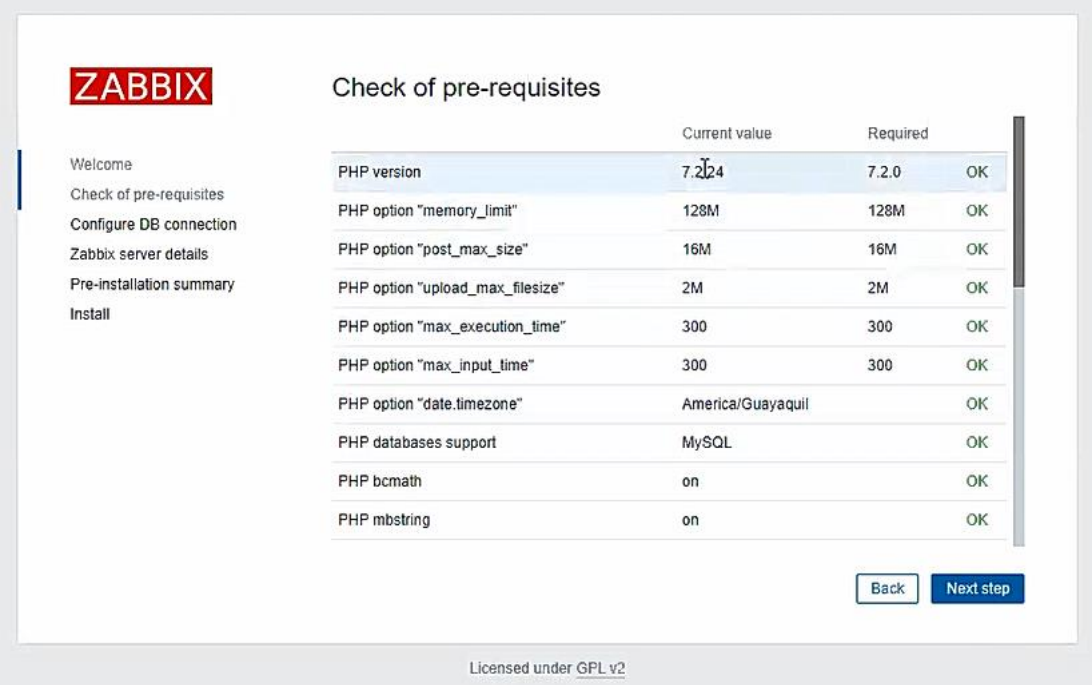


Figura 20. Requisitos previos en interfaz Web

- Conexión con base de datos local en el servidor, ingreso de credenciales.

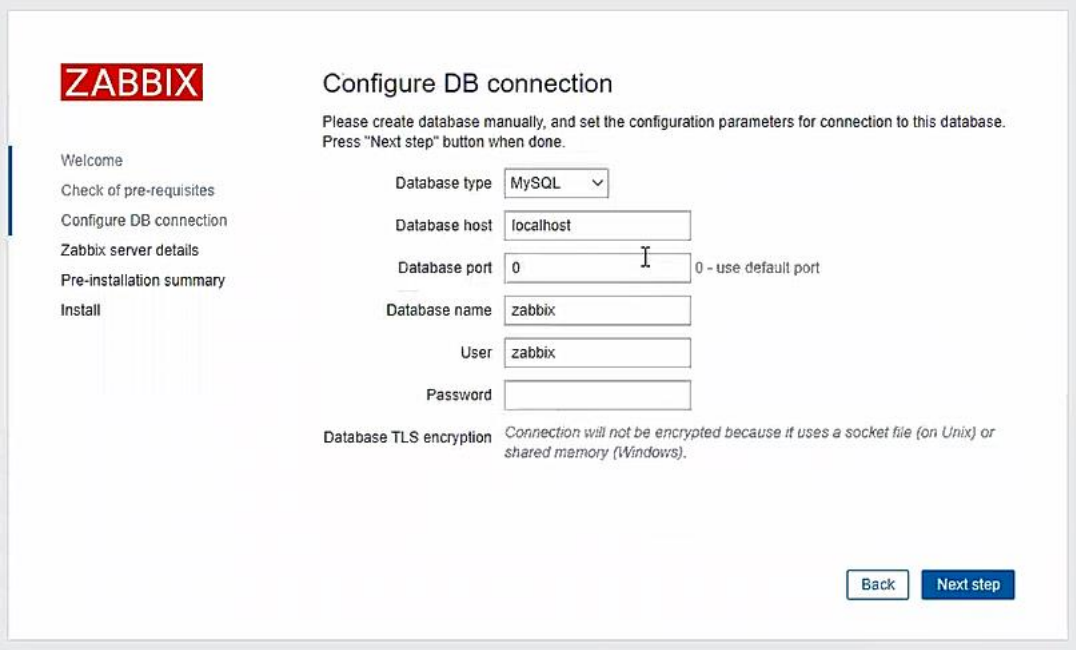


Figura 21. Configuración base de datos ZABBIX

- Resumen de configuración, se debe tener en cuenta el puerto asignado.

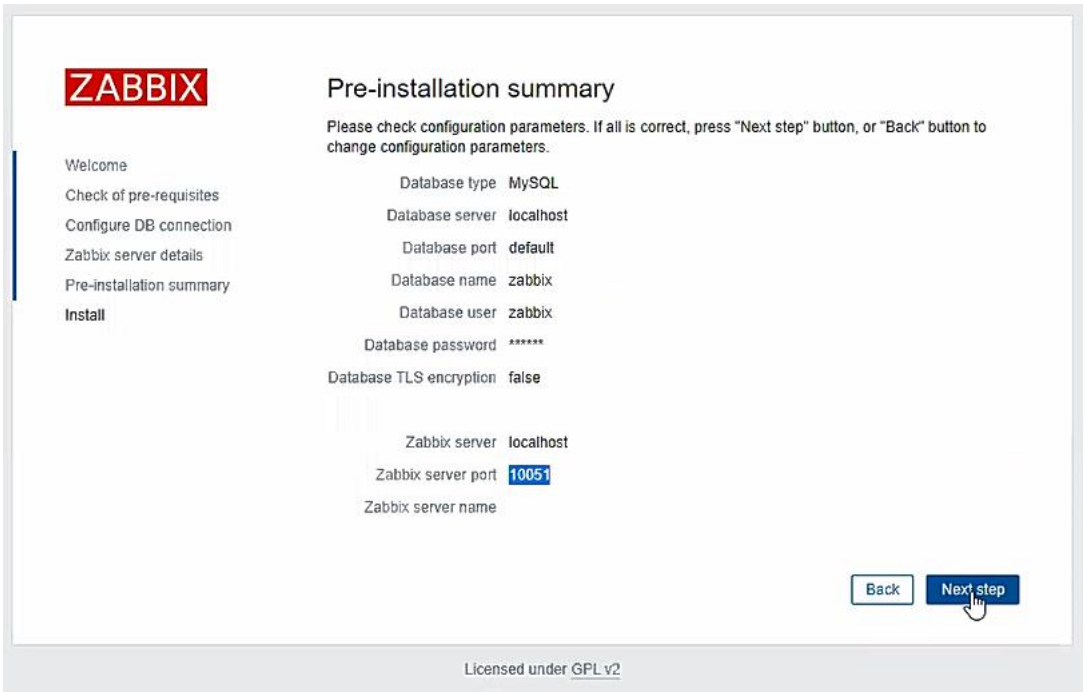


Figura 22. Resumen de configuración.

- Ingreso de credenciales para inicio de sesión, por defecto el usuario es Admin y la clave zabbix.

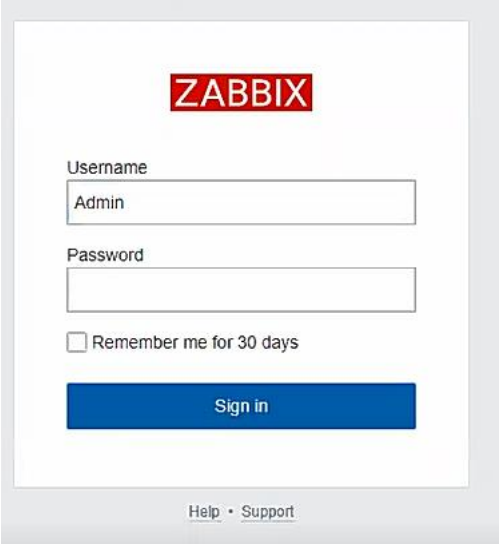


Figura 23. Log in ZABBIX

- Concluida instalación, se muestra el tablero de control del sistema ZABBIX.

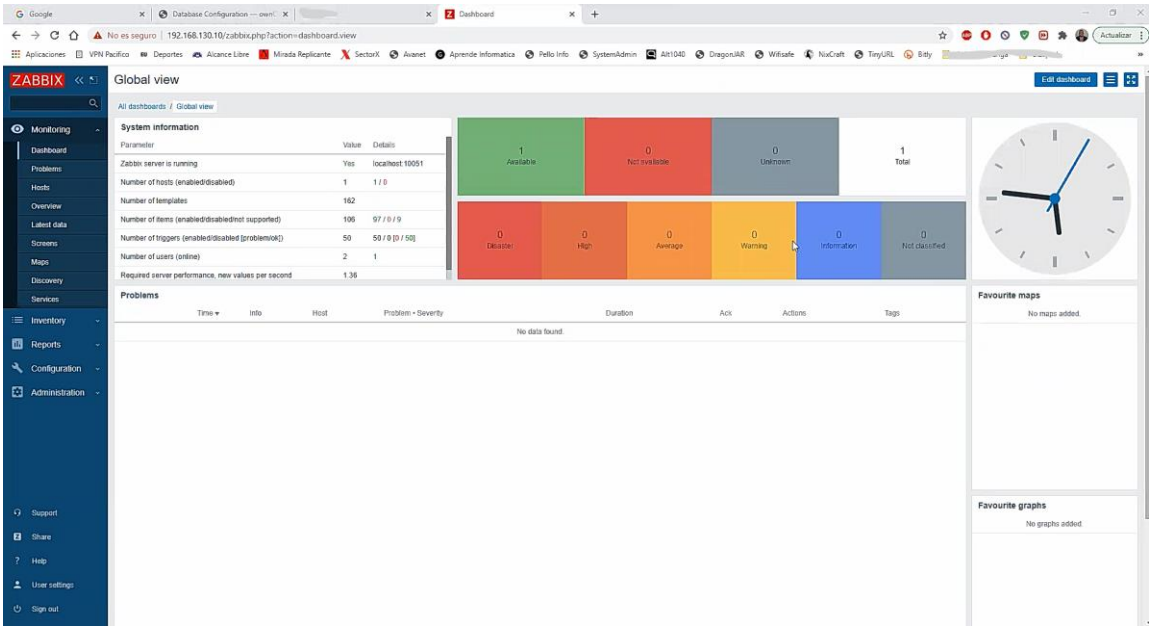


Figura 24. Dashboard ZABBIX

2.2.2 CONFIGURACIÓN

La infraestructura de TI que fue monitoreada se muestra en la siguiente tabla:

Nombre	**IP**	**Descripción**
Firewall	192.168.135.5	Correspondiente a oficina de Administración, responsable de red interna de la empresa.
Firewall	192.168.136.28	Corresponde a oficina de Granjas, responsable de DHCP.
Firewall	192.168.138.11	Corresponde a oficina de Nutrición, responsable de DHCP.
Firewall	192.168.139.11	Corresponde a oficina de Cárnicos, responsable de DHCP.
Switch Core	192.168.135.10	Responsable de administrar VLANs
Switch	192.168.135.11	Hub encargado de realizar la conexión de todos los dispositivos dentro de la red.
Servicio de impresión	192.168.135.107	Impresora en red marca RICOH
Servidor Active Directory	172.16.135.100	Servidor virtual con sistema operativo Windows Server.

Servicio DNS	172.16.135.100	Servidor virtual con sistema operativo Windows Server.
Servicio DHCP	172.16.135.100	Servidor virtual con sistema operativo Windows Server.
Servidor Antivirus	172.16.135.115	Servidor virtual con agente de seguridad en Linux.
Servicio de Respaldo	192.168.135.21	Servidor Linux, configurado con un sistema de almacenamiento en red.

Tabla 9. Dispositivos monitoreados

- Creación de grupos, se creó como primer paso. Estos nombres ayudan a identificar y agrupar los dispositivos.

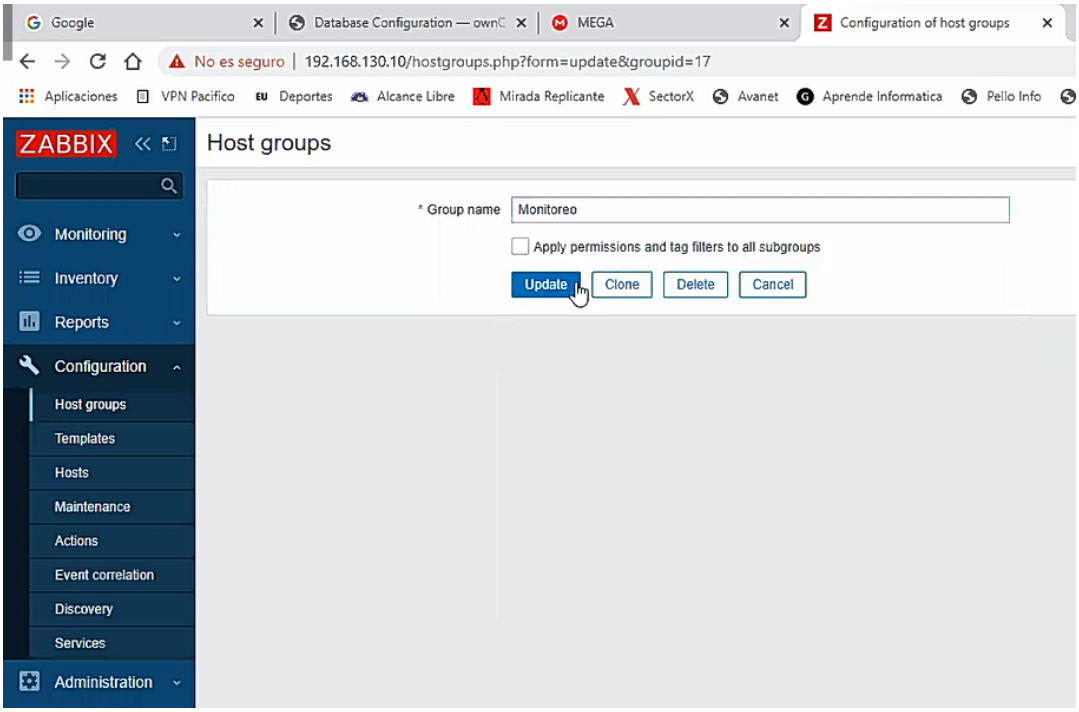


Figura 25. Creación de un nuevo grupo host

- Creación de plantillas, las plantillas tienen como objetivo ser un agente para el tipo de conexión. En este caso se creó una para el sistema operativo Windows.

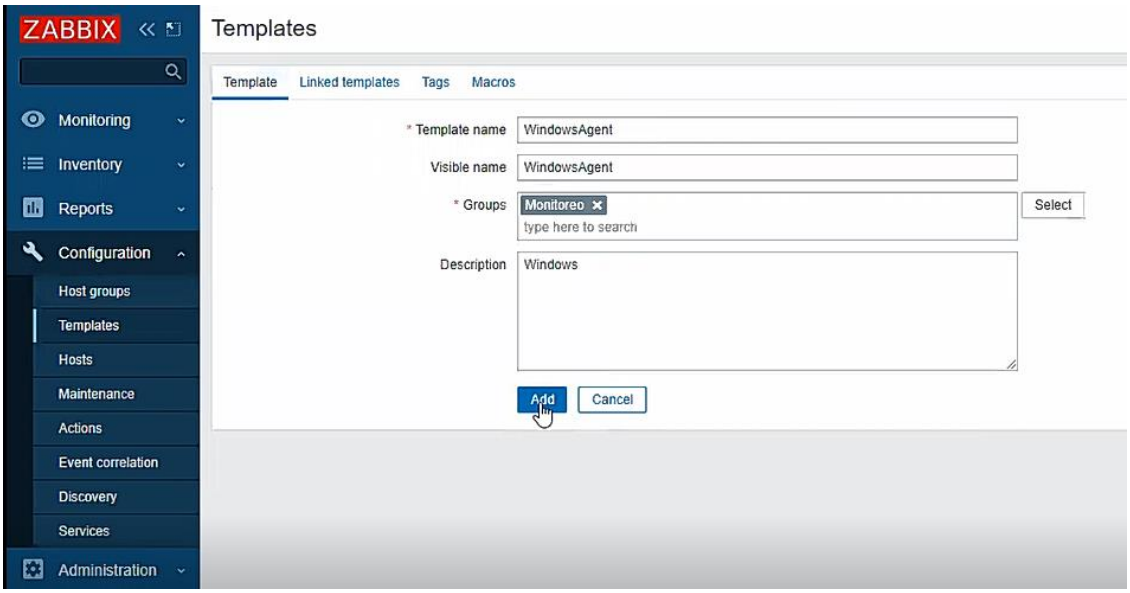


Figura 26. Creación de una nueva plantilla

Es muy importante añadir al grupo que se creó en el paso anterior, con el objetivo de tener agrupado nuestras plantillas y hosts.

