Universidad Nacional Pedro Ruiz Gallo

Facultad de Ingeniería Civil, Sistemas y Arquitectura

Escuela Profesional de Ingeniería de Sistemas

TRABAJO DE SUFICIENCIA PROFESIONAL

Sistema de monitoreo de la infraestructura de TI para gestionar incidentes de una empresa del rubro tecnológico

Para obtener el Título Profesional de:

INGENIERO DE SISTEMAS

Luis Ricardo Moran Chozo

Autor

Mag. Ing. Roberto Carlos Arteaga Lora

Asesor

LAMBAYEQUE – PERU

2024

Universidad Nacional Pedro Ruiz Gallo

Facultad de Ingeniería Civil, Sistemas y Arquitectura

Escuela Profesional de Ingeniería de Sistemas

TRABAJO DE SUFICIENCIA PROFESIONAL

Sistema de monitoreo de la infraestructura de TI para gestionar incidentes de una empresa del rubro tecnológico

Para obtener el Título Profesional de:

INGENIERO DE SISTEMAS

Aprobado por los miembros del Jurado:

Dr. Ing. Alberto Enrique Samillan Ayala

Presidente

Dr. Ing. Regis Jorge Alberto Diaz Plaza

Secretario

Ing. Cesar Augusto Guzman Valle

Vocal

LAMBAYEQUE – PERU

2024

Dedicatoria

A Dios, por brindarme salud, sabiduría y guiarme en mi camino profesional, además de ayudarme a no caer para lograr mis metas.

A mis padres Ricardo e Iraida por ser el pilar fundamental en mi vida y educación, por su incondicional apoyo, enseñanzas y valores brindados a lo largo de mi vida.

A mi hermana Rosa Katherine, por impulsarme a lograr este objetivo.

A mi novia Mixi, por su apoyo, comprensión y motivación para salir adelante.

A mi Abuelita Iraida Inoñan (QEPD), por inculcar los buenos valores, principalmente la humildad, ya que gracias a ello me ha permitido llegar lejos.

Agradecimientos

A Dios por brindarme salud para poder terminar mi carrera y mis proyectos.

A mis padres por estar presentes brindando el apoyo incondicional de inicio a fin de mi carrera y el desarrollo del proyecto.

A la Empresa donde trabajo, por brindarme la oportunidad de implementar el proyecto.

A mi colega Daniel Hinojo, por la orientación en el proyecto.

Al Ing. Roberto Arteaga, por apoyarme en la asesoría, quien con sus conocimientos y experiencia hicieron posible el logro de esta meta.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Para las empresas de hoy, que están basadas en tecnologías de información y comunicaciones, el recuperarse de una interrupción en su operación normal, a causa de un incidente o fallo, conlleva a un impacto económico, dado que no permite a los clientes realizar como se debe sus transacciones comerciales en la empresa, con el consiguiente impacto o daño a la imagen. La empresa objeto del presente trabajo tenía como problemática a la misma que de manera general se acaba de describir. Frente a esta situación, se decidió solucionar esto con la implementación de la herramienta de monitoreo, la cual fue seleccionada entre las más importantes, seleccionando a la herramienta Zabbix, que cuenta con excelentes funcionalidades, sumando a esto, es software libre. Además, se le ofreció al cliente el soporte de este sistema de gestión de incidentes, migrando de la herramienta anterior a Zabbix para todos los servicios y dispositivos que conforman a la infraestructura tecnológica de la empresa. Los resultados obtenidos muestran como significativa la mejora obtenida, en términos de límites de tiempo para la solución del problema y reacción temprana al incidente.

Palabras Clave: tecnología, incidente, transacciones, impacto, Zabbix, software libre.

ABSTRACT

For today's companies, which are based on information and communications technology, recovering from an interruption in their normal operation, due to an incident or failure, leads to an economic impact, since it does not allow customers to perform as expected. owes its commercial transactions to the company, with the consequent impact or damage to the image. The company that is the subject of this work had the same problems as those generally just described. Faced with this situation, it was decided to solve this with the implementation of the monitoring tool, which was selected among the most important, selecting the Zabbix tool, which has excellent functionalities, adding to this, it is free software. In addition, the client was offered the support of this incident management system, migrating from the previous tool to Zabbix for all the services and devices that make up the company's technological infrastructure. The results obtained show the improvement obtained as significant, in terms of time limits for solving the problem and early reaction to the incident.

Keywords: technology, incident, transactions, impact, Zabbix, free software.

INTRODUCCIÓN

Las empresas se mantienen en un mercado caracterizado por ser cada vez más competitivo, donde el cliente tiende a ser exigente. Las tecnologías de información (en adelante TI), han demostrado ser una potente herramienta de gestión de la información empresarial. Tomando en cuenta por un lado las oportunidades del mercado y las ventajas de la tecnología, las empresas deciden apoyarse fuertemente en activos de TI, para el soporte de sus operaciones y de esta manera obtener una ventaja competitiva, que les permita obtener una rentabilidad financiera, que haga viable su sostenibilidad en el tiempo.

La introducción de la tecnología en las empresas, pasó por un proceso que partió desde su adquisición para automatizar tareas y se dirigió con el paso del tiempo hacia la integración de la empresa. El mercado se dirige hacia Internet y la empresa asegura su presencia en esta importante red de información. Los empresarios adquieren tecnología para implementar su infraestructura tecnológica, mediante la cuál se ofrecen bienes y servicios a los clientes.

La infraestructura de TI, incluye la adquisición de equipos servidores, que serán utilizados en los diferentes servicios de red a implementar para clientes internos y externos. También, incluye medios de transmisión, equipos de interconexión como: switch, modem, router, access point. Toda esta infraestructura va acompañada de una arquitectura de red de datos como es TCP/IP, donde destacan diferentes protocolos de comunicación.

Es frecuente escuchar la “caida” del sistema, esto se podría deber a diferentes razones atribuibles principalmente a la falta de un área de TI en la empresa o si existe, esta no cuenta con el personal profesional que requiere. Este punto es de vital importancia, porque es conocido que la infraestructura de TI, puede estar muy bien diseñada e implementada. Sin embargo, durante su operación, puede presentar fallos que afecten su rendimiento, fallos que aunque no tenga mucha frecuencia, dependiendo de la criticidad del negocio, reflejan pérdidas significativas a la empresa.

Los incidentes en la infraestructura de TI, requieren que sean gestionados oportunamente, de tal manera que no afecte la disponibilidad ni el rendimiento del servicio. Existen diferentes herramientas de software propietario y libre, que cubren este requerimiento tan necesario en las empresas.

Frente a este panorama, surgen empresas de diferente envergadura, que dan soporte tecnológico a empresas que quisieran estar concentradas en sus procesos principales, en lo que se denomina outsourcing. Destacan en este rubro empresas como Amazon, que ofrecen

servicios de alta calidad a empresas de diferente rubro, como son universidades, colegios, institutos, empresas comerciales, etc. También, es importante mencionar a medianas empresas que ofrecen servicios de administración de servidores y de la seguridad de la información.

El presente trabajo de suficiencia profesional, atendiendo a esta necesidad, presenta la implementación de un sistema de monitoreo de la infraestructura de TI, para gestionar incidentes de una empresa del rubro tecnológico de la ciudad de Chiclayo. Este trabajo, se organizó de la siguiente manera: definición del problema, objetivos, limitaciones del informe, justificación del informe.

I. DEFINICIÓN DEL PROBLEMA

La gestión de la infraestructura de TI de la empresa, se realizaba con una herramienta de monitoreo, que estaba mal configurada y tenía limitadas opciones de configuración, esta aplicación fue implementada hace cuatro años, no tenía mantenimiento, no estaba cumpliendo con el adecuado monitoreo a los diferentes equipos que forman parte de la infraestructura tecnológica de la empresa. Además, los recursos del equipo donde fue instalado y configurado esta herramienta de software, ya no hacían posible aumentar dispositivos a monitorear, el servicio de monitoreo se saturaba y la página no respondía por muchas transacciones. Debido a esta situación, se reportaban muchos incidentes en la red de datos, que afectan a los servicios tecnológicos y por ende a los procesos de la empresa, estos incidentes no fueron detectados oportunamente (se notificaron por correo electrónico) y por lo mismo no pudieron ser atendidos, lo cual causaba muchas quejas al área de tecnologías de información de la empresa.

El crecimiento de las operaciones de la empresa, y la importancia de asegurar un buen servicio a sus clientes, hizo urgente la necesidad de implementar un sistema de monitoreo de la infraestructura tecnológica en la empresa. Los requerimientos de este sistema fueron: robustez, alineado a los objetivos de corto, mediano y largo plazo de la empresa, basado en software Open Source. El sistema sería para monitorear los servicios críticos, con la correspondiente visibilidad en tiempo real, de todos los recursos que conforman la infraestructura tecnológica, con notificaciones, para asegurar la disponibilidad permanente de los servicios, y una respuesta inmediata a cualquier incidente que se presente en la infraestructura de TI.

Identificada la problemática y captados los requerimientos del cliente, se le ofreció los servicios profesionales de un empresa que cuenta con personal experto en temas como: servicios de administración de redes de datos, de servidores, de sus dispositivos de red, soporte con mesa de ayuda, ciberseguridad, administrar desde data center, personal administrador de redes y servidores, para gestionar los incidentes en la infraestructura de red de datos, con el software Zabbix, que tiene todo lo que la empresa necesita, que se instalaría en un servidor de mayores recursos tecnológicos y virtualizado

La solución implementó la administración de 100 servidores (sus recursos), de aplicaciones, sitios, redes, servidores, certificados (vencimiento) y en el caso de la notificación, sería por correo electrónico y Telegram sincronizado.

II. OBJETIVOS

OBJETIVO GENERAL

- Implementar un sistema de monitoreo de la infraestructura de TI, para gestionar los incidentes de una empresa del rubro tecnológico.

OBJETIVOS ESPECÍFICOS

- Identificar los dispositivos y servicios principales de la infraestructura de TI de la empresa cliente.
- Seleccionar herramienta de monitoreo de código libre que se adecue a las necesidades de la infraestructura de TI, de la empresa cliente.
- Implementar la herramienta de monitoreo seleccionada, incorporando el sistema de alertas ante la presencia de fallos o posibles fallas en la infraestructura de TI de la empresa cliente.
- Evaluar el desempeño del sistema de monitoreo actual en relación a la gestión de incidentes.

LIMITACIONES DEL INFORME

A causa de la data sensible, el estudio presentará información general de la empresa, no se requirió datos propios como el nombre ni datos sobre sus operaciones.

El presente trabajo de investigación sólo considera la implementación del sistema de gestión de incidentes existentes en la infraestructura de TI de la empresa.

Los datos utilizados corresponden a información de carácter público y que no afecta la seguridad de la información de la empresa.

Delimitación Espacial

El presente trabajo de suficiencia profesional, se realizó en el área de tecnologías de información de la empresa objeto de interés.

Delimitación Temática

El presente trabajo de suficiencia profesional, comprende la gestión de incidentes en redes de datos de empresas.

JUSTIFICACIÓN DEL INFORME

Práctica

Para todos aquellos que quisieran comprender el proceso de implementar un sistema de gestión de incidentes y que les sirva de base para trabajos de mejora y porque no investigaciones en esta línea.

III. FUNDAMENTO TEÓRICO

MODELOS DE LAS REDES DE DATOS

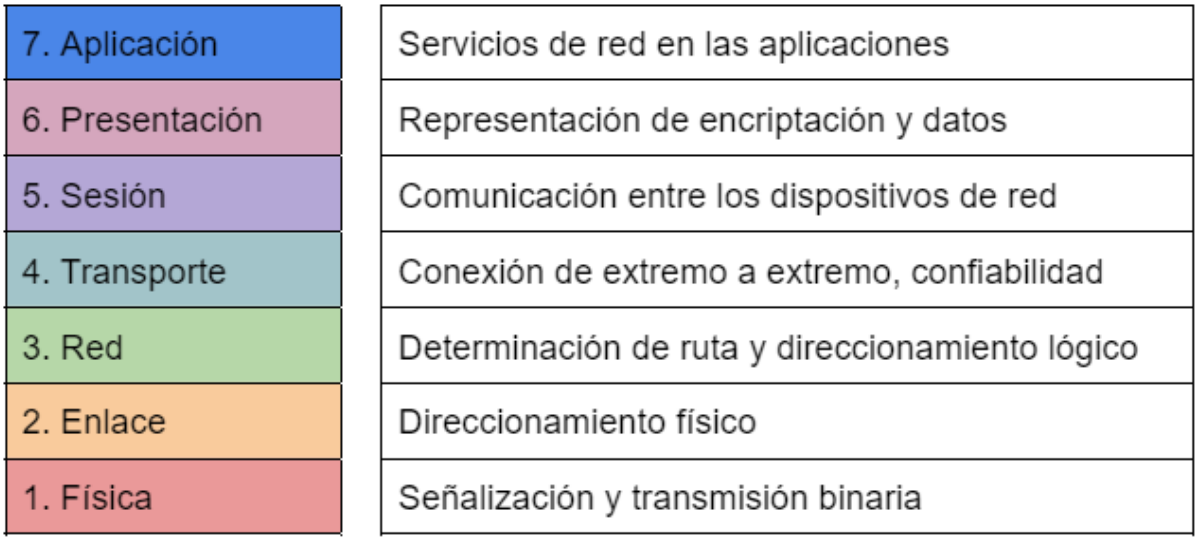
Las redes de datos se entienden mejor si son vistas, desde un modelo de referencia como es OSI; pero ya en su implementación desde la arquitectura TCP/IP, este facilita la interconexión entre cualquier equipo o tipo de red, al margen de la tecnología que se emplee.

MODELOS OSI

Producto del acuerdo entre fabricantes de tecnología surge el modelo de referencia OSI, al cumplir con requerimientos comunes en hardware y software, permite la interoperabilidad entre las diferentes tecnologías multifabricante (ARIGANELLO, 2016).

Las siglas del modelo OSI quiere decir interconexión de sistemas abiertos, representa al modelo en capas, cada una de ellas con su propia funcionalidad, esto permite que un programador trabaje en su área sin tener que depender de otras áreas. Las 7 capas (Aplicación, Presentación, Sesión, Transporte, Red, Enlace de Datos y Física) del modelo OSI, se aprecian en la siguiente figura.

Figura 1
Modelo OSI



Nota: Las siete capas del modelo OSI (ARIGANELLO, 2016).

- **Aplicación,** no comparte servicio con capas superiores, dado que es la capa más superior, emplea la funcionalidad de las capas inferiores para interactuar con el usuario de aplicaciones. Entre sus protocolos, destacan los que hacen posible contar con acceso remoto y correo electrónico.
- **Presentación,** en esta capa ve aspectos relacionados con asegurar que los datos o formatos de archivos enviados desde la capa de aplicación del emisor sean leídos por la capa de aplicación del sistema destino.
- **Sesión,** en esta capa se administran las comunicaciones entre entidades de la capa de presentación.

- **Transporte**, en esta capa se da la comunicación entre procesos, el control de flujo y la corrección de errores. También, los datos se manejan como segmentos, que se identifican con un número o puerto, que hace referencia a la aplicación.

- **Red,** en esta capa se tiene como principal funcionalidad al direccionamiento lógico, el enrutamiento de paquetes, empleando protocolos para esto.

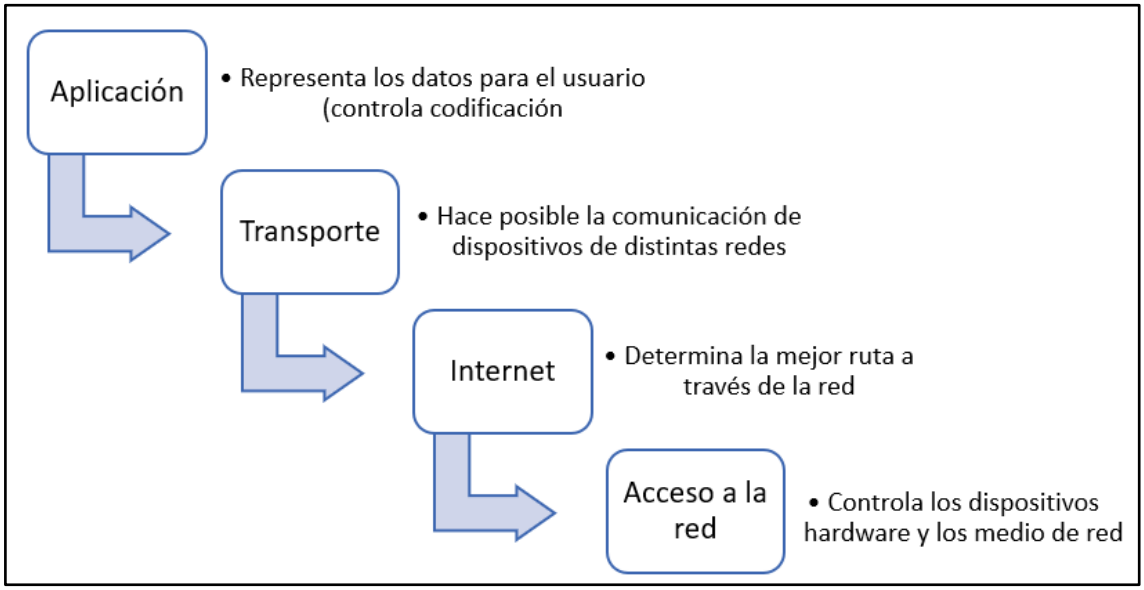
- E**nlace de datos,** en esta capa se trabaja con tramas, entre la capa emisora y receptora.

- F**ísica,** en esta capa se define toda la funcionalidad relacionada con aspectos eléctricos, electrónicos, su codificación para transmisión.

ARQUITECTURA TCP/IP

Su origen se remonta a los años sesenta, el Departamento de Defensa de EE.UU, necesitaba transmitir confiablemente datos a un destino cualquiera de red (Boronat & Montagud, 2013), esta arquitectura es el cimiento de Internet y está estructurada en cuatro capas: aplicación, transporte, Internet y acceso a red. En la figura 2, se distingue con claridad estas capas.

Figura 2
Arquitectura TCP/IP



Nota: Direccionamiento e interconexión de redes basado en TCP/IP (Boronat & Montagud, 2013)

Aplicación, en esta capa, se distingue a los siguiente protocolos: SNMP, FTP, Telnet y DHCP.

Transporte, en esta capa se atiende los requerimientos de la capa superior (aplicación), hace posible el envío de datos sin importar su contenido. Los protocolos principales de esta capa son: TCP (orientado a conexión) y UDP (no orientado a la conexión).

Internet, en esta capa, se ven aspectos de enrutamiento (toma en cuenta: el ancho de banda, cantidad de saltos, retardos, entre otros). En cuanto a protocolos, en esta capa destaca IP (IPv4 e IPv6).

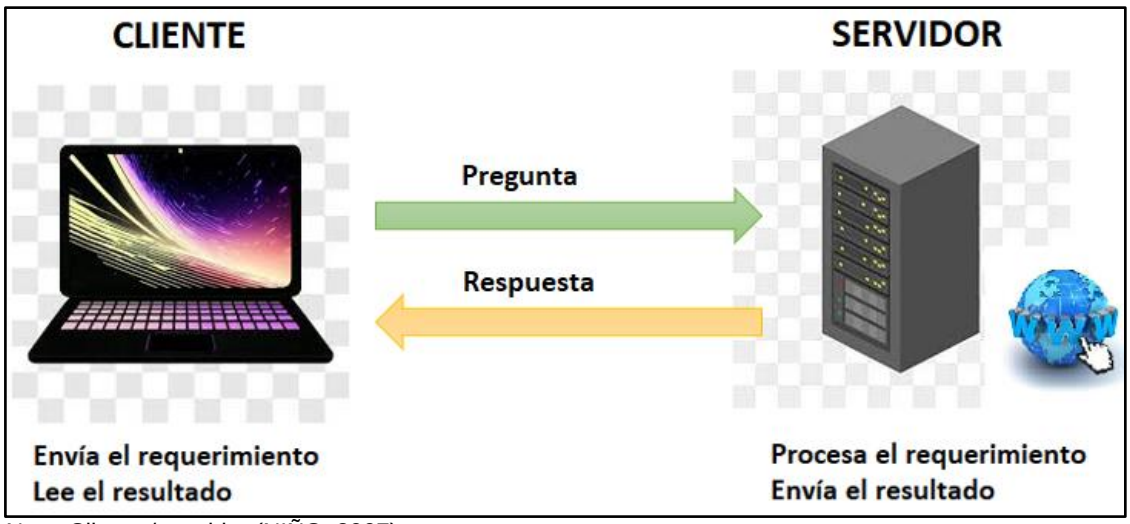
Acceso a red, en esta capa, se definen las tramas, en la comunicación por pares. La trama que más se emplea es la de tecnología Ethernet.

MODELO CLIENTE SERVIDOR

Aquí, el cliente envía un mensaje donde solicita un servicio específico a un servidor (solicita), enviando uno o más mensajes con la respuesta (responder) (Ver figura 3).

El proceso de cliente, permite al usuario preparar los requerimientos y entregarlos al servidor, esto se conoce con el término front-end. El cliente administra funciones como: manipular y desplegar los datos IGU (interfaz gráfica de usuario). El proceso servidor, atiende a varios clientes que solicitan algún recurso que administra. Esto se conoce como back-end. Es usual ver al servidor, administrar funciones que tienen relación con reglas de negocio y recursos de datos (TANENBAUM & WETHERALL, 2012).

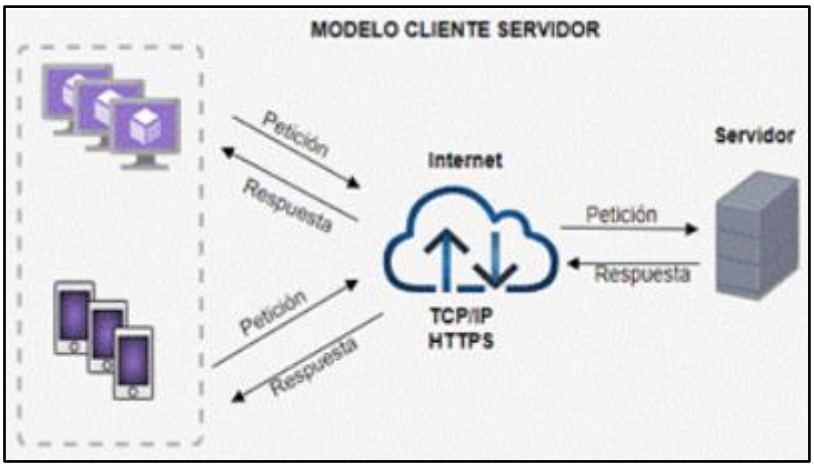
Figura 3
Modelo cliente/servidor



Nota: Cliente / servidor (NIÑO, 2007).

En la figura 4, se muestra otra representación del modelo cliente servidor.

Figura 4
Modelo cliente servidor



Nota: Protocolos TCP/IP de Internet (ESTRADA, 2004)

GESTIÓN DE INCIDENCIAS

Las fallas o caídas suelen estar presentes en las organizaciones, sino se está preparado, causan daño financiero, por esto se tiene que gestionar en la empresa las incidencias

Según (VAN BON et al., 2008, p.140), se entiende a la gestión de incidencias como el proceso que incluye a cualquier fallo o dificultad que fue reportado por algún usuario o detectado de manera automática por la herramienta de monitoreo de la empresa.

Según (GÓMEZ, 2012, p. 263), gestionar incidentes comprende, a los pasos a seguir cuando sucede una interrupción no planificada o la calidad del servicio de tecnología de información (TI), se ve mermada. De acuerdo a ITIL (biblioteca de infraestructura de TI), una deficiencia en el funcionamiento de un elemento, es considerada una incidencia.

Se puede coincidir con (LÓPEZ & VÁSQUEZ, 2016, p.52), en el sentido que, la gestión de incidencias tiene por propósito el resolver de forma rápida y eficaz cualquier incidente que interrumpa al servicio.

Finalmente, gestionar un incidente consiste en hacerse cargo de cualquier evento que de forma parcial o total interrumpa el trabajo de los trabajadores de TI de la empresa, para detectar estos fallos se requiere herramientas que hagan monitoreo e informen al trabajador de TI. Todo esto tiene que realizarse lo más rápido posible para así evitar la caída total del servicio (ORELLANA & ORTIZ, 2022).

INCIDENCIAS

Diferentes inconvenientes ocurren durante el funcionamiento de una organización, algunos de ellos más urgentes que los otros, esto se refleja en su impacto en el negocio, frecuentemente no se distingue por parte del usuario final si son realmente un problema. Ante este panorama, se puede definir a un incidente, como aquella interrupción no prevista o cuando ocurre una merma en la calidad del servicio de TI (VAN BON et al., 2008, p. 140). Para (GÓMEZ, 2012, p. 266), son aquellas incidencias que ocurrieron, pero que es posible vuelvan a suceder.

Se puede decir, a manera de conclusión que en las empresas, es probable que sucede de manera no prevista una interrupción, que cause un fallo parcial o total en el servicio, su solución requiere frecuentemente dedicación y tiempo, debido a que no son recurrentes e incluso casuística nueva (ORELLANA & ORTIZ, 2022).

LÍMITES DE TIEMPO

Cuando el tiempo de espera para solucionar un problema reportado por un usuario de la empresa es largo, es posible que no estén definidos los límites de tiempo de espera, en estos casos (VAN BON et al., 2008, p. 159), indica que cuando en el límite de tiempo no se pueden atender los incidentes o peticiones, estos deben ser escalados para su correcta solución. También, recomienda fijar límites de tiempo adecuados en cada una de las fases de resolución de problemas, atendiendo acuerdos de nivel de servicio y a los contratos de soporte.

