UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS

ESCUELA PROFESIONAL DE COMPUTACIÓN E INFORMÁTICA

TESIS

"Implementación de un Centro de Operaciones de Red para el Monitoreo de Servicios Inalámbricos en la Empresa Interconexiones Ocaney"

Para optar el título profesional de:
Ingeniero en Computación e Informática

Autor: Bach. Benito Calderón Lucero

Asesor: Dr. Ing. Gilberto Carrión Barco

Lambayeque, 2021

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS

ESCUELA PROFESIONAL DE COMPUTACIÓN E INFORMÁTICA

TESIS

"Implementación de un Centro de Operaciones de Red para el Monitoreo de Servicios Inalámbricos en la Empresa Interconexiones Ocaney"

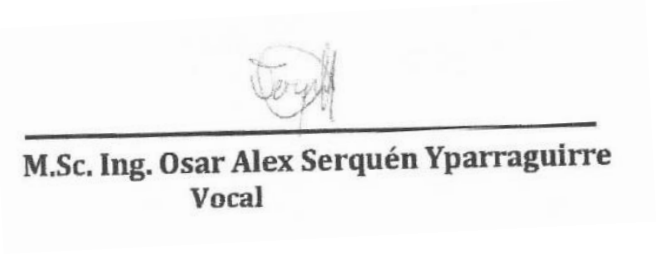
Para optar el título profesional de:

Ingeniero en Computación e Informática

APROBADO POR:

Dra. Ing. Jessie Leila Bravo Jaico
Presidente

M.Sc. Ing. Nilton César Germán Reyes
Secretario



M.Sc. Ing. Osar Alex Serquén Yparraguirre
Vocal

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE CIENCIAS FISICAS Y MATEMATICAS
DECANATO
Ciudad Universitaria - Lambayeque

ACTA DE SUSTENTACIÓN VIRTUAL N° 043-2021-D/FACFyM

Siendo las 10:00 am del día 15 de diciembre del 2021, se reunieron vía plataforma virtual, meet.google.com/jqx-gxsb-ptg miembros del jurado evaluador de la Tesis titulada:

IMPLEMENTACIÓN DE UN CENTRO DE OPERACIONES DE RED PARA EL MONITOREO DE SERVICIOS INALÁMBRICOS EN LA EMPRESA INTERCONEXIONES OCANEY

Designados por Decreto N° 008-2020-VIRTUAL-UI/FACFyM de fecha 29 setiembre 2020.
Con la finalidad de evaluar y calificar la sustentación de la tesis antes mencionada, conformada por los siguientes docentes:

Dra. Ing. Jessie Leila Bravo Jaico	Presidente
M.Sc. Ing. Nilton César Germán Reyes	Secretario
M.Sc. Ing. Oscar Alex Serquén Yparraguirre	Vocal

La tesis fue asesorada por el Dr. Gilberto Carrión Barco nombrado por Decreto N° 008-2020-VIRTUAL-UI/FACFyM de fecha 29 de setiembre de 2020.
El Acto de Sustentación fue autorizado por Resolución N°889-2021-VIRTUAL-D/FACFyM de fecha 02 diciembre 2021.
La Tesis fue presentada y sustentada por el Bachiller en Computación e Informática: **CALDERON LUCERO BENITO** y tuvo una duración de 60 minutos.
Después de la sustentación, y absueltas las preguntas y observaciones de los miembros del jurado se procedió a la calificación respectiva, otorgándole el Calificativo de (16) (dieciséis) en la escala vigesimal, mención Bueno.
Por lo que queda apto para obtener el Título Profesional de **Ingeniero en Computación e Informática** de acuerdo con la Ley Universitaria 30220 y la normatividad vigente de la Facultad de Ciencias Físicas y Matemáticas y la Universidad Nacional Pedro Ruiz Gallo.
Siendo las 11:00 am se dio por concluido el presente acto académico, dándose conformidad al presente acto con la firma de los miembros del jurado.

Dra. Ing. Jessie Leila Bravo Jaico
Presidente

M.Sc. Ing. Nilton César Germán Reyes
Secretario

M.Sc. Ing. Osar Alex Serquén Yparraguirre
Vocal

Dr. Gilberto Carrión Barco
Asesor

CERTIFICO: Que, es copia fiel del original
Fecha: 20 / 12 / 2021
M.Sc. Marco Antonio Martin Peralta Lui
SECRETARIO DOCENTE - FACFyM
VÁLIDO PARA TRÁMITES INTERNOS DE LA UNPRG

DEDICATORIA

En memoria de mi madre Juana, que desde el cielo nunca me deja de cuidar. A mi padre Presentación y mis hermanos por su apoyo incondicional en todo momento, que sin ellos no hubiera sido posible lograr mis sueños.

A mi tío Guillermo por cuidarme y darme los días más felices de mi infancia.

A Dios, por brindarme salud y fuerza para seguir adelante.

AGRADECIMIENTOS

A mi Padre Presentación por enseñarme y educarme con valores y darme los mejores consejos de vida.

A mi hermano Miguel, por su apoyo incondicional durante mi vida académica y ayudarme a conseguir mis metas, este logro también es de ti.

Índice General

Índice de tablas

Índice de figuras

Resumen

Un centro de operación de red, es el área que realiza la monitorización del estado de salud de los dispositivos de red y recursos de los sistemas informáticos de una empresa en tiempo real, cuyo objetivo es prevenir cualquier tipo de percance que pongan en riesgo la disponibilidad de las operaciones del negocio y garantizar su óptimo funcionamiento.

La presente investigación tuvo como objetivo establecer un sistema de monitoreo para los Servicios Inalámbricos en la Empresa Interconexiones Ocaney mediante la implementación de un Centro de Operaciones de Red para la gestión y administración centralizada de los equipos de telecomunicaciones.

La investigación fue de tipo aplicada, se utilizó un enfoque cuantitativo teniendo un alcance explicativo con diseño pre-experimental, la muestra utilizada fue de 12 sujetos los cuales conforman el personal administrado y soporte de la empresa Interconexiones Ocaney; a esta muestra se le aplicó una encuesta mediante un cuestionario conformado por 17 preguntas, teniendo como resultados la percepción del monitoreo de los servicios inalámbricos de la empresa y frente a ello se ha propuesto implementar un sistema de monitoreo de red para monitorizar y registrar el estado de salud de los distintos dispositivos de telecomunicaciones.