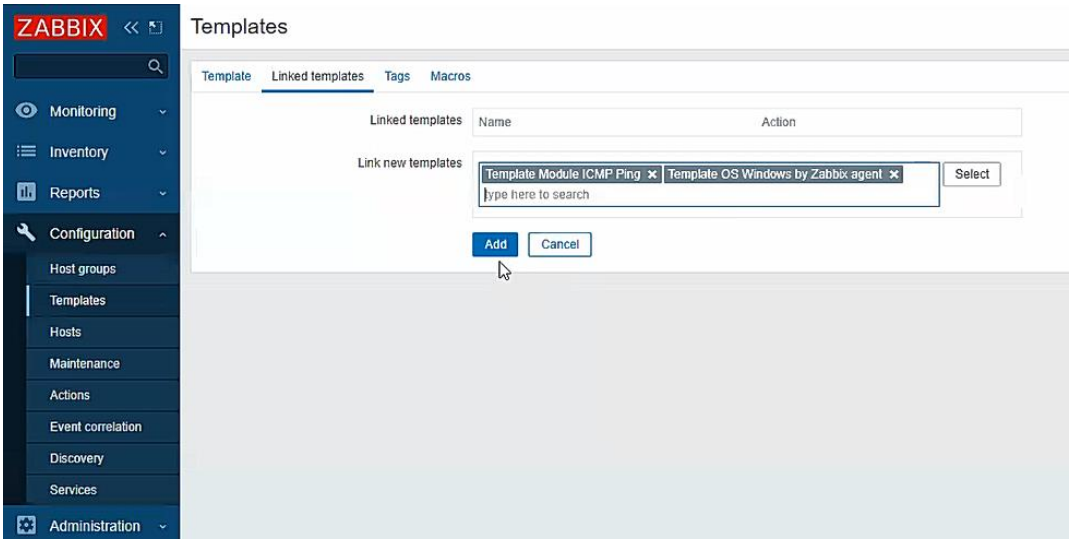


Figura 27. Selección de tipos de protocolos con sus plantillas

En la pestaña de “Linked” se añadió plantillas ya establecidas que son agentes configurados por defecto en el sistema. En este caso se quería saber el estado de un sistema operativo añadimos el protocolo ICMP que envía un ping y establece nuestra primera alerta de disponibilidad. También, se añadió la plantilla de zabbix agent. Esta plantilla muestra los parámetros críticos del dispositivo o sistema, como son: memoria RAM, estado de temperatura, uso del disco y tiempo de respuesta.

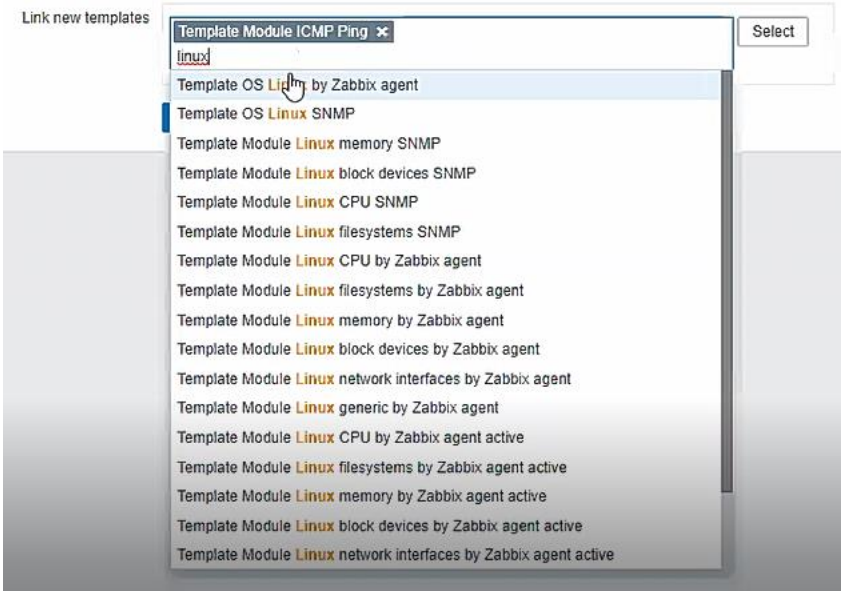


Figura 28. Ejemplo de plantillas Linux

Como se observó en la imagen anterior, Zabbix tiene una gran cantidad de plantillas dependiendo de las necesidades o el tipo de monitoreo que se va a realizar. Esto es una ventaja ya que podemos buscar solo por el nombre del fabricante y la plantilla con su agente está disponible para su selección.

- En el lado de nuestro host, se configuró la conexión de nuestro agente. En este caso se realizó con un dispositivo firewall.

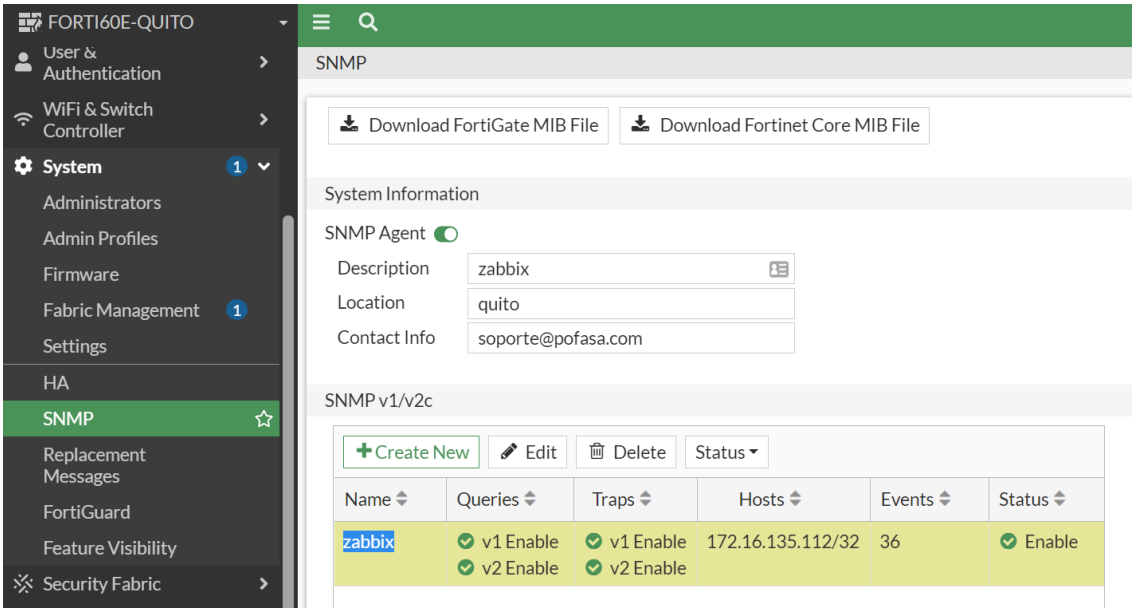


Figura 29. Configuración host

Trap Community: la cadena de comunidad se estableció en nuestro agente zabbix y en la configuración de SNMP de nuestro host.

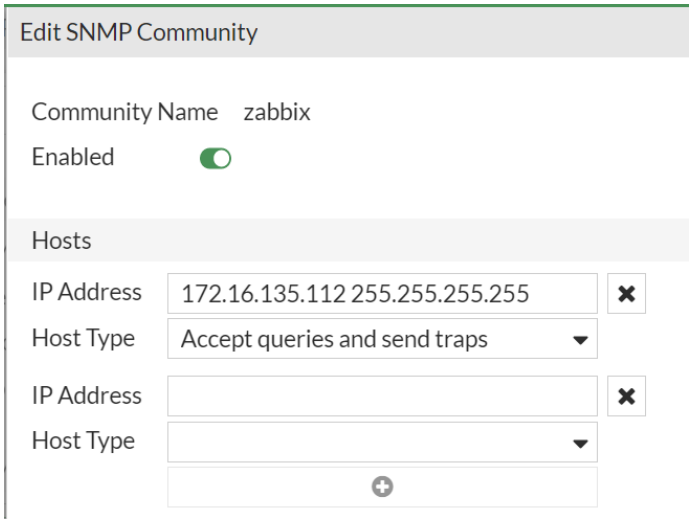


Figura 30. Configuración de comunidad SNMP

- Añadir un nuevo host a Zabbix. Se muestra la creación para el caso anterior del firewall.

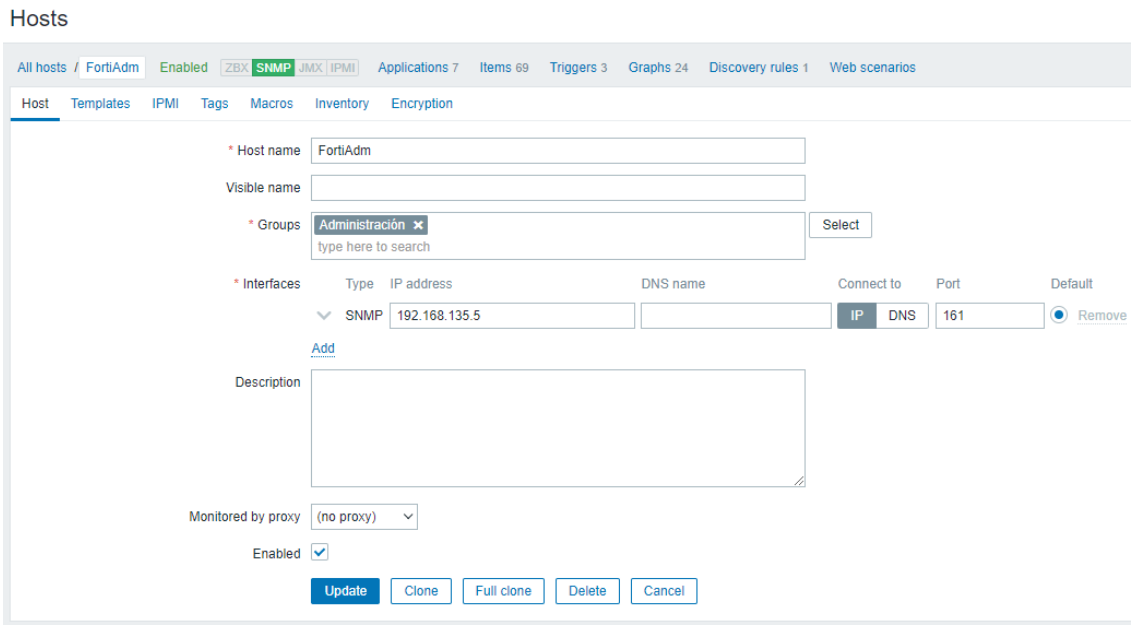


Figura 31. Configuración de host en ZABBIX

Host name: se ingresa el nombre de nuestro nuevo host.

Groups: se añade nuestro grupo creado en pasos anteriores.

Interfaces: se añade la dirección IP de nuestro host, por defecto el puerto se asigna automáticamente, pero si en el host cambiamos el puerto de comunicación SNMP se debe actualizar en nuestra consola ZABBIX.

SNMP versión: en nuestro caso de estudio se escogió la versión 2 ya que el fabricante recomienda trabajar con dicha versión.

- Configuración pestaña Macros, se procedió a ingresar la palabra zabbix en el campo "value" con el objetivo de tener una misma comunidad entre nuestro host y el agente zabbix.

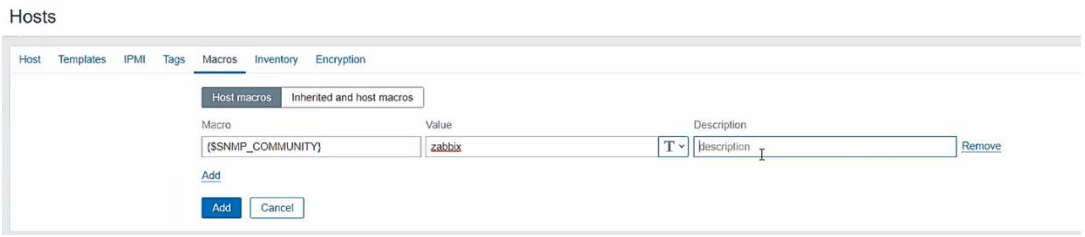


Figura 32. Configuración de pestaña Macros para comunidad

- Resultado en el centro de control de Zabbix, se pudo observar que no se muestra algún error en la consola por lo que el dispositivo fue añadido con existo.

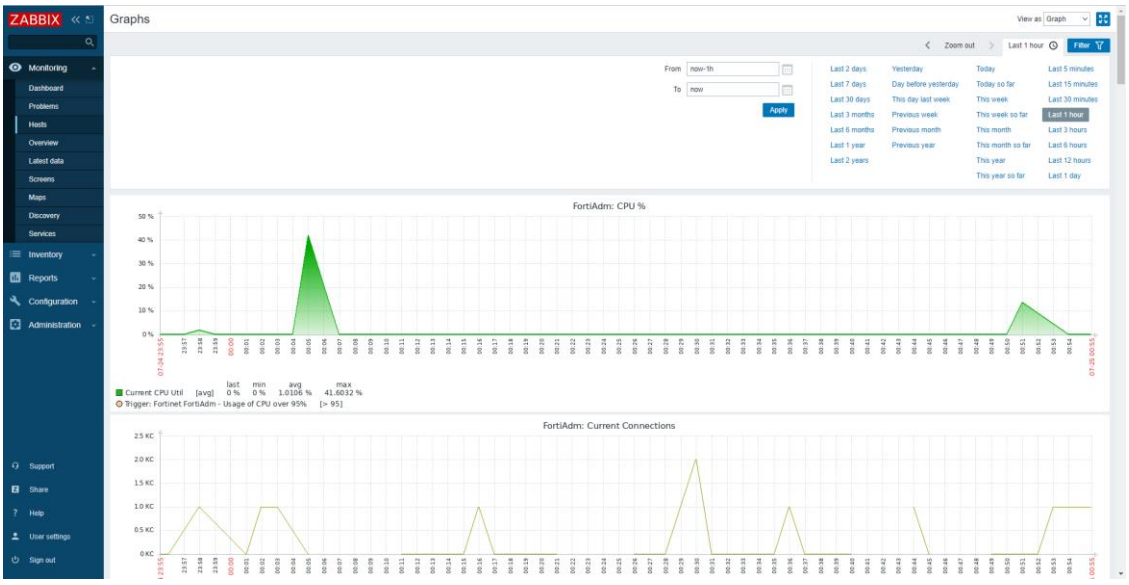


Figura 33. Resultado del host en centro de control

- En la consola se puede configurar reglas de descubrimiento a través de protocolos de comunicación y un rango de IP establecido.

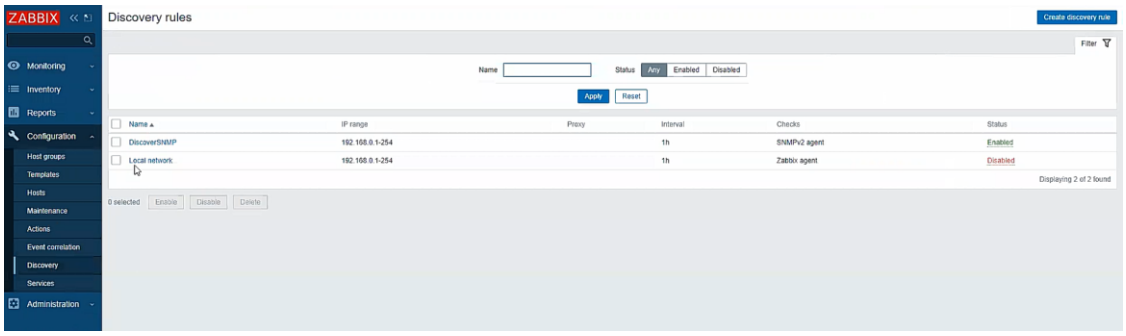


Figura 34. Reglas de descubrimiento SNMP

Por defecto la consola muestra una regla de SNMP.

- Se editó la regla de descubrimiento, para establecer el rango de IP utilizado en la red privada de la empresa.