Finalmente, se puede precisar que el tiempo de duración máxima, para dar solución a un incidente presentado, o atender peticiones de los usuarios, dentro del ciclo de vida del servicio, debe ser cumplido, ya que de esta forma se asegura un servicio de calidad. Esto teniendo en cuenta la existencia de acuerdos o contratos pactados, que se establecen con los proveedores que dan soporte al servicio (ORELLANA & ORTIZ, 2022).

MODELO DE INCIDENCIAS

Según (VAN BON et al., 2008, p. 141), los procesos deben tener un modelo de incidencias que oriente los pasos que se deben cumplir en su ejecución para que sea de la manera correcta y dentro de los límites de tiempo establecidos, evitando así interrupciones del servicio. Para (MÁLAGA, 2016, p. 12), un modelo de incidencia tiene definida la secuencia de pasos necesarios para gestionar al proceso que atiende una incidencia específica (ORELLANA & ORTIZ, 2022).

IMPACTO

Según (VAN BON et al., 2008, p. 140), un impacto “es el efecto de una incidencia sobre los procesos de negocio”. Para (GÓMEZ, 2012, p. 81), "El impacto en el negocio se relaciona con los objetivos de negocio, siendo el motivo para que se tenga en cuenta iniciativas de gestión del servicio". Finalmente, para (ORELLANA & ORTIZ, 2022), el impacto está dado por lo que afecta de manera positiva o negativa, tiene una causa que lo origina. En la gestión de incidencias, es el alcance que tiene el daño, que causa el fallo manifestado, puede afectar a cierta cantidad de personas de la empresa, les impide continuar con sus funciones diarias.

URGENCIA

Según (VAN BON et al., 2008, p. 140), la urgencia es determinar el tiempo que se tiene hasta que el impacto de la incidencia sobre el proceso de negocio sea significativo. Para (GÓMEZ, 2012, p. 42), la importancia de la urgencia radica en que basándose en el impacto de la incidencia sobre el negocio, la urgencia ayuda en la asignación de una prioridad a la ocurrencia de una incidencia o problema. Finalmente, para (ORELLANA & ORTIZ, 2022), la urgencia es que tan pronto debe atenderse la incidencia que sucedió, es conveniente siempre evitar llegar a una urgencia crítica ya que la consecuencia en un servicio caído.

PARÁMETROS CRÍTICOS DE MONITOREO

Aquellos elementos (software y hardware) que conforman la infraestructura tecnológica de la empresa, que cuando cambian de estado causan impactos que son significativos cuando se quiere alcanzar los objetivos de la empresa. Es importante permanentemente tenerlos identificados y medirlos ya que son muy esenciales en el funcionamiento correcto de la empresa (ORTIZ & MORI, 2017).

La selección de parámetros de monitoreo tiende a cambiar, esto depende de los tipos de componentes que constituyen la infraestructura de TI de la empresa. Sin embargo, casi siempre estos parámetros son comunes entre los dispositivos de TI; se puede mencionar a uso de la memoria de almacenamiento, uso de la tarjeta de red, del procesador, el estado del sensor de temperatura, etc. En la Tabla 1 se muestran los parámetros críticos de monitoreo:

Tabla 1
Parámetros críticos de monitoreo

Parámetros		Descripción
Sistema	1.	Utilización de la memoria RAM
	2.	Uso del procesador
	3.	Uso del disco duro
Entorno	1.	Estado del sensor de temperatura
	2.	Estado del sistema de suministro de energía
	3.	Estado del ventilador
Red	1.	Utilización de las interfaces de red
	2.	Tiempo de respuesta
	3.	Interconectividad entre los dispositivos

Nota: (ORTIZ & MORI, 2017)

Por esta razón, el propósito de los parámetros críticos de monitoreo sería asegurar un rendimiento óptimo de los elementos de la infraestructura de TI, estos indicadores deben ser medibles, para que quienes tienen a cargo el monitoreo de red en la empresa, puedan definir lineamientos que sean adecuados para la detección y creación de alertas debido a eventos fuera de rangos predefinidos a fin de hacer posible la toma de acciones que coadyuven a su corrección.

PARÁMETROS CRÍTICOS DE MONITOREO DE UN SWITCH

El switch, es un dispositivo que hace posible la interconexión de varios dispositivos en una red de datos. El hecho de que este dispositivo presente una falla, termina afectando a todos los usuarios conectados a la red de datos de área local de la empresa. Por esta razón, cualquier fallo o incidencia debe ser identificada a tiempo, para que de esta forma se eviten situaciones problema más grandes. A continuación, se presentan los parámetros críticos de monitoreo para el switch:

Tabla 2
Parámetros críticos de monitoreo de un switch

Parámetros	Descripción
Red	1. Asequibilidad del switch 2. Asequibilidad de los puertos del switch 3. Uso del ancho de banda por puerto del switch

Nota: (ORTIZ & MORI, 2017)

PARÁMETROS CRÍTICOS DE MONITOREO DE UN ROUTER

El router es un dispositivo que hace posible el enrutamiento de los paquetes de datos, haciendo posible la interconexión de diferentes redes de datos. A diferencia del switch, es posible contar con puertas de acceso a Internet. Dentro de la infraestructura tecnológica cumple un rol importante, por esta razón sus parámetros críticos tienen que ser monitoreados. A continuación, se presentan los parámetros críticos de monitoreo para el router:

Tabla 3
Parámetros críticos de monitoreo de un router

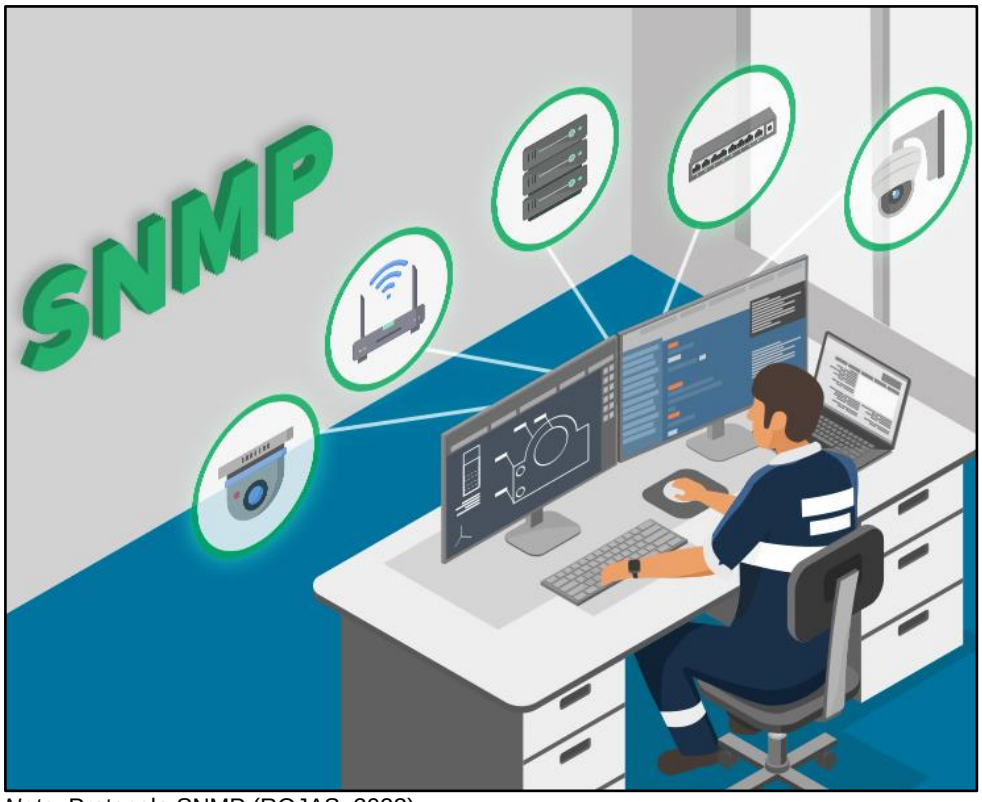
Parámetros	Descripción
Router	1. Asequibilidad del router 2. Asequibilidad de los puertos del router 3. Uso del ancho de banda por puerto del router

Nota: (ORTIZ & MORI, 2017)

PROTOCOLO SIMPLE PARA LA ADMINISTRACIÓN DE RED (SNMP)

El protocolo SNMP, está implementado a nivel de la capa de aplicación de la arquitectura TCP/IP, hace posible el intercambio de información de gestión de dispositivos de red, mediante SNMP es posible administrar dispositivos de red como: switch, router, firewall, UPS, servidores, impresoras en red IP, etc. (SOSSA, 2015).

Figura 5
Protocolo Simple de administración de red o SNMP.



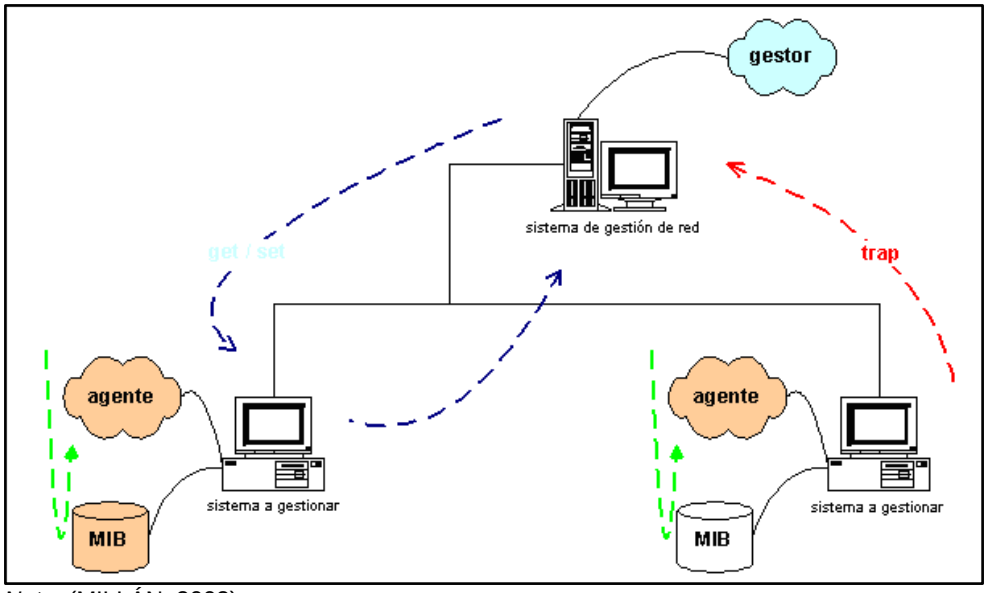
Nota: Protocolo SNMP (ROJAS, 2023).

La manera de cómo funciona el protocolo SNMP, se fundamenta en dos elementos clave, por un lado se tiene al supervisor y por otro a los agentes. El rol del supervisor es adquirir datos y realizar pedidos SNMP, mientras que los agentes conectan los dispositivos a la red de datos, con esto recogen información sobre diferentes objetos (SOSSA, 2015).

Para (LAGO & MERA, 2013), los elementos de SNMP son:

- **Estación de gestión (Administrador):** Sistema de nodo basado en interfaz gráfica de usuario centralizado, es utilizado en el monitoreo de la red. Tiene interacción bidireccional con el flujo de información entre el nodo administración y los elementos de la red.
- **Agente del administrador:** Agente basado en software, cuando recibe consultas SNMP, proporciona el estado y las estadísticas sobre un nodo de red, su ubicación es un proceso local y para proporcionar información se asocia con los dispositivos SNMP.
- **Base de información de administración (MIB):** Contiene atributos del dispositivo que se está gestionando como el nombre, estado, tipo de datos, derechos de acceso.
- **Protocolo de administración de red:** Son protocolos que de forma fácil, hacen posible el seguimiento y la creación de informes acerca de datos como: tráfico de red.

Figura 6
Esquema de una red gestionada con SNMP



Nota: (MILLÁN, 2003).

HERRAMIENTAS DE MONITOREO DE REDES DE DATOS

Existen diferentes herramientas de monitoreo de redes y servidores, entre comerciales y libres, capaces de atender requerimientos avanzados, que permitan supervisar y asegurar la adecuada operatividad de la infraestructura tecnológica. A continuación, se distinguen las características más importantes a las siguientes:

- Visualizar en gráficos, en un resumen o reporte que permita comprender la información
- Visualizar de manera centralizada a los equipos, servicios, software, versiones y hardware.
- Alertas de los dispositivos de la infraestructura de TI que presentan problemas de tipo inminente o que ya ocurrieron.
- Tener disponible una base de datos histórica, que contenga información de los diferentes dispositivos a monitorear.

A continuación, se presentan algunas de las más importantes herramientas de monitoreo (TRONCOSO, 2023).

CACTI

Esta herramienta es empleada por muchas empresas para gestionar y supervisar redes de datos y centros de datos (GITHUB, 2024).. De esta herramienta se puede decir que presenta una interfaz fácil e intuitiva, lo cual es de mucha ayuda en empresas del tamaño de la red de datos local y en redes más grandes y complejas, donde existan miles de dispositivos. La herramienta recopila datos, tiene soporte SNMP, en el caso de requerir la creación de gráficos de tráfico con MRTG (CACTI, 2024). Se pueden distinguir a las características siguientes:

- A nivel local y remoto se recopilan datos.
- Las redes existentes son detectadas.
- Se puede tener automatizada la gestión de dispositivos.
- Para el caso de los gráficos, existen plantillas.
- En el caso de requerir de forma personalizada adquirir datos existen métodos.
- Es posible administrar dominios, usuarios y grupos.
- Para cuentas locales, es posible contar con nivel C3 en la configuración de seguridad
- Claves que cuentan con sistemas criptográficos.
- Gestión de cambios en complejidad, historial y contraseñas de forma forzada
- Las cuentas cuentan con soporte de bloqueo.

ICINGA

Icinga es una herramienta de monitorización escalable, extensible, que hace posible comprobar para los recursos de red su disponibilidad y de ser necesario notificar a los administradores de red, la existencia de interrupciones. Además, crea data con fines de elaboración de informes. Es de código abierto (*Wikipedia*, 2024), capaz de monitorizar entornos complejos que se puedan encontrar en ubicaciones diferentes. Es importante mencionar que, mantiene la configuración y la compatibilidad de su plugins con Nagios, así como la mejora en la versión de su CGI (FREE SOFTWARE MAGAZINE, 2024).

MUNIN

Esta herramienta examina todos los equipos y recuerda lo que vio, puede monitorear de forma fácil el rendimiento de la infraestructura tecnológica y de sus computadoras; presentando informes gráficos mediante su interfaz web gráfica. Hace énfasis en la capacidad plug and play que significa conectar y usar. Luego emplea una gran cantidad de plugins de monitoreo (MUNIN, 2024).

NAGIOS

Es una herramienta bastante conocida y utilizada por las funcionalidades que ofrece para supervisar para servicios de red su disponibilidad, el estado de los dispositivos, y los recursos del sistema. Cuenta con interfaz web, sus alertas son en tiempo real, proporciona con detalle una vista de la infraestructura de red, hace posible identificar de manera rápida a los problemas y que sea posible corregir con algunas acciones.

- Como ventaja se puede decir que tiene una gama amplia de complementos y plugins, que permiten supervisar exhaustivamente todas las alertas que suceden en tiempo real.
- Como desventaja se puede mencionar que requiere una compleja configuración inicial, sumado a esto una poco intuitiva interfaz de usuario.

Cuenta con versión de código abierto y de pago de acuerdo a la necesidad de la empresa (TRONCOSO, 2023).

PANDORA FMS

Herramienta de monitoreo que provee un panorama completo de la infraestructura de TI, es escalable y flexible. Hace posible el monitoreo de diferentes elementos como: redes, servicios, servidores y aplicaciones. Con avanzadas capacidades de visualización e interfaz intuitiva, hace fácil solución y detección eficiente de problemas (TRONCOSO, 2023).

- Como ventaja se puede mencionar a una interfaz intuitiva, escalable y con una cobertura amplia de monitoreo.
- Como desventaja se decir que es necesario para su configuración inicial, dominar conocimientos técnicos, si se requiere avanzadas características, estas están disponibles en la versión Enterprise.

ZABBIX

Es una herramienta de software libre, su diseño hace posible la supervisión del rendimiento y la disponibilidad de los diferentes dispositivos que conforman la infraestructura de TI.

Permite registrar virtualmente diferentes tipos de datos de la red de datos. Simultáneamente permite el monitoreo de miles de servidores, dispositivos de red y máquinas virtuales, esto lo hace en tiempo real con un excelente rendimiento. Sumado a su característica de almacenamiento de datos, se puede mencionar a que es posible visualizar gráficos, descripciones, mapas, pantallas, etc. También, con el propósito de crear alertas, tiene maneras flexibles de realizar análisis de los datos (*Zabbix*, 2024).

ZENOSS CORE

Herramienta servidor y de gestión de red, libre de código abierto, bajo licencia pública general (GNU)

Es posible hacer monitoreo al inventario, disponibilidad, configuración, eventos y rendimiento, desde su interfaz web. También, en tiempo real hacer análisis y modelado de tal forma que se asegure la actividad del servicio, da un unificado panorama, flexible y abierta arquitectura adaptable a cualquier ambiente

Respecto a su diseño es para pequeñas implementaciones, que tienen una básica infraestructura para tradicionales sistemas como: dispositivos de red, almacenamiento, servidores (Zenoss Inc, 2024).

IV. DESARROLLO DE LA SOLUCIÓN

SITUACIÓN DE LA GESTIÓN DE INCIDENTES ENCONTRADA EN LA EMPRESA

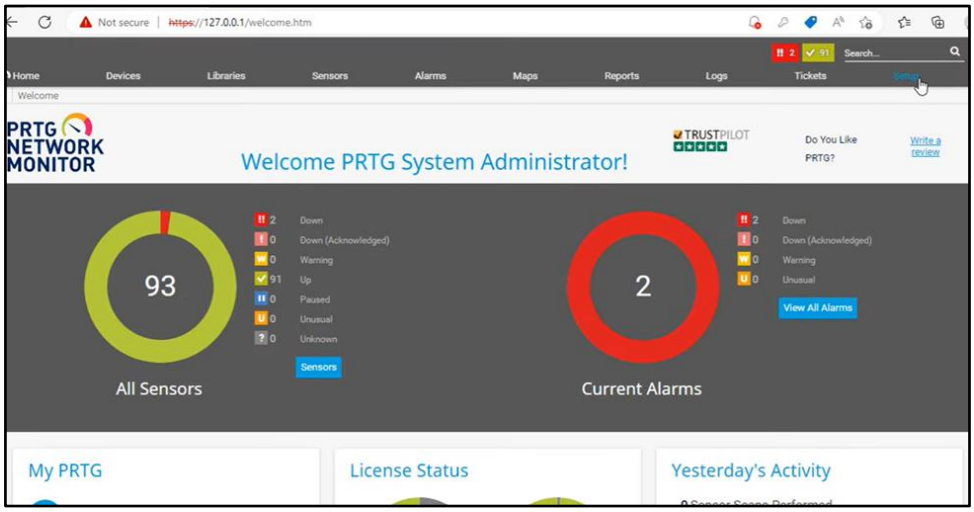
Actualmente la Empresa del rubro tecnológico cuenta con una herramienta de monitoreo PRTG Network Monitor, que le permite monitorear el comportamiento de su infraestructura de TI, sin embargo, a medida que la empresa fue creciendo, la herramienta empezó a presentar inconsistencias en su funcionamiento, esto debido a la mala configuración e implementación del sistema.

Cuando se presentaban incidencias con los dispositivos monitoreados, el sistema demora en alertar y notificar, lo cual no permitía la atención de incidentes de manera oportuna y esto se ocasionado por las siguientes causas:

- Dependencias del rendimiento del servidor.
- Limitaciones de herramienta.

Debido a esto se propuso la implementación de un nuevo sistema de monitoreo con una herramienta Open Source, que maneje configuraciones robustas y que sea escalable en el tiempo.

Figura 7
Interfaz de sistema de monitoreo PRTG



Nota: Sistema PRTG de la empresa.

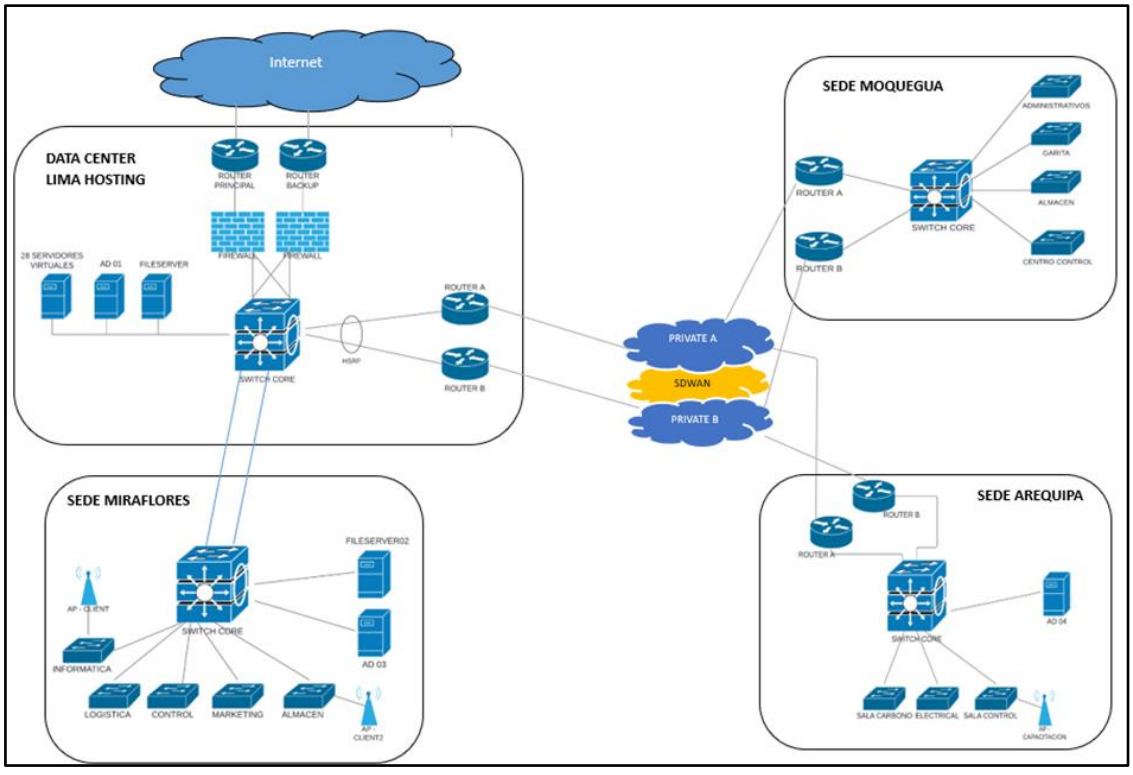
IDENTIFICAR LOS DISPOSITIVOS Y SERVICIOS PRINCIPALES DE LA INFRAESTRUCTURA DE TI DE LA EMPRESA CLIENTE.

Durante el proceso de implementación del proyecto, se identificaron los dispositivos y servicios de TI críticos que son considerados importantes para la continuidad de la operación de la empresa cliente. Posteriormente estos dispositivos fueron configurados en el sistema de monitoreo.

Topología de red de la empresa Cliente.

En la figura 8, se presenta la topología de la infraestructura tecnológica de la empresa cliente, la cual tiene su Data Center hosteado en un proveedor, además cuenta con 3 sedes importantes para su operación.

Figura 8
Topología de red de la empresa cliente



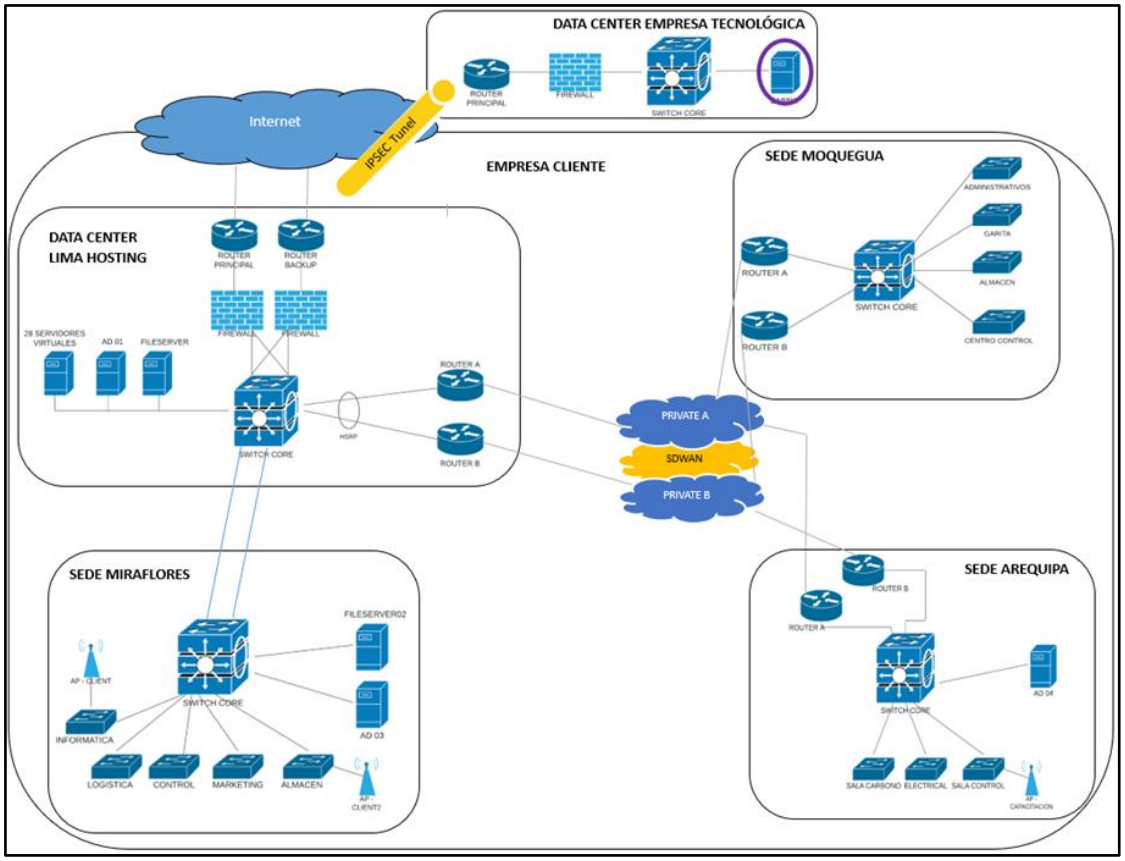
Nota: Empresa Cliente

Topología de red propuesta.