Para poder implementar el Centro de Operaciones de Red se hará uso del sistema de monitorización Zabbix y se integrará con la herramienta Grafana para optimizar la visualización y el formato de los datos del estado de salud de los dispositivos de red, Las cuales se simuló y se realizaron las pruebas, las cuales fueron satisfactorias.

Palabras clave: monitoreo de red, gestión de red, servicios inalámbricos, Zabbix, centro de operación de red, Grafana, osTicket, protocolo simple de administración de red, CentOS 7, tacacs, población, materiales, resultados, ancho de banda.

Abstract

A network operation center is the area that monitors the health status of network devices and resources of the computer systems of a company in real time, the objective of which is to prevent any type of mishap that puts availability at risk. of business operations and guarantee its optimal functioning.

The objective of this research was to establish a monitoring system for Wireless Services in the Interconexiones Ocaney Company through the implementation of a Network Operations Center for the centralized management and administration of telecommunications equipment.

The research was of an applied type, a quantitative approach was used having an explanatory scope with a pre-experimental design, the sample used was of 12 subjects who make up the managed and support staff of the Interconexiones Ocaney company; A survey was applied to this sample by means of a questionnaire made up of 17 questions, having as results the perception of the monitoring of the company's wireless services and against this it has been proposed to implement a network monitoring system to monitor and record the status of the different telecommunications devices.

In order to implement the Network Operations Center, the Zabbix monitoring system will be used and it will be integrated with the Grafana tool to optimize the visualization and format of the health status data of the network devices, which was simulated and they carried out the tests, which were satisfactory.

Keywords: network monitoring, network management, wireless services, zabbix, network operation center, Grafana, osTicket, simple network management protocol, CentOS 7, tacacs, population, materials, results, bandwidth.

Introducción

Cualquier empresa que presta un servicio de telecomunicaciones, su infraestructura de red es uno de sus componentes más importantes. Si dejara de funcionar por algún problema, los clientes quedan sin conectividad y esto afecta la producción del día a día, causando muchos contratiempos, malestar e inclusive grandes pérdidas económicas y si estos problemas se vuelven una constante y la atención que les brindan no es oportuna ni eficiente, lo más probable es que los abonados decidan migrar a otros proveedores de servicio.

Por lo mencionado en el punto anterior, es de vital importancia que los proveedores de servicio de telecomunicaciones cuenten con un sistema de monitorización de red que les pueda servir de apoyo para identificar proactivamente posibles fallos en la red y ayudar a ubicar en qué punto se encuentra el problema y de acuerdo con ello el operador de red analice las causas de la falla y tome una acción siguiendo un procedimiento previamente establecido. Contar con un sistema de monitorización adecuado permitirá a las empresas de telecomunicaciones ofrecer un servicio de calidad a sus abonados. (PandoraFMS, 2017).

Cisco, uno de los líderes en la industria de las telecomunicaciones, ofrece una diversidad de equipos, desde Routers, Switches, monitorización y seguridad para cubrir todas las necesidades de los administradores de tecnología de la información, en las pequeñas, medianas y grandes empresas. Administrar una gran variedad de equipos de red, es una tarea compleja que implica enfrentarse a muchos desafíos como, por ejemplo, configurar, ofrecer disponibilidad del servicio, rendimiento, capacidad de los dispositivos de red, almacenar registros de los eventos de la red para un posterior análisis, entre otros. (ManageEngine, 2020).

El Centro de Operación de Red es el área encargado de proveer apoyo de ingeniería para problemas de conectividad y trabajar como enlace entre otros otras áreas dentro de la organización. Ellos son responsables de resolver y prevenir corte de servicios de datos tanto en los sistemas de conexión física y cableada, ellos se comunican con mesa de ayuda y otros profesionales de sistemas residentes para proveer solución a los problemas de una manera rápida.

El personal del área de Centro de Operación de Red resuelve problemas de conectividad y monitorea los servicios en tiempo real, ellos configuran e instalan equipos de red según sea necesario, también participan en la actualización de proyectos para un soporte de sistema más eficiente. Otra tarea realizada por el personal del área de Centro de Operación de Red incluye ejecutar un mantenimiento de los dispositivos de red (PayScale, 2020).

CAPITULO I

1.1. Descripción de la Organización

La empresa Interconexiones Ocaney es un proveedor de servicio de telecomunicaciones que ofrece Internet, datos, telefonía y seguridad a múltiples clientes, especializada en el desarrollo de proyectos rurales para diversas empresas del sector cafetalero y financiero de la región Jaén. Dentro de esta, se encuentra el área de tecnologías de la información que actualmente no se encuentra organizada. Dicha área es fundamental para ofrecer un servicio eficiente y de calidad. Dado que no cuenta con una correcta gestión y administración de sus equipos de telecomunicaciones, ocasiona demora en la atención de las averías, generando malestar en sus clientes, pérdida de tiempo al no saber en qué equipo se encuentra el problema y no saber cómo solucionar rápidamente.

1.2. Misión

Brindar soluciones completas en el rubro de telecomunicaciones y tecnologías de la información, de manera eficiente, oportuna e innovadora, ofreciendo un asesoramiento personalizado según las necesidades de nuestros clientes.

1.3. Visión

Ser una empresa líder en el rubro de telecomunicaciones y tecnología de la información en la región Jaén. Tener el reconocimiento por su excelencia operativa impulsada por el talento humano y guiada por un modelo de negocio que comparte responsabilidades.

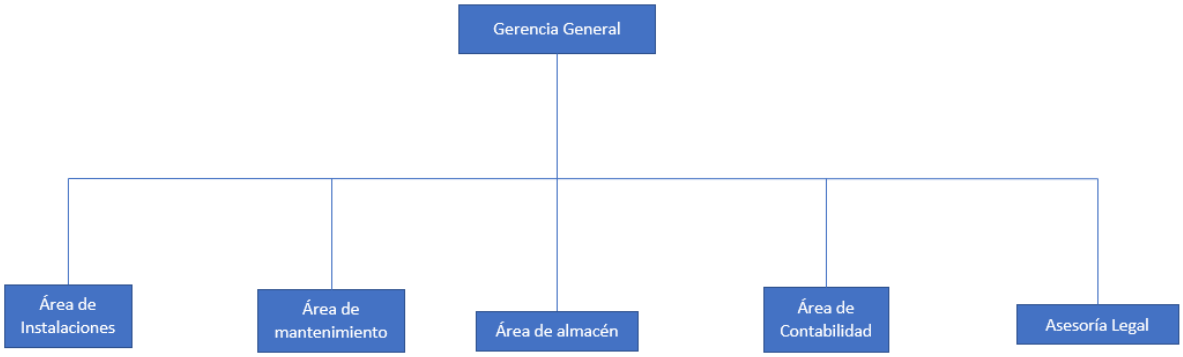
1.4. Objetivos

Nuestro principal objetivo es poder ofrecer a todos nuestros clientes de la región Jaén, servicio de Internet, datos, telefonía y seguridad con lo último en tecnología y contar con el respaldo de grandes marcas en el sector. Contamos con diversos socios estratégicos líderes en el mercado que brindan garantía y calidad en todos nuestros proyectos.