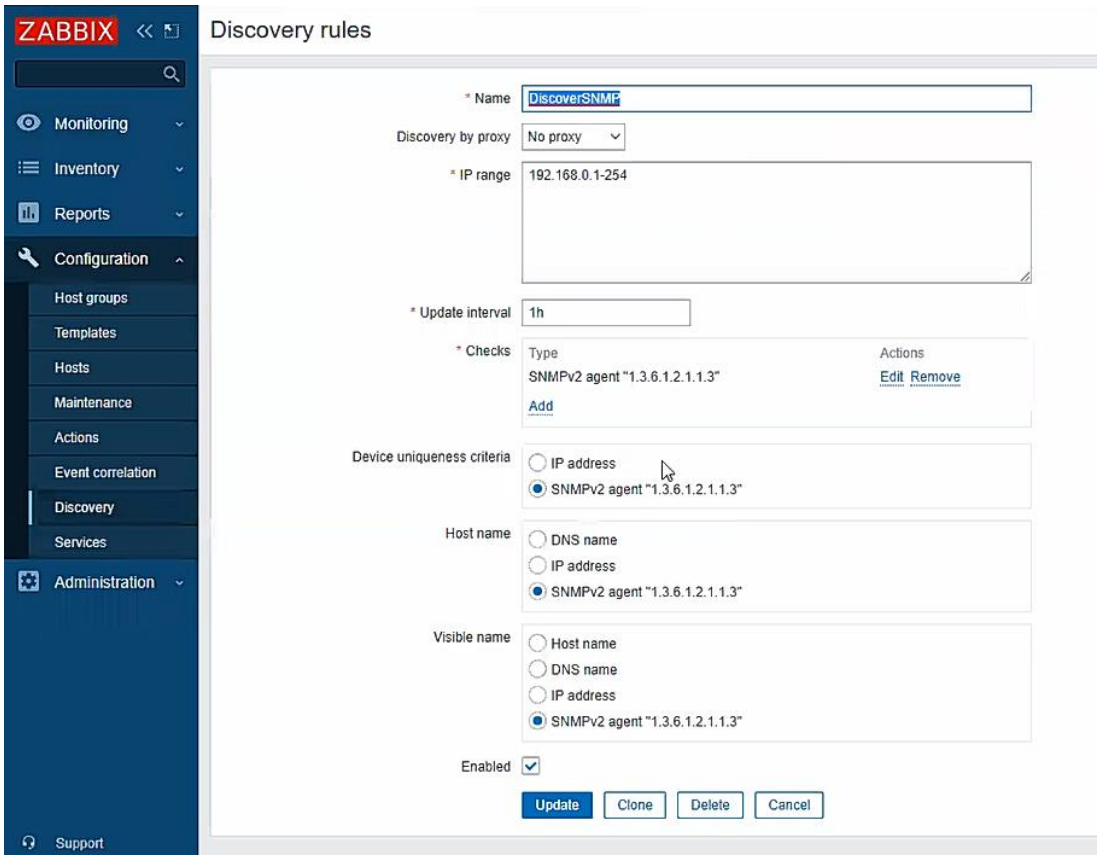


Figura 35. Configuración de regla SNMP

Name: se ingresó el nombre de la regla

Discovery by proxy: en el caso de la empresa POFASA, no cuenta con un proxy.

IP Range: se ingresó el rango de IPs donde la herramienta analiza los dispositivos y servicios que tengan acceso al protocolo SNMP.

Update Interval: el intervalo de actualización es recomendable poner 24 horas ya que consume muchos recursos el reconocimiento.

Checks: aquí podemos escoger el tipo de protocolo de comunicación se va a utilizar con su respectivo puerto y añadir el nombre de la comunidad que se va a utilizar.

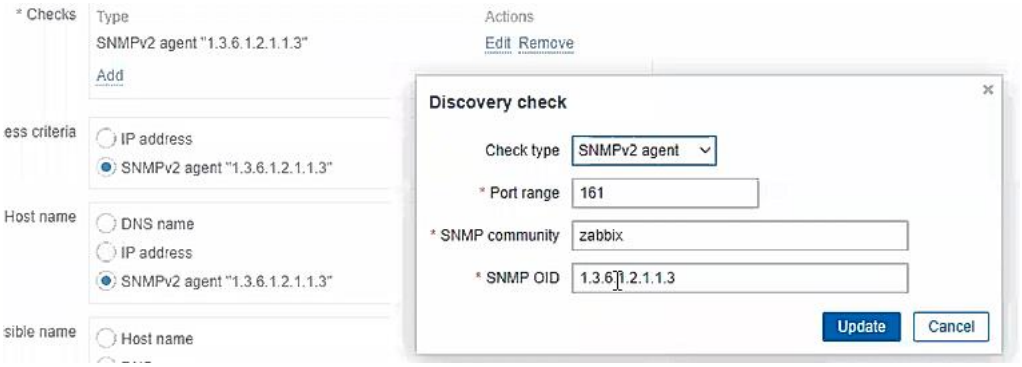


Figura 36. Configuración de protocolo de descubrimiento

SNMP OID: en este campo se ingresó el identificador de objeto de los parámetros a monitorear, por defecto tenemos temperatura, almacenamiento, memoria RAM y utilización de interfaces.

- Configuración de notificaciones, se procedió a crear un grupo de notificaciones.

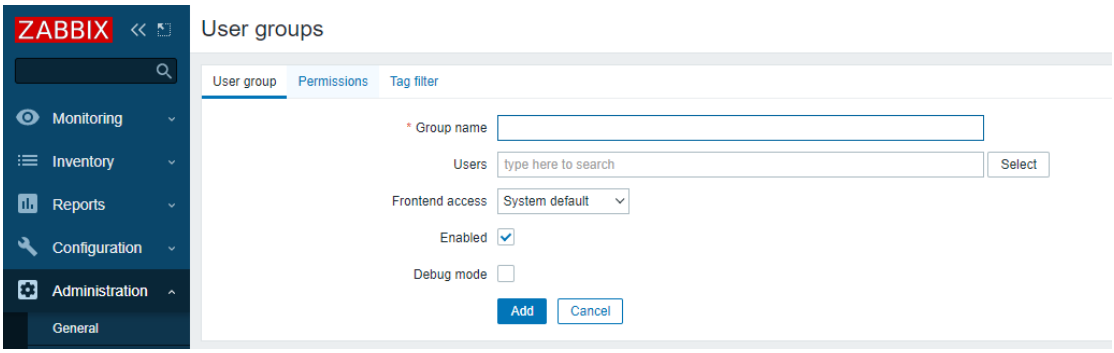


Figura 37. Creación grupo notificaciones

- Creación de usuario para reporte de notificaciones.

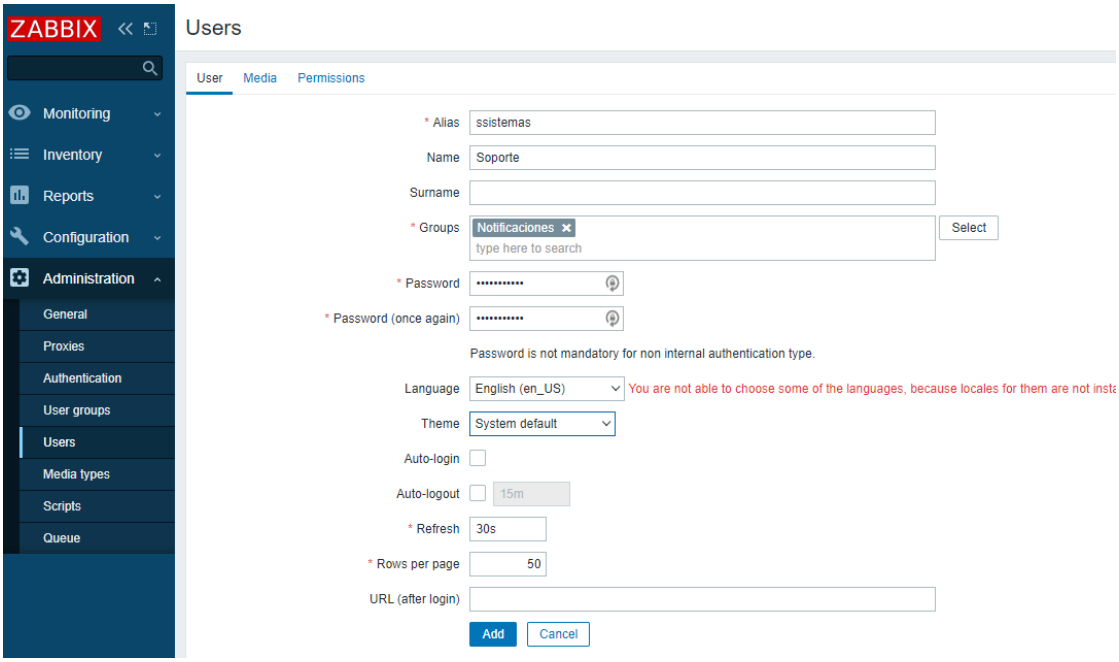


Figura 38. Creación usuario para notificaciones

Alias: nombre de usuario para inicio de sesión.

Groups: se añadió el grupo creando en el paso anterior, notificaciones.

Password: se ingresó una contraseña de alta seguridad.

- En la pestaña Media se realizó la creación de tipo de notificaciones que recibe el usuario

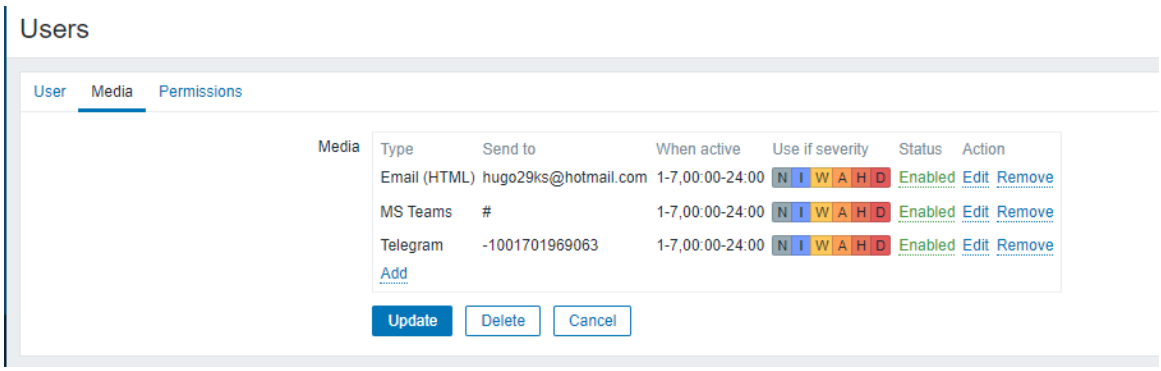


Figura 39. Resumen del tipo de notificaciones por usuario

- Se añadió y escogió el tipo de notificación.

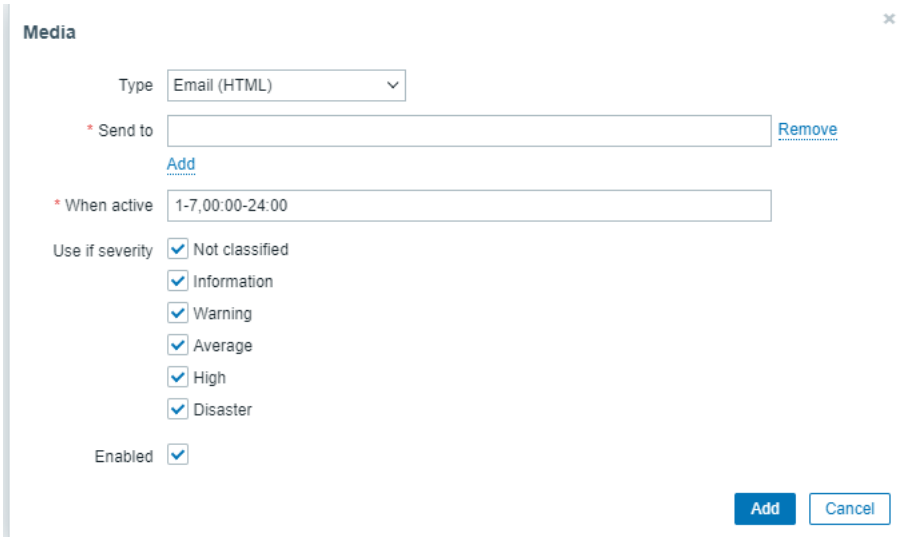


Figura 40. Tipo de notificación

Type: se puede escoger el tipo de notificación, tenemos por correo, Telegram y Microsoft Teams.

When active: se puede escoger todos los días de la semana y las 24 horas del día.

Use if severity: se escogió todas las opciones de grados de incidencia para no perder ningún reporte.

- Se procedió a configurar las acciones para activar los desencadenadores para las notificaciones.

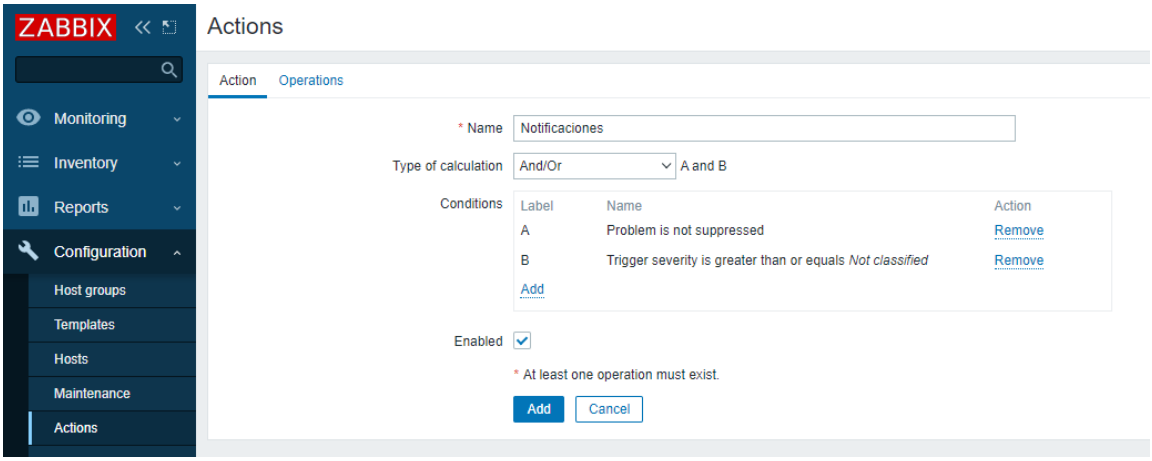


Figura 41. Configuración de acciones

Name: se añadió el nombre de la acción, en este caso notificaciones.

Conditions: se procedió a añadir las condiciones para activar el desencadenador. En este caso se añadió si el problema no está reprimido y la severidad no está clasificada.

- En la pestaña operaciones, se configuró el tiempo de duración de los pasos establecidos en el ítem anterior.

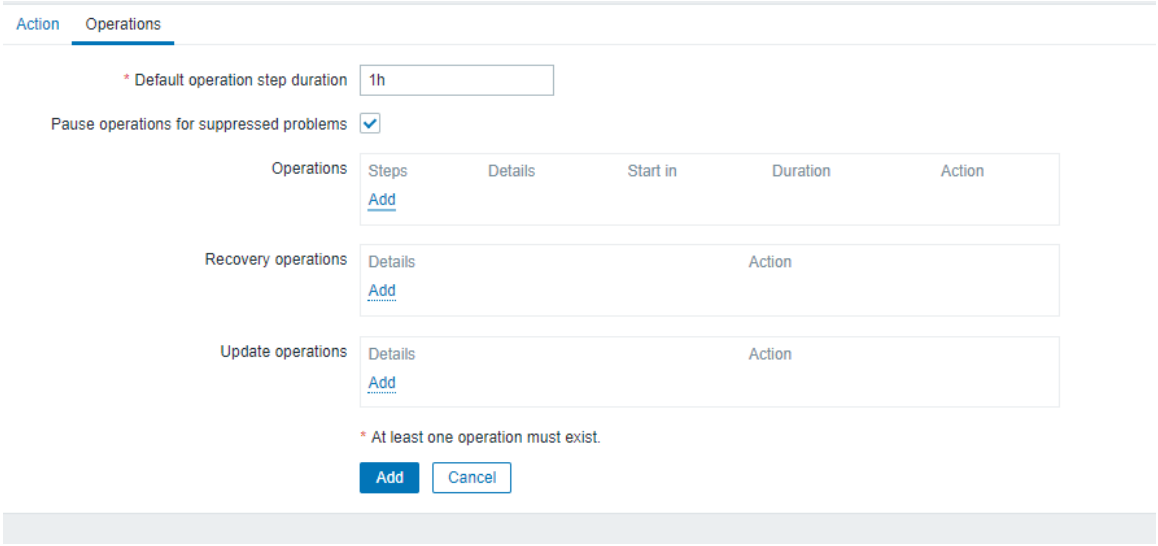


Figura 42. Configuración de operaciones en menú acciones

- Se procedió añadir las operaciones del desencadenador.