A continuación, se presenta la topología de red propuesta para la implementación del sistema de monitoreo, en la cual el servidor de monitoreo se encuentra en el Data

Center de la empresa tecnológica y se conecta mediante VPN a la red de la empresa CLIENTE.

Figura 9
Topología de red propuesta



Nota: Elaboración propia

Dispositivos de TI de la empresa CLIENTE.

En la tabla 4, se muestra el total de equipos y servicios de TI que van a ser monitoreados por el sistema.

Tabla 4
Equipos y servicios de TI empresa Cliente

TIPO DE EQUIPO	CANTIDAD
Router	8
Switch	16
Firewall	2
Access Point	3
Servidores Físicos	6
Servidores virtuales	28
Sitios Web	4
TOTAL	**67**

Nota: Elaboración propia

En la tabla 5, se muestra la cantidad de equipos y servicios de TI por sede.

Tabla 5
Equipos y servicios de TI por sedes de la empresa Cliente

TIPO DE EQUIPO	DC LIMA	MIRAFLORES	AREQUIPA	MOQUEGUA	CANTIDAD
Router	4	-	2	2	8
Switch	1	6	4	5	16
Firewall	2	-	-	-	2
Access Point	-	2	1	-	3
Servidores Físicos	3	2	1	-	6
Servidores virtuales	28	-	-	-	28
Sitios Web	4	-	-	-	4
		TOTAL			67

Nota: Elaboración propia

SELECCIONAR HERRAMIENTA DE MONITOREO DE CÓDIGO LIBRE QUE SE ADECUE A LAS NECESIDADES DE LA INFRAESTRUCTURA DE TI DE LA EMPRESA CLIENTE.

Teniendo en cuenta el trabajo de (MORI, 2021 & CASTRO, 2015) y pruebas de herramientas de monitoreo de uso libre, con licencia GPL, se elaboró una tabla resumen que considera a las herramientas de monitoreo para gestión de incidentes más importantes a ser consideradas para evaluarlas y producto de ello, seleccionar a la más adecuada para la empresa y de esta manera proceder con su implementación.

Del análisis comparativo de las herramientas, se destaca que la que cumple con todas las características evaluadas es Zabbix.

Tabla 6

Comparación de herramientas de monitoreo

SISTEMA	GRÁFICAS	INFORMES	GRUPOS LÓGICO	AUTO DESCUBRIMIENTO	AGENTES	SNMP	PLUGINS	APLICACIÓN WEB	ALERTAS	MONITOREO DISTRIBUIDO	BASE DE DATOS	LICENCIA
NAGIOS	SI	SI	SI	SI	SI	A TRAVÉS DE PLUGINS	SI	SOLO VISUALIZA	SI	SI	SQL	GPL
ZABBIX	SI	SI	SI	SI	SI	SI	SI	CONTROL TOTAL	SI	SI	POSTGRESQL MYSQL ORACLE	GPL
ZENOSS	SI	NO	SI	SI	SNMP, WMI, JMX, etc	SI	SI	CONTROL TOTAL	SI	SI	RRDTOOL Y MySQL	GPL
ICINGA	SI	SI	SI	NO	SI	SI	SI	CONTROL TOTAL	SI	SI	POSTGRESQL	GLP
PRTG NETWORK MONITOR	SI	SI	SI	SI	SI	SI	SI	CONTROL TOTAL	SI	SI	SQL	COMERCIAL
MUNIN	SI	NO	NO	SI	NO	SI	SI	CONTROL TOTAL	SI	NO	RRDTOOL	GLP
PANDORA FMS	SI	EN TIEMPO REAL O PROGRAMADO	SI	SI	CON/SIN AGENTE	SI	SI	CONTROL TOTAL	SI	SI	MySQL Y ORACLE	GPL Y COMERCIAL
CACTI	SI	SI	NO	A TRAVÉS DE PLUGINS	SI	SI	SI	CONTROL TOTAL	SI	NO	RRDTOOL MYSQL	GPL
OPEN NMS	SI	SI	SI	SI	SNMP, WMI, JMX, USANDO NRPE	SI	SI	CONTROL TOTAL	ENRUTA, ESCALAS Y HORARIOS	CLIENTE MÍNIMO O SNMP PROXY	JROBIN, RRDTOOL Y POSTGRESQL	GPL

Nota:(MORI, 2021 & CASTRO, 2015).

IMPLEMENTAR LA HERRAMIENTA DE MONITOREO SELECCIONADA, INCORPORANDO EL SISTEMA DE ALERTAS ANTE LA PRESENCIA DE FALLOS O POSIBLES FALLOS EN LA INFRAESTRUCTURA DE TI DE LA EMPRESA CLIENTE.

Requerimientos del sistema:

Para poder establecer los requerimientos del sistema, se estableció el tamaño del entorno de acuerdo con la cantidad de dispositivos identificados a monitorear.

Tabla 7
Requerimientos del sistema

Name	Platform	CPU/Memory	Database	Monitored hosts
Small	CentOS	Virtual Appliance	MySQL InnoDB	100
Medium	CentOS	2 CPU cores/2GB	MySQL InnoDB	500
Large	RedHat Enterprise Linux	4 CPU cores/8GB	RAID10 MySQL InnoDB or PostgreSQL	>1000
Very large	RedHat Enterprise Linux	8 CPU cores/16GB	Fast RAID10 MySQL InnoDB or PostgreSQL	>10000

Nota: (Zabbix SIA, 2024)

La empresa del rubro tecnológico tiene 4 clientes a las cuales les brinda el servicio de monitoreo de su infraestructura de TI, con un promedio de 500 dispositivos monitoreados, de acuerdo con el crecimiento y proyección a futuro se seleccionó la creación de un servidor de tipo Very Large.

Tabla 8
Requerimientos utilizados para el sistema

Recursos	Detalle
CPU	8 cores
RAM	16 GB
HDD	400 GB
IP	172.22.134.51
OS	Red Hat Enterprise Linux Server 7
Hostname	Zabbix

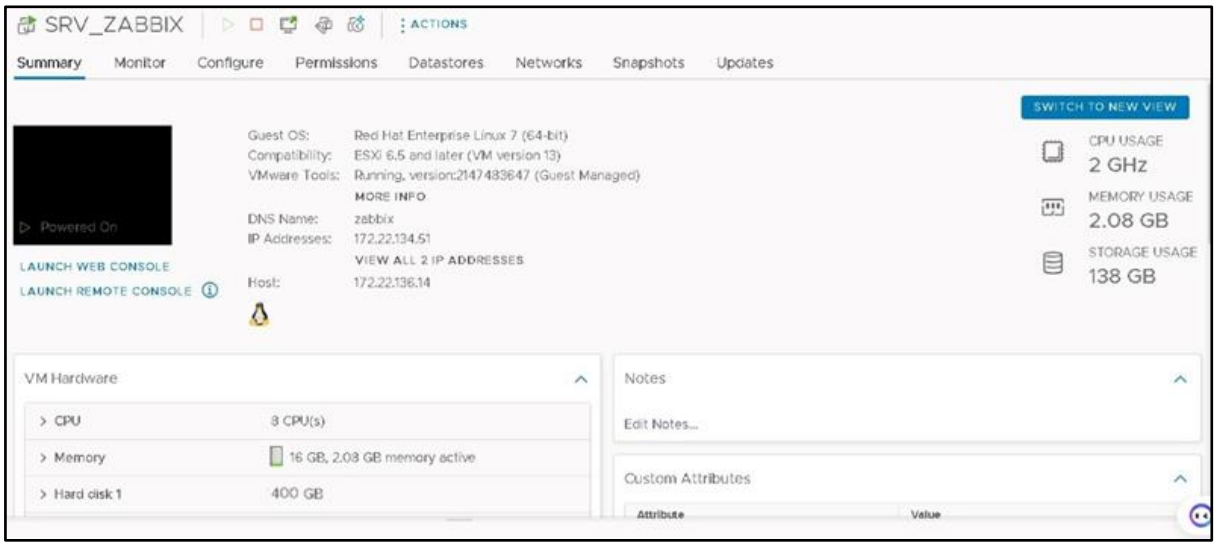
Nota: Elaboración propia

Creación de servidor Zabbix.

La empresa tiene una infraestructura de virtualización con tecnología VMWARE en la cual se creó una máquina virtual de tipo Very Large para satisfacer las necesidades de los clientes, por consiguiente, posee licencia para el sistema operativo Red Hat Enterprise Linux Server.

A continuación, en la figura 4 se muestran las características del servidor creado.

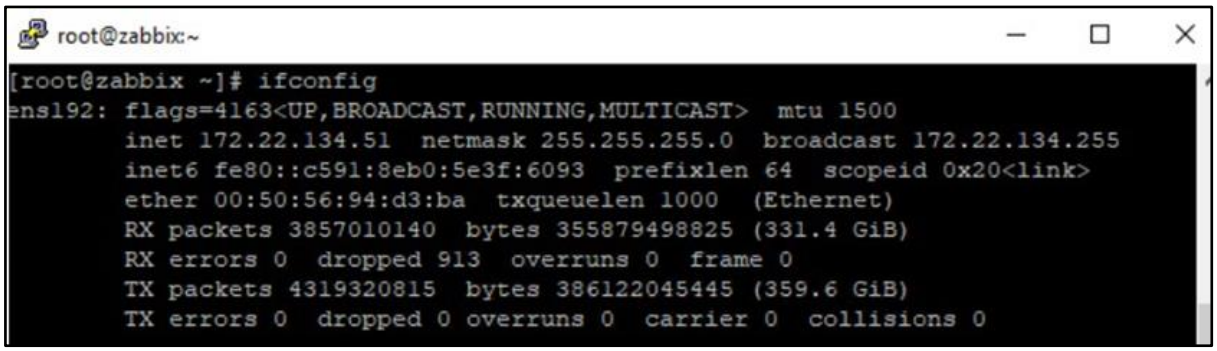
Figura 10
Servidor virtual



Nota: VMware empresa rubro tecnológico.

Se realizó la configuración de red en el servidor implementado.

Figura 11
Configuraciones de red



Nota: Elaboración propia

Implementación del sistema.

Instalación de Zabbix

- Para realizar la instalación, debemos descargar los paquetes desde la página oficial de Zabbix (https://repo.zabbix.com), para la implementación trabajamos con Zabbix versión 5.0

Figura 12
Instalación de Zabbix

Nota: Elaboración propia

Figura 13
Instalar los paquetes frontend de Zabbix

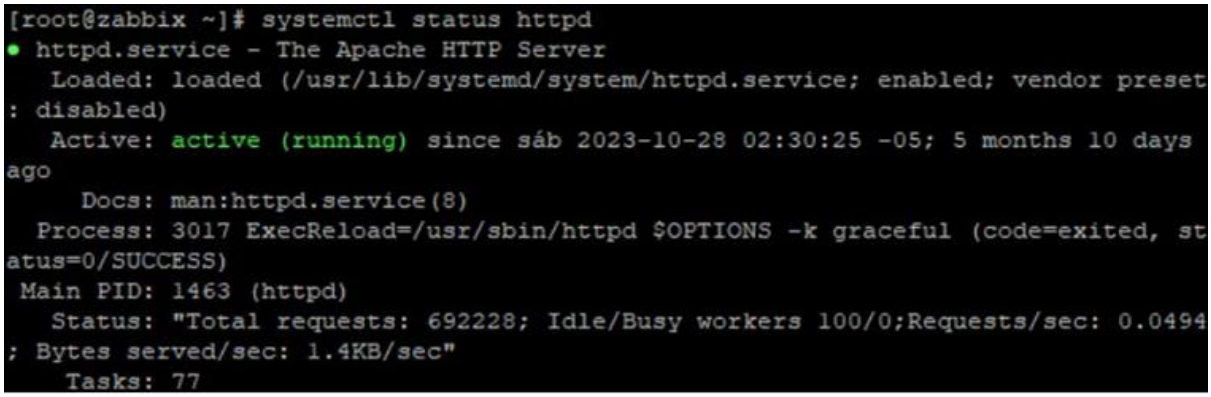
Nota: Elaboración propia

- Iniciamos los servicios de Zabbix, MYSQL y Apache con el fin de poder configurar el sistema

Figura 14
Inicio de servicios mysql

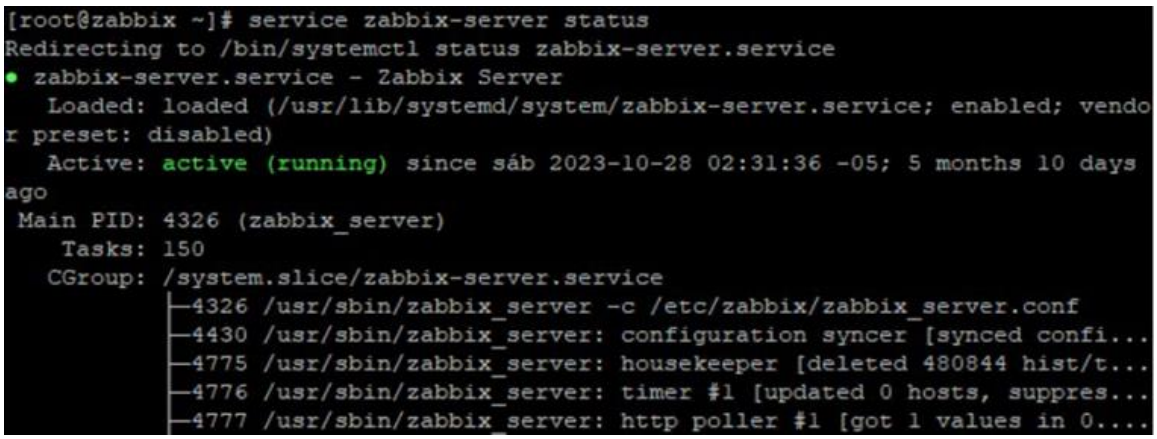
Nota: Elaboración propia

Figura 15
Inicio de servicios Apache



Nota: Elaboración propia

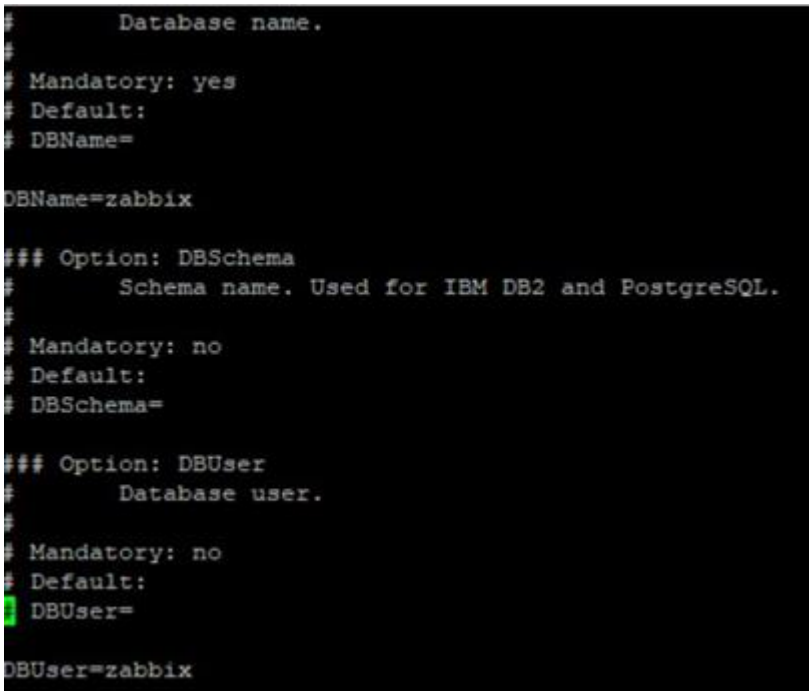
Figura 16
Inicio de servicios Zabbix -server



Nota: Elaboración propia

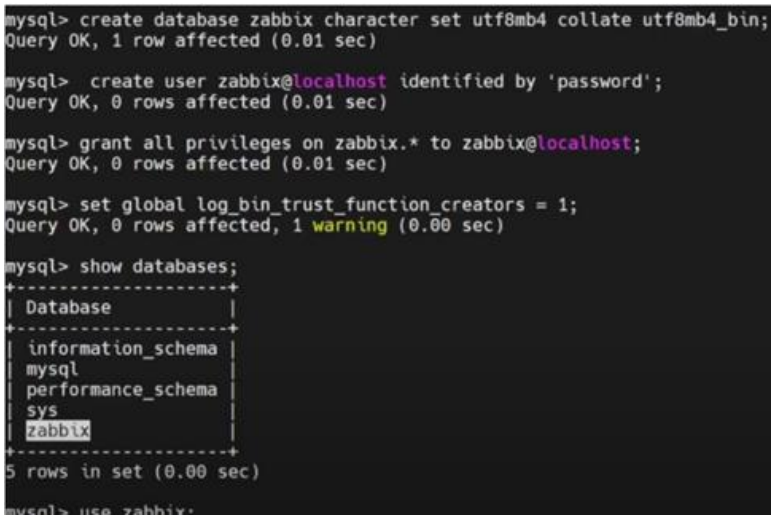
- Realizamos la configuración de la BD MYSQL para el almacenamiento de datos.

Figura 17
Configuración de usuario de BD



Nota: Elaboración propia

Figura 18
Configuración de mysql

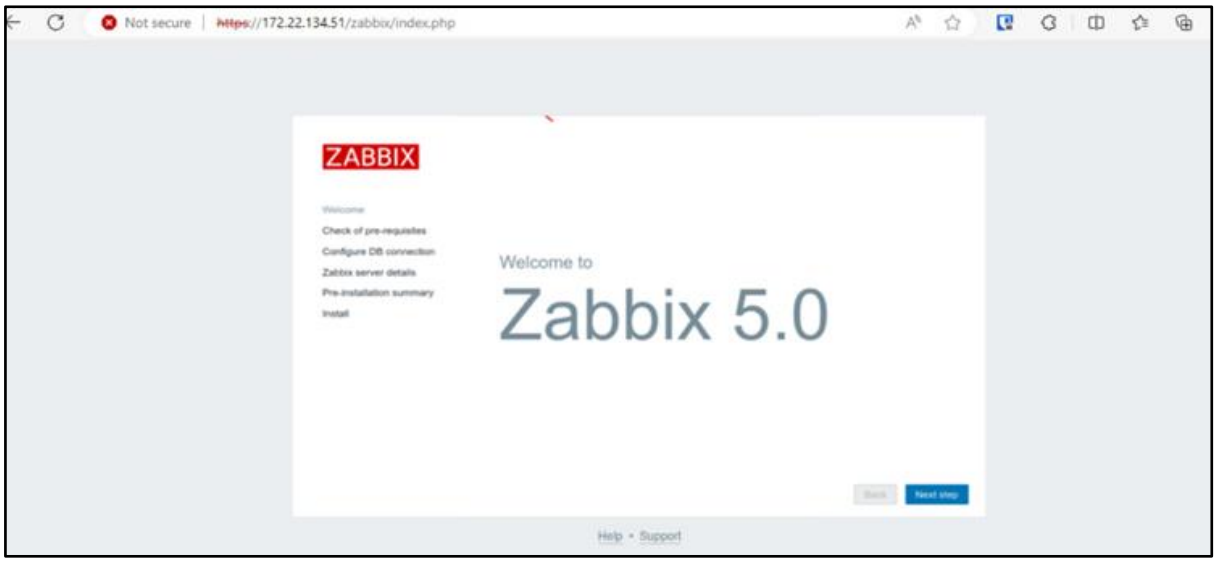


Nota: Elaboración propia

Configuración Web de Zabbix.

- Iniciamos la página de Zabbix con la URL https://172.22.134.51/zabbix/index.php

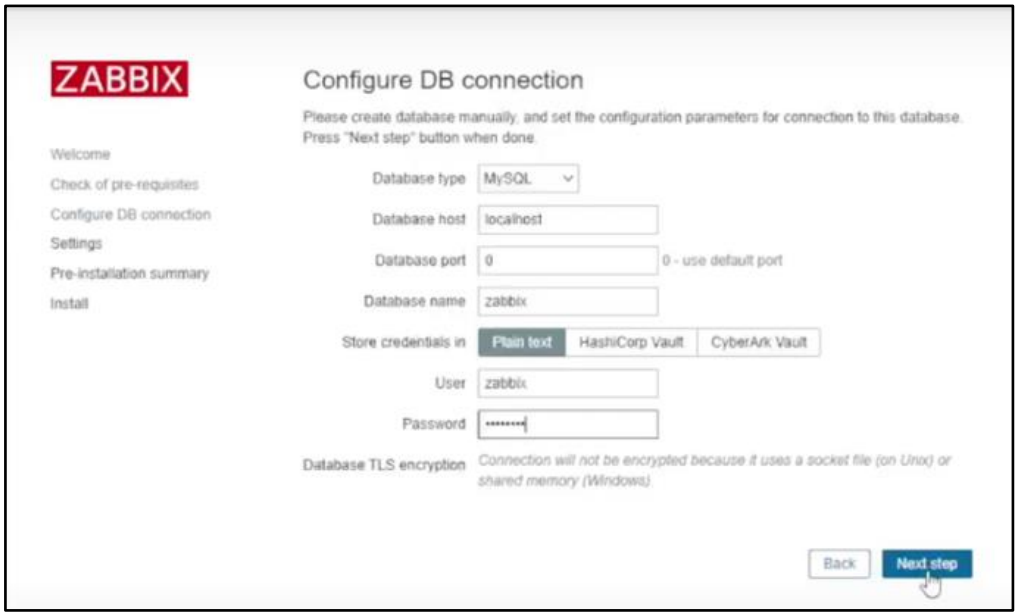
Figura 19
Interfaz web de Zabbix



Nota: Elaboración propia

- Configuramos la conexión de la Base de Datos MYSQL.

Figura 20
Conexión a la Base de Datos

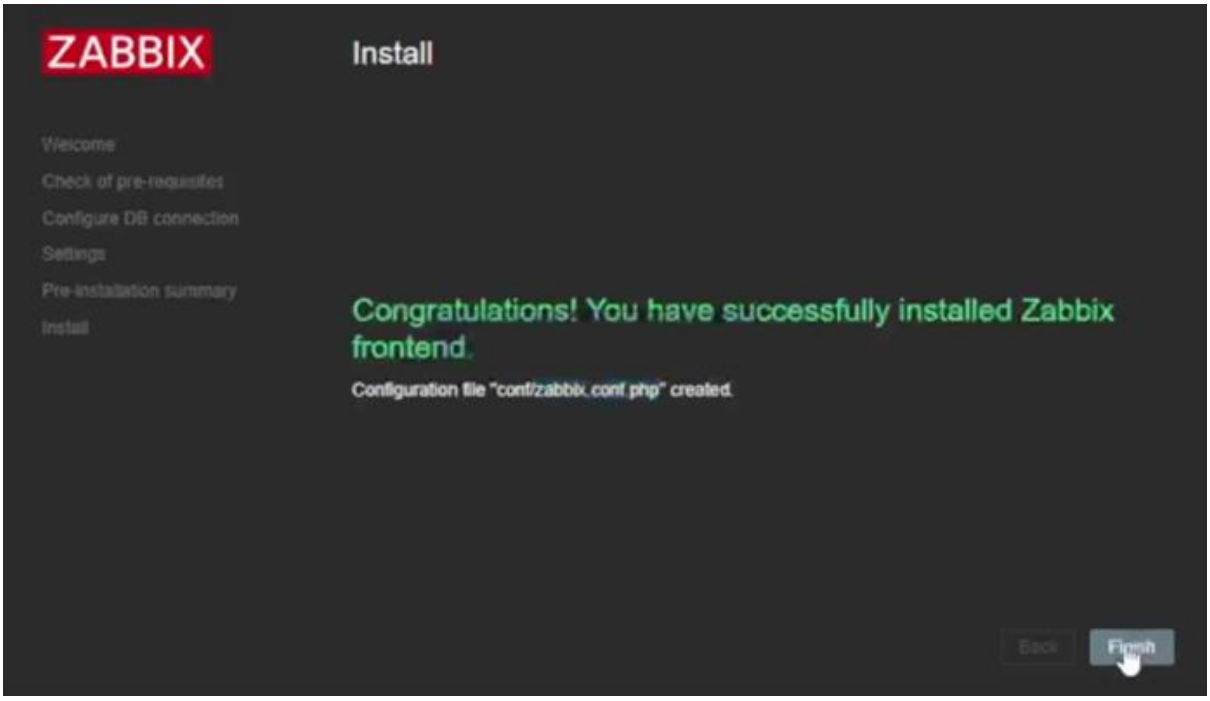


Nota: Elaboración propia

Figura 21
Resumen de parámetros de base de datos

Nota: Elaboración propia

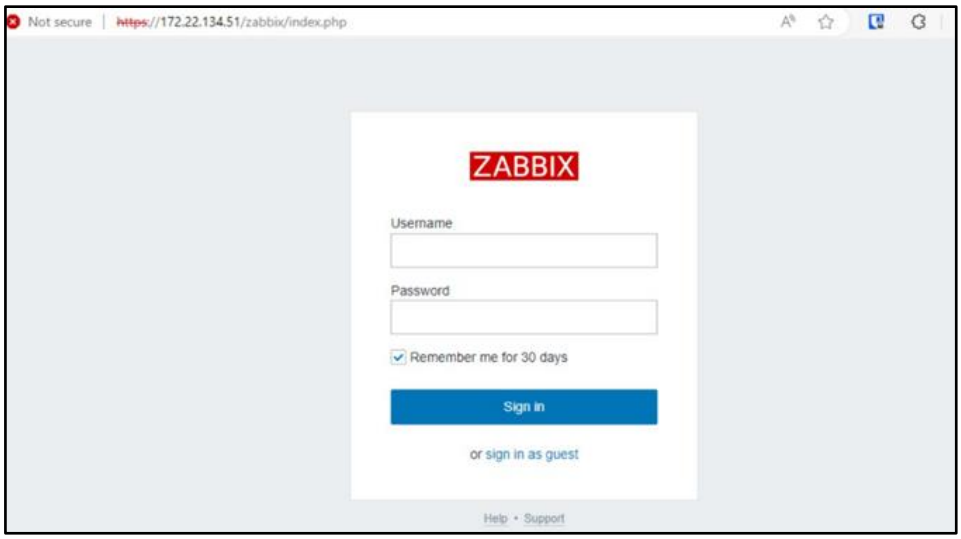
Figura 22
Estado de instalación



Nota: Elaboración propia

- Ingresamos con el usuario creado.