1.5. Estructura Orgánica

Figura **1**

Organigrama de la Organización



Fuente: Elaboración propia.

1.6. Formulación del problema de investigación

Se plantea lo siguiente: ¿De qué manera la Implementación de un Centro de Operaciones de Red mejorará el monitoreo de Servicios Inalámbricos en la Empresa Interconexiones Ocaney?

1.7. Justificación

La presente investigación se justifica porque su realización busca resolver el problema que presenta la empresa Interconexiones Ocaney, el cual no cuenta con una correcta gestión y administración de sus equipos de telecomunicaciones, generando demora en la atención de las averías y ocasionando malestar en sus clientes, por lo mismo el presente proyecto se plantea la implementación de un Centro de Operaciones de Red para así poder tener una gestión y administración centralizada de los servicios inalámbricos y poder brindar un servicio eficiente y de calidad.

1.8. Hipótesis

Mediante la implementación de un centro de operaciones de red se mejorará el monitoreo de los servicios inalámbricos de la Empresa Interconexiones Ocaney.

1.9. Objetivos

1.9.1. Objetivo General

Establecer un sistema de monitoreo para los Servicios Inalámbricos en la Empresa Interconexiones Ocaney mediante la implementación de un Centro de Operaciones de Red para la gestión y administración centralizada de los equipos de telecomunicaciones.

1.9.2. Objetivos Específicos

- Caracterizar el monitoreo de servicios inalámbricos mediante la revisión de literatura en fuentes primarias y secundarias.
- Diagnosticar el estado actual de los servicios inalámbricos prestados por la empresa Interconexiones Ocaney mediante el uso de instrumentos de recolección de datos.
- Implementar el centro de operaciones de red mediante el uso de tecnologías de Monitorización.
- Gestionar el centro de operaciones de red según los estándares de servicios de TI para monitorear los servicios inalámbricos.
- Monitorear los dispositivos de red utilizando el protocolo simple de administración de red.

1.10. Diseño teórico

En los antecedentes internacionales tenemos a: Zhao & Yu (2020) Con el fin de resolver los problemas de confusión y pérdida de objetivos en la tecnología de monitoreo remoto de redes inalámbricas, este documento propone un algoritmo de seguimiento para objetos en movimiento. Finalmente, con el fin de verificar la efectividad y practicidad del algoritmo propuesto, en la parte experimental se realiza la simulación y análisis experimental del algoritmo basado en el sistema software AVR. Los resultados experimentales muestran que el algoritmo de video vigilancia remota inalámbrico propuesto tiene un efecto obvio en la resolución del problema del caos anormal y la pérdida de objetos. En la última parte de este artículo, se centra en el análisis de las técnicas de procesamiento y análisis de vídeo en el contexto de objetos en movimiento y objetos de interferencia múltiple.

Según Wilson & Stevens (2020). En muchas aplicaciones, es de interés identificar si la red cambia de alguna manera significativa y cuándo. El monitoreo de la red es el campo de estudio que aborda la identificación en tiempo real de dichos cambios en los datos basados en la red. El monitoreo de la red, por ejemplo, ha jugado un papel importante en la vigilancia sindrómica y el seguimiento de la propagación de la epidemia, así como en el seguimiento de la información difundida al inicio de los movimientos sociales, incluidas las protestas, los disturbios y los levantamientos. Muchas metodologías existentes en esta área se basan en principios basados en el control de procesos estadísticos. Por lo tanto, existe una oportunidad importante para una contribución significativa en esta área por parte de los miembros de la comunidad de control de calidad.

Como señala (Hegde et al., 2015). La gestión de la red se vuelve muy compleja a medida que las redes crecen en tamaño, complejidad y heterogeneidad. Para hacer frente a un entorno de este tipo, es necesario planificar y gestionar las redes. Estas Las tareas de gestión requieren estadísticas de red obtenidas de mediciones en línea, estadísticas de red típicas como la utilización, el tiempo de actividad del enlace y la tasa de error de bits, etc. crucial para la actividad de gestión de la red. Frente a ello diseña e implementa Netmon, una herramienta para supervisión del rendimiento de una red de paquetes de datos. Estimas

estadísticas de rendimiento de la red, tiempos de actividad del enlace, tasas de error de bits en los enlaces utilizando protocolo simple de administración de red.

Citando a (Becerra Orrala, 2016). Implementa un sistema de monitoreo de red mediante protocolo de mensajes de control de Internet y protocolo simple de administración de red, para que los administradores de tecnología de la información puedan monitorear el estado de salud y rendimiento de los dispositivos de red. Utilizó el método analítico para construir un procedimiento que conlleve a la correcta monitorización y gestión. Definió los requisitos básicos del sistema de monitoreo para la generación y recolección de información, implantando así el monitoreo del tráfico de los dispositivos de red, las pruebas realizadas del monitoreo de interfaces de red, consumo de procesador y memoria en los equipos compatibles con el protocolo simple de administración de red fueron satisfactorias; y por último comprobó el monitoreo del protocolo de mensajes de control de Internet en todos los dispositivos de red.

En los antecedentes nacionales Como plantea Anytech (2019). En el mundo de la gestión de servicios de tecnologías de la información, un centro de operación de red es un equipo de ingenieros de telecomunicaciones encargados de supervisar, monitorear y administrar decenas de plataformas, aplicaciones y páginas web, las 24 horas durante los 365 días del año. Los Ingenieros a cargo de un centro de operación de red son especialistas en identificar tanto problemas como incidentes relacionados a los sistemas monitoreados. Cuentan con el conocimiento para poder mitigar los daños que podrían estar afectando a la producción, así como también para prever futuras fallas creando planes de contingencia, automatizando procesos y ofreciendo respuestas rápidas ante situaciones críticas. Las empresas que deseen que sus redes, servidores y computadoras tengan disponibilidad en el mayor tiempo posible, necesita de un centro de operación de red, que van a ser los responsables de administrar y monitorear en tiempo real el funcionamiento de los dispositivos de red y así evitar en lo posible cualquier degradación de su servicio.