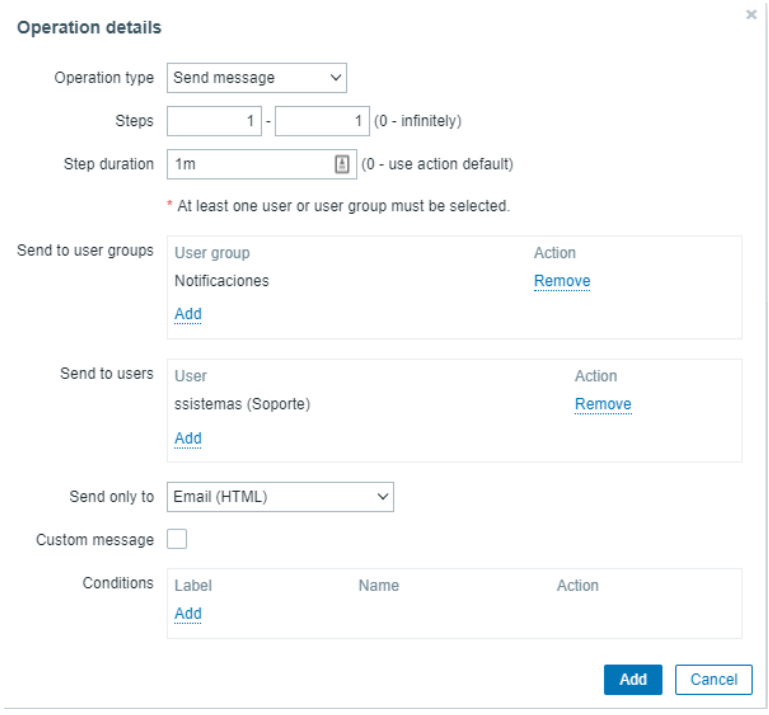


Figura 43. Detalles de operaciones en la configuración.

Se agregó el tipo de operación y lo más importante es añadir al grupo que tiene los usuarios de notificación. Además, se escogió el tipo de notificación en la opción “send only to” para escoger de tipo correo, Teams o Telegram.

- Configuración realizada para nuestro caso de estudio.

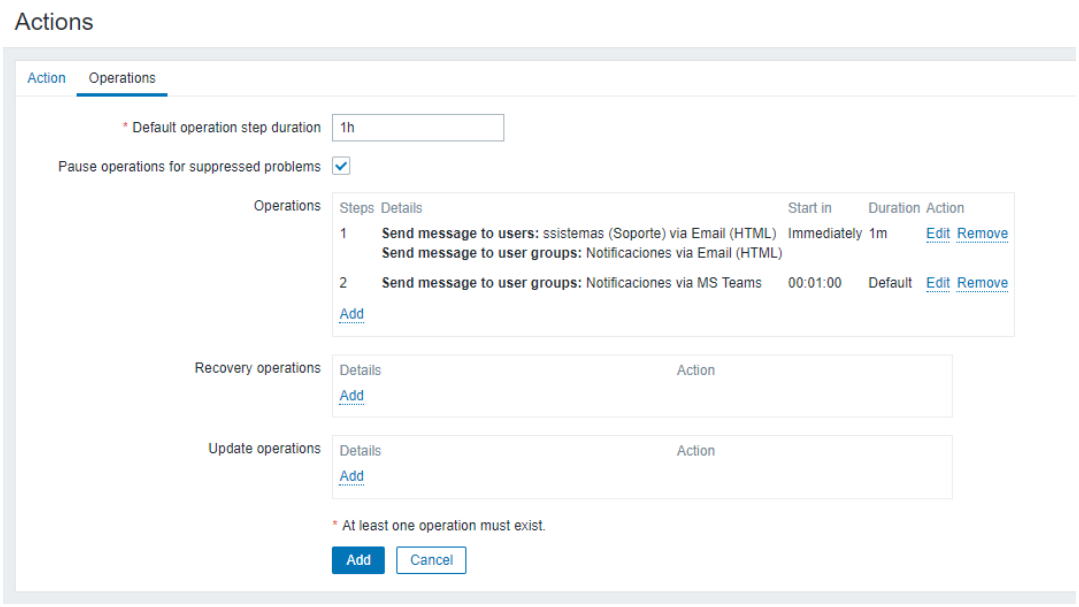


Figura 44. Configuración final de las operaciones en el menú de acciones

- Procedimiento para configurar servicios de notificadores. En pestaña media types.

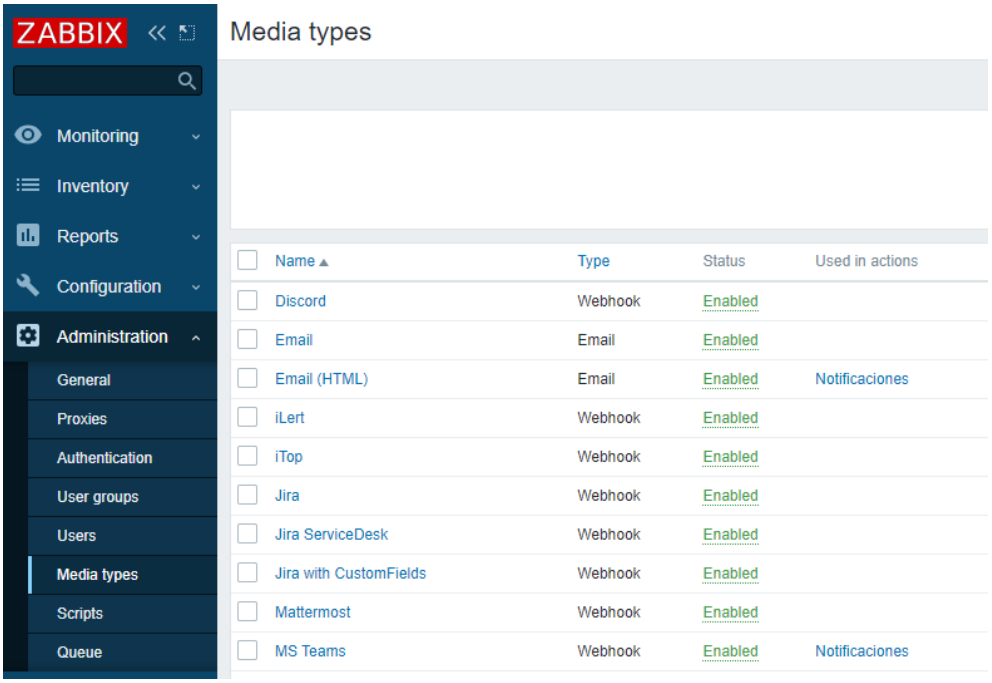


Figura 45. Configuración Media Types

- Configuración correo electrónico

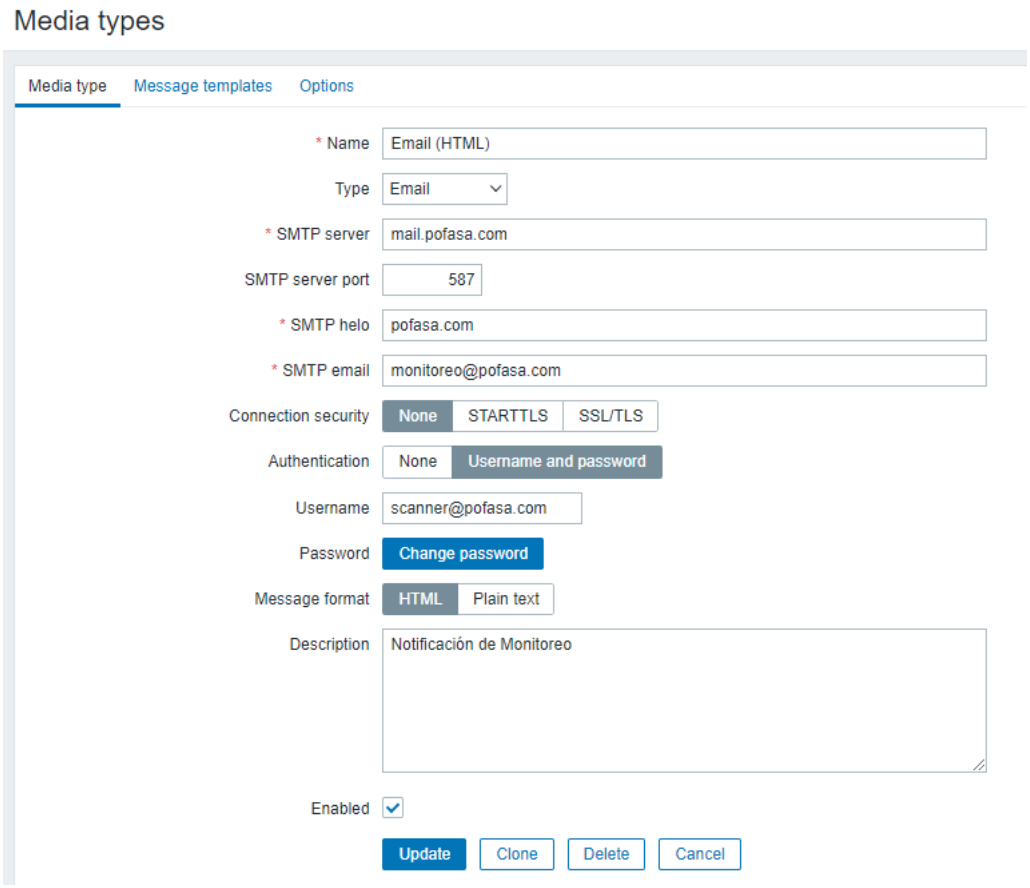


Figura 46. Configuración correo electrónico

Name: se puede cambiar el nombre de la configuración.

Type: se dejó por defecto.

SMTP: se ingresó la dirección del servidor de correo electrónico.

SMTP port: se ingresó el puerto por defecto que es 587

SMTP email: se ingesó la dirección de correo para autenticación del sistema.

- Se procedió a guardar la configuración y realizar una prueba.

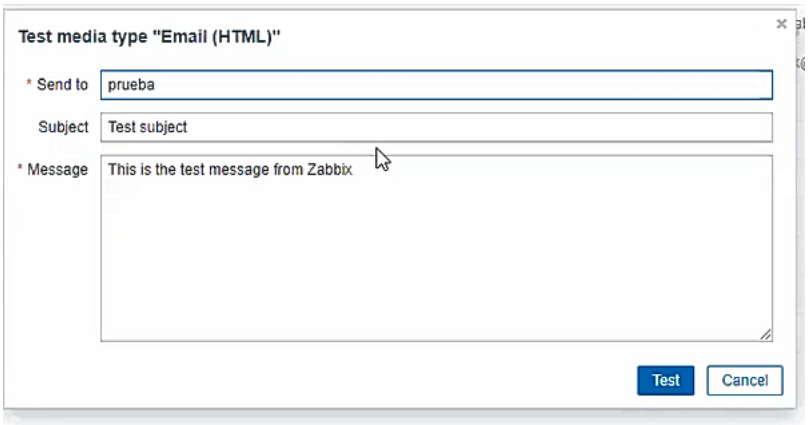


Figura 47. Test de email

- Configuración Microsoft Teams, como primer paso se añadió en un canal el conector de Zabbix.

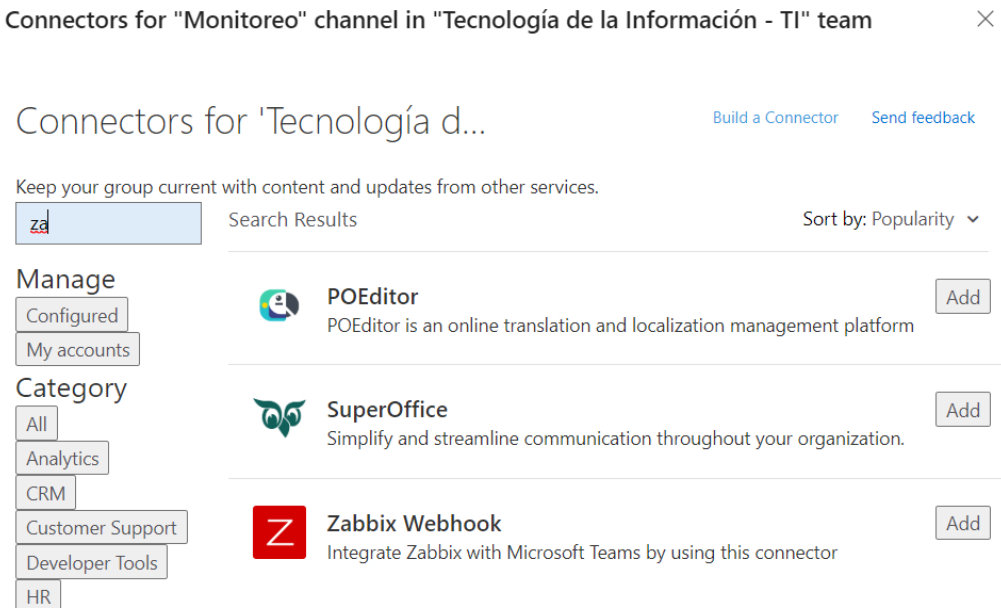


Figura 48. Conector Zabbix en Ms Teams

- Añadido el conector se procedió a copiar la dirección de web hook para añadir a la consola Zabbix.

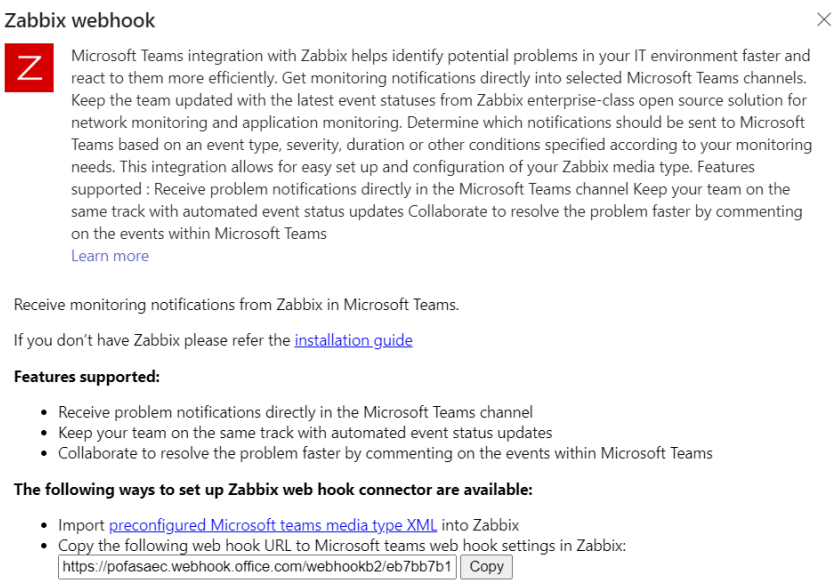


Figura 49. Configuración de conector Zabbix en Ms Teams

- Microsoft Teams muestra el conector añadido y configurado en el canal de monitoreo del área de TI.

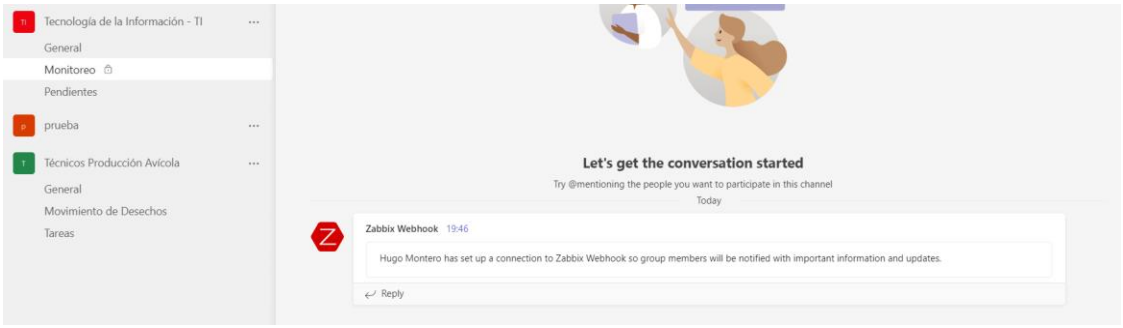


Figura 50. Pantalla de prueba de conector Zabbix en Ms Teams

- Configuración consola Zabbix para Microsoft Teams.

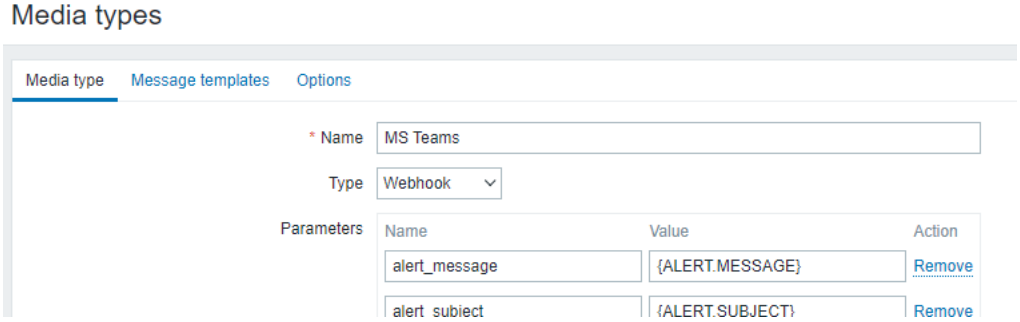


Figura 51. Configuración de Ms Teams en consola Zabbix

La configuración del tipo de parámetros queda por defecto para los mensajes. Solo se añadió la URL proporcionada por Teams en el parámetro “teams_endpoint”.