Figura 23
Inicio de sesión en Zabbix



Nota: Elaboración propia

Definición de equipos TI, servicios TI y Parámetros a monitorear.

Una vez finalizada la instalación del servidor Zabbix, se añadieron los dispositivos y servicios que serán monitoreados.

Equipos y servicios TI monitoreados.

En la Tabla 9 muestra los equipos y servicios que fueron identificados para ser monitoreados por el sistema.

Tabla 9

Equipos y servicios críticos de la empresa Cliente

ITEM	SEDE	EQUIPO	NAME	DESCRIPCIÓN	IP
1	DC LIMA	SWITCH	SWLIMCORE01	SW CORE DC LIMA	192.168.55.1
2	MIRAFLORES	SWITCH	SWMIRCORE01	SW CORE MIRAFLORES	192.168.55.3
3	MIRAFLORES	SWITCH	SWMIRINFO01	SWITCH DE ACCESO INFORMATICA	192.168.55.31
4	MIRAFLORES	SWITCH	SWMIRLOG01	SWITCH DE ACCESO LOGÍSTICA	192.168.55.32
5	MIRAFLORES	SWITCH	SWMIRCTR01	SWITCH DE ACCESO CONTROL	192.168.55.36
6	MIRAFLORES	SWITCH	SWMIRMKT01	SWITCH DE ACCESO MARKETING	192.168.55.40
7	MIRAFLORES	SWITCH	SWMIRALM01	SWITCH DE ACCESO ALMACEN	192.168.55.42
8	MOQUEGUA	SWITCH	SWMOQCORE01	SWITCH CORE MOQUEGUA	192.168.58.1
9	MOQUEGUA	SWITCH	SWMOQADM01	SWITCH DE ACCESO ADMINISTRATIVOS	192.168.58.112
10	MOQUEGUA	SWITCH	SWMOQGAR01	SWITCH DE ACCESO GARITA	192.168.58.114
11	MOQUEGUA	SWITCH	SWMOQALM01	SWITCH DE ACCESO ALMACEN 1	192.168.58.116
12	MOQUEGUA	SWITCH	SWMOQCTR01	SWITCH DE ACCESO CENTRO DE CONTROL	192.168.58.117
13	AREQUIPA	SWITCH	SWARECORE01	SWITCH CORE AREQUIPA	192.168.53.1
14	AREQUIPA	SWITCH	SWARECAR01	SWITCH DE ACCESO SALA CARBONO	192.168.53.2
15	AREQUIPA	SWITCH	SWAREELE01	SWITCH DE ACCESO ELECTRICIDAD	192.168.53.3
16	AREQUIPA	SWITCH	SWARESAL01	SWITCH DE ACCESO SALA CONTROL	192.168.53.4
17	DC LIMA	ROUTER	RP_LIM01	ROUTER INTERNET PRINCIPAL	190.216.189.118
18	DC LIMA	ROUTER	RP_LIM02	ROUTER INTERNET SECUNDARIO	190.216.189.119
19	DC LIMA	ROUTER	RSD_LIMA	ROUTER SDWAN - A	172.19.240.2
20	DC LIMA	ROUTER	RSD_LIMB	ROUTER SDWAN - B	172.19.240.6
21	AREQUIPA	ROUTER	RSD_AREA	ROUTER SDWAN - A	172.16.101.7
22	AREQUIPA	ROUTER	RSD_AREB	ROUTER SDWAN - B	172.16.101.4
23	MOQUEGUA	ROUTER	RSD_MOQA	ROUTER SDWAN - A	172.16.103.4
24	MOQUEGUA	ROUTER	RSD_MOQB	ROUTER SDWAN - B	172.16.103.3
25	DC LIMA	FIREWALL	PA-MASTER	FIREWALL MASTER	192.168.55.10
26	DC LIMA	FIREWALL	PA-SLAVE	FIREWALL SLAVE	192.168.55.11
27	MIRAFLORES	ACCESS POINT		ACCESS POINT INFORMATICA	192.168.35.16
28	MIRAFLORES	ACCESS POINT		ACCESS POINT CLIENTES	192.168.35.17
29	AREQUIPA	ACCESS POINT		ACCESS POINT CAPACITACIÓN	192.168.28.20
30	DC LIMA	SERVIDOR FISICO	SLIMADP01	DOMAIN CONTROLLER PRINCIPAL	192.168.65.40
31	DC LIMA	SERVIDOR FISICO	SLIMFILE01	FILESERVER LIMA	192.168.65.42
32	DC LIMA	SERVIDOR FISICO	SLIMAPI01	SERVIDOR APLICACIÓN FACTURACIÓN	192.168.65.48
33	DC LIMA	SERVIDOR VIRTUAL	SLIMARP01	SERVIDOR CONTROL DE ACCESOS	192.168.65.50
34	DC LIMA	SERVIDOR VIRTUAL	SLIMADM01	SERVIDOR ADMINISTRADOR	192.168.65.41
35	DC LIMA	SERVIDOR VIRTUAL	SLIMARP02	SERVIDOR CONTROL DE GESTION	192.168.65.43
36	DC LIMA	SERVIDOR VIRTUAL	SLIMDBD01	SERVIDOR BASE DE DATOS DESARROLLO	192.168.65.51
37	DC LIMA	SERVIDOR VIRTUAL	SLIMDBP01	SERVIDOR BASE DE DATOS PRODUCCIÓN	192.168.65.47
38	DC LIMA	SERVIDOR VIRTUAL	SLIMAD02	DOMAIN CONTROLLER SECUNDARIO	192.168.65.46
39	DC LIMA	SERVIDOR VIRTUAL	SLIMFLEX01	SERVIDOR APLICACION CLIENTE	192.168.65.49
40	DC LIMA	SERVIDOR VIRTUAL	SLIMAIO02	SERVIDOR APLICACION COMERCIAL	192.168.65.44
41	DC LIMA	SERVIDOR VIRTUAL	EEPLIMSKAP01	SERVIDOR ANTIVIRUS	192.168.65.45
42	DC LIMA	SERVIDOR VIRTUAL	SLIMLNP01	SERVIDOR DE REPORTES	192.168.65.61
43	DC LIMA	SERVIDOR VIRTUAL	SLIMSNPP01	SERVIDOR APLICACIÓN SHAREPOINT FRONT	192.168.65.65
44	DC LIMA	SERVIDOR VIRTUAL	SLIMSNPP02	SERVIDOR APLICACIÓN SHAREPOINT BACK	192.168.65.54
45	DC LIMA	SERVIDOR VIRTUAL	SLIMRAP03	SERVIDOR CONTROL DE GESTION	192.168.65.55
46	DC LIMA	SERVIDOR VIRTUAL	SLIMRAQ01	SERVIDOR VENTAS	192.168.65.56
47	DC LIMA	SERVIDOR VIRTUAL	SLIMACP03	SERVIDOR APLICACION DE ACCESOS	192.168.65.63
48	DC LIMA	SERVIDOR VIRTUAL	SLIMACP04	SERVIDOR APLICACION DE ACCESOS 2	192.168.65.58
49	DC LIMA	SERVIDOR VIRTUAL	SLIMSSI01	SERVIDOR APLICACIÓN EXTRANET FRONT	192.168.65.59
50	DC LIMA	SERVIDOR VIRTUAL	SLIMSSI02	SERVIDOR APLICACIÓN EXTRANET BACK	192.168.65.60
51	DC LIMA	SERVIDOR VIRTUAL	SLIMSOL01	SERVIDOR DE DESARROLLADORES	192.168.65.52
52	DC LIMA	SERVIDOR VIRTUAL	SLIMSSP02	SERVIDOR DE INFRAESTRUCTURA	192.168.65.62
53	DC LIMA	SERVIDOR VIRTUAL	SLIMSSP03	SERVIDOR PARA USUARIOS CRÍTICOS	192.168.65.57
54	DC LIMA	SERVIDOR VIRTUAL	SLIMSSP04	SERVIDOR INTRANET	192.168.65.64
55	DC LIMA	SERVIDOR VIRTUAL	SLIMWSUS01	SERVIDOR WSUS SERVIDORES	192.168.65.53
56	DC LIMA	SERVIDOR VIRTUAL	SLIMWSUS02	SERVIDOR WSUS WORKSTATIONS	192.168.65.69
57	DC LIMA	SERVIDOR VIRTUAL	SLIMH2HB01	SERVIDOR APLICACIÓN H2H BACK	192.168.65.67
58	DC LIMA	SERVIDOR VIRTUAL	SLIMH2HF01	SERVIDOR APLICACIÓN H2H FRONT	192.168.65.68
59	DC LIMA	SERVIDOR VIRTUAL	SLIMP2PB01	SERVIDOR APLICACIÓN PROVEEDORES BACK	192.168.65.66
60	DC LIMA	SERVIDOR VIRTUAL	SLIMP2PF01	SERVIDOR APLICACIÓN PROVEEDORES FRONT	192.168.65.70
61	MIRAFLORES	SERVIDOR FISICO	SMIRAD03	DOMAIN CONTROLLER MIRAFLORES	192.168.56.120
62	MIRAFLORES	SERVIDOR FISICO	SMIRFILE02	FILESERVER MIRAFLORES	192.168.56.118
63	AREQUIPA	SERVIDOR FISICO	SAREAD04	DOMAIN CONTROLLER AREQUIPA	192.168.57.110
64	DC LIMA	SITIO WEB		MONITOREO SITIO WEB EXTRANET	https://nuevaextranet.cliente.pe
65	DC LIMA	SITIO WEB		MONITOREO SITIO WEB MI CLIENTE	https://micliente.cliente.pe
66	DC LIMA	SITIO WEB		MONITOREO SITIO WEB FICHA DIGITAL	https://sisgas.cliente.pe
67	DC LIMA	SITIO WEB		MONITOREO SITIO WEB KIOSKO	https://kiosko.cliente.pe

Nota: Elaboración propia

Parámetros de monitoreo.

En la Tabla 10 se establecen los parámetros de monitoreo comunes a los dispositivos y servicios de TI.

Tabla 10
Parámetros de monitoreo

PARÁMETROS	DESCRIPCIÓN
SISTEMA	Uso de CPU
	Uso de memoria
	Uso de disco duro
RED	Disponibilidad (ping)
	Tiempo de respuesta
	Interfaces de red
SITIO WEB	Estado HTTP 200

Nota: Elaboración propia

En la Tabla 11 se establecen los niveles de alertas de monitoreo a los dispositivos y servicios de TI.

Tabla 11
Niveles de alertas

GRAVEDAD	DESCRIPCIÓN	COLOR
Warning	Problema potencial que podría requerir investigación o acción, pero que no es crítico.	Amarillo
Average	Problema importante que debe abordarse relativamente pronto para evitar problemas mayores.	Naranja
High	Problemas críticos que necesitan atención inmediata para evitar interrupciones significativas.	Rojo

Nota: Elaboración propia

Valores de niveles de gravedad

Tabla 12
Valores máximos WARNING

Item	Parámetro	Valor máximo
1	Uso de CPU	70%
2	Uso de Memoria	70%
3	Uso de Disco Duro	70%

Nota: Elaboración propia

Tabla 13
Valores máximos AVERAGE

Item	Parámetro	Valor máximo
1	Uso de CPU	80%
2	Uso de Memoria	80%
3	Uso de Disco Duro	80%
4	Disponibilidad PING	Últimos 5 min <100 paquetes perdidos
5	Interface de RED	Ancho de banda al 80%

Nota: Elaboración propia

Tabla 14
Valores máximos HIGH

Item	Parámetro	Valor máximo
1	Uso de CPU	90%
2	Uso de Memoria	90%
3	Uso de Disco Duro	90%
4	Disponibilidad PING	Ping no disponible
5	Interface de RED	Link Down
6	Sitio WEB	/=200

Nota: Elaboración propia

Añadir dispositivo y servicio al Sistema.

Establecidos los dispositivos y servicios que se monitorearán, se procedió a configurar cada equipo seleccionando los templates correspondientes para el monitoreo de recursos de acuerdo con la tabla 6 indicada en puntos anteriores.

La conexión entre el Zabbix y la empresa Cliente es por VPN, en ambos Firewall se deben habilitar los puertos 10050, 10051 y 161 que utiliza Zabbix para realizar monitoreo.

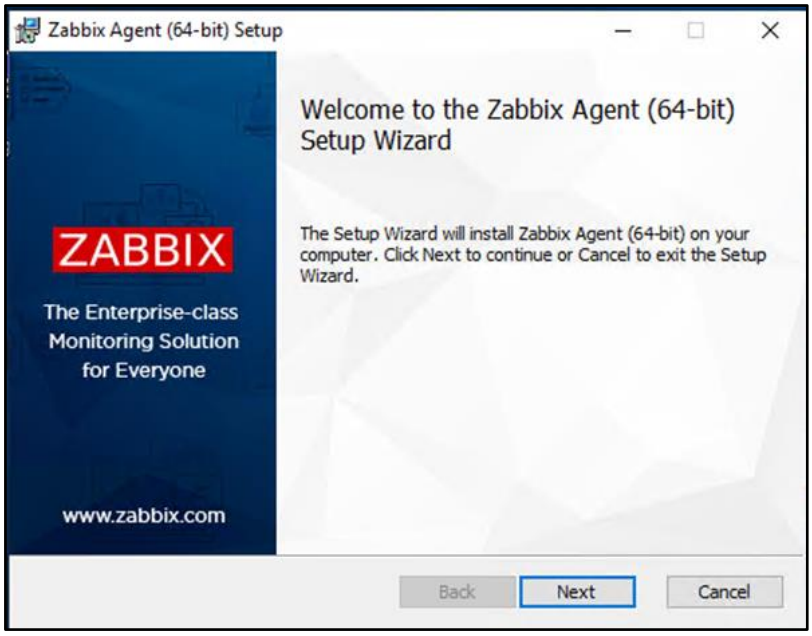
Monitoreo por agentes Zabbix.

Instalación de agente Zabbix en dispositivo Windows.

Realizamos la descarga del agente Zabbix desde la página oficial de Zabbix (https://www.zabbix.com/download_agents), en la implementación se utilizó el agente versión 5.2.4.

En la figura 24 se muestra la instalación del agente Zabbix.

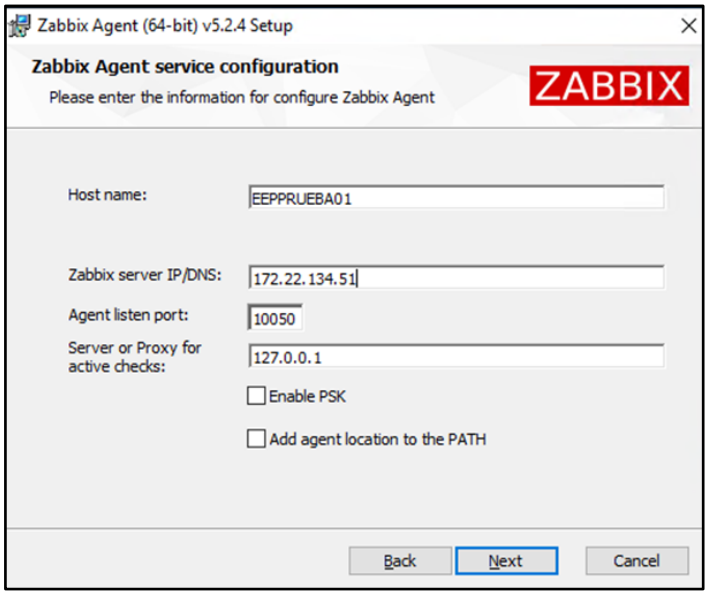
Figura 24
Instalación de agente Zabbix



Nota: Elaboración propia

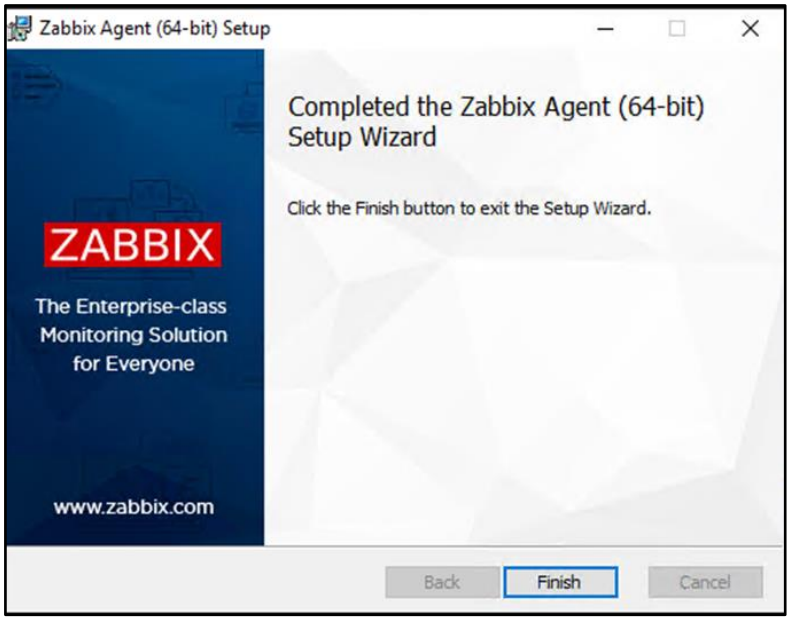
En la figura 25 se muestran los parámetros que se deben colocar de acuerdo con el nombre del equipo apuntando a la IP del servidor Zabbix.

Figura 25
Instalación de agente Zabbix



Nota: Elaboración propia

Figura 26
Instalación completa de agente Zabbix

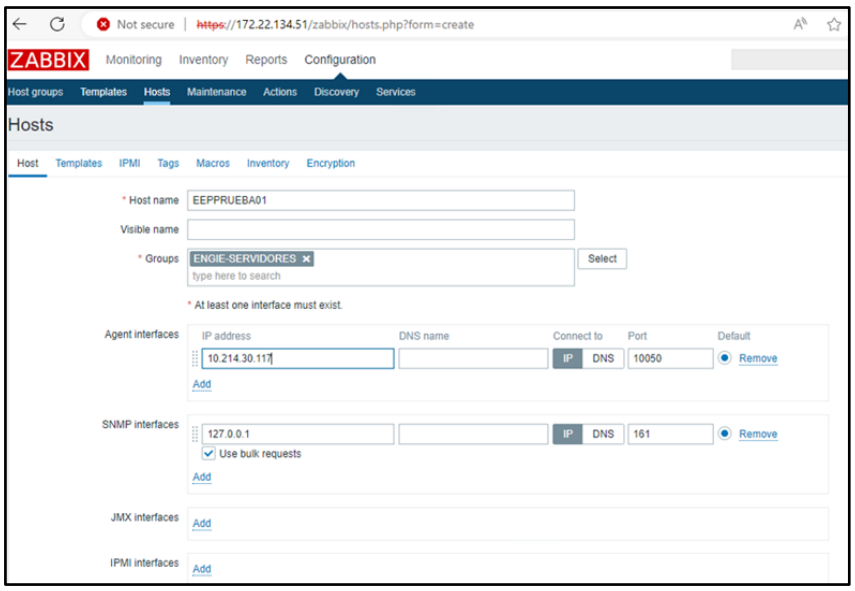


Nota: Elaboración propia

Configuración del dispositivo en el sistema Zabbix.

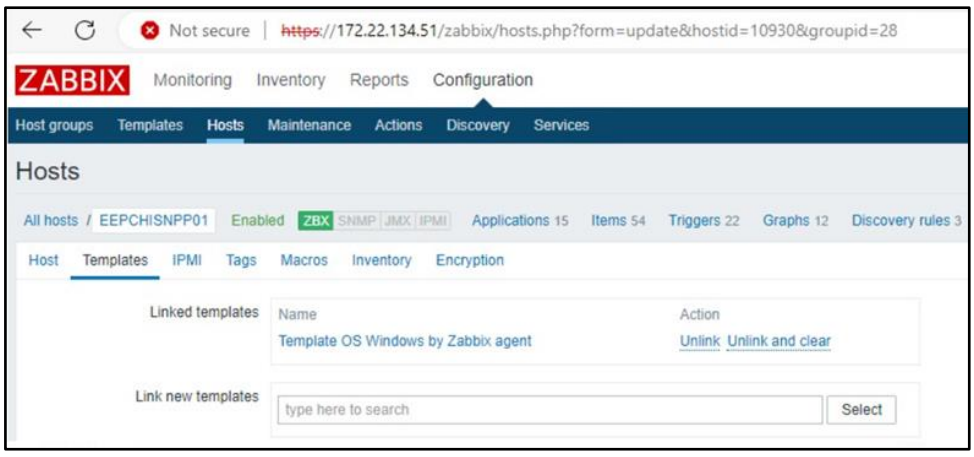
En la figura 27 se muestra la configuración de parámetros que se debe realizar para que el servidor Zabbix reconozca el agente instalado en el equipo del punto anterior.

Figura 27
Configuración de parámetros del agente en Zabbix



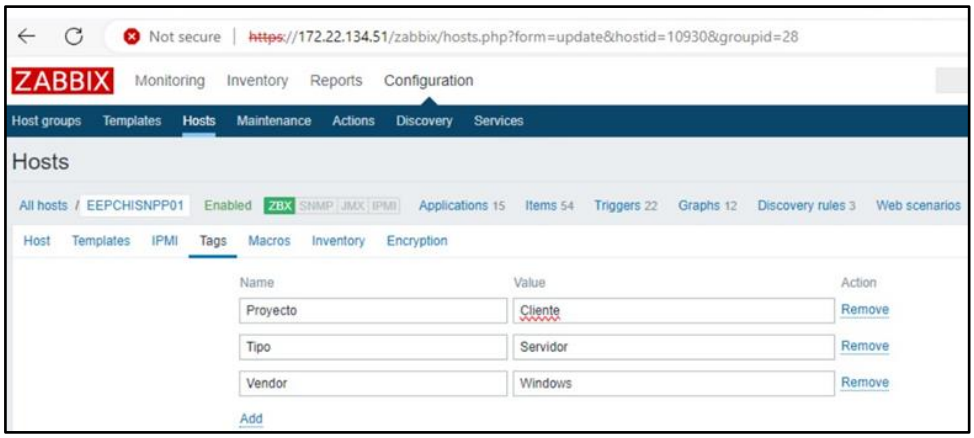
Nota: Elaboración propia

Figura 28
Selección de Template de monitoreo



Nota: Elaboración propia

Figura 29
Etiquetas de identificación del dispositivo



Nota: Elaboración propia

Campos obligatorios:

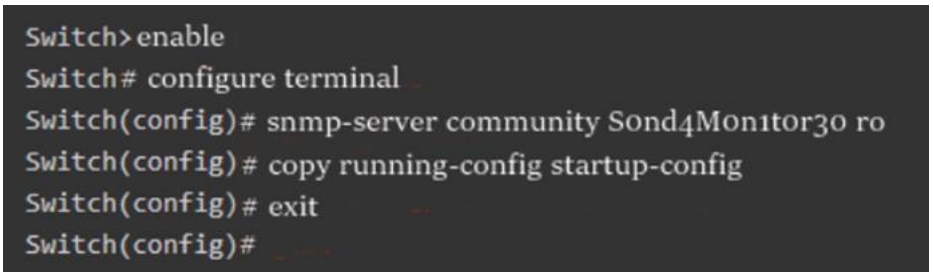
- HOSTNAME: Colocaremos el nombre con el cual identificamos al agente del dispositivo o servicio de TI.
- GROUPS: Elegiremos a qué grupo pertenece el equipo, por ejemplo, Servidores, aplicaciones, equipos de comunicación.
- DIRECCIÓN IP: Colocaremos la dirección IP del dispositivo o servicio de TI, que se desea monitorear.
- PORT: Colocamos el puerto correspondiente que utiliza Zabbix para el monitoreo.
- TEMPLATE: Seleccionamos el template correspondiente para cada dispositivo o servicio de TI.
- TAGS: Colocamos una etiqueta que identifique a cada dispositivo o servicio de TI.

Monitoreo por SNMP en Zabbix.

Habilitar el protocolo SNMP en Switch.

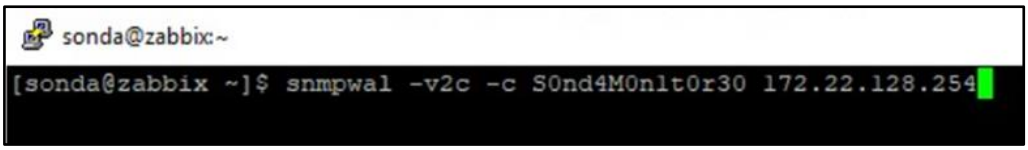
Utilizando la consola SSH, nos conectamos al equipo y configuramos el protocolo SNMP.