Desde el punto de vista de Quispe Bustincio (2018). Implementa un sistema de monitoreo y control de red mediante el uso de la herramienta Nagios, con lo cual logró monitorear exitosamente los servicios y dispositivos de red de un canal de televisión; garantizando una respuesta rápida y oportuna para solucionar los

fallos que se presenten en la monitorización de los dispositivos de red, mejorando la administración y gestión de los servicios y equipos de telecomunicaciones en el canal de televisión. Realizó un estudio de diseño cuasi experimental tipo descriptivo. Logró implementar de manera satisfactoria un sistema de monitorización para el área de soporte en dicho canal de televisión, donde cuenta con monitoreo y gestión del tráfico de red y correcto seguimiento de los casos de averías, estado de los equipos y servicios que ocurren en la red generando una alarma o notificación en caso de suceder un error.

En los antecedentes locales según (Bravo & Lucero, 2017). Diseñan una red de telemedicina en el Centro Poblado de Huayrul del distrito de Incahuasi que consiste interconectar mediante un enlace inalámbrico el centro de salud de Huayrul con el Hospital Regional de Lambayeque para que los pobladores de Huayrul reciban una mejor atención médica. Eligieron la opción de un radio enlace entre la sede principal y la sede remota, debido a su bajo costo en comparación a un enlace por fibra óptica y además su fácil implementación por parte de cualquier operador que ofrece dicho servicio. Propone utilizar las frecuencias libres de la banda 5.8 GHZ, debido que no está siendo muy usada y no está demasiado congestionado como lo es la banda de 2.4 GHz la cual es muy usada por distintas empresas en la zona donde propone implementar y de esta manera poder aprovechar eficientemente.

Desde el punto de vista de CAMPOS BANCES (2015). Propone implementar un sistema de monitoreo del centro de datos de la universidad Santo Toribio de Mogrovejo de Chiclayo. El objetivo primordial de la propuesta es asegurar la continuidad de los servicios informáticos que brinda el central de datos monitoreando la temperatura y la humedad del lugar donde se encuentra instalado físicamente los equipos de red. El entorno donde aplicó la investigación fue un diseño cuasi experimental. Según sus conclusiones del investigador, la implementación de la propuesta conllevó a un aumento en el índice de satisfacción entre los usuarios de la red de la universidad Santo Toribio de Mogrovejo, porque brinda una mejor gestión y monitorización del estado de salud de los equipos de red en el centro de datos.

1.11. Bases teóricas

Dentro de las bases teóricas podemos conceptualizar a las siguientes: las redes empresariales proporcionan soporte de aplicaciones y de recursos a los usuarios locales y remotos, en cualquier lugar en la que se encuentren y en cualquier momento. La intranet y extranet forman la estructura de estas redes y a menudo incorporan tantas tecnologías LAN como WAN. Para conseguir una red eficiente y segura, es necesario controlar los patrones de flujo del tráfico tanto interno como externo.

A medida que las empresas crecen y evolucionan también lo hace sus necesidades de comunicación por red para proporcionar acceso a la información y a los recursos compartidos. Sin la red, muchas de las actividades normales de la empresa no podrían completarse, lo que tendría como resultado unas significativas pérdidas financieras y una disminución de la base de clientes. Las redes deben diseñarse y mantenerse apropiadamente para reducir la posibilidad de interrupciones en el servicio. En el entorno empresarial, los usuarios se han acostumbrado a esperar que estos servicios estén disponibles de la forma diseñada durante el 99,999 por ciento del tiempo. Esto quiere decir que puede haber un máximo de algo más de cinco minutos de interrupción en el servicio de red a lo largo de un año. Muchos proveedores de servicio garantizan este nivel de fiabilidad y están dispuestos a firmar contratos que imponen grandes penalizaciones financieras si no cumplen dicho compromiso (Reid et al., 2009).

Una de las primeras tareas del personal de soporte de redes es familiarizarse con la estructura de red actual. Las redes empresariales disponen de muchos hosts y dispositivos de red todos ellos interconectados entre sí mediante distintas tecnologías, cable de cobre, fibra óptica y tecnologías inalámbricas. Las estaciones de trabajo del usuario final, los servidores y los dispositivos de red, como los switches y routers, deben documentarse.

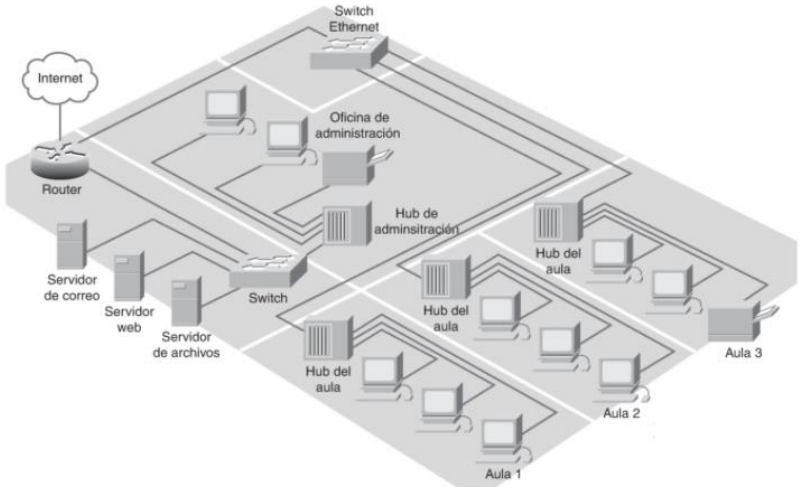
Los diagramas de la infraestructura de red hacen un seguimiento de la ubicación, función y estado de los dispositivos. Los diagramas de topología representan la red física o lógica.

Un mapa de topología física muestra cómo están distribuidos en la red los dispositivos y los medios de trasmisión. Un mapa de topología lógica muestra la

manera como los dispositivos están interconectados dentro de la red, independientemente de su ubicación física. Es primordial que la documentación de la red sea precisa y se mantenga actualizada (Castano Ribes, 2013).