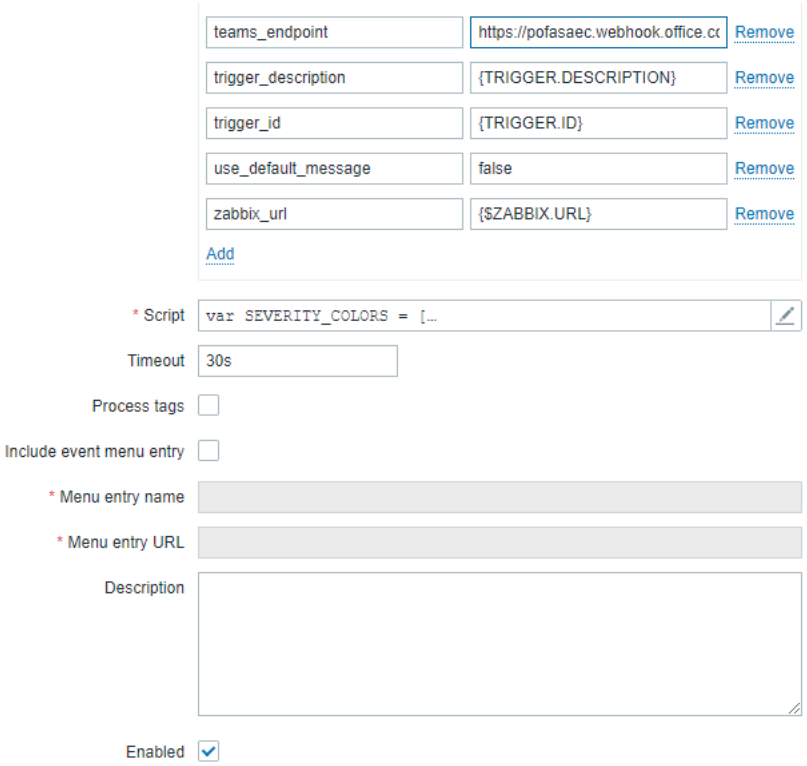


Figura 52. Configuración de Microsoft Teams en consola Zabbix

- Configuración de notificaciones Telegram, este proceso se creó un grupo de monitoreo en Telegram, y se añadió un bot que genera nuestro token e ID de grupo. En la consola de Zabbix debemos ingresar nuestro token de Telegram.

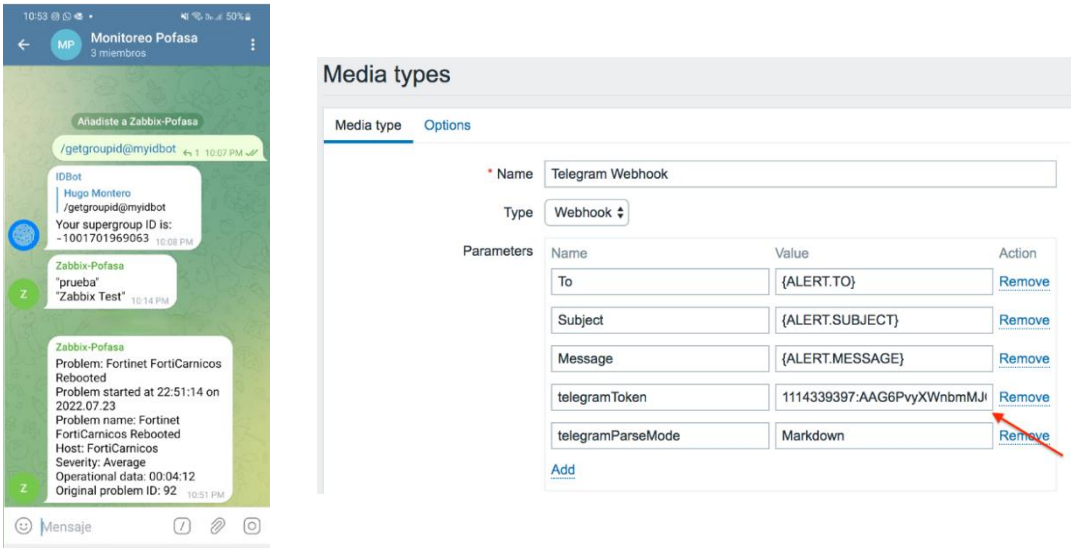


Figura 53. Configuración de Telegram

- Se realizó una prueba ingresando el código de grupo y token de nuestro Telegram.

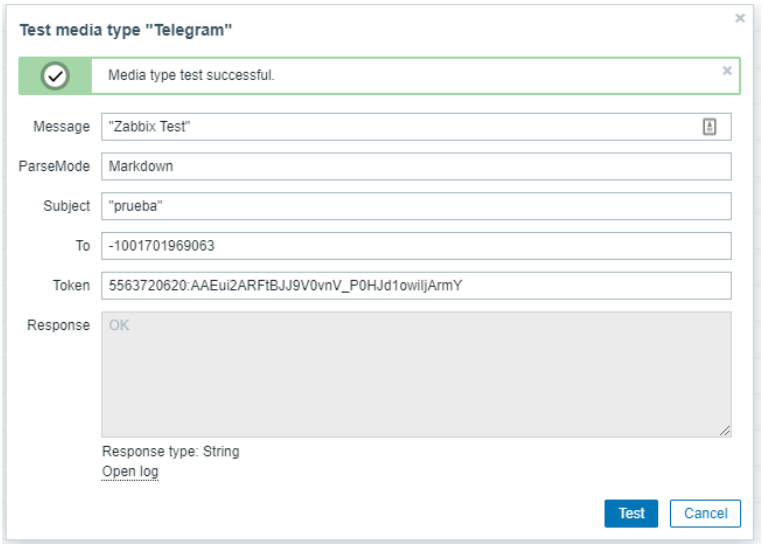


Figura 54. Test de Telegram

2.2.3 PRUEBAS

Para la realización de las pruebas se procedió a la desconexión de un dispositivo crítico, el firewall perdió comunicación con el sistema de monitoreo por 3 minutos y esta acción activó el desencadenador de notificaciones para las 3 plataformas configuradas. Además, en el cuadro de control se muestra el problema y las acciones realizadas.

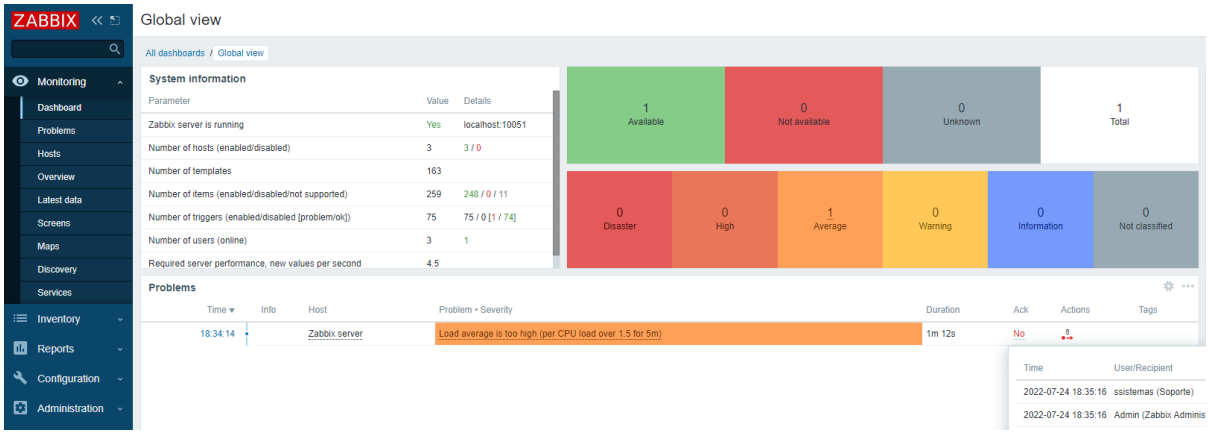


Figura 55. Dashboard con problema encontrado

Por temas de seguridad la empresa no permitió la desconexión de dispositivos o servicios en cada una de las áreas porque estaban en producción y no tenían una bitácora de reinicios programados por lo cual no se autorizó el procedimiento de prueba. A continuación, se muestra los resultados con la desconexión del firewall que se autorizó para pruebas.

- Notificación de correo:

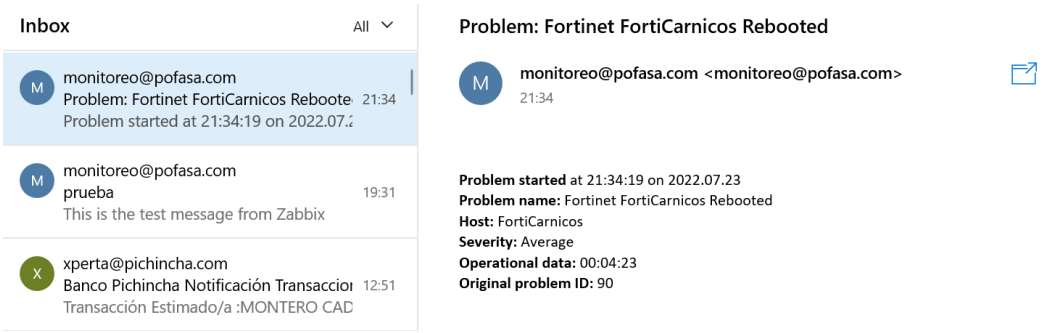


Figura 56. Notificación de correo electrónico

- Notificación de Microsoft Teams

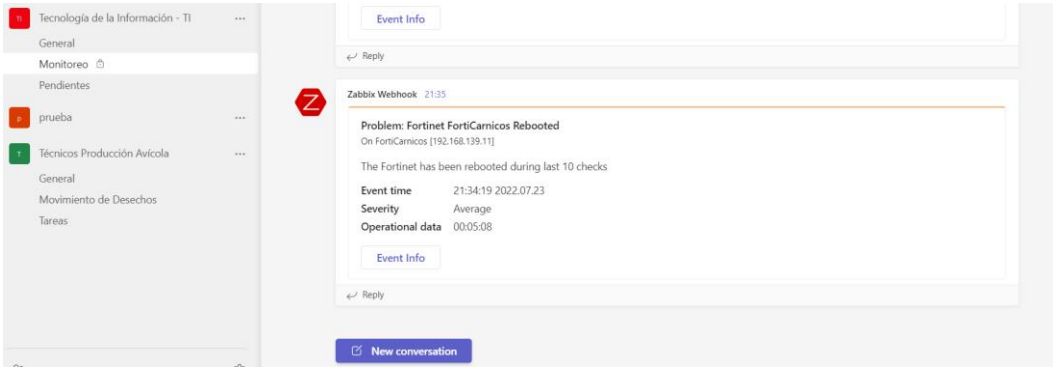


Figura 57. Notificación de Ms Teams

- Notificación de Telegram

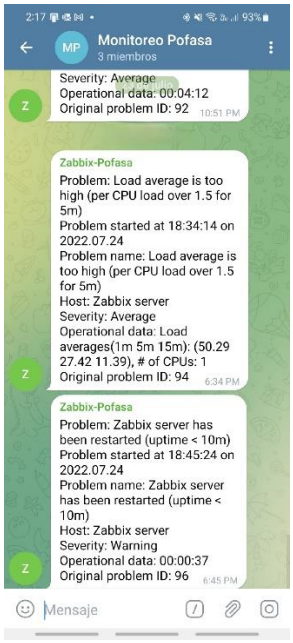


Figura 59. Notificación de Telegram

2.3 FASE DE VERIFICACIÓN

Una vez culminada la fase de implementación, se procede con la fase de verificación (Check) del modelo PDCA; con la finalidad de comprobar el cumplimiento de los objetivos de monitoreo por parte del sistema de monitoreo. En la fase de análisis, se detallan los objetivos de monitoreo de la presente investigación.

OBJETIVO	CUMPLIMIENTO DEL MONITOREO
Identificar la infraestructura critica que debe ser monitorizada en base a los procesos que maneja la empresa como su prioridad.	✓
Establecer las responsabilidades del personal a cargo de los dispositivos y servicios, eliminando la duplicidad de funciones e incertidumbre sobre el estado de la infraestructura.	✓
Mantener la disponibilidad y conectividad de los servicios utilizados por el personal que labora en la empresa.	✓
Establecer notificaciones en diferentes plataformas para los dispositivos de la infraestructura de TI.	✓

Tabla 10. Cumplimiento de objetivos de fase de verificación

Para la realización de las pruebas de carga al servidor asignado se utilizó la herramienta Apache JMeter; el cual es un software de código abierto diseñado en JAVA, se puede utilizar para simular una carga pesada en un servidor, grupo de servidores y red, con el objetivo de analizar el rendimiento general bajo diferentes tipos de carga [20].

El sistema de monitoreo se asignó a 4 usuarios concurrentes, los cuales son encargados de la supervisión de la infraestructura en cada una de sus áreas u oficinas donde laboran. La prueba de carga con la herramienta JMeter se realizó con 10 usuarios concurrentes por la tendencia de crecimiento de la infraestructura y el cumplimiento de los requisitos mostrados por la guía de Zabbix. Por esta razón se mantuvo la configuración inicial de nuestro servidor Linux. Se muestra a continuación la configuración de la herramienta:

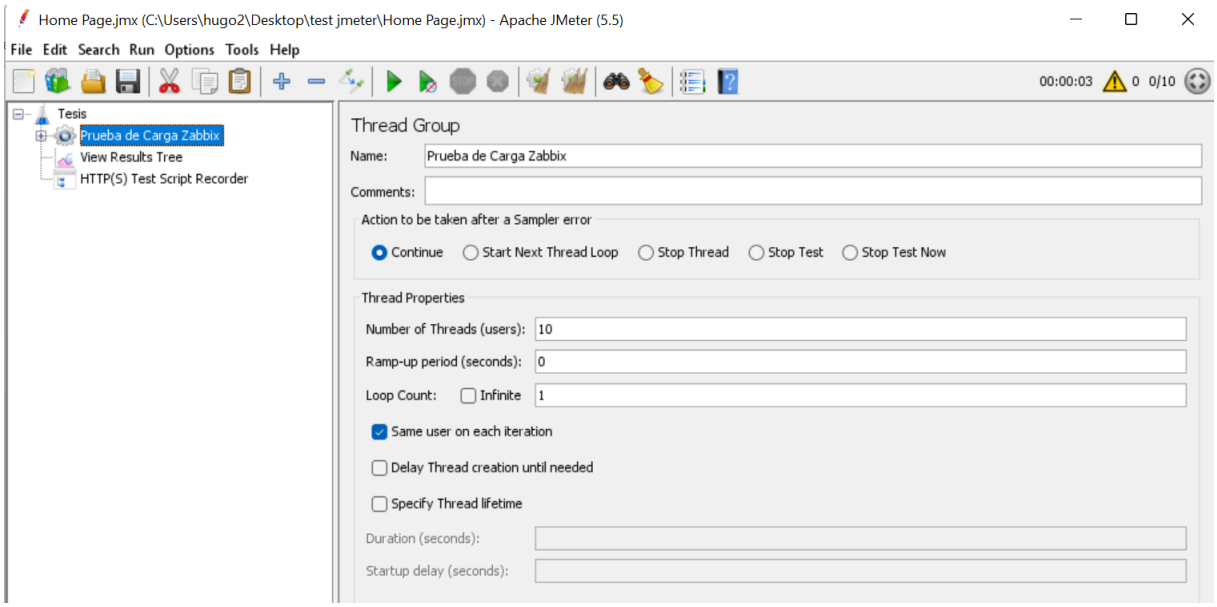


Figura 60. Configuración JMeter

La herramienta tiene la facilidad de capturar las solicitudes HTTP a través del navegador para ejecutar las pruebas de carga con el número de usuarios que necesitemos en nuestro servidor de monitoreo.