Figura 30
Configuración SNMP Switch



Nota: Elaboración propia

Figura 31
Comando para verificar conexión al switch

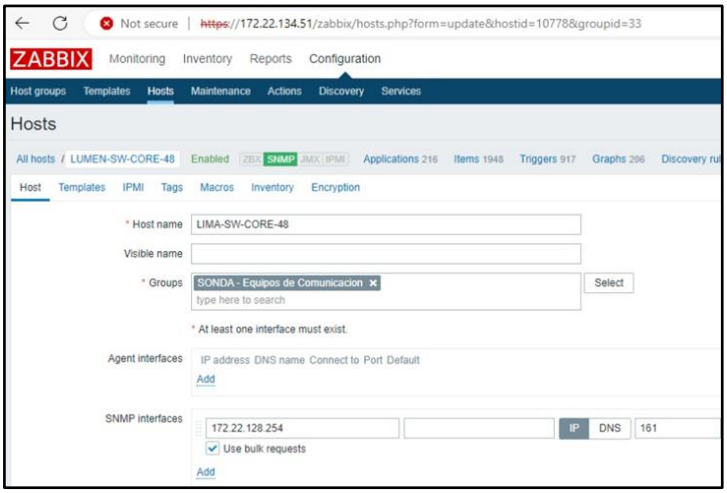


Nota: Elaboración propia

Configuración del dispositivo en Zabbix

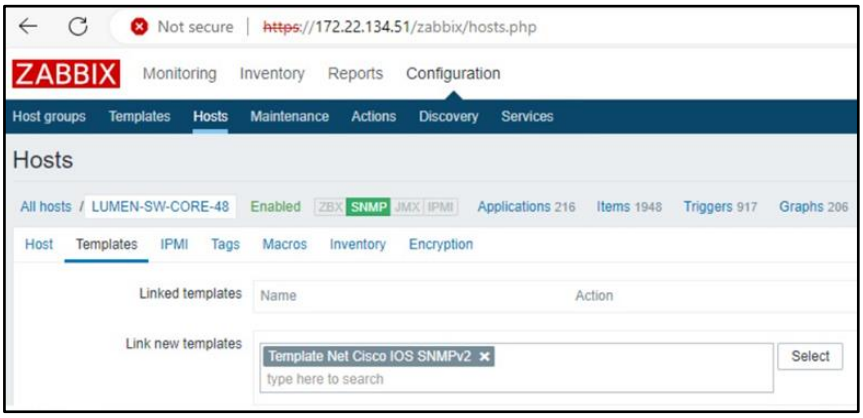
En la figura 32 se muestra la configuración de parámetros que se debe realizar para que el servidor Zabbix reconozca el equipo por SNMP.

Figura 32
Configuración de parámetros del dispositivo en Zabbix



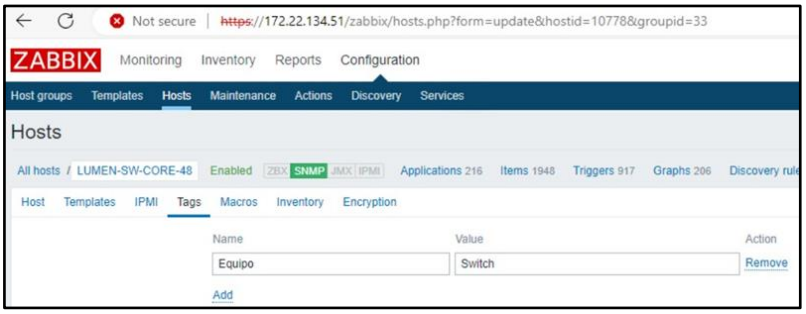
Nota: Elaboración propia

Figura 33
Selección de Template de monitoreo



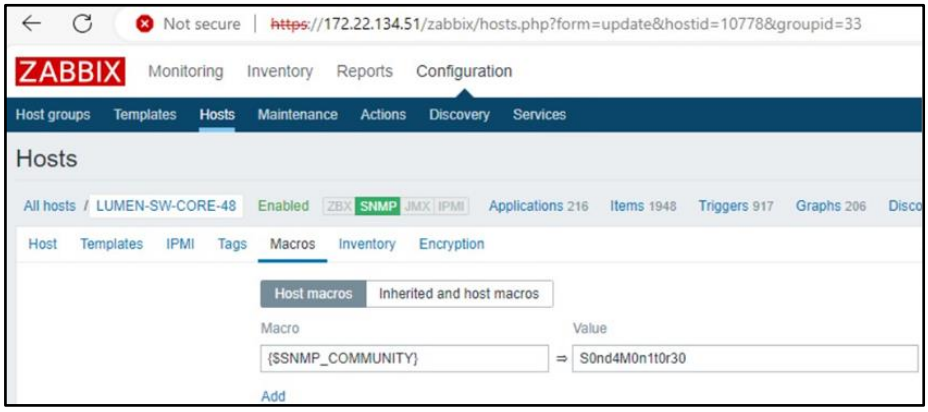
Nota: Elaboración propia

Figura 34
Etiquetas de identificación del dispositivo



Nota: Elaboración propia

Figura 35
SNMP comunidad del dispositivo



Nota: Elaboración propia

Campos obligatorios:

- HOSTNAME: Colocaremos el nombre con el cual identificamos al agente del dispositivo o servicio de TI.
- GROUPS: Elige a qué grupo pertenece el equipo, por ejemplo, Servidores, aplicaciones, equipos de comunicación.
- SNMP INTERFACE: Seleccionaremos monitoreo por SNMP
- DIRECCIÓN IP: Colocamos la dirección IP del dispositivo o servicio de TI de deseamos monitorear.
- PORT: Colocamos el puerto correspondiente que utiliza Zabbix para el monitoreo SNMP.
- TEMPLATE: Seleccionamos el template correspondiente para cada dispositivo o servicio de TI.
- HOST MACROS: Colocamos la comunidad SNMP que se colocó en el dispositivo a monitorear.
- TAGS: Colocamos una etiqueta que identifique a cada dispositivo o servicio de TI.

Monitoreo de sitios web.

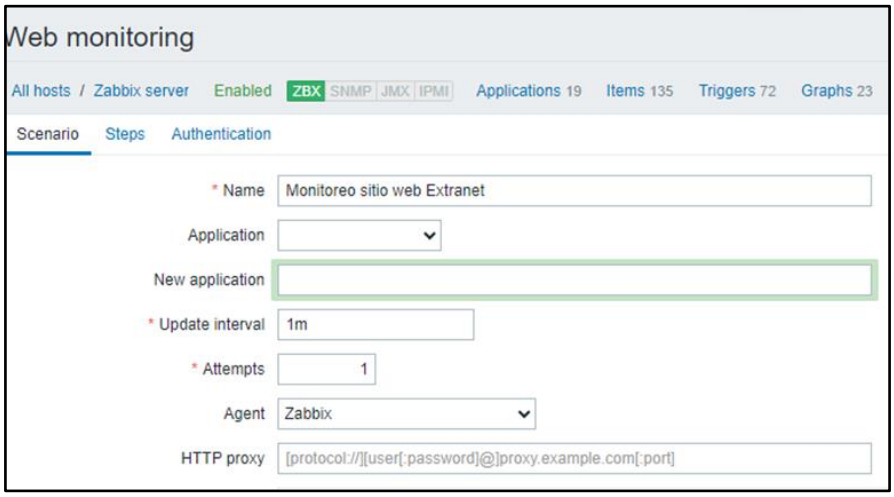
Configuración de Sitio Web en Zabbix.

Se utilizará las configuraciones web propias del servidor Zabbix, en la cual se realizará el monitoreo del código de estado de HTTP, se enfocará en los 2 códigos más importantes:

- 200: La solicitud fue recibida, entendida y aceptada con éxito.
- 400: La solicitud contiene una sintaxis incorrecta o no se puede cumplir .

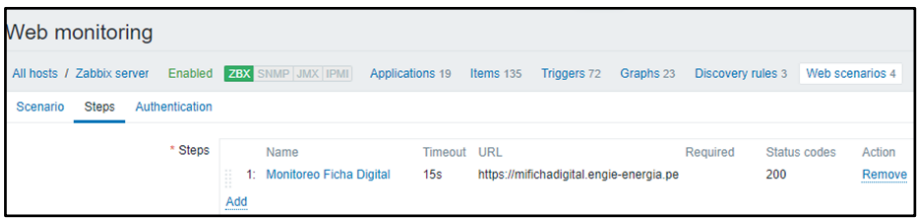
En la figura 36 se muestra la configuración de parámetros que se debe realizar para el monitoreo de los sitios web

Figura 36
Configuración de monitoreo Web



Nota: Elaboración propia

Figura 37
Configuración de steps estatus 200

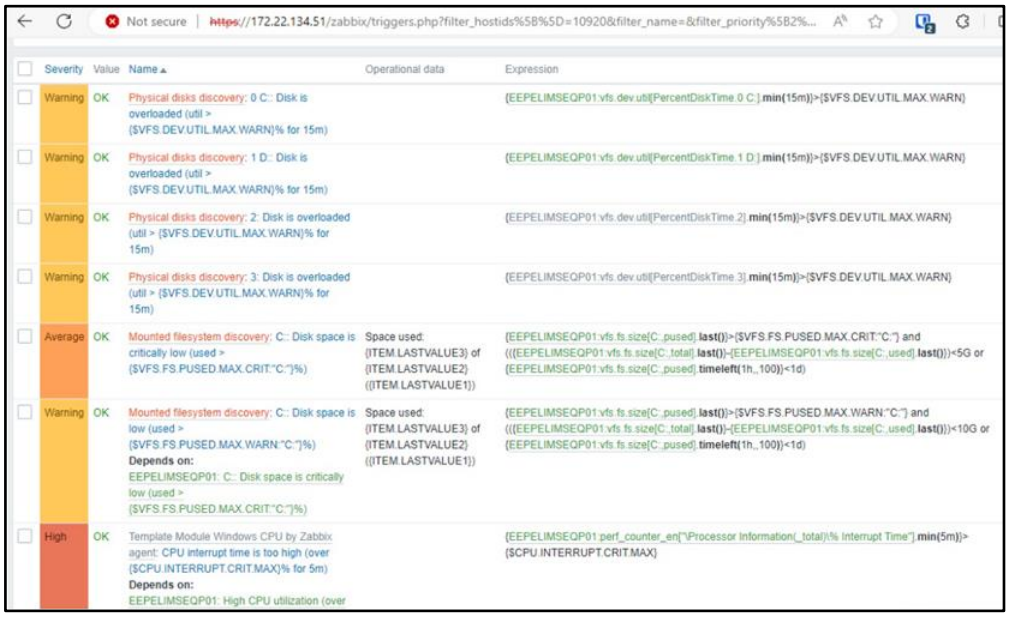


Nota: Elaboración propia

Alertas en dispositivos y servicios de TI.

De acuerdo con la tabla indicada en el punto anterior donde se muestran los valores máximos de los parámetros a monitorear, estos no deben exceder, en caso excedan se genera la alerta correspondiente.

Figura 38
Alertas configuradas en servidores

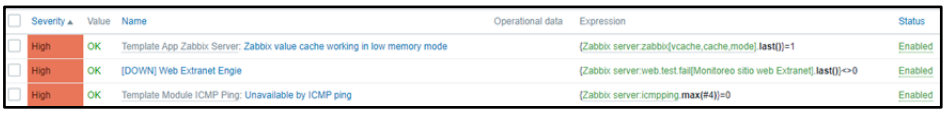


Nota: Elaboración propia

Figura 39
Alertas configuradas de interfaces en Switch

Nota: Elaboración propia

Figura 40
Alertas configuradas de Sitios web



Severity ▲	Value	Name	Operational data	Expression	Status
High	OK	Template App Zabbix Server: Zabbix value cache working in low memory mode		{Zabbix server:zabbix[vcache,cache,mode].last()}=1	Enabled
High	OK	[DOWN] Web Extranet Engie		{Zabbix server:web.test.fail[Monitoreo sitio web Extranet].last()}<>0	Enabled
High	OK	Template Module ICMP Ping: Unavailable by ICMP ping		{Zabbix server:icmpping.max(#4)}=0	Enabled

Nota: Elaboración propia

Notificaciones.

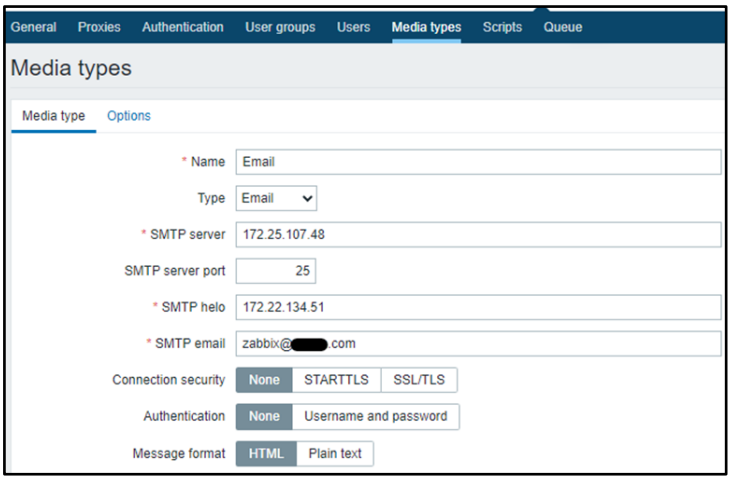
Una vez que Zabbix se encuentre configurado con el monitoreo de los diversos dispositivos y servicios de TI, los operadores deben estar en constante visualización de la plataforma para poder verificar que ocurra alguna incidencia, adicional a ello es necesario configurar las notificaciones que alertan al operador ante alguna incidencia.

En el sistema de monitoreo se van a configurar notificaciones a través de correo corporativo y Telegram.

Notificaciones por correo corporativo

Esta configuración se debe realizar dentro de la opción Media Type en Zabbix, en la cual colocaremos el servidor SMTP y el correo electrónico que enviará la notificación.

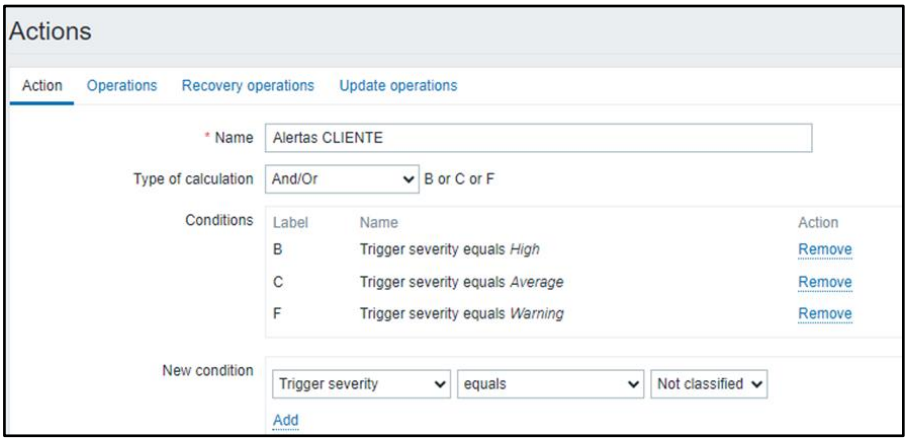
Figura 41
Configuración de SMTP



Nota: Elaboración propia

En acciones, se configuran las alertas que se van a notificar.

Figura 42
Configuración de acciones de alertas



Nota: Elaboración propia

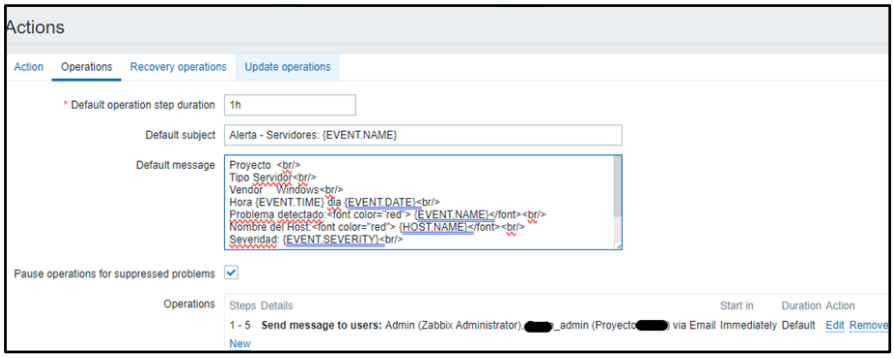
En Operaciones, configuramos lo siguientes:

Mensaje de alerta: Plantilla de mensaje cuando surge una alerta.

Mensaje de alerta resuelta: Plantilla de mensaje cuando la alerta se resolvió.

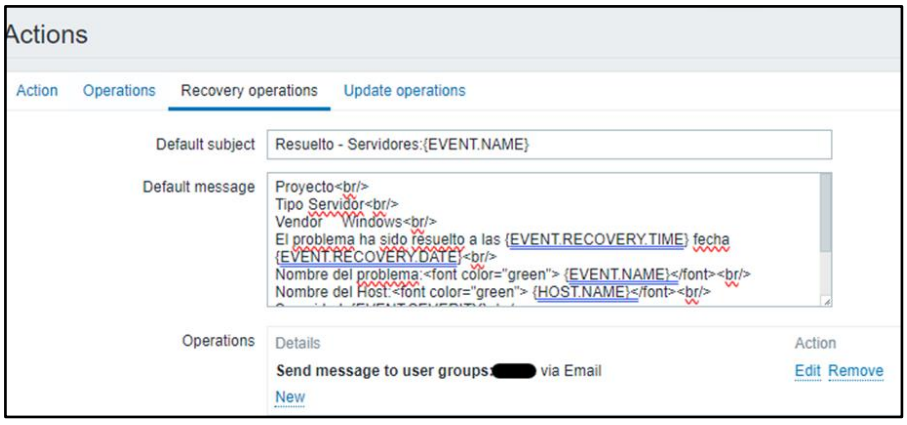
Grupo de usuarios administradores: Usuarios administradores que se van a alertar en la notificación.

Figura 43
Configuración de mensajes de alerta



Nota: Elaboración propia

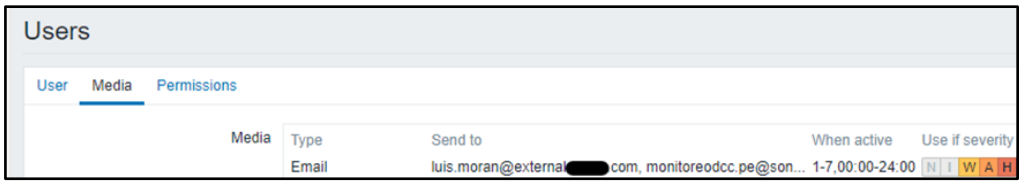
Figura 44
Configuración de mensajes de alerta resuelta



Nota: Elaboración propia

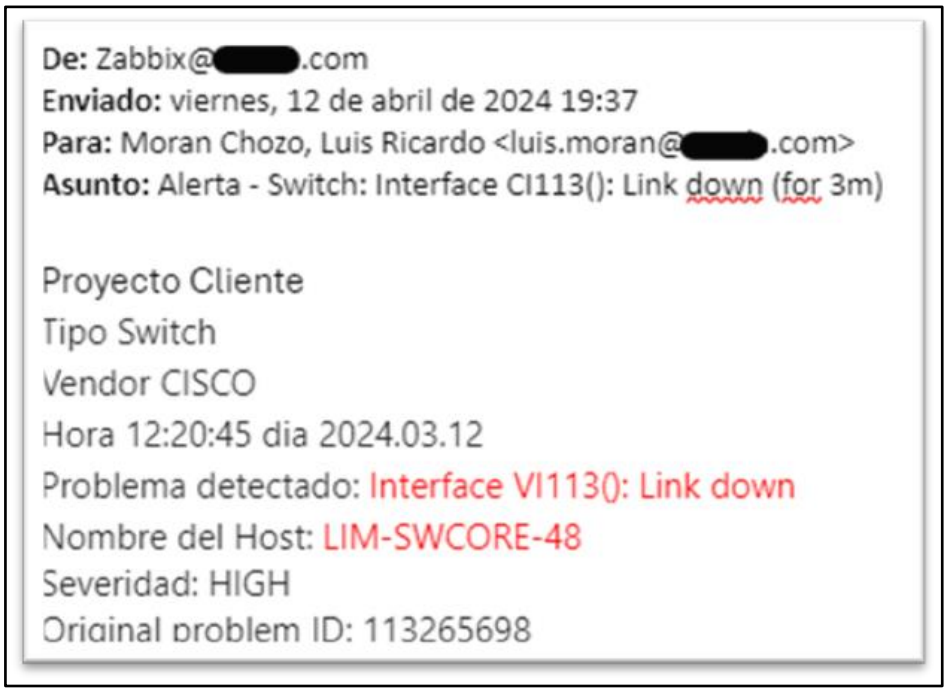
En Usuarios configuramos los usuarios que van a recibir las notificaciones por correo corporativo.

Figura 45
Configuración de correos corporativos



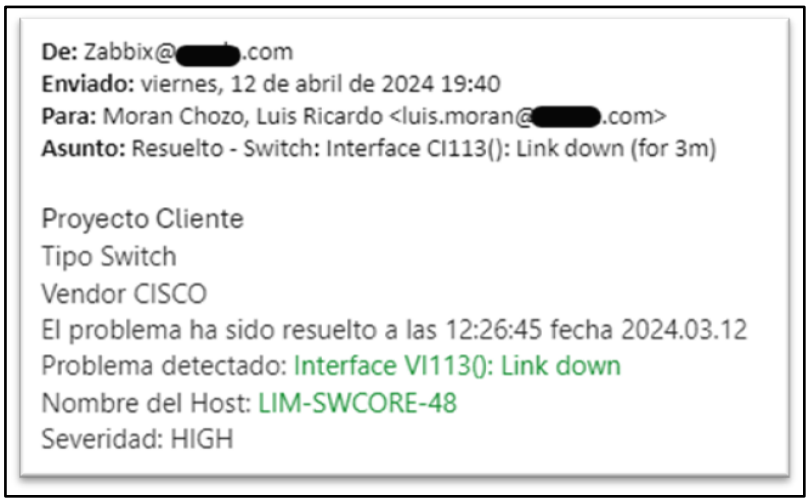
Nota: Elaboración propia

Figura 46
Notificaciones de alerta por correo



Nota: Elaboración propia

Figura 47
Notificaciones de alerta resuelta por correo

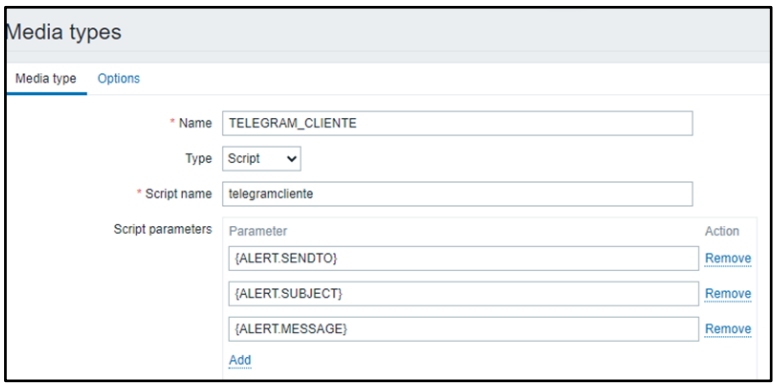


Nota: Elaboración propia

Notificaciones por Telegram.

Esta configuración se debe realizar dentro de la opción Media Type en Zabbix, en la cual colocaremos el script del ID del grupo creado en Telegram.

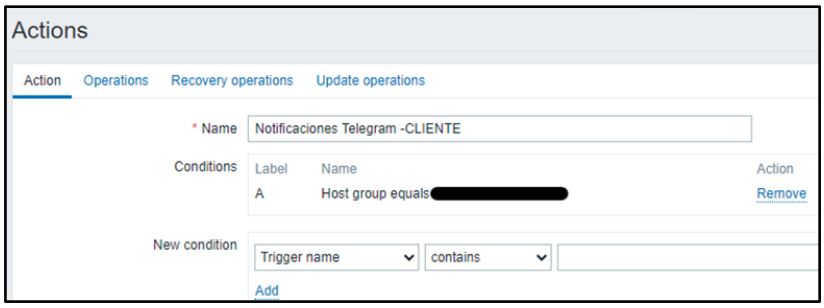
Figura 48
Configuración de Telegram



Nota: Elaboración propia

En acciones, se configuran las alertas que se van a notificar.

Figura 49
Configuración de acciones para Telegram



Nota: Elaboración propia

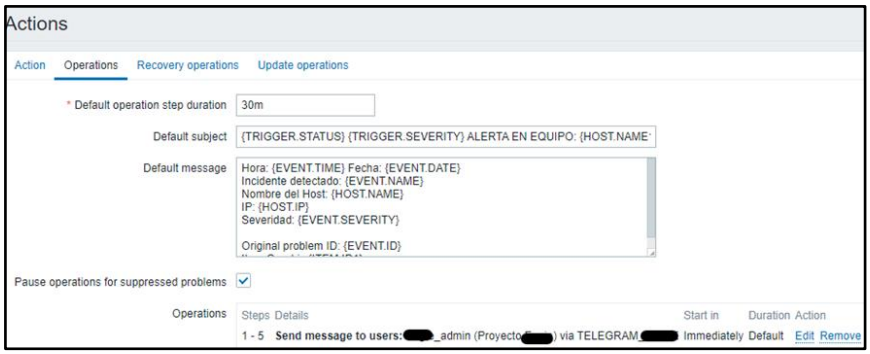
En Operaciones, configuramos lo siguientes:

Mensaje de alerta: Plantilla de mensaje cuando surge una alerta.

Mensaje de alerta resuelta: Plantilla de mensaje cuando la alerta se resolvió.