Figura 2

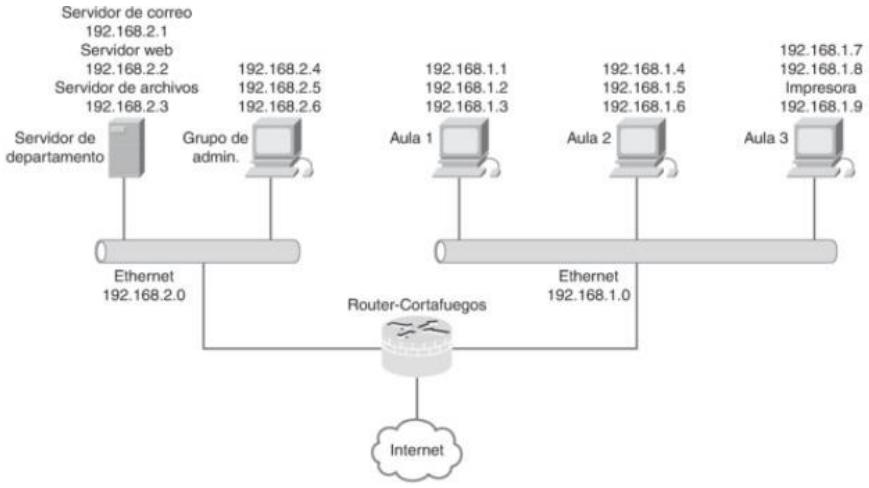
Topología Física



Fuente: (Reid et al., 2009).

Figura 3

Topología Lógica



Fuente: (Reid et al., 2009).

En las redes empresariales además de los diagramas de red, se emplean otros tipos de documentación muy importantes, como son un plan de continuidad del negocio, un plan de seguridad empresarial, un plan de mantenimiento de la red y un acuerdo del nivel de servicio.

El plan de continuidad de negocio identifica los pasos que se deben dar para que la empresa siga funcionando en el caso que se produzcan un desastre natural o provocado por el hombre. El plan de seguridad de la empresa impide accesos no autorizados a los recursos y activos de la organización. El plan de mantenimiento de la red minimiza el tiempo de parada definiendo los procedimientos de mantenimiento hardware y software. El acuerdo del nivel de servicio garantiza los parámetros del servicio, definiendo el nivel de rendimiento del proveedor de servicio.

La mayoría de las redes empresariales disponen de un Centro de Operación de Red que permiten gestionar y monitorizar todos los recursos de la red, También suele llamarse Centro de Datos. Los empleados de un NOC de una empresa dan soporte tanto a las ubicaciones locales como las remotas. Además de la administración de red y proporcionarla soporte, muchos NOC también proporcionan recursos centralizados, como por ejemplos servidores y dispositivos de almacenamientos de datos. Los servidores llevan a cabo funciones: realización de copias de seguridad y el equilibrio de carga (Reid & Lorenz & Schmidt, 2009).

Un centro de operación de red, es el área que realiza la monitorización del estado de salud de los dispositivos de red y recursos de los sistemas informáticos de una empresa en tiempo real, cuyo objetivo es prevenir cualquier tipo de percance que pongan en riesgo la disponibilidad de las operaciones del negocio y garantizar su óptimo funcionamiento, en el caso de que suceda una incidencia, ofrecer una respuesta rápida y oportuna (Think networks, 2020).

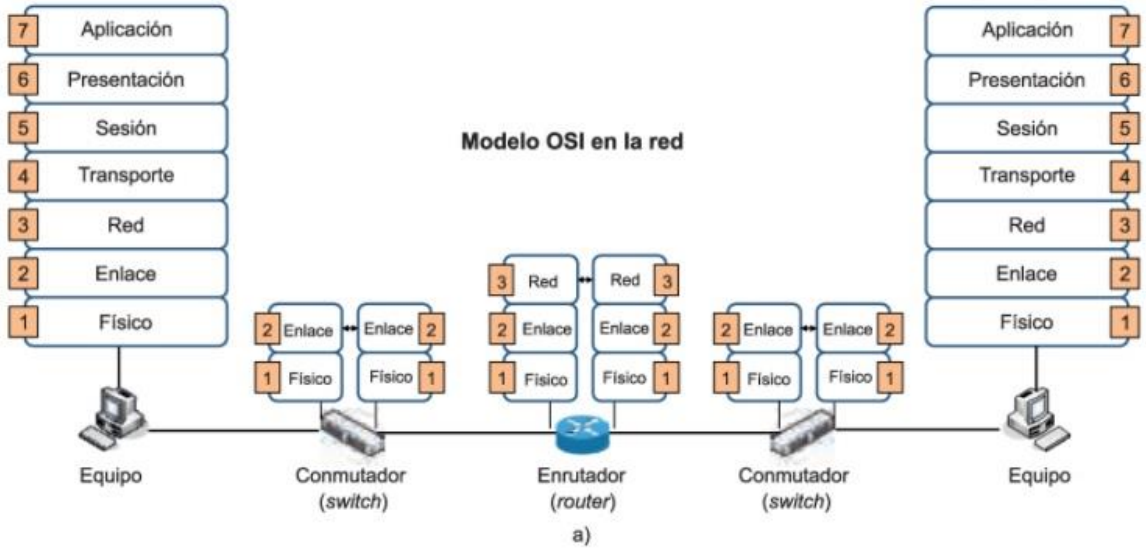
Con todo lo anterior, la monitorización de la red, se han transformado en una parte esencial de los actuales sistemas de información en donde un gran número de dispositivos se encuentran interconectados entre sí. Debido al gran número de redes en el mercado, surge la necesidad de estandarizar, las cuales garantizan la comunicación entre diferentes dispositivos de redes y evitar que intereses privados determinen normas (Manuel Sánchez Rubio, 2020).

Un estándar es un modelo que se propone para que distintos fabricantes lo sigan y fabriquen componentes compatibles entre sí. Pueden ser de organismos oficiales o de jure y de iniciativa propia de las empresas también llamadas de facto.

Por ejemplo, tenemos a ISO un organismo de jure, que desarrollo el modelo de referencia de siete niveles para interconexión de sistemas abiertos (OSI) que establece un marco de referencia para la determinación de arquitecturas de interconexión de sistemas de comunicaciones. No importa la localización geográfica o el lenguaje utilizado: todos deben amoldarse a unas normas mínimas para poder comunicarse entre sí (López & Padilla, 2013).

Figura 4

Modelo de referencia OSI



Fuente: (López & Padilla., 2013).