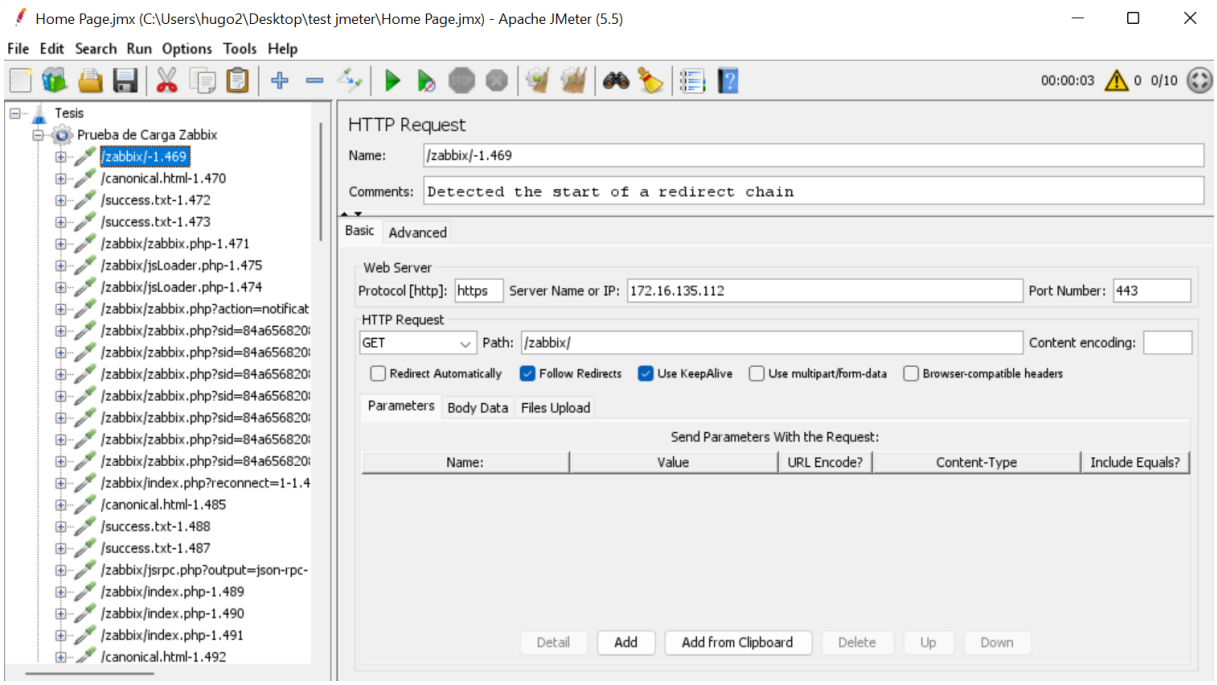


Figura 61. Configuración de HTTP Request en JMeter

Concluida la prueba, se muestra a continuación los resultados de todas las solitudes realizadas.

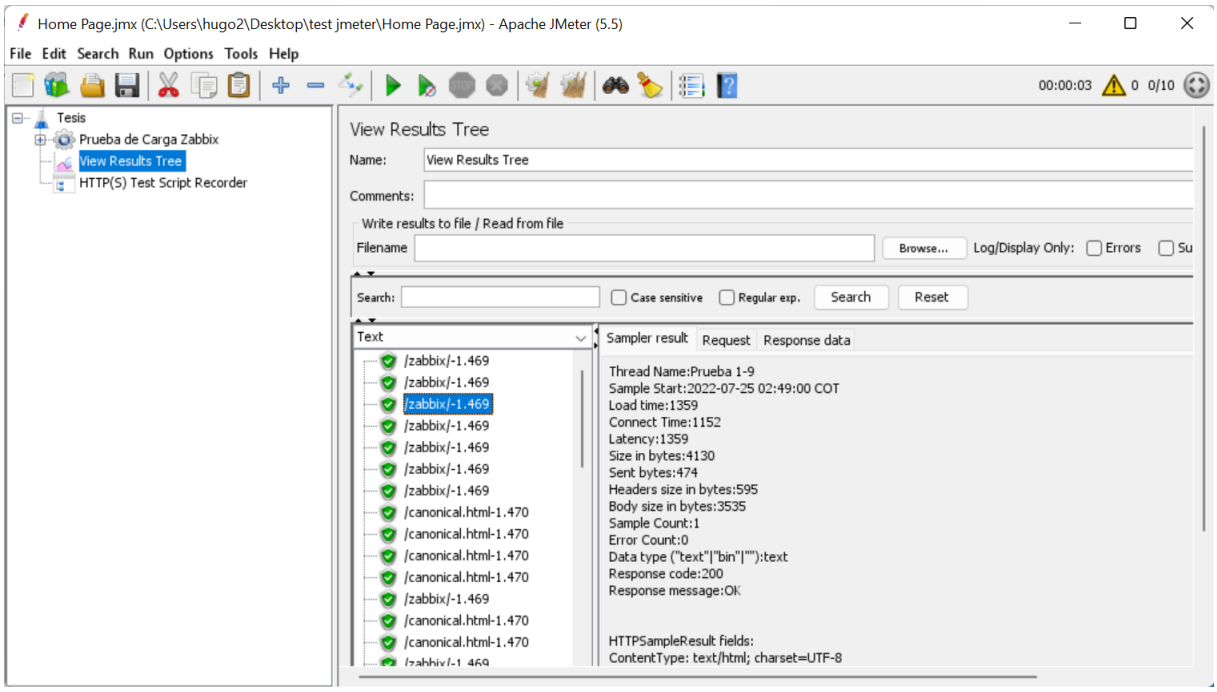


Figura 62. Vista de árbol de resultados JMeter

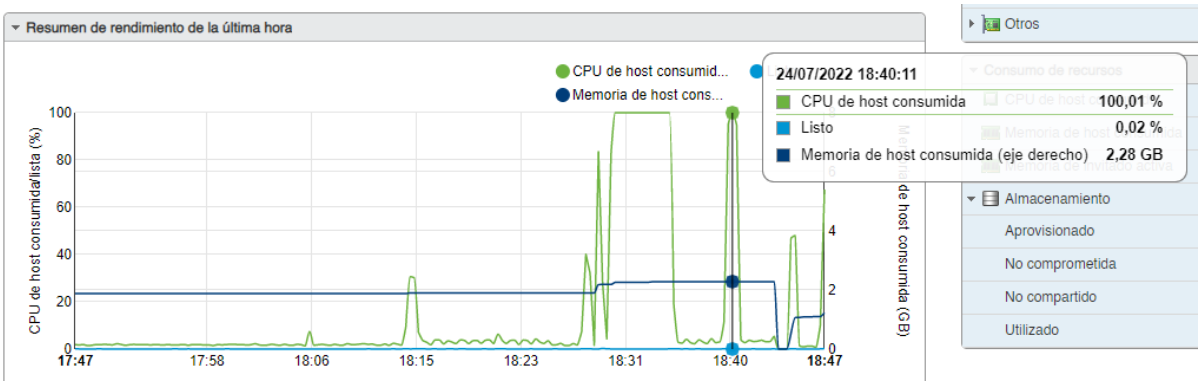


Figura 63. Gráfico de rendimiento de sistema VMWARE

La consola de administración de máquinas virtuales VMWARE, mostró que el consumo de CPU superó el 100% y el uso de memoria RAM también aumenta ligeramente. Por esta razón la prueba no fue superada con 10 usuarios concurrentes con la configuración del servidor asignado por parte de la empresa POFASA.

Por lo tanto, conforme a lo implementado y a los objetivos establecidos para el monitoreo de la red LAN de la empresa POFASA, el sistema permitió la implementación completa de todos los parámetros de monitoreo, pero no supera las pruebas de carga para 10 usuarios concurrentes.

2.4 FASE DE ACTUAR

Los objetivos establecidos por el jefe del área de TI de la empresa POFASA, fueron implementados en su totalidad.

OBJETIVOS	RESULTADOS	OBSERVACIÓN
Identificar la infraestructura critica que debe ser monitorizada en base a los procesos que maneja la empresa como su prioridad.	Implementado en la fase de monitoreo	Ninguna
Establecer las responsabilidades del personal a cargo de los dispositivos y servicios, eliminando la duplicidad de funciones e incertidumbre sobre el estado de la infraestructura.	Implementado en la fase de monitoreo	Ninguna
Mantener la disponibilidad y conectividad de los servicios utilizados por el personal que labora en la empresa.	Implementado en la fase de monitoreo	Ninguna
Establecer notificaciones en diferentes plataformas para los dispositivos de la infraestructura de TI.	Implementado en la fase de monitoreo	Ninguna

Tabla 11. Resultados de fase de optimización

Además, se realizó el cambio de números de CPUs asignados al servidor Linux para el sistema de monitoreo y se aumentó la memoria RAM. Se tuvo asignado 2 CPUs y 4 GB de RAM.

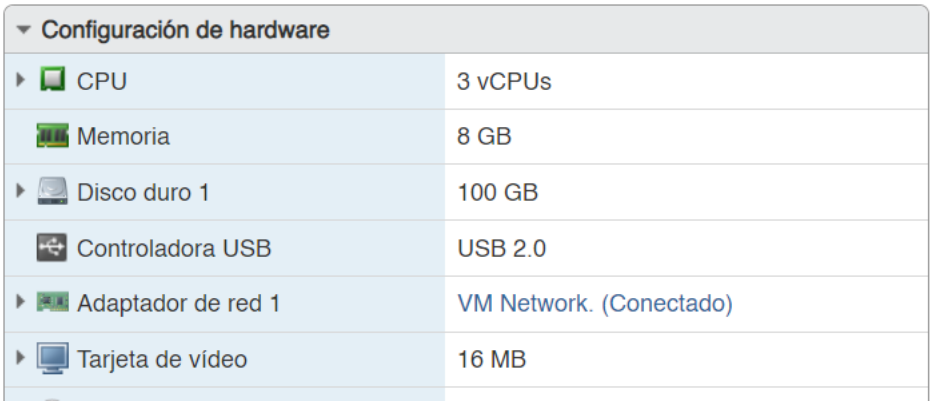


Figura 64. Gráfico de configuración de hardware

La empresa decidió aumentar 1 CPU más y 4 GB más de memoria RAM. Por lo que se realizó nuevamente la prueba de carga con esta nueva configuración para el sistema de monitoreo. Mostrando los siguientes resultados en la consola de administración VMWARE.

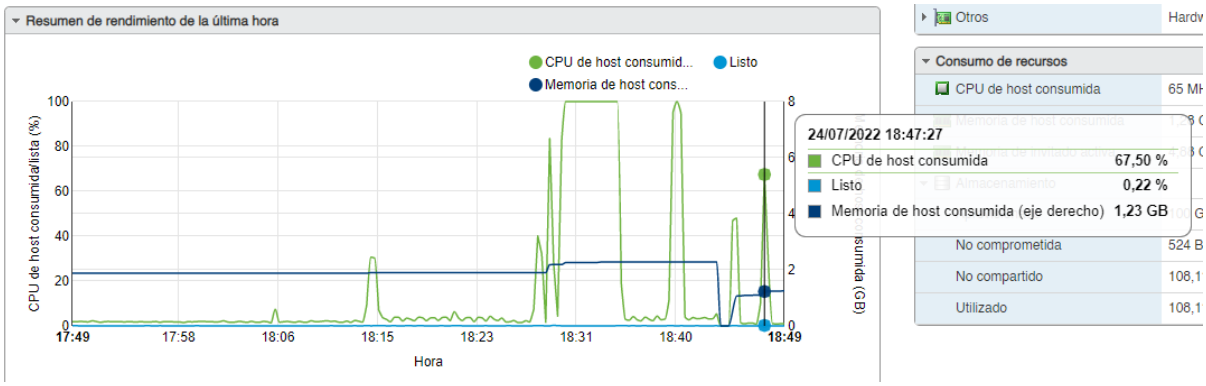


Figura 65. Gráfico de rendimiento de sistema FINAL

Como podemos observar en la imagen, el consumo de CPU alcanzó un máximo del 67.5% a diferencia de la prueba anterior donde supera el 100%. La memoria RAM consumida es de 1.23 GB a diferencia de los 2.28 GB consumidos en la anterior prueba. Todas las carencias fueron resueltas en esta fase por lo que el sistema de monitoreo Zabbix queda implementado en su totalidad en la red LAN de la empresa POFASA.

3 RESULTADOS Y DISCUSIÓN

3.1 ANÁLISIS DE LOS RESULTADOS

En el capítulo 2 se realizó una encuesta a 18 usuarios que utilizan dispositivos o servicios de la infraestructura de TI a pesar de no ser parte del área. A continuación, se muestra los resultados de la encuesta después de la implementación del sistema de monitoreo ZABBIX.

- **Tiempo de Respuesta**

  ¿Cuál es el tiempo promedio de atención de incidentes de infraestructura TI?

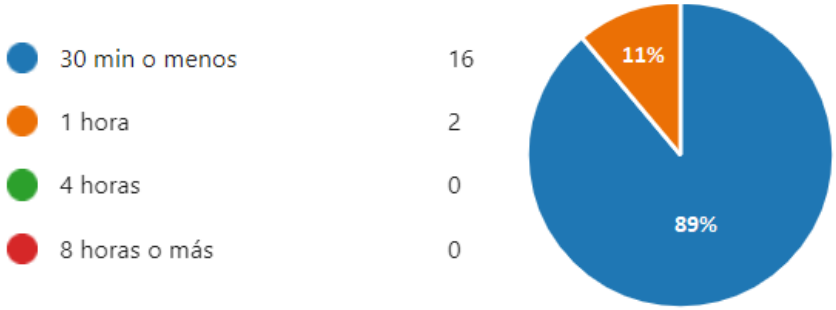


Figura 66. Resultados de encuesta pregunta 1

- **Exactitud al encontrar el incidente**

  ¿Cuánto tiempo lleva en promedio identificar el dispositivo o servicio de TI que está causando el incidente?

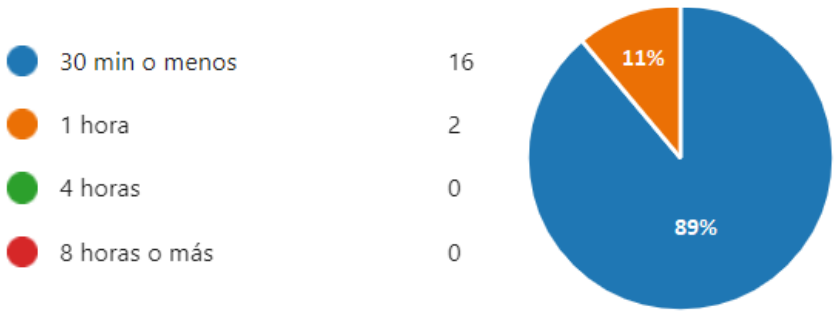


Figura 67. Resultados de encuesta pregunta 2

- **Satisfacción del usuario**

  ¿Cómo calificaría el método actual para monitorear la infraestructura de TI de la empresa?

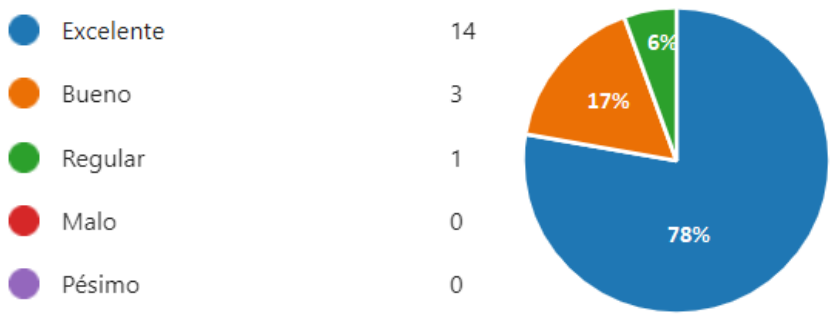


Figura 68. Resultados de encuesta pregunta 3

- **Integridad**

  ¿Confía en el método actual para monitorear la infraestructura de TI de la empresa?

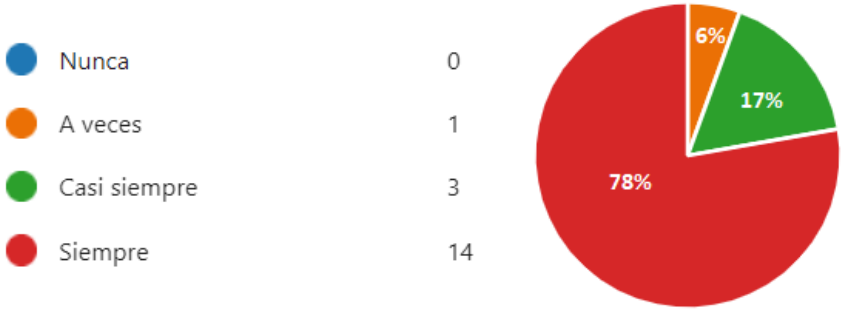


Figura 69. Resultados de encuesta pregunta 4

- **Calidad de Servicio**

  ¿Cuántas quejas se realizan cada semana sobre la disponibilidad del servicio y mal funcionamiento de los dispositivos en la red?