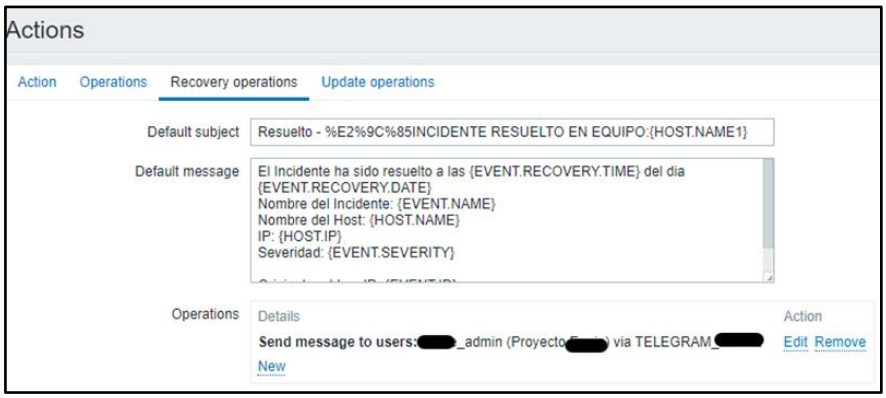
Grupo de usuarios administradores: Usuarios administradores que se van a alertar en la notificación.

Figura 50
Configuración de mensajes de alerta Telegram



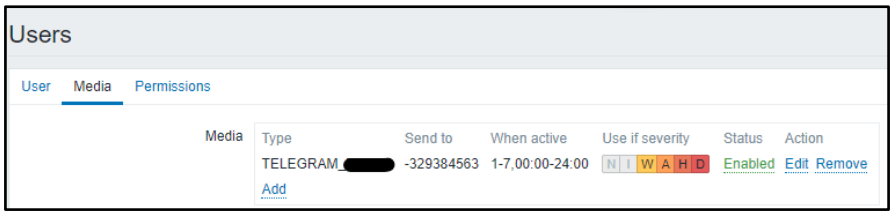
Nota: Elaboración propia

Figura 51
Configuración de mensajes de alerta resuelta Telegram



Nota: Elaboración propia

Figura 52
Configuración del ID de Grupo de Telegram

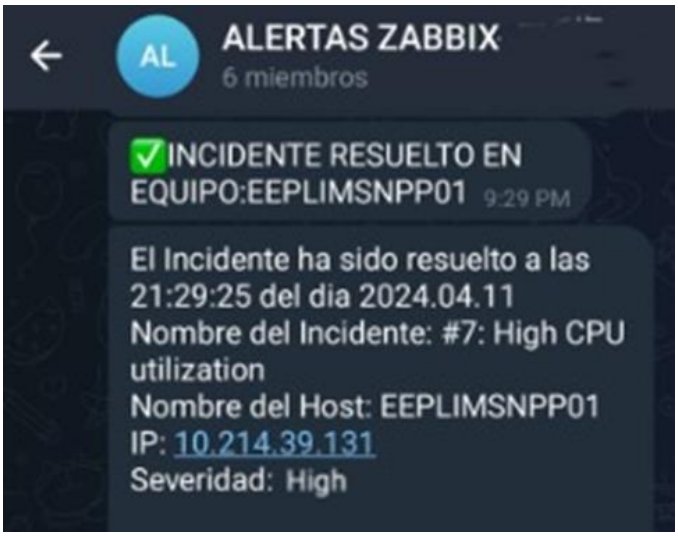


Nota: Elaboración propia

Figura 53
Notificaciones de alertas en Telegram

Nota: Elaboración propia

Figura 54
Notificaciones de alertas resueltas en Telegram



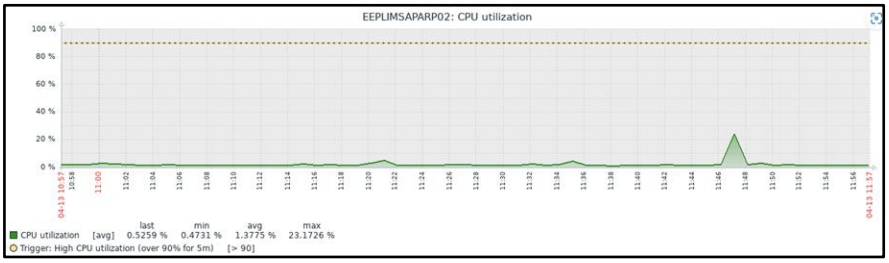
Nota: Elaboración propia

Gráficas de monitoreo.

En esta sección se obtienen las gráficas de cada equipo o grupo de equipos configurados de acuerdo a los templates de monitoreo de recursos.

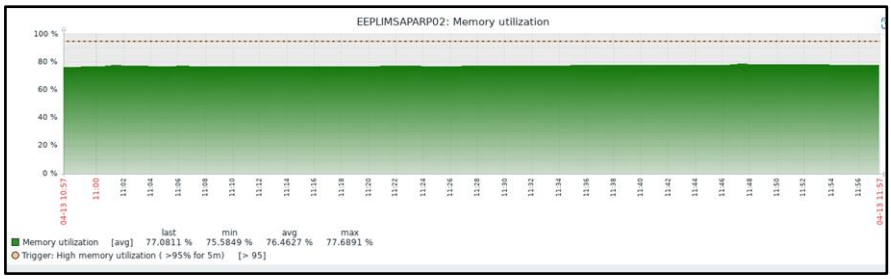
Se pueden visualizar gráficas por periodos de tiempos que ayudan a analizar el estado en el tiempo de los equipos monitoreados.

Figura 55
Gráfica de Utilización de CPU



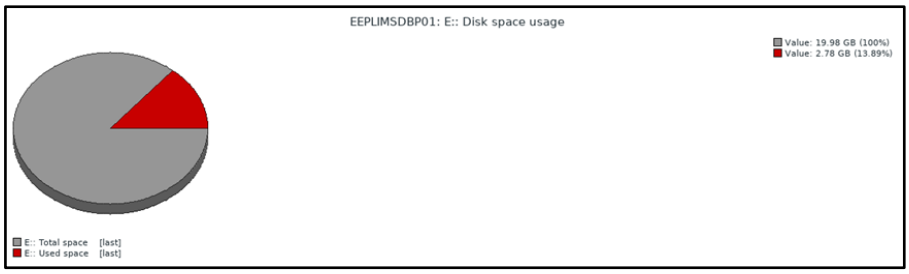
Nota: Elaboración propia

Figura 56
Gráfica de Utilización de Memoria RAM



Nota: Elaboración propia

Figura 57
Gráfica de Utilización de Disco duro



Nota: Elaboración propia

Mapas de red.

En el mapa de red podemos visualizar el estado de los equipos configurados en Zabbix.

En la implementación se elaboró el mapa de red con todos los dispositivos de la empresa Cliente.

Figura 58
Mapa de red de Infraestructura Cliente

Nota: Elaboración propia

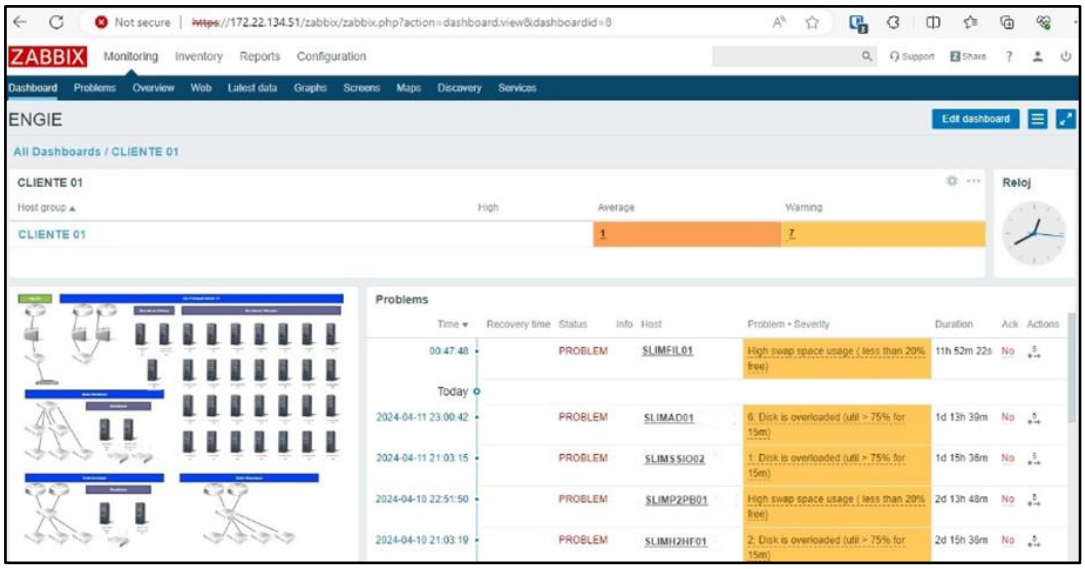
Dashboard Principal.

En el Panel principal de Zabbix se visualiza la información más relevante del monitoreo, la cual se puede personalizar de acuerdo a nuestras expectativas.

En el Dashboard de la implementación del sistema se consideró mostrar lo siguiente:

- Niveles de alertas: Muestra la cantidad de alertas por cada nivel (Warning, Average, High).
- Problemas: Muestra la lista de los problemas presentes en los equipos.
- Mapa de red: Muestra el estado de todos los equipos monitoreados.
- Reloj: Muestra la hora actual.

Figura 59
Panel principal de monitoreo Zabbix.



Nota: Elaboración propia

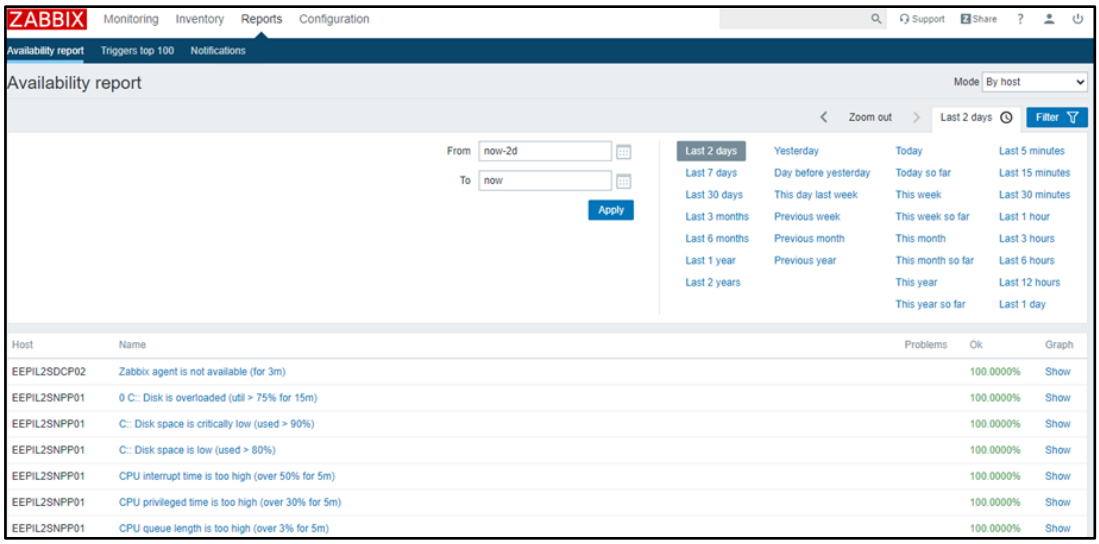
Reportes.

Reportes de disponibilidad

En esta sección podemos visualizar los reportes del estado de la disponibilidad de los servicios y dispositivos monitoreados en un periodo de tiempo determinado.

En la Figura 51 muestra el estado de los recursos y servicios de un servidor.

Figura 60
Reportes de disponibilidad



Nota: Elaboración propia

EVALUAR EL DESEMPEÑO DEL SISTEMA DE MONITOREO ACTUAL EN RELACIÓN A LA GESTIÓN DE INCIDENTES.

Resultados

Haciendo uso del sistema anterior PRTG y el sistema implementado Zabbix, se realizaron pruebas con el propósito de determinar mejoras.

TIEMPO DE NOTIFICACIÓN DE UNA INCIDENCIA.

A) Resultados antes de la implementación del sistema.

Según los resultados de las pruebas realizadas al sistema anterior implementado ver (Anexo 3), se obtiene lo siguiente:

Tabla 15
Indicador 1 – Antes de implementar el sistema

Tiempo de notificación de incidencia (segundos)		Forma de medida
Sistema PRTG	Correo electrónico	Se utilizó el sistema de monitoreo antiguo
322	490	

Nota: Reportes de notificaciones de PRTG

B) Resultados con la implementación del sistema.

Según los resultados de las pruebas realizadas al sistema implementado ver (Anexo 4), se obtiene lo siguiente:

Tabla 16
Indicador 1 – Con la implementación del sistema.

Tiempo de notificación de incidencia (segundos)			Forma de medida
Sistema Zabbix	Correo electrónico	Telegram	Se utilizó el sistema de monitoreo actual
59	77	60	

Nota: Reportes de notificaciones de Zabbix

Interpretación de los resultados.

Como se puede visualizar en las tablas N° 15 y N° 16, el resultado del antes y después de la implementación del sistema de monitoreo, con la implementación se ha reducido el tiempo de entrega de notificaciones ante una incidencia de un dispositivo o servicios de TI monitoreado, donde:

- Se redujo el tiempo a 59 segundos promedio para mostrar la incidencia en el sistema de monitoreo.
- Se redujo el tiempo a 77 segundos promedio para mostrar la notificación en la bandeja de correo corporativo.
- Se implementó la notificación por Telegram, con un tiempo de 60 segundos para mostrar la notificación.

TIEMPO DE ATENCIÓN DE LA INCIDENCIA

Así mismo, en base a la información recopilada mediante el cuestionario ver (Anexo 2 y 3) aplicado al personal de TI de la empresa tecnológica (4 Administradores y 3 operadores de TI), se obtuvo lo siguiente,

A) Resultados antes de la implementación del sistema.

Tabla 17
Indicador 3 – Antes de implementar el sistema

Indicador	0 a 30 Min	31 Min a 1 hora	1 a 4 horas
Tiempo de atención de la incidencia	30%	60%	10%

Nota: Elaboración propia

B) Resultados con la implementación del sistema.

Tabla 18
Indicador 3 – Con la implementación del sistema

Indicador	0 a 30 min	31 a 1 hora	1 a 2 horas
Tiempo de atención de la incidencia	80%	15%	5%

Nota: Elaboración propia

Interpretación de los resultados.

Como se puede visualizar en las tablas N° 17 y N° 18, el resultado del antes y después de la implementación del sistema de monitoreo, con la implementación se ha reducido el tiempo de atención de un incidente de un dispositivo o servicios de TI monitoreado por parte de los administradores y operadores de TI, donde:

- Antes de la implementación el 30% de atención de un incidente era de 0 a 30 minutos, el 60% era de 31 minutos a 1 hora y el 10% de 1 a 4 horas.
- Con la implementación el 80% de atención de un incidente es de 0 a 30 minutos, el 15% es de 31 minutos a 1 hora y el 5% de 1 a 2 horas.

En conclusión, la implementación del sistema ayudó a que la mayor parte de los incidentes (80%) se atendieran entre 0 a 30 minutos.

CONCLUSIONES

- Se identificaron satisfactoriamente los dispositivos y servicios de la infraestructura de TI del Cliente, los cuales se incorporaron al sistema de monitoreo implementado.
- Teniendo en cuenta sus características funcionales, se seleccionó para la implementación a la herramienta de monitoreo Zabbix, la cual es software libre, y ayuda notablemente en la detección de incidentes que afectan a los dispositivos y servicios de la infraestructura de TI del cliente.
- Se implementó el sistema de monitoreo con la herramienta de software Zabbix, incorporando los dispositivos y servicios de TI que requieren ser monitoreados, se incluyeron alertas y notificaciones que permiten tener una inmediata atención y solución de incidentes presentados en la organización.
- Se logró mejorar la gestión de incidentes de la empresa tecnológica, la cual fue sustentada en base a tiempos. Primero, se redujo el tiempo a 59 segundos promedio para mostrar la incidencia en el sistema de monitoreo; se redujo el tiempo a 77 segundos promedio para mostrar la notificación en la bandeja de correo corporativo y se implementó la notificación por Telegram, con un tiempo de 60 segundos para mostrar la notificación. Segundo, antes de la implementación el 30% de las atenciones de incidentes era de 0 a 30 minutos, el 60% era de 31 minutos a 1 hora y el 10% de 1 a 4 horas y con la implementación el 80% de atención de un incidente es de 0 a 30 minutos, el 18% es de 31 minutos a 1 hora y el 2% de 1 a 2 horas.

RECOMENDACIONES

- De acuerdo a las actualizaciones de versiones que lanza Zabbix, se recomienda actualizar a una versión más actual y estable, esto permitiría de ser necesario incluir más funciones al sistema.
- Se recomienda incorporar al sistema de monitoreo, una conexión con un sistema de tickets, esto permitiría generar tickets automáticamente para el registro de atenciones de incidentes.
- Se recomienda realizar un respaldo diario del servidor Zabbix, ya que actualmente solo se respalda de manera semanal.
- Se recomienda a los administradores y operadores de sistemas que eliminen los host dados de bajas para que no muestren el sistema de monitoreo.

REFERENCIAS BIBLIOGRÁFICAS

Ariganello, E. (2016). *Redes Cisco - Guía de estudio para la certificación CCNA Routing y Switching* (4a ed.). España. https://books.google.com.ec/books?id=tpBFDwAAQBAJ&printsec=frontcover&hl=es#v=onepage&q&f=false

Boronat, F., & Montagud, M. (2013). *Direccionamiento e interconexión de redes basada en TCP/IP (IPv4/IPv6, DHCP, NAT, Encaminamiento RIP y OSPF)* (1a ed.). España.

Cacti. (2024). *Cacti* [Desarrollo]. About Cacti. https://www.cacti.net/

Carracedo, J. (2011, January). *Introducción a la seguridad en redes telemáticas*. https://docplayer.es/21468617-Leccion-4-introduccion-a-la-seguridad-en-redes-telematicas.html

Casas, R., & Sempértegui, M. (2017). *Implementación de un Sistema de Monitoreo y Supervisión de la Infraestructura y Servicios de red para optimizar la Gestión de TI en la Universidad Nacional Pedro Ruiz Gallo*. Universidad Nacional Pedro Ruiz Gallo.

Castro, J. (2015). *Optimización de la administración en la red de datos de la universidad técnica del norte implementando un sistema de monitoreo de equipos y servicios utilizando software libre*. Universidad Técnica del Norte.

Estrada, A. (2004). PROTOCOLOS TCP/IP DE INTERNET. *Revista Digital Universitaria*, *5*(8), 7. https://www.revista.unam.mx/vol.5/num8/art51/sep_art51.pdf

Free Software Magazine. (2024, April 18). *Nagios* [Informativo]. Nagios vs. Icinga: La Verdadera Historia de Uno de Los Forks Más Candentes Del Software Libre. http://freesoftwaremagazine.com/articles/nagios_and_icinga/

Github. (2024). *Cacti* [Repositorio]. Github. https://github.com/Cacti/cacti

Gómez, V. (2012). *Curso de Fundamentos de ITIL®* (2011th ed.). Madrid (España).

Lago, A., & Mera, D. (2013). *Implementación virtual de redes LAN, enfocadas en el análisis comparativo de las ventajas y desventajas del uso y aplicación de las diferentes versiones del protocolo SNMP* [Tesis, ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL]. https://www.dspace.espol.edu.ec/bitstream/123456789/42243/1/D-84286.pdf

Lerena, S. (2023, June 20). PandoraFMS. Community by Pandora FMS. https://pandorafms.com/blog/es/monitoreo-de-red-que-debemos-saber/

Linux Journal. (2009). Munin—the Raven Reports. https://www.linuxjournal.com/article/10248

López, Y., & Vásquez, A. (2016). *La Gestión de Servicios de soporte técnico en el ciclo de vida del desarrollo de software*. *10*, 46–60. http://rcci.uci.cu

Luna, D. (2015, August 19). *Nagios*. ¿Qué es Nagios? https://www.nagios.org/about/

Málaga, G. (2016). *Modelo de Gestión de Incidentes Basado en ITIL v.3*. Universidad Privada de Tacna.

Millán, R. (2003). *Qué es... SNMPv3 (Simple Network Management Protocol version 3)*. Componentes Básicos de SNMP. https://www.ramonmillan.com/tutoriales/snmpv3.php

Montenegro. (2018, December 21). *Rivas*. Monitoreo de TI: 5 Razones Para Llevarlo a Cabo En Tu Empresa. https://www.gb-advisors.com/es/monitoreo-de-ti/

Mori, A. (2021). *Sistema de monitoreo de infraestructura de TI y su influencia en la gestión de incidencias en la red LAN de la empresa Electro Oriente S.A. – Unidad de Negocios Bellavista* [Tesis]. Universidad Nacional de San Martín.

Munin. (2024). *Munin*. Munin. https://munin-monitoring.org/

Niño, M. (2007). Diseño de una Herramienta Web para Manipular Imágenes Médicas. *Revista Capital Intelectual*, *17*, p 7.

Orellana, I., & Ortiz, E. (2022). *Implementación de la gestión de servicios de TI basados en ITIL v3 para la mejora de la gestión de incidencias en la empresa Solgas 2021*. Universidad Tecnológica del Perú.

Ortiz, M., & Mori, A. (2017, June). *Biblioteca UPAGU*. 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. http://repositorio.upagu.edu.pe/handle/UPAGU/278

Quispe, J. (2019). *Implementación de un prototipo de monitoreo de dispositivos de comunicación y usuarios finales utilizando el protocolo SNMP basada en software libre para una empresa e-Commerce*. Universidad Nacional Mayor de San Marcos.

Redes Lan 2016. (2016, March 8). Nagios. https://redeslan2016.wordpress.com/2016/03/08/nagios/

Rojas, J. (2023, June 22). *Tecnoseguro*. Protocolo SNMP y Su Relación Con Videovigilancia. https://www.tecnoseguro.com/analisis/pro/protocolo-snmp-videovigilancia

Sossa, W. (2015). *Manual De Aplicación Snmp App* (2a ed.). Colombia. https://www.calameo.com/read/004616184bd10d34e0641

Tanenbaum, A., & Wetherall, D. (2012). *Redes de computadoras* (5th ed.). México. https://bibliotecavirtualapure.wordpress.com/wp-content/uploads/2015/06/redes_de_computadoras-freelibros-org.pdf

Troncoso, N. (2023). *Layer 123*. Las 5 Mejores Herramientas Open Source Gratuitas Para El Monitoreo de Redes y Servidores, Más Un Bonus Adicional. https://layer1234.cl/2023/05/30/herramientas-monitoreo-redes-servidores/

Van Bon, J., De Jong, A., Kolthof, A., Pieper, M., Tjassing, R., Van Der Veen, A., & Verheijen, T. (2008). *Gestión de Servicios TI basado en ITIL® V3 - Guia de Bolsillo* (1a ed.). Holanda.

Wikipedia. (2024, January 18). Icinga. https://es.wikipedia.org/wiki/Icinga

Zabbix. (2024). Explora Las Funciones de Zabbix. https://www.zabbix.com/features

Zabbix SIA. (2024). *Documentation ZABBIX*. https://www.zabbix.com/documentation/4.4/en/manual/installation/requirements

Zenoss Inc. (2024). *Zenoss*. Zenoss Own IT. https://www.zenoss.com/

ANEXOS

ANEXO 01: Cuestionario de monitoreo al sistema anterior

Cuestionario informativo: "SISTEMA DE MONITOREO ACTUAL"

El objetivo de este cuestionario es recopilar información acerca del sistema de monitoreo actual que maneja la organización, esto nos permitirá entender las necesidades y requerimientos con respecto a la administración de monitoreo y gestión de incidentes

. **1. ¿Monitorea la infraestructura de TI de su organización?**

Marca solo un óvalo.

- Si
- No

2. En caso la pregunta 1 sea SI. ¿Qué tipo de monitoreo realiza en la infraestructura de TI (Dispositivos y servicios de TI)?

Marca solo un óvalo.

- Manual
- Sistema informático propietario.
- Sistema informático Libre
- Ninguno

3. Indique el sistema informático que utiliza.

Marca solo un óvalo.

- Zabbix
- PRTG
- CACTI
- SOLARWINDS
- Otros: _____

4. ¿Qué tiempo monitorea su infraestructura?

Marca solo un óvalo.

- Siempre (diario).
- Casi siempre (semanal).
- Muy a menudo (Mes).
- Aveces (Año).
- Nunca.

5. ¿Su sistema actual es eficente en el monitoreo?

Marca solo un óvalo.

- SI
- Aveces
- No

6.Si la respuesta es NO o AVECES, indique que mejoraria.

7. ¿Su sistema cuenta con envío de notificaciones de alertas?

Marca solo un óvalo.

- SI
- NO

8. Si su resuesta es SI, ¿Las notificaciones de alertas, cada que tiempo las revisa?

Marca solo un óvalo.

- Siempre
- A veces
- Nunca

9. Con el sistema actual ¿Qué tiempo promedio le toma dar respuesta a una incidencia?

Marca solo un óvalo.

- Inmediatamente llegue la notificación (0 a 10 Min).
- Cuando lo visualice en el sistema (11 a 30 min).
- Inmediatemente le informe Mesa de Ayuda (31 min a 1 hora).

10. Con el sistema actual. ¿Qué tiempo promedio le toma solucionar una incidencia leve?

Marca solo un óvalo.

- 0 a 30 min.
- 31 min a 1 hora.
- 1 a 2 horas.
- 2 a 5 horas.

11. Con el sistema actual. ¿Qué tiempo promedio le toma solucionar una incidencia grave?

Marca solo un óvalo.

- 0 a 30 min.
- 31 min a 1 hora.
- 1 a 2 horas.
- 2 a 5 horas.

ANEXO 02: Resultados del cuestionario aplicado al personal del TI de la empresa tecnológica con el sistema de monitoreo actual.