Cada capa se encarga de satisfacer una serie de requisitos distintos, según el nivel en que nos encontremos. La capa física es el encargado de las conexiones de un dispositivo hacia la red. Capa de enlace se ocupa del direccionamiento físico, del acceso al medio. Capa de red se ocupa de establecer el enrutamiento entre una o más redes. Capa de transporte se encargar de efectuar el transporte de los datos. La capa de sesión se encarga de mantener y controlar el enlace establecido dos dispositivos. La capa de presentación se encarga de la representación de la información de modo adecuado. La capa de aplicación es la capa encarga de ofrecer a las aplicaciones la posibilidad de acceder a los servicios de las demás capas (López & Padilla, 2013).

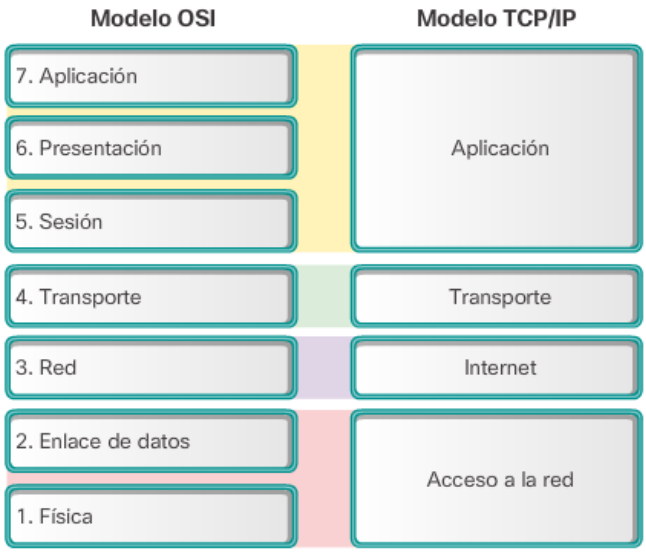
En efecto, el modelo de referencia OSI es utilizado como un modelo teórico, ahora bien, el protocolo TCP/IP considerado estándar de facto, es el modelo de

arquitectura de red funciona en la práctica. Presenta gran fiabilidad y relativa facilidad para el enrutamiento de paquetes. Se estructura en capas y, en cada una de ellas, aparece la correspondiente PDU encapsulada (Castano Ribes, 2013).

Dicho brevemente las capas des modelo TCP/IP son: Capa de acceso que provee la transmisión de datos independientemente de la red que haya sido configurada. Capa de Internet encargada de transmitir datagramas utilizando como direccionamiento los números de dirección IP. Capa de transporte encargada de realizar una transmisión fiable entre las aplicaciones que quieren comunicarse. Capa de aplicación contiene las aplicaciones de red que usarán los servicios ofrecidos por las capas inferiores (Castano Ribes, 2013).

Figura 5

Comparativa entre modelo OSI y TCP/IP



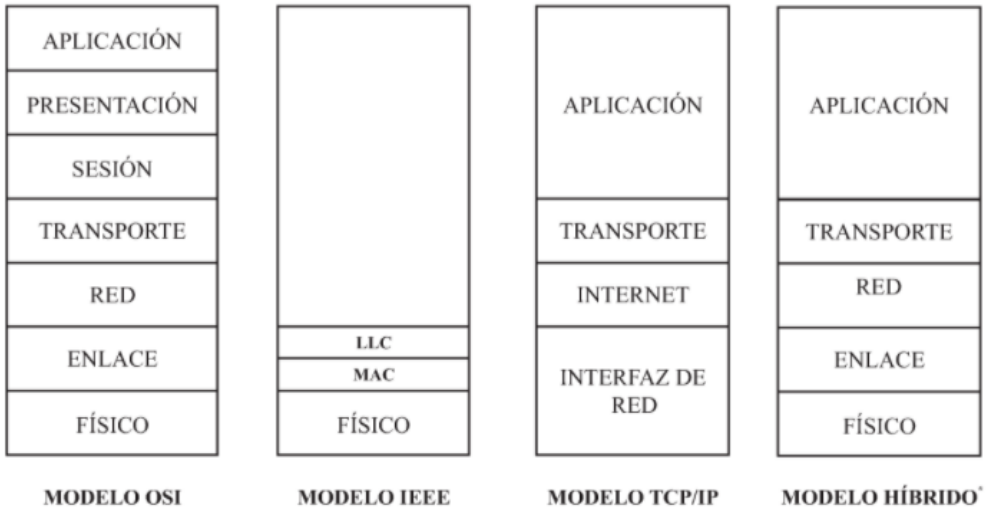
Fuente: (Interpolados, 2017)

De igual modo, el modelo de referencia IEEE, se estableció para elaborar un estándar de comunicación entre los dispositivos en LAN. El estándar 802 de IEEE para LAN es vital, siendo tomado por el ISO como la base para el estándar ISO 8802. Consta de: nivel físico que trata la relación con el medio de transmisión y el nivel de enlace se divide en dos subniveles: control de enlace lógico (LLC), cuyo objetivo es manejar distintos tipos de servicios de comunicación que se pueden ofrecer a través del medio y control de acceso al

medio (MAC), que ofrece la dirección física del equipo conectado a la red (Sánchez & Barchino, 2020).

Figura 6

Comparación entre los distintos modelos



Fuente: (Sánchez & Barchino, 2020).

En cuanto a tipos de redes existen múltiples clasificaciones respecto a los principios que se tenga en cuenta, por ejemplo, según su extensión: Redes LAN, limitado físicamente a un edificio. Redes WAN que permite interconectar ciudades entre sí o incluso todo un país. Según el tipo de acceso a la red: red pública, donde los nodos acceden a la red utilizando la dirección IP que le proporciona su proveedor de servicio. Red privada, que usa una dirección IP especial que se define como privada. Según el medio de transmisión pueden ser: Red cableada, los equipos terminales se conectan a la red mediante un cable. Red inalámbrica, que permite transmitir y recibir información mediante ondas electromagnéticas, esto se logra gracias a las antenas que disponen las tarjetas de red de los ordenadores y de los dispositivos de red (Castano Ribes, 2013).

También la red se puede clasificar por su tecnología, tenemos redes Brocadas: donde el medio transmitido es compartido, es decir los paquetes se envían a toda la red, aunque vayan dirigidos a un único destinatario. Enlaces punto a punto: donde la información se transmite solo a la estación a la cual va dirigida, estos enlaces pueden ser, en función del sentido de la transmisión; simplex (transmisión en un solo sentido), half-duplex (transmisión en ambos sentidos,

pero no simultaneo) y full dúplex (transmisión en ambos sentidos a la vez) (Sánchez & Barchino, 2020).