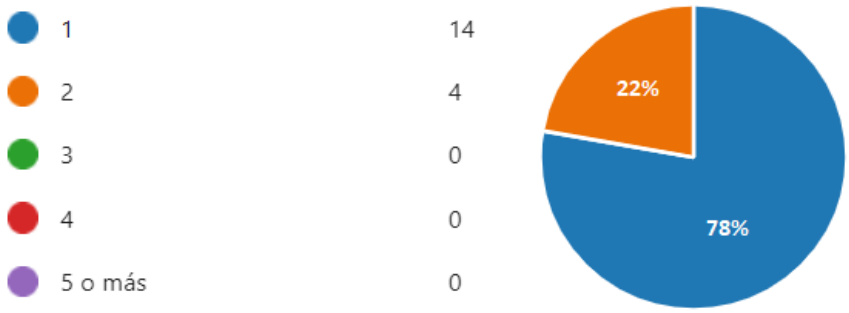


Figura 70. Resultados de encuesta pregunta 5

3.1.1 INDICADORES

- **Tiempo de Respuesta**

  Antes de la implementación:

Pregunta	30 min o más	1 hora	4 horas	8 horas o más
1	-	32%	58%	11%

Tabla 12. Resultados antes de la implementación pregunta 1

Después de la implementación:

Pregunta	30 min o más	1 hora	4 horas	8 horas o más
1	89%	11%	-	-

Tabla 13. Resultados después de la implementación pregunta 1

Como podemos observar en las tablas 5 y 6 se reduce el tiempo de respuesta para la atención de incidentes dentro de la infraestructura de TI. Antes de la implementación teníamos que el mayor porcentaje representaba 4 horas, lo cual causaba mucho malestar dentro de los usuarios de los diferentes sistemas y dispositivos. Una de las razones principales es no tener una acción preventiva por parte del área de TI de la empresa POFASA, ya que el personal a cargo se rige solo a las solicitudes presentadas durante su día a día, por lo cual cuando existía un problema con varios dispositivos en el mismo momento, el tiempo de respuesta sube considerablemente. A través de la implementación del sistema de monitoreo se pudo reducir en 0 el tiempo de respuesta mayor a 8 horas, por lo general los incidentes reportados que tenían dicha duración, se presentaban en horas de salida de oficina o durante la noche por lo que el personal a cargo no se encontraba en la ubicación físicamente. Estos incidentes ocasionaban retrasos en el inicio de actividades de un día posterior. La herramienta Zabbix ayuda a gestionar de manera oportuna las notificaciones y alertas cuando un dispositivo o servicio presenta fallos en tiempo real.

Podemos afirmar a través de este indicador que la implementación cumplió con las expectativas del área de TI, reduciendo tiempos de trabajo y duplicidad de funciones en incidentes leves y sobre todo en incidentes graves.

- **Exactitud al encontrar el incidente**

Antes de la implementación:

Pregunta	30 min o más	1 hora	2 horas	6 horas o más
2	-	32%	42%	26%

Tabla 14. Resultados antes de la implementación pregunta 2

Después de la implementación:

Pregunta	30 min o más	1 hora	2 horas	6 horas o más
2	89%	11%	-	-

Tabla 15. Resultados después de la implementación pregunta 2

Como podemos observar en la tabla 7 y 8, existe una mejor exactitud para encontrar incidentes, la manera de medir esto es a través del tiempo. Entre menor tiempo tengamos, mayor es el porcentaje de respuesta para el indicador de la pregunta 2. El principal problema que tenía la empresa y el área de TI era que debían revisar el estado físico de los equipos en caso de perder comunicación con ellos, era imposible ingresar a la consola de administración del fabricante. Ya que la empresa cuenta con sucursales distantes dentro de Quito, encontrar con exactitud el incidente era una tarea que llevaba alrededor de 2 horas y su solución podía tomar solo 2 minutos, por ejemplo, cuando un switch tenía una variación de voltaje el equipo solo se debe reiniciar, pero al no contar con un proceso automatizado se debe buscar y verificar entre los diferentes dispositivos de comunicación de un cuarto de datos. El sistema monitoreo reduce a menos de la mitad los tiempos del indicador a pesar de que la pregunta fue respondida por personal fuera del área de TI, demuestra que existe un mejor manejo y solución de los incidentes reportados dentro de las estaciones de trabajo del personal encuestado.

Podemos afirmar a través de este indicador que la implementación cumplió con las expectativas del área de TI porque corto tiempo de exactitud para las incidencias graves y leves dentro de la infraestructura de TI.

- **Satisfacción del usuario**

Antes de la implementación:

Pregunta	Pésimo	Malo	Regular	Bueno	Excelente
3	37%	37%	26%	-	-

Tabla 16. Resultados antes de la implementación pregunta 3

Después de la implementación:

Pregunta	Pésimo	Malo	Regular	Bueno	Excelente
3	-	-	6%	17%	78%

Tabla 17. Resultados después de la implementación pregunta 3

Como podemos observar en la tabla 9 y 10, el porcentaje de satisfacción por parte del personal de la empresa estaba entre pésimo y malo. Por esta razón el personal del área de TI tenía una mala reputación en cuanto a la resolución de incidentes. El motivo principal de la calificación fue no contar con un sistema de alertas preventivas y sobre todo tener que revisar cada consola de administración para saber el estado actual de los dispositivos y servicios de la empresa. Además, los mantenimientos eran correctivos en lugar de preventivos por esta razón los incidentes reportados eran difíciles de resolver y tomaban bastante tiempo, lo cual para un usuario o personal de la empresa era malo el servicio.

Después de la implementación del sistema de monitoreo, el área de TI de la empresa tiene una calificación mejor (excelente). El motivo principal fue el correcto funcionamiento del sistema ZABBIX, ya que el personal encargado podía estar un paso adelante, anticipando el error y la solución del incidente antes que el usuario final se percate de la falla. Podemos afirmar a través de este indicador que la implementación cumplió con las expectativas del área de TI porque mejoraron su satisfacción ante el personal de la empresa y redujeron tiempos de servicio.

- **Integridad**

Antes de la implementación:

Pregunta	Nunca	A veces	Casi Siempre	Siempre
4	47%	42%	11%	-

Tabla 18. Resultados antes de la implementación pregunta 4

Después de la implementación:

Pregunta	Nunca	A veces	Casi Siempre	Siempre
4	-	6%	17%	78%

Tabla 19. Resultados después de la implementación pregunta 4

Como podemos observar en la tabla 11 y 12, esta pregunta esta correlacionada con la satisfacción porque el personal no tenía una seguridad con las personas encargadas del área de TI por lo que antes de la implementación este indicador tiene un porcentaje alto en la opción NUNCA. Todo esto era preocupante para el jefe del área de TI ya que no se contaba con la confianza suficiente con su equipo de trabajo. El sistema realizó un cambio completo en la actividad de monitoreo, de tener un monitoreo manual a uno automatizado. Por esta razón, el porcentaje cambio a la opción SIEMPRE ya que los usuarios pudieron observar que se estaba utilizando la tecnología para el reporte y resolución de incidentes de los dispositivos y servicios asignados a ellos.

- **Calidad de Servicio**

Antes de la implementación:

Pregunta	1	2	3	4	5 o más
5	-	5%	42%	32%	21%

Tabla 20. Resultados antes de la implementación pregunta 5

Después de la implementación:

Pregunta	1	2	3	4	5 o más
5	78%	32%	-	-	-

Tabla 21. Resultados después de la implementación pregunta 5

Como podemos observar en la tabla 13 y 14, la calidad servicio en base a la disponibilidad de la conexión era bastante alto en 1 semana se podía tener 5 veces o más. Lo que nos muestra la tabla 13 es que antes de la implementación tenemos como mínimo 2 caídas de servicio y con un promedio de 3 caídas. En cambio, con la implementación del sistema tenemos como máximo 2 perdidas de disponibilidad por semana y mínimo 1, las cuales dependen del proveedor de servicios de internet o red interna. Por ejemplo, un corte de fibra en la red principal o un corte de energía, son incidentes monitorizados pero su solución depende de personal externo.

El sistema de monitoreo ZABBIX influye de manera positiva en la gestión de incidentes dentro de la infraestructura de TI, ya que cumplen con los objetivos establecidos por la empresa POFASA a través de los 5 indicadores tomados en este capítulo se corrobora la satisfacción total de la herramienta por porta del personal del área de TI y por el personal a cargo de dispositivos y servicios que ayudan a cumplir sus funciones.

Además, influye en el tiempo de respuesta para la resolución de incidentes y reduce el tiempo para encontrar el servicio o el dispositivo que causa dicho incidente, mejorando la calidad de servicio que brinda el área de TI y aumentando la confiablidad e integridad en sus funciones.

3.2 DISCUSIÓN

Actualmente los sistemas de monitoreo automatizados ayudan en la administración de la infraestructura de TI, como se pudo observar en los resultados la aceptación es bastante alta porque el usuario administrador o encargado de dicha infraestructura ya no debe estar pendiente de un monitor o varios monitores para revisar a tiempo real el estado de cada servicio y dispositivo. De igual manera se pudo comparar los resultados obtenidos con tesis de sistemas de monitoreo de otros países, donde los indicadores son similares en cuanto a la reducción de tiempos de servicio y satisfacción con el usuario. De esta manera existe un ahorro en la cantidad de recursos económicos utilizados, la cantidad de funciones asignadas y el tiempo para realizar sus labores.

Además, los protocolos de comunicación SNMP y WMI tienen un papel importante en los resultados de la disponibilidad porque mantiene la información actualiza de los parámetros críticos y estos son obtenidos por el sistema de monitore ya que algunos fabricantes no tienen una conexión directa con Zabbix a través de su agente de instalación. Por lo que, la comunicación es establecida directamente por estos protocolos transmitiendo toda la información necesaria para el correcto monitoreo y facilitando las notificaciones por diferentes medios de comunicación.

Los resultados investigados en documentos de tesis de sistemas de monitoreo muestran algunas similitudes y cambios sintácticos con los resultados obtenidos en este proyecto, pero en última instancia son los mismos, por lo que el sistema de monitoreo de infraestructura de TI es una gestión de incidentes positiva, se puede decir que está ayudando a la empresa y al área responsable. Para los objetivos de este proyecto en la empresa POFASA, se logró reducir el tiempo de respuesta para responder a incidentes, reducir el tiempo para encontrar incidentes o fallas en la infraestructura de TI y mejorar la calidad del servicio en las áreas de TI. Se aumenta la credibilidad de los usuarios en los mecanismos de monitoreo de la infraestructura de TI, reduce la tasa de quejas del personal a cargo de servicios o dispositivos de TI y aumente la productividad del personal responsable de monitorear y administrar incidentes.

4 CONCLUSIONES

Este capítulo contiene las conclusiones y recomendaciones a las que se llegó tras la realización de este proyecto. A continuación, se presentan las conclusiones, seguidas de las recomendaciones.

4.1 CONCLUSIONES

- La comparativa de los sistemas de monitoreo se realizó a través del informe presentado en la página de Gartner, donde se muestra las herramientas de código abierto y de licencia pagada. Se seleccionaron 3, las cuales son Zabbix, Nagios XI y Pandora FMS. En base a la investigación realizada, se descartó a Nagios XI porque muchas empresas y usuarios comenzaron a migrar a Zabbix por el mal rendimiento que estaba presentando. De igual manera con Pandora FMS, la herramienta tiene dos versiones una de licencia pagada y otra de código abierto lamentablemente la de código abierto no recibe el soporte adecuado para la implementación en pequeñas y medianas empresas, además que en foros especializados recibían muchas quejas cuando se añaden muchos hosts. ZABBIX tiene un mejor manejo de la información en su base de datos para guardar datos históricos y con sus requerimientos mínimos de instalación puede llegar a manejar 100 hosts en su consola, por esta razón es el sistema que mejor se acopló a los objetivos de la empresa y sobre todo buscaban un sistema de código abierto ya que no se tiene un presupuesto asignado para el monitoreo de infraestructura de TI porque la mayoría de las empresas dentro de ecuador no lo ven como algo necesario, pero si realizan un análisis de costo, tiempo y duplicidad de funcionas dentro del personal encargado se pudo observar que el beneficio es mucho más alto que el costo de implementación.

- Los parámetros críticos dentro de una empresa pueden variar dependiendo del giro de negocio que tenga dicha empresa. Por lo general manejan la misma arquitectura de red para la conectividad de la infraestructura de TI. Por esta razón los fabricantes publican en su documentación las recomendaciones para el monitoreo de sus dispositivos con el objetivo de alargar su vida útil. La empresa POFASA estableció los objetivos a cumplir con el sistema de monitoreo y la infraestructura critica que forma parte esencial de sus operaciones. Como la empresa tiene equipos CISCO y HP en sus cuartos de datos de sus sucursales, se procedió a investigar los parámetros recomendados a monitorear por

parte de estos fabricantes. Obteniendo como punto de partida la tabla 1 del documento de tesis, esta tabla fue la guía de parámetros críticos a medir en el resto de los dispositivos y servicios de los diferentes fabricantes dentro de la infraestructura de TI. Dicha infraestructura se mantendrá monitoreada en tiempo real para garantizar su operatividad y disponibilidad con sus respectivos servicios.

- La implementación del sistema de monitoreo en la empresa POFASA se realizó sobre una máquina virtual en Linux dentro de un servidor en el cuarto de datos de su oficina matriz. El resultado permitió obtener una herramienta de alta importancia dentro de las funciones del área de TI porque cuenta con los siguientes beneficios: una consola general, notificaciones inteligentes a través de la configuración de parámetros de aceptación, herramienta multi plataforma, los tiempos de administración se reducen considerablemente y el uso de la red puede ser optimizado a través de los diferentes reportes que genera el sistema.

- El sistema de monitoreo seleccionado Zabbix, tiene un cuadro de control donde se puede observar los dispositivos y servicios de TI (host) añadidos a la consola de administración. Cuando un dispositivo es añadido a nuestra consola tarda alrededor de 30 minutos en mostrar nuestros primeros gráficos de monitoreo, la gran ventaja del sistema es tener en una sola pantalla y en un solo cuadro de control los parámetros críticos configurados por dispositivo. En las pruebas realizadas se pudo observar como el cuadro de control envía una alerta visual durante un incidente localizado sobre uno de nuestros dispositivos. Cuando el incidente es una desconexión se pudo observar la hora exacta de la perdida de conexión y la hora de reconexión, mostrando el intervalo de tiempo de afectación en las operaciones del dispositivo o servicio de TI.

- La generación de alertas por medios de comunicación como son correo electrónico, Microsoft Teams y Telegram permite la mejora continua de la infraestructura de TI porque se obtiene un estado en tiempo real de los diferentes incidentes de cada dispositivo o servicio. El sistema de alertas implementado envía un correo electrónico de manera automática al personal encargado de la infraestructura en el área de TI en caso de presentar un incidente o fallo dentro de la red interna de la empresa. A través del sistema el incidente es resuelto de manera rápida y no genera inconvenientes dentro de las labores del personal de la empresa.

- En el capítulo 3 se evaluó la satisfacción que tenía el personal con el sistema actual de monitoreo contra el sistema automatizado de monitoreo, donde los resueltos de las encuestas cambiaron de pésimo a excelente. De igual manera el tiempo de respuesta tuvo uno reducción de 4 horas a 30 minutos. Demostrando que un sistema de monitoreo tiene muchos beneficios dentro de una empresa porque ayuda a mitigar los riesgos y genera confianza con el personal del área de TI que tiene a cargo la infraestructura, mejorando la satisfacción sobre la resolución de incidentes.

4.2 RECOMENDACIONES

- Utilizar sistemas de monitoreo en la infraestructura de TI porque tiene los siguientes beneficios: prevención de problemas, ayuda en la toma de decisiones, ahorro de tiempo del personal de TI, prevención de pérdidas económicas y mejora del rendimiento de la red interna de la empresa.

- Actualizar o migrar el sistema de monitoreo a otro sistema operativo Linux que tenga soporte de actualización de parches por motivos de seguridad sobre la herramienta implementada. Ya que la empresa POFASA proporcionó una máquina virtual en CentOS el cual tuvo soporte hasta diciembre del 2021.

- Tener un buen manejo de comandos y del sistema operativo Linux, al ser un sistema de código abierto se necesita instalar librerías y herramientas como requisitos previos para la implementación del sistema Zabbix. Cuando se tiene un error en la instalación de requisitos previos, el sistema no inicia correctamente por lo cual no se puede continuar con su configuración.

- En la administración del sistema de monitoreo se recomienda crear nuevos usuarios y contraseñas robustas para mejorar la seguridad, ya que si un intruso ingresa a nuestro sistema puede tener acceso a los dispositivos monitoreados y cambiar la configuración o alterar su funcionamiento a través de los protocolos y agentes de comunicación utilizados en la implementación.

- Utilizar la plataforma Telegram para las alertas del sistema porque tiene un mejor rendimiento a diferencia del correo electrónico donde el cual puede tardar en llegar el

mensaje por el servicio que está configurado actualmente. Además, el área de TI siempre está pendiente de su teléfono por los reportes de incidentes de todas las áreas.

- Asignar a una persona para la administración del sistema de monitoreo que visualice de manera constante y en tiempo real todo lo que está ocurriendo con los dispositivos y servicios, además realizar informes del estado de cada uno de ellos, con el objetivo de aumentar la eficacia del sistema implementado.