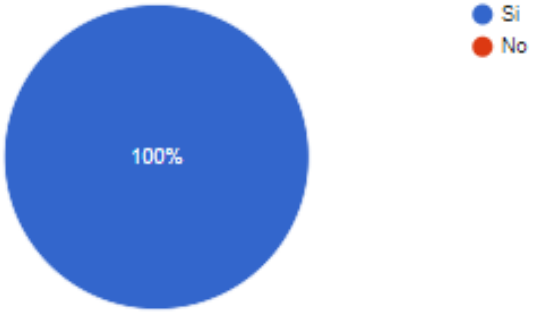
Cuestionario informativo: "SISTEMA DE MONITOREO ACTUAL"

7 respuestas

Publicar análisis

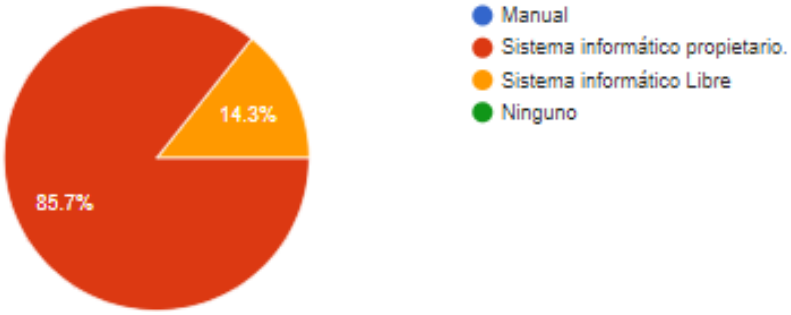
1. ¿Monitorea la infraestructura de TI de su organización? Copiar

7 respuestas



2. En caso la pregunta 1 sea SI. ¿Qué tipo de monitoreo realiza en la infraestructura de TI (Dispositivos y servicios de TI)? Copiar

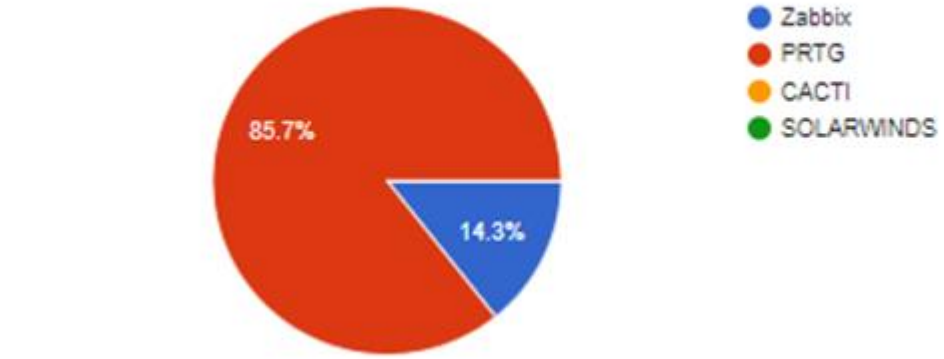
7 respuestas



3. Indique el sistema informático que utiliza.

Copiar

7 respuestas



4. ¿Qué tiempo monitorea su infraestructura?

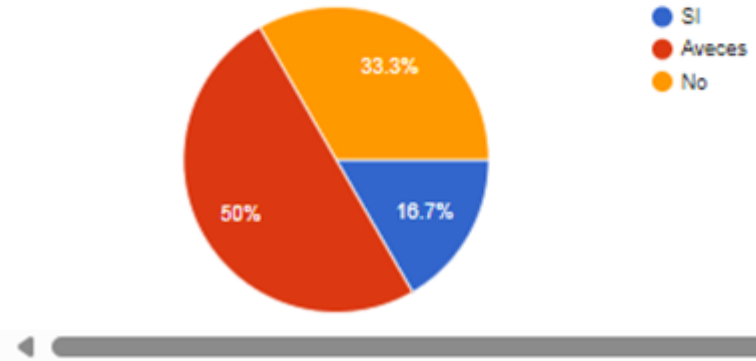
Copiar

6 respuestas

5. ¿Su sistema actual es eficente en el monitoreo?

Copiar

6 respuestas



6.Si la respuesta es NO o AVECES, indique que mejoraria.

7 respuestas

Mejoraría:
1. Tiempo de alertas en el sistemas.
2. Tiempo de notificaciones.
3. lentitud en el sistema de monitoreo.
4. Limitaciones en añadir más dispositivos.

Demoran las alertas y notificaciones
añadimos más dispositivos y genera lentitud.
Monitoreo a destiempo.

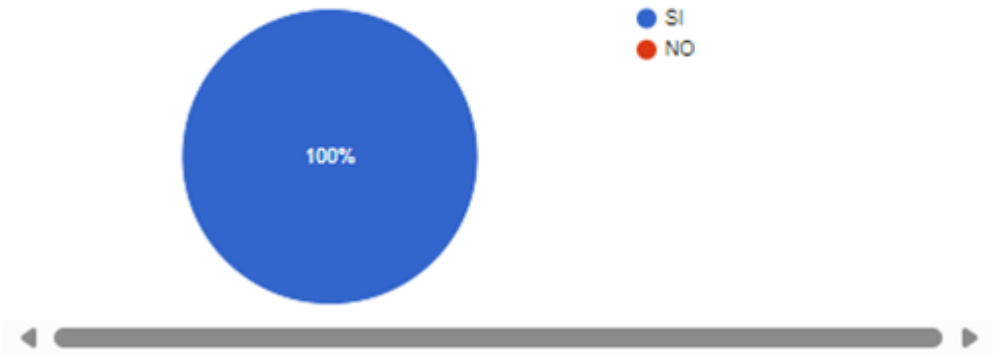
Los tiempos de alertas en el sistema, los tiempos de notificación en el correo, mejorar los recursos del servidor.

Alertas, notificaciones, más dispositivos, un sistema más robusto.

Implementar un mejor sistema ya que el actual tenemos inconvenientes con el monitoreo.

7. ¿Su sistema cuenta con envío de notificaciones de alertas? Copiar

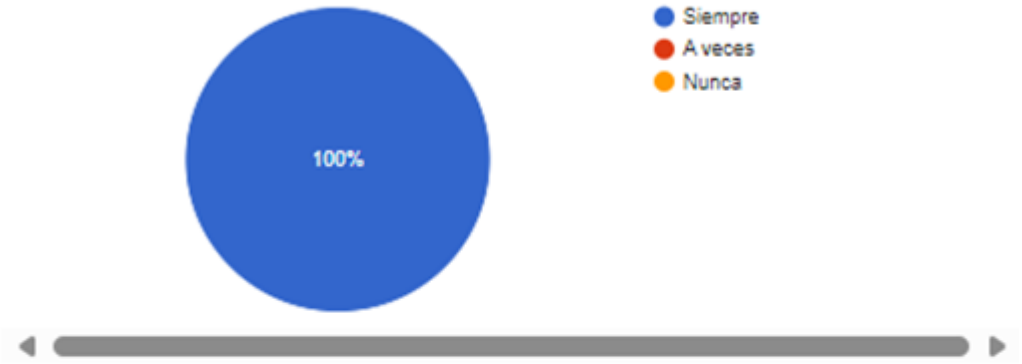
7 respuestas



8. Si su resuesta es SI, ¿Las notificaciones de alertas, cada que tiempo las revisa?

Copiar

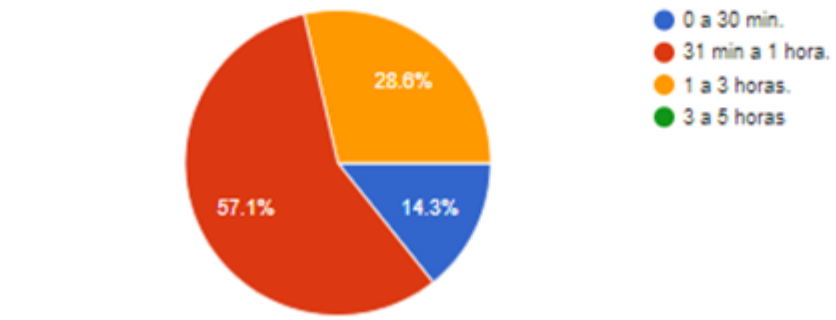
7 respuestas



9. Con el sistema actual. ¿Qué tiempo promedio le toma solucionar una incidencia?

Copiar

7 respuestas



ANEXO 03: Resultados del cuestionario aplicado al personal del TI de la empresa tecnológica con el sistema implementado.

Cuestionario informativo: "SISTEMA DE MONITOREO Implementado"

7 respuestas

Publicar análisis

1. ¿Monitorea la infraestructura de TI de su organización?

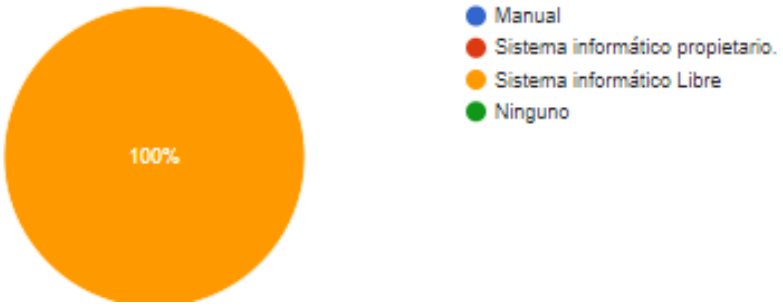
Copiar

7 respuestas

2. En caso la pregunta 1 sea SI. ¿Qué tipo de monitoreo realiza en la infraestructura de TI (Dispositivos y servicios de TI)?

Copiar

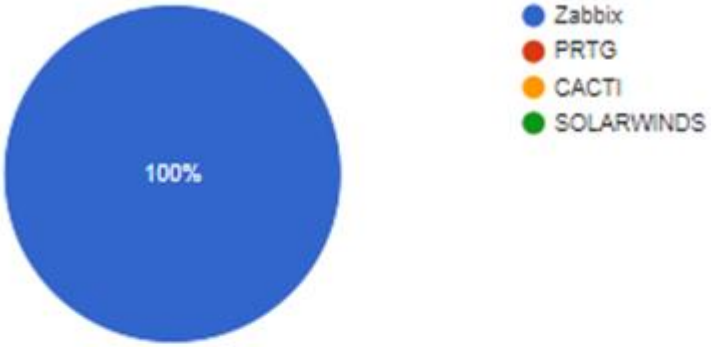
7 respuestas



3. Indique el sistema informático que utiliza.

Copiar

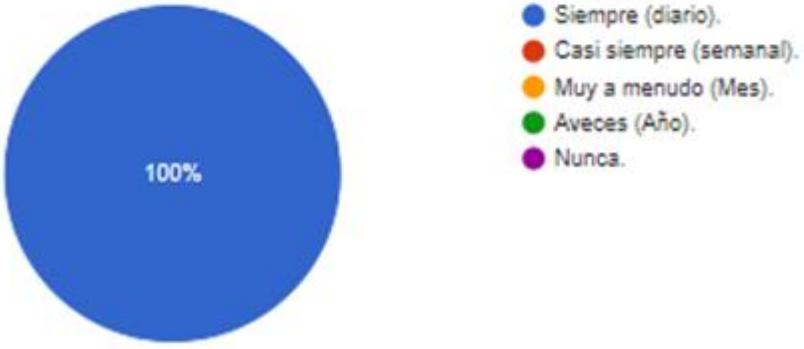
7 respuestas



4. ¿Qué tiempo monitorea su infraestructura?

Copiar

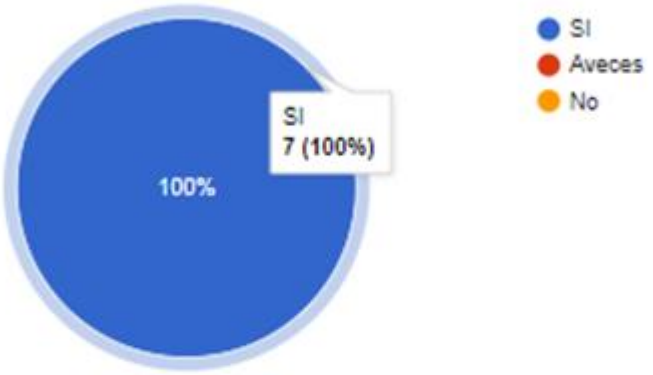
7 respuestas



5. ¿Su sistema actual es eficente en el monitoreo?

Copiar

7 respuestas



6.Si la respuesta es NO o AVECES, indique que mejoraria.

0 respuestas

Todavía no hay respuestas para esta pregunta.

8. Si su resuesta es SI, ¿Las notificaciones de alertas, cada que tiempo las revisa?

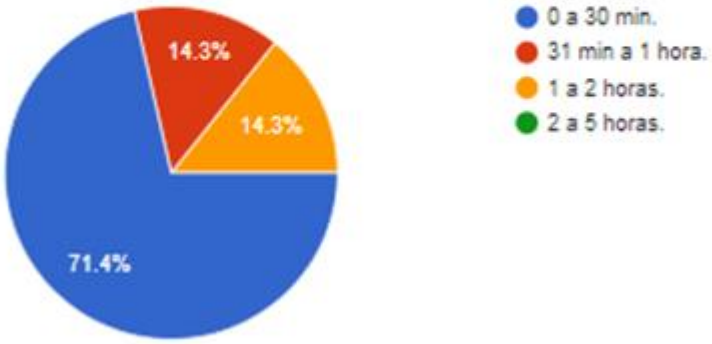
Copiar

7 respuestas

9. Con el sistema Implementado. ¿Qué tiempo promedio le toma solucionar una incidencia?

Copiar

7 respuestas



ANEXO 04: Pruebas de incidencias con el sistema anterior.

Prueba	Hora de incidencia	Hora de alerta en el sistema	Hora de notificación en el correo	Tiempo en notificar en el sistema (Segundos)	Tiempo en notificar en el correo (Segundos)
1	9:16:30	9:21:30	9:22:32	300	362
2	11:30:40	11:36:21	11:37:45	341	425
3	12:38:25	12:45:22	12:47:34	417	549
4	14:23:40	14:29:32	14:33:31	352	591
5	13:16:21	13:23:20	13:25:19	419	538
6	10:53:14	10:59:10	11:01:11	356	477
7	15:25:56	15:30:43	15:33:00	287	424
8	16:24:16	16:29:18	16:28:54	302	424
9	17:03:57	17:07:53	17:12:51	236	534
10	8:31:12	8:36:15	8:39:35	303	503
11	9:20:59	9:26:35	9:30:09	336	550
12	8:22:48	8:28:10	8:28:42	322	354
13	14:06:55	14:13:39	14:14:06	404	431
14	11:58:45	12:04:10	12:05:38	325	413
15	11:38:41	11:43:12	11:46:27	271	466
16	13:12:53	13:18:20	13:20:41	327	468
17	12:52:57	12:58:01	13:00:14	304	437
18	15:25:17	15:31:47	15:33:07	390	470
19	15:29:13	15:34:36	15:38:29	323	556
20	15:08:40	15:13:55	15:16:23	315	463
21	17:58:16	18:04:54	18:04:18	398	362

Prueba	Hora de incidencia	Hora de alerta en el sistema	Hora de notificación en el correo	Tiempo en notificar en el sistema (Segundos)	Tiempo en notificar en el correo (Segundos)
22	16:43:09	16:49:12	16:50:14	363	425
23	9:49:14	9:54:20	9:55:40	306	386
24	11:13:33	11:18:20	11:20:20	287	407
25	15:48:48	15:54:05	15:55:43	317	415
26	12:10:23	12:15:57	12:16:22	334	359
27	9:32:19	9:37:41	9:41:01	322	522
28	8:57:49	9:03:51	9:04:19	362	390
29	13:17:52	13:23:03	13:26:07	311	495
30	14:23:07	14:28:46	14:31:43	339	516
31	9:31:44	9:36:34	9:41:24	290	580
32	9:00:38	9:06:51	9:09:24	373	526
33	15:29:19	15:34:32	15:38:44	313	565
34	17:29:10	17:33:40	17:36:53	270	463
35	12:47:00	12:51:31	12:54:27	271	447
36	17:09:31	17:15:25	17:17:37	354	486
37	15:16:37	15:21:14	15:22:50	277	373
38	15:52:12	15:57:01	16:00:34	289	502
39	17:55:51	18:01:36	18:05:21	345	570
40	16:07:00	16:13:40	16:14:26	400	446
41	16:16:45	16:22:10	16:22:45	325	360
42	13:43:07	13:48:14	13:52:08	307	541
43	17:32:10	17:37:38	17:40:09	328	479

Prueba	Hora de incidencia	Hora de alerta en el sistema	Hora de notificación en el correo	Tiempo en notificar en el sistema (Segundos)	Tiempo en notificar en el correo (Segundos)
44	12:28:08	12:33:34	12:37:44	326	576
45	8:43:41	8:49:29	8:49:47	348	366
46	13:07:07	13:12:38	13:16:52	331	585
47	11:45:02	11:50:30	11:54:26	328	564
48	15:27:21	15:32:28	15:33:17	307	356
49	15:38:47	15:44:53	15:45:01	366	374
50	10:38:00	10:44:39	10:46:52	399	532
51	17:46:24	17:52:49	17:53:15	385	411
52	11:47:34	11:52:54	11:55:44	320	490
53	10:20:24	10:26:39	10:28:36	375	492
54	16:35:53	16:41:41	16:42:55	348	422
55	10:52:46	10:58:45	10:58:54	359	368
56	12:43:36	12:49:30	12:53:19	354	583
57	11:22:51	11:27:26	11:29:56	275	425
58	16:43:18	16:49:34	16:51:37	376	499
59	10:05:30	10:10:48	10:11:22	318	352
60	13:36:03	13:42:27	13:44:32	384	509
61	17:20:12	17:24:44	17:27:30	272	438
62	8:28:58	8:35:34	8:36:54	396	476
63	15:47:09	15:52:00	15:53:26	291	377
64	9:33:22	9:38:47	9:42:36	325	554
65	11:53:06	11:58:13	12:02:55	307	589

Prueba	Hora de incidencia	Hora de alerta en el sistema	Hora de notificación en el correo	Tiempo en notificar en el sistema (Segundos)	Tiempo en notificar en el correo (Segundos)
66	12:00:44	12:06:26	12:07:07	342	383
67	8:14:32	8:19:59	8:21:55	327	443
68	9:05:15	9:11:50	9:12:52	395	457
69	16:51:01	16:56:49	17:00:27	348	566
70	9:57:48	10:02:31	10:05:39	283	471
71	16:28:41	16:34:32	16:36:47	351	486
72	15:19:34	15:24:57	15:26:30	323	416
73	17:09:51	17:15:56	17:17:39	365	468
74	15:07:37	15:12:12	15:17:04	275	567
75	8:47:23	8:51:57	8:53:57	274	394
76	8:14:38	8:21:21	8:20:52	403	374
77	8:10:35	8:17:10	8:18:59	395	504
78	13:24:10	13:28:56	13:32:03	286	473
79	9:49:22	9:54:45	9:56:59	323	457
80	12:38:37	12:43:48	12:46:39	311	482
81	13:09:04	13:14:39	13:15:40	335	396
82	11:49:16	11:55:22	11:55:49	366	393
83	11:54:00	12:00:25	12:00:12	385	372
84	13:23:31	13:29:41	13:30:59	370	448
85	11:47:46	11:52:55	11:56:40	309	534
86	13:06:13	13:11:03	13:12:09	290	356
87	9:01:40	9:06:56	9:08:33	316	413

Prueba	Hora de incidencia	Hora de alerta en el sistema	Hora de notificación en el correo	Tiempo en notificar en el sistema (Segundos)	Tiempo en notificar en el correo (Segundos)
88	9:54:29	9:59:06	10:01:44	277	435
89	10:00:34	10:06:25	10:10:12	351	578
90	17:46:42	17:52:07	17:56:13	325	571
91	11:12:05	11:16:54	11:21:03	289	538
92	16:04:53	16:09:41	16:11:35	288	402
93	11:42:53	11:47:29	11:52:34	276	581
94	9:21:32	9:26:46	9:30:08	314	516
95	16:49:21	16:55:28	16:56:07	367	406
96	17:31:38	17:36:51	17:38:43	313	425
97	12:05:36	12:10:08	12:13:21	272	465
98	12:08:45	12:14:48	12:17:21	363	516
99	14:33:31	14:38:16	14:41:57	285	506
100	11:11:56	11:16:30	11:17:56	274	360
101	11:11:11	11:17:10	11:18:09	359	418
102	13:00:36	13:05:22	13:08:28	286	472
103	9:46:37	9:53:12	9:54:11	395	454
104	15:55:07	16:00:44	16:00:57	337	350
105	9:22:53	9:28:18	9:29:53	325	420
106	9:09:35	9:15:45	9:16:53	370	438
107	11:31:01	11:37:43	11:36:58	402	357
108	17:40:27	17:44:58	17:49:55	271	568
109	11:00:18	11:05:42	11:07:38	324	440

Prueba	Hora de incidencia	Hora de alerta en el sistema	Hora de notificación en el correo	Tiempo en notificar en el sistema (Segundos)	Tiempo en notificar en el correo (Segundos)
110	8:34:30	8:39:35	8:41:48	305	438
111	8:59:06	9:04:10	9:08:41	304	575
112	14:52:54	14:59:07	15:01:04	373	490
113	16:33:08	16:38:57	16:41:14	349	486
114	17:57:47	18:03:36	18:06:17	349	510
115	10:58:49	11:04:47	11:08:15	358	566
116	10:07:04	10:11:53	10:16:41	289	577
117	16:30:30	16:36:44	16:39:50	374	560
118	9:36:19	9:41:57	9:43:01	338	402
119	16:51:44	16:58:14	16:58:10	390	386
120	8:35:15	8:40:54	8:43:11	339	476
121	14:53:56	14:59:19	15:02:52	323	536
122	8:42:01	8:47:53	8:51:24	352	563
123	17:11:27	17:16:44	17:20:35	317	548

Prueba	Hora de incidencia	Hora de alerta en el sistema	Hora de notificación en el correo	Tiempo en notificar en el sistema (Segundos)	Tiempo en notificar en el correo (Segundos)
124	8:41:49	8:46:56	8:50:14	307	505
125	14:46:13	14:51:31	14:54:11	318	478
126	16:24:04	16:28:35	16:32:00	271	476
127	17:11:53	17:18:13	17:21:09	380	556
128	12:38:57	12:45:21	12:47:10	384	493
129	10:38:16	10:44:57	10:44:56	401	400
130	12:04:14	12:09:19	12:12:51	305	517
131	17:40:16	17:45:02	17:48:39	286	503
132	15:05:17	15:09:54	15:12:02	277	405
133	16:19:43	16:25:21	16:28:21	338	518
134	10:19:17	10:23:53	10:28:54	276	577
135	14:08:58	14:14:27	14:17:16	329	498
136	17:18:55	17:25:26	17:27:50	391	535
137	17:53:34	17:58:58	18:00:03	324	389

Prueba	Hora de incidencia	Hora de alerta en el sistema	Hora de notificación en el correo	Tiempo en notificar en el sistema (Segundos)	Tiempo en notificar en el correo (Segundos)
138	13:54:17	13:59:42	14:02:08	325	471
139	13:10:49	13:17:24	13:18:55	395	486
140	13:06:47	13:12:52	13:15:30	365	523
141	8:55:11	8:59:52	9:04:51	281	580
142	14:22:52	14:27:55	14:31:04	303	492
143	11:10:12	11:15:57	11:17:58	345	466
144	15:21:37	15:27:19	15:28:40	342	423
145	13:35:50	13:41:27	13:43:12	337	442
146	14:32:00	14:37:04	14:41:48	304	588
147	10:53:53	10:59:25	11:00:36	332	403
148	13:44:59	13:49:49	13:50:49	290	350
149	12:07:47	12:12:33	12:13:46	286	359
150	13:17:24	13:22:47	13:25:31	323	487
151	13:22:50	13:28:18	13:28:43	328	353

Prueba	Hora de incidencia	Hora de alerta en el sistema	Hora de notificación en el correo	Tiempo en notificar en el sistema (Segundos)	Tiempo en notificar en el correo (Segundos)
152	15:20:05	15:25:04	15:26:38	299	393
153	15:58:32	16:03:56	16:06:25	324	473
154	11:08:14	11:13:33	11:15:18	319	424
155	17:25:25	17:31:01	17:34:46	336	561
156	11:39:01	11:44:39	11:44:53	338	352
157	17:52:08	17:58:06	17:58:23	358	375
158	9:00:59	9:06:29	9:10:09	330	550
159	11:54:41	11:59:23	12:03:22	282	521
160	12:49:55	12:55:11	12:58:03	316	488
161	17:17:02	17:22:31	17:25:45	329	523
162	9:30:48	9:37:23	9:40:35	395	587
163	16:40:16	16:44:59	16:49:15	283	539
164	11:00:34	11:07:01	11:08:18	387	464
165	10:56:51	11:02:12	11:06:05	321	554

Prueba	Hora de incidencia	Hora de alerta en el sistema	Hora de notificación en el correo	Tiempo en notificar en el sistema (Segundos)	Tiempo en notificar en el correo (Segundos)
166	8:16:14	8:21:53	8:22:40	339	386
167	9:52:26	9:57:44	10:01:16	318	530
168	13:49:46	13:56:19	13:56:40	393	414
169	8:14:12	8:20:57	8:20:56	405	404
170	13:30:23	13:35:45	13:38:28	322	485
171	11:46:34	11:51:22	11:56:19	288	585
172	14:06:01	14:10:37	14:14:45	276	524
173	15:26:55	15:33:08	15:34:11	373	436
174	17:55:04	18:00:55	18:03:46	351	522
175	17:15:19	17:21:47	17:23:29	388	490
176	12:38:05	12:44:09	12:44:07	364	362
177	10:37:17	10:42:08	10:43:50	291	393
178	13:36:13	13:42:52	13:43:43	399	450
179	11:42:19	11:48:28	11:51:13	369	534

Prueba	Hora de incidencia	Hora de alerta en el sistema	Hora de notificación en el correo	Tiempo en notificar en el sistema (Segundos)	Tiempo en notificar en el correo (Segundos)
180	17:13:54	17:18:45	17:20:36	291	402
181	10:14:37	10:19:43	10:21:19	306	402
182	10:44:43	10:50:24	10:52:33	341	470
183	12:23:58	12:29:42	12:33:16	344	558
184	9:54:58	10:00:35	10:01:42	337	404
185	17:11:18	17:16:54	17:18:38	336	440
186	12:27:10	12:33:39	12:35:51	389	521
187	15:35:39	15:40:17	15:44:38	278	539
188	12:37:16	12:42:25	12:45:05	309	469
189	8:48:07	8:53:40	8:54:49	333	402
190	16:09:13	16:15:51	16:18:06	398	533
191	9:18:04	9:22:46	9:26:30	282	506
192	17:38:07	17:44:37	17:45:30	390	443
193	8:20:00	8:25:07	8:26:14	307	374

Prueba	Hora de incidencia	Hora de alerta en el sistema	Hora de notificación en el correo	Tiempo en notificar en el sistema (Segundos)	Tiempo en notificar en el correo (Segundos)
194	15:54:15	16:00:43	16:00:25	388	370
195	14:09:06	14:14:48	14:18:23	342	557
196	17:58:20	18:04:04	18:04:13	344	353
197	12:20:07	12:25:10	12:28:03	303	476
198	17:18:21	17:24:54	17:25:23	393	422
199	14:20:02	14:25:37	14:29:23	335	561
200	8:00:08	8:05:35	8:06:42	327	394
Promedio				322	490

Anexo 05: Pruebas de incidencias con el sistema implementado.