Otro punto importante es la interconexión entre redes, donde los principales elementos que permiten realizar la interconexión entre dispositivos de redes son los Switches, Routers y Gateway. La gran diferencia entre dichos dispositivos de red está en el nivel del modelo de referencia OSI en el que actúan (Sánchez & Barchino, 2020).

Figura 7

Ubicación en el modelo OSI de los Switches, Router y Gateway

Fuente: (Sánchez & Barchino, 2020).

Ahora bien, un Switch es un dispositivo de red que trabaja en la capa 2 del modelo OSI que pueden aprender de manera dinámica las direcciones MAC de los dispositivos conectados a sus puertos inspeccionando la dirección MAC origen de las tramas entrantes en cada puerto del Switch. Así mismo se tiene un Switch multinivel que puede tomar decisiones de re direccionamiento a partir de información de capas superiores como direcciones IP. Los Routers son unos dispositivos de la capa 3 del modelo OSI, lo que implica que sus decisiones de re direccionamiento se basan en información de direcciones lógicas de red. Un Gateway es un transformador de protocolo que provee servicios de traducción entre LAN´s o aplicaciones incompatibles (Guerra Soto, 2016).

Así mismo tenemos otros dispositivos de interconexión de redes como, por ejemplo: Firewalls que se emplea para proteger una red de tráfico malicioso o acceso a ciertos servicios mediante el filtrado de paquetes. Balanceadores de carga que pueden remitir los paquetes entrantes a múltiples dispositivos ocultos mediante una única dirección IP. Concentrador VPN que se puede utilizar

cuando el número de sedes remotas a conectar con la sede central es elevado, la carga de los procesos paralelos de cifrado-descifrado de la información y autenticación de usuarios legítimos de cada uno de los túneles establecidos puede llegar a resultar demasiado elevada para el Router (Guerra Soto, 2016).

Otro punto importante son los servicios **Inalámbricos,** son redes que utilizan ondas electromagnéticas para interconectar los dispositivos entre dos puntos distintos, sin la necesidad de utilizar cables de por medio que ocupen espacio. Las redes inalámbricas ayudan en muchos aspectos. En unos casos se utilizan en sustitución a las redes cableadas porque es más rápido de implementar por su facilidad de instalación, mientras que en otros casos se emplean para suministrar acceso a datos corporativos desde ubicaciones remotas (cita, 2018)

Las principales ventajas de las redes Inalámbricas son: Rápida instalación sin requerir permisos de instalación de obra, levantar las calles. Movilidad es decir el medio de transmisión no está sujeto a ningún cable. Menos coste de manteniendo, al no tener cableado los costos se reducen. Productividad, proporcionar la colaboración, el teletrabajo. Es la única solución para zonas inaccesibles a las que no es posible llegar con red cableada, como es el caso de zonas rurales (Andreu, 2011).

Las redes Inalámbricas se pueden clasificar en: Redes inalámbricas de área personal (WPAN) que posibilita la comunicación en un determinado rango de distancias muy cortas, unos 10 metros. Redes inalámbricas de área local (WLAN) diseñadas para suministrar acceso inalámbrico en sitios con un rango hasta 100metros, utilizadas generalmente en el hogar, oficina, escuela, etc. Redes inalámbricas de área metropolitana (WMAN) también denominado WiMAX, abocado a suministrar una alta velocidad de transmisión de datos mediante el uso de redes inalámbricas de área metropolitana, lo permite que las redes inalámbricas LAN más pequeñas puedan ser interconectadas por WiMAX creando una red gran red de área metropolitana. Según lo mencionado anteriormente, la creación de redes entre ciudades puede lograrse sin la necesidad de cableado costoso. Las redes inalámbricas de área amplia, se extienden aproximadamente unos 50Km (Salazar, 2016).

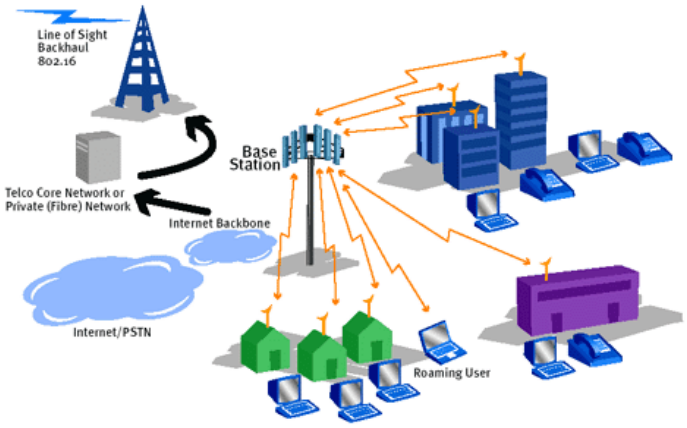
Figura 8

Ejemplo de WLAN

Fuente: (Internet Paso a Paso, 2018)

Figura 9

Ejemplo de WMAN



Fuente: (Tipos de redes, 2017)

Las redes inalámbricas se dividen en: Enlaces punto a punto en la que cada canal de datos se usa para comunicar únicamente dos nodos. Enlace punto multipunto es cuando tenemos varios nodos hablando con un punto de acceso central. Enlace punto multipunto donde cada estación de la red transporta el tráfico de otras estaciones de red y todos se comunican directamente entre sí (Flickenger, 2008).

Para realizar una instalación de una infraestructura de red inalámbrica es necesario, en primer lugar, establecer una planificación de la ubicación que va a ocupar cada punto de acceso, el canal que va a utilizar y las conexiones de red cableadas que se van a necesitar. Posteriormente, será necesario establecer los parámetros de la red inalámbrica en cuanto a identificar a utilizar (SSID), canales y mecanismos de seguridad (Molina Robles & Polo Ortega, 2014).

Una infraestructura de red inalámbrica está formada por los siguientes elementos: los ordenadores con sus adaptadores de red inalámbricos, los puntos de acceso inalámbricos, dedicados a gestionar las comunicaciones entre los equipos, los concentradores y conmutadores para conectar los puntos de acceso entre sí a través de cableado, y los encaminadores inalámbricos para permitir la comunicación con redes de área extensa como Internet (Molina Robles & Polo Ortega, 2014).