5 REFERENCIAS BIBLIOGRAFÍCAS

[1] B. Cisneros, “IMPLEMENTACIÓN DE UN NUEVO SISTEMA DE MONITOREO EN GMD PARA AUMENTAR LA EFICACIA OPERATIVA”, 2016. Consultado: sep. 13, 2022. [En línea]. Available: https://repositorio.usil.edu.pe/items/8c6b03f2-6b03-4cc5-add2-32c7757048f5

[2] V. Arrebola, “Sistema Monitorización de Servidor Linux”, p. 73, 2010.

[3] J. Alfaro, “Metodología Para La Gestion De Riesgos Ti Basada En Cobit 5”, Instituto Tecnológico de Costa Rica, 2017. [En línea]. Available: https://repositoriotec.tec.ac.cr/bitstream/handle/2238/11060/metodologia_gestion_riesgos_ti_basada_cobit5.pdf?sequence=1

[4] Pollo Favorito SA, “Infraestructura Pofasa”, 2019. www.pofasa.com (consultado sep. 13, 2022).

[5] M. Ortiz y A. Mori, “Influencia de la implementación de un sistema de monitoreo de infraestructura TI para gestionar las incidencias en la red LAN del Hospital Regional de Cajamarca”, 2017. [En línea]. Available: http://repositorio.upagu.edu.pe/handle/UPAGU/278

[6] D. Garay, “Implementación De La Herramienta Centreon Para El Monitoreo De La Infraestructura De T.I. En La Empresa América Móvil Perú S.a.C”, 2018. [En línea]. Available: http://repositorio.autonoma.edu.pe/bitstream/AUTONOMA/678/1/GARAY CAPCHA%2C DAVID ENRIQUE.pdf

[7] OGC, “Itil V3 Continual Service Improvement (Cst)”, en *Service Management*, 3a ed., vol. 34, núm. 19, APMG Service Desk, 2007, pp. 1–396.

[8] S. Ríos, “ITIL v3 Manual Íntegro”, *B-able*, p. 101, 2014, [En línea]. Available: http://www.biable.es/wp-content/uploads/2014/ManualITIL.pdf

[9] M. Sokovic, D. Pavletic, y K. KERN Pipan, “Quality Improvement Methodologies”, vol. 65, núm. 6, pp. 1283–1296, 2010, doi: 10.1016/j.pcl.2018.07.011.

[10] K. A. Maduranga, “Investigate Windows Management Instrumentation (WMI) Attacks in Windows Operating Systems A dissertation submitted for the Degree of Master of Science in Information Security”, 2016. [En línea]. Available: https://dl.ucsc.cmb.ac.lk/jspui/bitstream/123456789/3905/1/2013mis016.pdf

[11] D. Mauro y K. Schmidt, *Essential SNMP*, 2a ed. oreilly.com, 2005.

[12] N. S.C., *Network Basic, ICMP*. Noite.pl, 2020.

[13] Cisco Systems Inc., “Best Practices for MonitoringCisco Unified Communications ManagerCisco Unified Communications Managerwith Cisco Unified Operations Managerwith Cisco Unified Operations Manage”, 2009.

[14] J. GARCIA y C. ROA, “DISEÑO DE UNA HERRAMIENTA DE MONITOREO Y CONTROL DE SERVIDORES UTILIZANDO COMO EJE PRINCIPAL CACTI. APLICADO A UNA PYME MEDIANA”, 2020. [En línea]. Available: https://repository.ucc.edu.co/bitstream/20.500.12494/16571/3/2020-Herramienta_monitoreo_servidores.pdf

[15] Gartner Inc, “IT INFRASTRUCTURE MONITORING TOOLS REVIEWS AND RATINGS”, 2021. https://www.gartner.com/reviews/market/it-infrastructure-monitoring-tools (consultado ene. 01, 2022).

[16] Station IT Central, “Peer Awards”, 2021. https://www.peerspot.com/categories/network-monitoring-software (consultado ene. 01, 2022).

[17] Zabbix LLC, “Zabbix Documentation 5.0”, 2020. https://www.zabbix.com/documentation (consultado feb. 01, 2022).

[18] Pandora FMS, “PandoraFMS Documentation”, 2021. https://pandorafms.com/manual/en/documentation/start (consultado feb. 02, 2022).

[19] N. Enterprises, “NagiosXI User Guia”, 2021. https://assets.nagios.com/downloads/nagiosxi/guides/user/ (consultado feb. 02, 2022).

[20] Apache Software Foundation, “Apache JMeter™”. https://jmeter.apache.org/index.html (consultado feb. 02, 2022).

6 ANEXOS

A MODELO DE ENCUESTA

B CAPTURAS DE PANTALLA DE UMBRAL DE PRUEBAS

A MODELO DE ENCUESTA

1. ¿Cuál es el tiempo promedio de atención de incidentes de infraestructura TI?

- 30 min o menos
- 1 hora
- 4 horas
- 8 horas o más

2. ¿Cuánto tiempo lleva en promedio identificar el dispositivo o servicio de TI que está causando el incidente?

- 30 min o menos
- 1 hora
- 2 horas
- 6 horas o más

3. ¿Cómo calificaría el método actual para monitorear la infraestructura de TI de la empresa?

- Excelente
- Bueno
- Regular
- Malo
- Pésimo

4. ¿Confía en el método actual para monitorear la infraestructura de TI de la empresa?

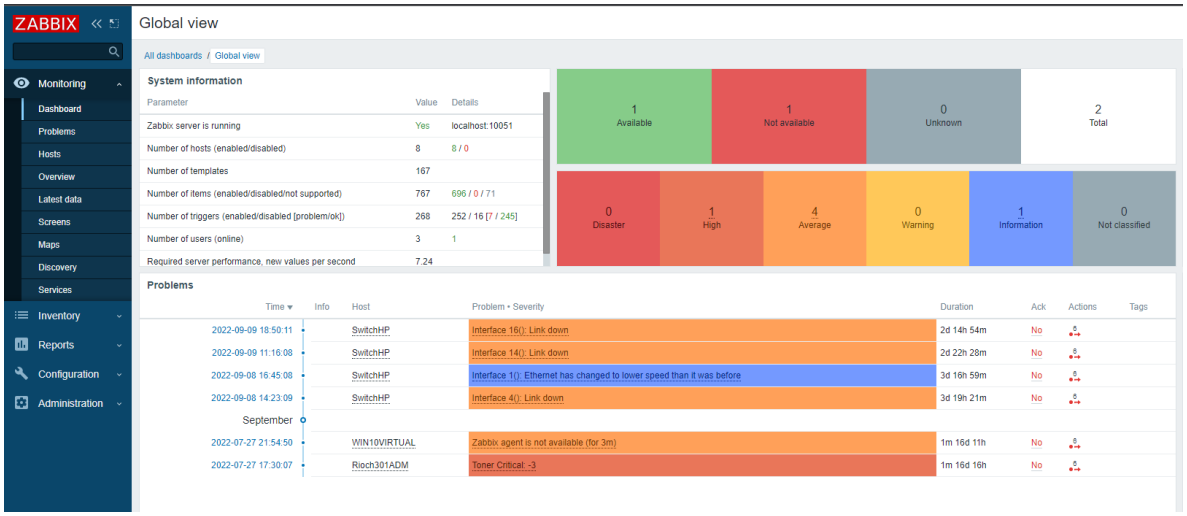
- Nunca
- A veces
- Casi siempre
- Siempre

5. ¿Cuántas quejas se realizan cada semana sobre caídas del servicio y mal funcionamiento de los dispositivos en la red?

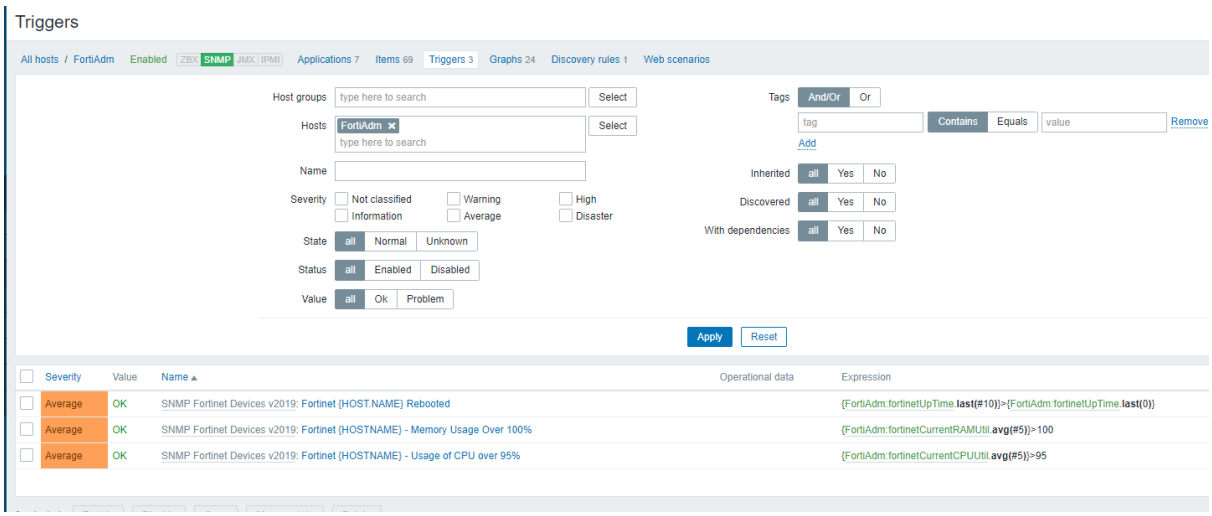
- 1
- 2
- 3
- 4
- 5 o más

B CAPTURAS DE PANTALLA DE UMBRAL DE PRUEBAS

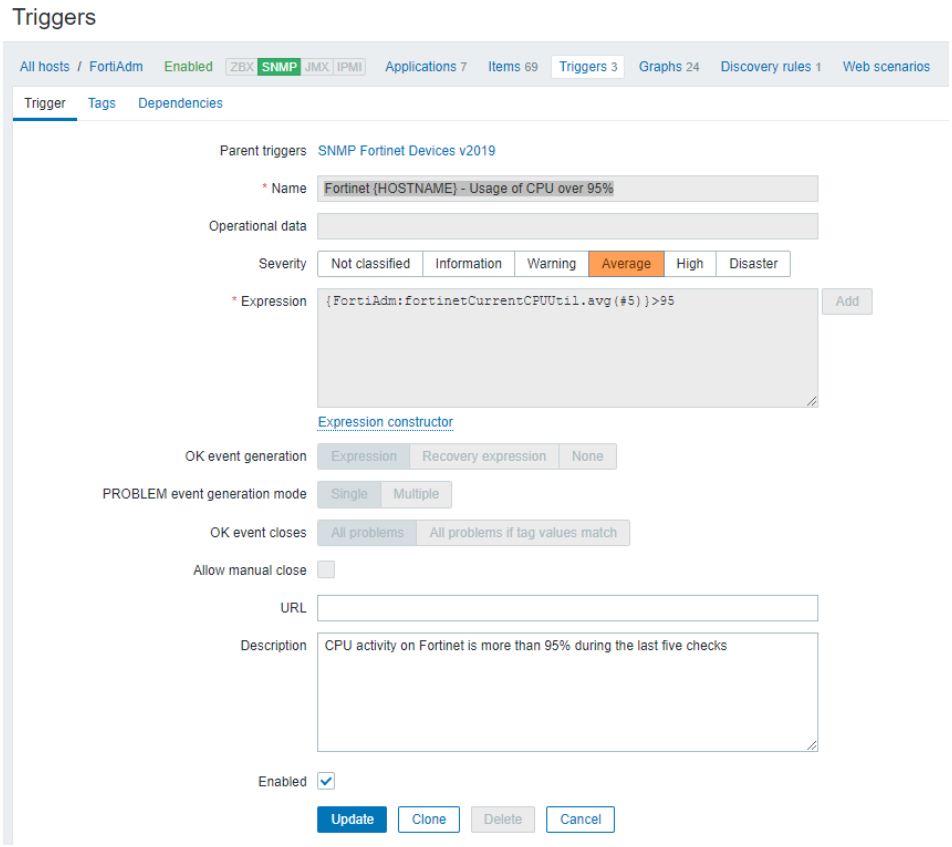
- Estado del cuadro de control Zabbix, con alertas de diferentes colores que demuestran el grado o tipo de severidad del incidente.



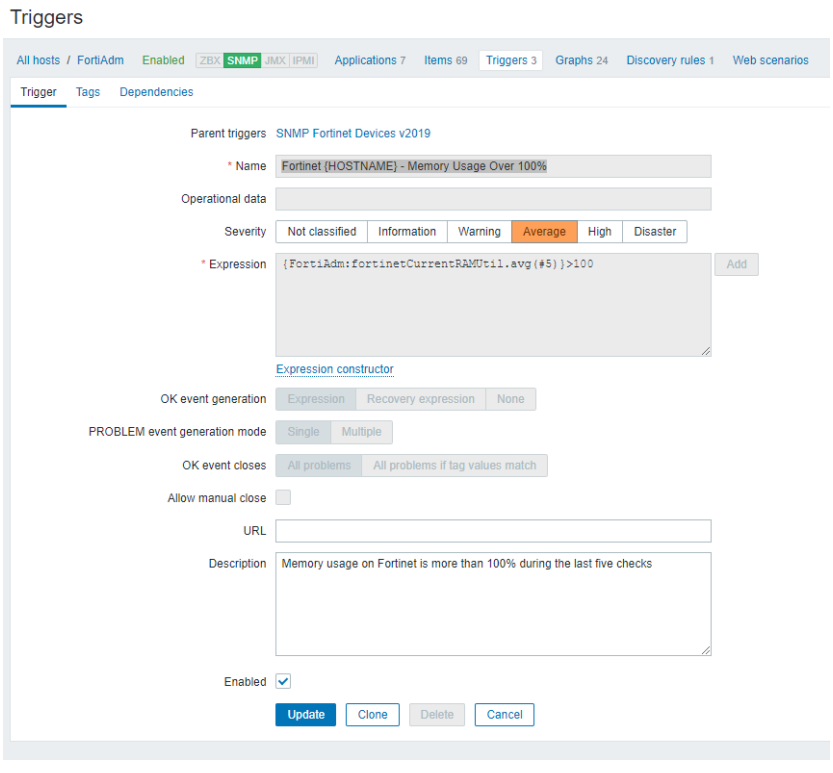
- Disparadores de alertas para Firewall Fortinet. Se muestra en base a la tabla de parámetros de monitoreo: estado de energía, memoria usada y cpu utilizado.



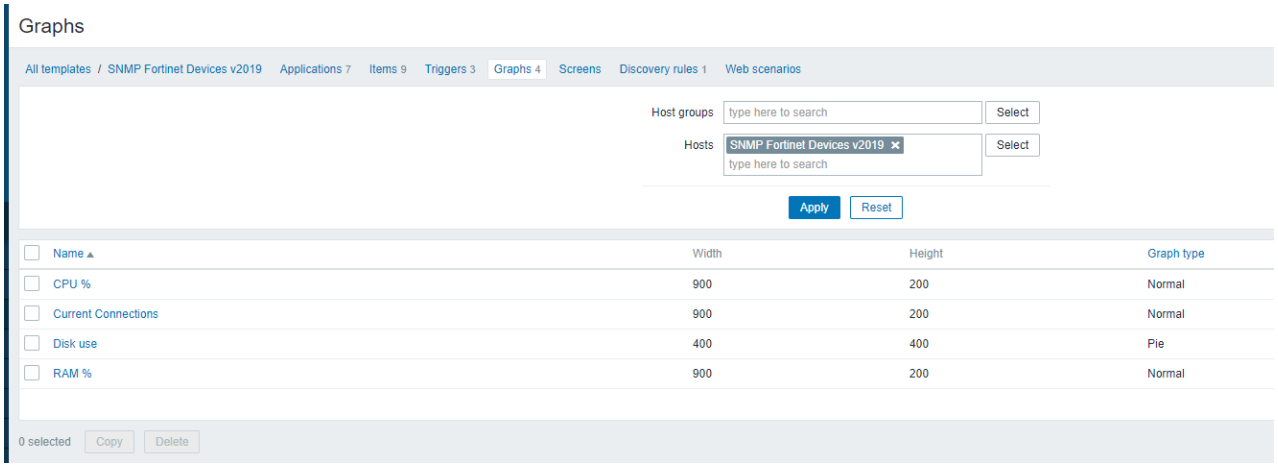
- Los disparadores pueden ser modificados su umbral de tolerancia para levantar un incidente con alerta. Por ejemplo, en el campo “Expression” se puede observar la expresión que delimita el porcentaje de CPU utilizado para levantar una notificación y de igual manera el grado de severidad establecido.



- De igual manera se pudo observar con el umbral de la memoria RAM utilizada. Se puede establecer diferentes umbrales en cada parámetro a monitorear dependiendo de la importancia que tenga dentro de la empresa el control de dicho recurso.



- Gráficos de parámetros críticos monitoreados en Firewall.



- Resumen de incidentes notificados de un switch monitoreado en cuadro de control.