Prueba	Hora de incidencia	Hora de alerta en el sistema	Hora de notificación en el correo	Hora de notificación en Telegram	Tiempo en notificar en el sistema (Segundos)	Tiempo en notificar en el correo (Segundos)	Tiempo en notificar en Telegram (Segundos)
1	20:16:30	20:17:25	20:17:35	20:17:29	55	65	59
2	20:49:40	20:50:25	20:50:40	20:50:28	45	60	48
3	9:28:25	9:29:21	9:29:34	9:29:23	56	69	58
4	12:12:40	12:13:21	12:13:38	12:13:25	41	58	45
5	21:16:21	21:17:26	21:17:39	21:17:28	65	78	67
6	10:39:14	10:40:15	10:40:32	10:40:17	61	78	63
7	14:25:56	14:26:54	14:27:13	14:26:56	58	77	60
8	17:45:16	17:46:19	17:46:38	17:46:22	63	82	66
9	13:03:57	13:05:01	13:05:29	13:05:03	64	92	66
10	11:31:12	11:32:16	11:32:46	11:32:18	64	94	66
11	12:57:12	12:58:14	12:58:16	12:58:12	62	64	60
12	17:23:53	17:24:50	17:25:01	17:24:41	57	68	48
13	12:19:46	12:20:36	12:20:59	12:20:46	50	73	60
14	16:41:28	16:42:29	16:42:58	16:42:15	61	90	47
15	15:02:29	15:03:21	15:04:02	15:03:14	52	93	45
16	8:53:45	8:54:47	8:55:12	8:54:33	62	87	48
17	15:46:38	15:47:27	15:48:06	15:47:32	49	88	54
18	15:58:03	15:59:08	15:59:21	15:59:02	65	78	59
19	14:57:43	14:58:31	14:59:06	14:58:39	48	83	56
20	8:42:43	8:43:27	8:43:46	8:43:38	44	63	55
21	8:39:48	8:40:46	8:41:11	8:40:36	58	83	48

Prueba	Hora de incidencia	Hora de alerta en el sistema	Hora de notificación en el correo	Hora de notificación en Telegram	Tiempo en notificar en el sistema (Segundos)	Tiempo en notificar en el correo (Segundos)	Tiempo en notificar en Telegram (Segundos)
22	8:40:06	8:41:04	8:41:30	8:41:01	58	84	55
23	13:14:26	13:15:22	13:15:52	13:15:31	56	86	65
24	12:34:10	12:34:54	12:35:15	12:35:09	44	65	59
25	15:58:50	15:59:32	16:00:00	15:59:53	42	70	63
26	16:41:17	16:42:18	16:42:23	16:42:17	61	66	60
27	16:03:18	16:04:17	16:04:40	16:04:10	59	82	52
28	13:46:02	13:47:04	13:47:31	13:47:04	62	89	62
29	9:35:53	9:36:34	9:37:10	9:36:42	41	77	49
30	15:36:02	15:36:55	15:37:09	15:37:02	53	67	60
31	13:10:46	13:11:37	13:11:56	13:11:44	51	70	58
32	14:31:09	14:32:08	14:32:18	14:32:05	59	69	56
33	9:41:38	9:42:34	9:42:38	9:42:33	56	60	55
34	14:03:56	14:04:37	14:05:20	14:04:57	41	84	61
35	9:13:18	9:14:17	9:14:22	9:14:16	59	64	58
36	16:55:00	16:55:52	16:56:32	16:56:00	52	92	60
37	16:07:50	16:08:36	16:09:17	16:08:46	46	87	56
38	17:14:13	17:15:10	17:15:40	17:15:13	57	87	60
39	13:42:31	13:43:16	13:43:57	13:43:17	45	86	46
40	11:52:40	11:53:34	11:53:45	11:53:39	54	65	59
41	12:51:37	12:52:18	12:53:09	12:52:27	41	92	50
42	11:51:23	11:52:23	11:52:52	11:52:17	60	89	54
43	12:04:38	12:05:35	12:06:00	12:05:26	57	82	48

Prueba	Hora de incidencia	Hora de alerta en el sistema	Hora de notificación en el correo	Hora de notificación en Telegram	Tiempo en notificar en el sistema (Segundos)	Tiempo en notificar en el correo (Segundos)	Tiempo en notificar en Telegram (Segundos)
44	11:35:40	11:36:22	11:37:09	11:36:42	42	89	62
45	11:59:11	11:59:52	12:00:20	12:00:05	41	69	54
46	8:58:53	8:59:48	9:00:02	8:59:45	55	69	52
47	15:41:12	15:41:54	15:42:13	15:42:03	42	61	51
48	11:12:39	11:13:38	11:14:05	11:13:44	59	86	65
49	15:20:50	15:21:41	15:22:16	15:21:40	51	86	50
50	8:03:45	8:04:41	8:05:18	8:04:39	56	93	54
51	15:45:05	15:46:04	15:46:19	15:46:02	59	74	57
52	12:05:59	12:06:48	12:07:01	12:07:02	49	62	63
53	11:17:22	11:18:21	11:18:33	11:18:10	59	71	48
54	15:22:45	15:23:47	15:24:09	15:23:49	62	84	64
55	13:44:06	13:44:56	13:45:12	13:44:53	50	66	47
56	14:42:02	14:43:06	14:43:27	14:42:50	64	85	48
57	15:37:14	15:37:58	15:38:21	15:38:15	44	67	61
58	10:14:46	10:15:33	10:15:55	10:15:33	47	69	47
59	16:13:45	16:14:49	16:15:00	16:14:37	64	75	52
60	15:44:55	15:46:00	15:46:09	15:45:54	65	74	59
61	10:18:48	10:19:44	10:20:21	10:19:36	56	93	48
62	11:40:54	11:41:51	11:42:06	11:41:46	57	72	52
63	12:30:35	12:31:25	12:31:59	12:31:41	50	84	66
64	14:23:30	14:24:31	14:24:54	14:24:21	61	84	51
65	11:33:06	11:33:49	11:34:24	11:34:03	43	78	57

Prueba	Hora de incidencia	Hora de alerta en el sistema	Hora de notificación en el correo	Hora de notificación en Telegram	Tiempo en notificar en el sistema (Segundos)	Tiempo en notificar en el correo (Segundos)	Tiempo en notificar en Telegram (Segundos)
66	12:12:25	12:13:23	12:13:47	12:13:28	58	82	63
67	12:22:23	12:23:15	12:23:55	12:23:25	52	92	62
68	13:31:42	13:32:45	13:33:14	13:32:28	63	92	46
69	9:14:36	9:15:25	9:15:52	9:15:37	49	76	61
70	10:50:18	10:51:03	10:51:50	10:51:16	45	92	58
71	14:46:23	14:47:17	14:47:39	14:47:16	54	76	53
72	15:02:21	15:03:05	15:03:55	15:03:12	44	94	51
73	11:19:50	11:20:38	11:21:14	11:20:43	48	84	53
74	15:26:23	15:27:08	15:27:41	15:27:14	45	78	51
75	15:10:22	15:11:15	15:11:38	15:11:20	53	76	58
76	9:01:59	9:03:04	9:03:11	9:02:46	65	72	47
77	8:50:29	8:51:28	8:51:52	8:51:30	59	83	61
78	17:53:37	17:54:28	17:54:56	17:54:42	51	79	65
79	16:17:18	16:18:08	16:18:18	16:18:17	50	60	59
80	17:02:23	17:03:09	17:03:47	17:03:29	46	84	66
81	14:07:35	14:08:38	14:08:48	14:08:31	63	73	56
82	13:27:05	13:28:05	13:28:11	13:28:05	60	66	60
83	16:08:33	16:09:29	16:09:51	16:09:29	56	78	56
84	9:00:16	9:01:06	9:01:48	9:01:05	50	92	49
85	9:51:21	9:52:11	9:52:27	9:52:25	50	66	64
86	12:01:48	12:02:46	12:03:05	12:02:41	58	77	53
87	8:52:31	8:53:14	8:53:50	8:53:34	43	79	63

Prueba	Hora de incidencia	Hora de alerta en el sistema	Hora de notificación en el correo	Hora de notificación en Telegram	Tiempo en notificar en el sistema (Segundos)	Tiempo en notificar en el correo (Segundos)	Tiempo en notificar en Telegram (Segundos)
88	9:55:53	9:56:50	9:56:58	9:56:52	57	65	59
89	11:42:28	11:43:10	11:43:54	11:43:28	42	86	60
90	17:22:31	17:23:26	17:23:34	17:23:26	55	63	55
91	16:25:23	16:26:16	16:26:42	16:26:23	53	79	60
92	16:09:24	16:10:20	16:10:48	16:10:20	56	84	56
93	15:40:47	15:41:36	15:42:05	15:41:32	49	78	45
94	10:53:29	10:54:10	10:54:40	10:54:24	41	71	55
95	15:32:27	15:33:15	15:33:27	15:33:23	48	60	56
96	13:48:41	13:49:32	13:50:01	13:49:31	51	80	50
97	10:17:36	10:18:34	10:19:07	10:18:24	58	91	48
98	10:14:13	10:15:06	10:15:39	10:15:09	53	86	56
99	16:25:24	16:26:16	16:26:57	16:26:24	52	93	60
100	9:24:50	9:25:54	9:26:00	9:25:51	64	70	61
101	8:00:24	8:01:29	8:01:54	8:01:11	65	90	47
102	8:48:12	8:49:05	8:49:19	8:49:07	53	67	55
103	8:59:38	9:00:31	9:00:52	9:00:35	53	74	57
104	8:44:13	8:45:18	8:45:27	8:45:13	65	74	60
105	11:36:39	11:37:40	11:37:57	11:37:43	61	78	64
106	15:46:24	15:47:11	15:47:33	15:47:14	47	69	50
107	10:59:12	11:00:02	11:00:34	11:00:08	50	82	56
108	10:40:10	10:40:56	10:41:19	10:41:04	46	69	54
109	14:23:42	14:24:32	14:25:13	14:24:41	50	91	59

Prueba	Hora de incidencia	Hora de alerta en el sistema	Hora de notificación en el correo	Hora de notificación en Telegram	Tiempo en notificar en el sistema (Segundos)	Tiempo en notificar en el correo (Segundos)	Tiempo en notificar en Telegram (Segundos)
110	12:15:06	12:16:00	12:16:15	12:15:56	54	69	50
111	11:46:05	11:47:07	11:47:28	11:47:11	62	83	66
112	17:15:12	17:15:58	17:16:34	17:15:58	46	82	46
113	17:15:11	17:16:09	17:16:22	17:15:56	58	71	45
114	15:30:49	15:31:36	15:32:23	15:31:39	47	94	50
115	16:16:53	16:17:38	16:18:02	16:17:43	45	69	50
116	9:29:51	9:30:38	9:30:55	9:30:36	47	64	45
117	10:00:28	10:01:30	10:01:59	10:01:24	62	91	56
118	16:08:40	16:09:37	16:10:10	16:09:42	57	90	62
119	12:23:11	12:24:13	12:24:20	12:24:03	62	69	52
120	9:46:23	9:47:05	9:47:40	9:47:20	42	77	57
121	13:39:04	13:40:00	13:40:34	13:39:57	56	90	53
122	16:06:14	16:07:05	16:07:26	16:07:13	51	72	59
123	8:16:32	8:17:33	8:17:38	8:17:17	61	66	45
124	10:18:09	10:19:03	10:19:38	10:19:04	54	89	55
125	8:25:48	8:26:48	8:27:21	8:26:33	60	93	45
126	17:29:39	17:30:21	17:31:10	17:30:28	42	91	49
127	15:45:03	15:45:51	15:46:30	15:45:59	48	87	56
128	14:42:20	14:43:20	14:43:35	14:43:05	60	75	45
129	12:56:41	12:57:34	12:57:49	12:57:37	53	68	56
130	16:26:32	16:27:30	16:27:32	16:27:24	58	60	52
131	14:14:02	14:14:44	14:15:26	14:14:57	42	84	55

Prueba	Hora de incidencia	Hora de alerta en el sistema	Hora de notificación en el correo	Hora de notificación en Telegram	Tiempo en notificar en el sistema (Segundos)	Tiempo en notificar en el correo (Segundos)	Tiempo en notificar en Telegram (Segundos)
132	17:57:24	17:58:28	17:58:24	17:58:14	64	60	50
133	17:21:44	17:22:40	17:23:04	17:22:39	56	80	55
134	11:08:00	11:08:42	11:09:30	11:08:45	42	90	45
135	16:23:49	16:24:48	16:24:50	16:24:52	59	61	63
136	16:21:39	16:22:41	16:22:43	16:22:31	62	64	52
137	15:02:00	15:02:54	15:03:14	15:02:45	54	74	45
138	17:00:42	17:01:46	17:01:52	17:01:28	64	70	46
139	17:35:49	17:36:38	17:37:13	17:36:35	49	84	46
140	13:01:27	13:02:21	13:02:38	13:02:20	54	71	53
141	17:28:57	17:30:02	17:30:17	17:29:58	65	80	61
142	14:00:20	14:01:05	14:01:52	14:01:11	45	92	51
143	13:08:04	13:08:56	13:09:25	13:08:54	52	81	50
144	8:32:06	8:33:02	8:33:21	8:32:54	56	75	48
145	14:24:49	14:25:52	14:26:13	14:25:43	63	84	54
146	8:27:16	8:28:00	8:28:27	8:28:18	44	71	62
147	8:26:41	8:27:34	8:28:03	8:27:34	53	82	53
148	15:45:23	15:46:21	15:46:49	15:46:16	58	86	53
149	10:26:53	10:27:39	10:28:01	10:27:44	46	68	51
150	13:08:34	13:09:19	13:10:06	13:09:40	45	92	66
151	17:46:26	17:47:21	17:47:35	17:47:15	55	69	49
152	14:03:09	14:03:56	14:04:25	14:04:10	47	76	61
153	9:30:36	9:31:20	9:31:40	9:31:22	44	64	46

Prueba	Hora de incidencia	Hora de alerta en el sistema	Hora de notificación en el correo	Hora de notificación en Telegram	Tiempo en notificar en el sistema (Segundos)	Tiempo en notificar en el correo (Segundos)	Tiempo en notificar en Telegram (Segundos)
154	15:56:10	15:57:05	15:57:36	15:57:02	55	86	52
155	13:28:09	13:29:02	13:29:22	13:29:07	53	73	58
156	16:34:35	16:35:35	16:35:36	16:35:24	60	61	49
157	16:20:09	16:21:10	16:21:39	16:21:02	61	90	53
158	9:00:46	9:01:51	9:02:10	9:01:34	65	84	48
159	17:16:50	17:17:40	17:18:18	17:17:49	50	88	59
160	17:42:32	17:43:25	17:43:32	17:43:22	53	60	50
161	9:31:41	9:32:27	9:32:56	9:32:34	46	75	53
162	14:05:22	14:06:06	14:06:22	14:06:14	44	60	52
163	8:23:36	8:24:19	8:24:47	8:24:34	43	71	58
164	11:17:36	11:18:34	11:18:49	11:18:40	58	73	64
165	9:02:19	9:03:23	9:03:27	9:03:08	64	68	49
166	13:56:48	13:57:49	13:57:56	13:57:34	61	68	46
167	13:13:20	13:14:14	13:14:28	13:14:05	54	68	45
168	16:45:15	16:46:20	16:46:34	16:46:05	65	79	50
169	12:38:09	12:39:09	12:39:24	12:39:07	60	75	58
170	10:04:24	10:05:13	10:05:51	10:05:24	49	87	60
171	14:52:30	14:53:35	14:53:35	14:53:18	65	65	48
172	15:32:28	15:33:16	15:33:46	15:33:22	48	78	54
173	11:25:03	11:25:47	11:26:37	11:26:01	44	94	58
174	10:01:32	10:02:28	10:03:04	10:02:21	56	92	49
175	14:21:53	14:22:34	14:22:58	14:22:53	41	65	60

Prueba	Hora de incidencia	Hora de alerta en el sistema	Hora de notificación en el correo	Hora de notificación en Telegram	Tiempo en notificar en el sistema (Segundos)	Tiempo en notificar en el correo (Segundos)	Tiempo en notificar en Telegram (Segundos)
176	13:35:32	13:36:33	13:36:39	13:36:27	61	67	55
177	14:29:45	14:30:34	14:31:11	14:30:37	49	86	52
178	11:07:49	11:08:47	11:09:11	11:08:51	58	82	62
179	17:43:14	17:43:59	17:44:24	17:44:18	45	70	64
180	13:49:02	13:50:02	13:50:11	13:49:54	60	69	52
181	15:45:06	15:45:55	15:46:29	15:46:11	49	83	65
182	17:42:26	17:43:09	17:43:52	17:43:12	43	86	46
183	11:25:08	11:26:04	11:26:24	11:26:05	56	76	57
184	9:03:00	9:03:51	9:04:15	9:03:46	51	75	46
185	9:14:24	9:15:13	9:15:41	9:15:30	49	77	66
186	17:10:39	17:11:32	17:12:03	17:11:25	53	84	46
187	15:43:23	15:44:19	15:44:49	15:44:10	56	86	47
188	15:16:13	15:17:11	15:17:31	15:17:19	58	78	66
189	15:56:10	15:57:03	15:57:13	15:57:15	53	63	65
190	13:36:20	13:37:01	13:37:52	13:37:06	41	92	46
191	15:53:54	15:54:48	15:55:19	15:54:48	54	85	54
192	13:54:38	13:55:23	13:55:49	13:55:29	45	71	51
193	16:42:36	16:43:29	16:43:39	16:43:29	53	63	53
194	14:40:07	14:41:00	14:41:37	14:41:04	53	90	57
195	16:39:24	16:40:12	16:40:54	16:40:28	48	90	64
196	11:45:55	11:46:49	11:47:27	11:46:55	54	92	60
197	13:31:04	13:31:53	13:32:09	13:31:51	49	65	47

Prueba	Hora de incidencia	Hora de alerta en el sistema	Hora de notificación en el correo	Hora de notificación en Telegram	Tiempo en notificar en el sistema (Segundos)	Tiempo en notificar en el correo (Segundos)	Tiempo en notificar en Telegram (Segundos)
198	14:26:07	14:27:00	14:27:35	14:27:13	53	88	66
199	16:49:30	16:50:28	16:50:33	16:50:23	58	63	53
200	14:20:15	14:21:12	14:21:24	14:21:11	57	69	56
PROMEDIO					59	77	60

turnitin

Recibo digital

Este recibo confirma quesu trabajo ha sido recibido por Turnitin. A continuación podrá ver la información del recibo con respecto a su entrega.

La primera página de tus entregas se muestra abajo.

Autor de la entrega:	LUIS RICARDO MORAN CHOZO
Título del ejercicio:	Trabajos de suficiencia profesional
Título de la entrega:	SISTEMA DE MONITOREO DE LA INFRAESTRUCTURA DE TI PA...
Nombre del archivo:	TRABAJO_DE_SUFICIENCIA_LUIS_MORAN.pdf
Tamaño del archivo:	8.34M
Total páginas:	110
Total de palabras:	16,228
Total de caracteres:	78,978
Fecha de entrega:	25-abr.-2024 02:37a. m. (UTC-0500)
Identificador de la entre...	2360038028

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE INGENIERÍA CIVIL DE SISTEMAS Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

"SISTEMA DE MONITOREO DE LA INFRAESTRUCTURA DE TI PARA GESTIONAR INCIDENTES DE UNA EMPRESA DEL RUBRO TECNOLÓGICO"

TRABAJO DE SUFICIENCIA PROFESIONAL

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS

PRESENTADO POR EL BACHILLER:

LUIS RICARDO MORAN CHOZO

LAMBAYEQUE – PERÚ
2024

MA. ING. ROBERTO CARLOS ARTEAGA LORA
DNI 16755764

SISTEMA DE MONITOREO DE LA INFRAESTRUCTURA DE TI PARA GESTIONAR INCIDENTES DE UNA EMPRESA DEL RUBRO TECNOLÓGICO

INFORME DE ORIGINALIDAD

14%	14%	1%	3%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	5%
2	repositorio.unsm.edu.pe Fuente de Internet	4%
3	1library.co Fuente de Internet	1%
4	repositorio.utp.edu.pe Fuente de Internet	1%
5	www.coursehero.com Fuente de Internet	<1%
6	repositorio.untels.edu.pe Fuente de Internet	<1%
7	mendillo.info Fuente de Internet	<1%
8	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	<1%

MA. ING. ROBERTO CARLOS ARTEAGA LORA
DNI 16755764

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE INGENIERÍA CIVIL, DE SISTEMAS Y ARQUITECTURA
UNIDAD DE INVESTIGACIÓN

"Año del Bicentenario de la consolidación de nuestra independencia y de la conmemoración de las heroicas batallas de Junín y Ayacucho"

CONSTANCIA DE APROBACIÓN DE ORIGINALIDAD DE TRABAJO DE SUFICIENCIA PROFESIONAL

Según Res. N° 659-2020-R

Yo, ARTEAGA LORA ROBERTO CARLOS, asesor del trabajo de suficiencia profesional del bachiller:

LUIS RICARDO MORAN CHOZO

TITULADA:

"Sistema de monitoreo de la infraestructura de TI para gestionar incidentes de una empresa del rubro tecnológico"

Luego de la revisión exhaustiva del documento constato que la misma tiene un índice de similitud de 14% verificable en el reporte de similitud del programa TURNITIN.

El suscrito analizó dicho reporte y concluyó que, cada una de las coincidencias detectadas NO CONSTITUYEN PLAGIO. A mi leal saber y entender, el trabajo de suficiencia profesional cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad Nacional Pedro Ruiz Gallo.
Se expide la presente según lo dispuesto en la Resolución Nº 659-2020-R, de fecha 8 de setiembre de 2020, que aprueba la directiva para la evaluación de originalidad de los documentos académicos, de investigación formativa y para la obtención de Grados y Títulos de la UNPRG:

Lambayeque, 25 de abril de 2024

Atentamente,

MA. ING. ROBERTO CARLOS ARTEAGA LORA
DNI 16755764

Se adjunta:
- Recibo digital de Turnitin
- Revisión de informe en Turnitin

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE INGENIERÍA CIVIL DE SISTEMAS Y DE ARQUITECTURA
DECANATO

ACTA DE SUSTENTACIÓN
N° 571-2024-FICSA-D

Siendo las 12:00m horas del día 24 mayo del 2024, se reunieron los miembros del jurado del trabajo de suficiencia profesional titulada: **"SISTEMA DE MONITOREO DE LA INFRAESTRUCTURA DE TI PARA GESTIONAR INCIDENTES DE UNA EMPRESA DEL RUBRO TECNOLÓGICO" con código N° IS_V_SP_2023_020, y Resolución Decanal Virtual N° 644-2023-UNPRG-FICSA;** con la finalidad de Evaluar y Calificar la sustentación del trabajo de suficiencia profesional antes mencionada, conformado por los siguientes docentes:

DR. ING. ALBERTO ENRIQUE SAMILLAN AYALA	**PRESIDENTE**
DR. ING. REGIS JORGE ALBERTO DIAZ PLAZA	**SECRETARIO**
ING. CESAR AUGUSTO GUZMAN VALLE	**VOCAL**

Asesorado por MSC. ING. ROBERTO CARLOS ARTEAGA LORA

El acto de sustentación fue autorizado por **OFICIO VIRTUAL N° 082-2024-UIFICSA**, el trabajo de suficiencia profesional fue presentado y sustentado por el Bachiller: **LUIS RICARDO MORAN CHOZO,** tuvo una duración de 45 minutos Después de la sustentación, y absueltas las preguntas y observaciones de los miembros del jurado; se procedió a la calificación respectiva:

	NUMERO	LETRAS	CALIFICATIVO
LUIS RICARDO MORAN CHOZO	20	Veinte	EXCELENTE

Por lo que queda **APTO** para obtener el Título Profesional de **INGENIERO DE SISTEMAS** de acuerdo con la Ley Universitaria 30220 y la normatividad vigente de la Facultad de Ingeniería Civil De Sistemas y de Arquitectura de la Universidad Nacional Pedro Ruiz Gallo.

Siendo las 12:45 p del mismo día, se dio por concluido el presente acto académico, dándose conformidad al presente acto, con la firma de los miembros del jurado.

DR. ING. ALBERTO ENRIQUE SAMILLAN AYALA
PRESIDENTE

DR. ING. REGIS JORGE ALBERTO DIAZ PLAZA
SECRETARIO

ING. CESAR AUGUSTO GUZMAN VALLE
VOCAL

MSC. ING. ROBERTO CARLOS ARTEAGA LORA
ASESOR