Los mecanismos más importantes que se emplean para mejorar la seguridad de una infraestructura de red inalámbrica son: cifrado de la comunicación y autorización de acceso por la lista de direcciones MAC. Los métodos de cifrado de las comunicaciones inalámbricas que más se utilizan son: WEB, WPA, WPA2 e IPSEC (Molina Robles & Polo Ortega, 2014).

Otro punto es el diagnostico de averías en las redes inalámbricas, los errores más habituales son: Indicadores luminosos, errores de hardware y software, conexión a servicios de red: Utilización de credenciales de usuarios incorrectos, carencia de nivel de permisos adecuado por el usuario, Exceso de número máximo de usuarios autorizados (Guerra Soto, 2016).

Cuando se pretende determinar si un error es debido a un fallo en el equipo del usuario o tiene su origen en el servidor, un indicativo suele ser si el error se produce únicamente en un equipo, siendo síntoma de un fallo en el mismo, o el mismo error es común a todos los equipos de un segmento de red, lo que suele ser síntoma de fallo en el servidor. La incorrecta conexión o estado del cableado suele ser también una fuente habitual de problemas. Una forma de determinar un posible error es comprobar el LED de enlace en la tarjeta de red (Guerra Soto, 2016).

En general, desde el punto de vista del administrador, las redes inalámbricas requieren mayor esfuerzo para su correcta configuración. Además, pese a que no existen en su parte radio los problemas asociados al cableado, también existen diferentes problemas asociados con la capa física, tales como interferencia: inherentes a la utilización del canal radio como medio de transmisión. Configuración: los errores en la configuración de las WAP, de los Router inalámbricos o la existencia de inconsistencias entre las configuraciones de los puntos de acceso y las estaciones pueden también ser el origen de problemas. Cifrado incorrecto: para asegurar el mayor nivel de seguridad, la conexión inalámbrica debe cifrarse con el algoritmo criptográfico más robusto. Canal incorrecto: las redes inalámbricas emplean diferentes frecuencias dentro de la banda comprendida entre los 2.4 y los 5Ghz. Latencia: al ser medio inalámbrico un recurso compartido entre todos los clientes de la red, cuando mayor sea su número de clientes inalámbricos, menor será el rendimiento de todos ellos. Rebotes, En una red inalámbrica que dé cobertura a una gran extensión geográfica deberán instalarse los repetidores y reflectores necesarios para poder garantizar la cobertura exclusivamente en el área deseada (Guerra Soto, 2016).

De todo lo planteado hasta ahora requiere disponer de un sistema de **gestión** y **monitorización** de sus dispositivos para asegurar su uso, disponibilidad, evitar fallos en la red, brindar soluciones rápidas. Para poder ofrecer este nivel de servicio es necesario disponer de herramientas que permiten la gestión de fallos, usuarios y seguridad. Los elementos de un sistema de gestión de red: el gestor, parte de la aplicación que impone las bases de la gestión y recibe los inputs de los diferentes dispositivos de la red. El agente, tiene la función de responder a las bases impuestas por el gestor. El protocolo de gestión, conjuntos de reglas que gestionan los procesos y elementos del sistema de gestión. La base de datos de información de Gestión, conjuntos de objetos gestionados que representan recursos de red. (Guerra Soto, 2016).

Los mecanismos de monitorización empleados para el intercambio de información entre el gestor y los agentes son: Sondeo(polling), Acceso periódico del gestor a los agentes para determinar si se produjo una modificación en su estado. Notificaciones, los agentes envían notificaciones al gestor cuando

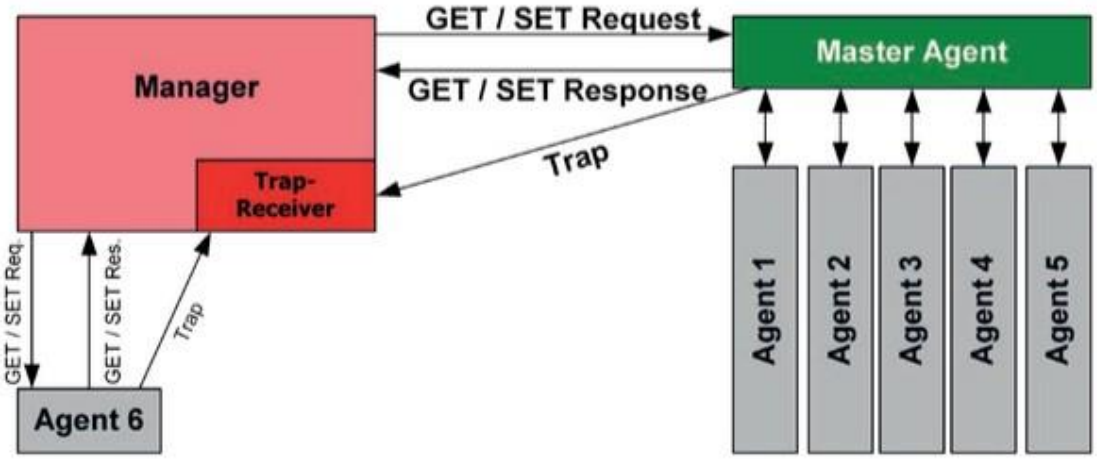
suceden determinados eventos. Mixtos, se incorporan estaciones intermedias, dedicadas a la recolección local de datos (Guerra Soto, 2016).

En definitiva**, Monitoreo** de la red es la utilización de registros y herramientas de análisis para resolver con exactitud el flujo de tráfico, el uso consumo de ancho de banda, estado de salud, entre otras características de la red. Las distintas herramientas de monitorización nos proporcionarán cifras numéricas y gráficas del estado de salud de la red. Esto nos ayudará a visualizar con precisión lo que está aconteciendo en la red, de tal manera que sepamos cuáles son los ajustes que necesitamos realizar (Flickenger, 2008).

De lo anterior, la IETF define a SNMP que permite a los dispositivos de red compartir información sobre ellos mismos y sus actividades. El protocolo simple de administración de red comprende de: Manager que es un sistema de gestión de red que emplea SNMP para sondear y recibir datos de los dispositivos de red. Agente que es un proceso que se ejecuta en el dispositivo de red que se está monitorizado. A su vez los datos se almacenan en una base de datos el cual se llama gestión de información base lo cual se actualiza en tiempo real (Ariganello & Barrientos Sevilla, 2015).

Figura 10

Esquema de funcionamiento del protocolo SNMP



Fuente: (Guerra Soto, 2016)

Actualmente, existen tres versiones del protocolo SNMP: Versión 1: utiliza protocolos como UDP, IP, OSI. Versión 2: incluye mejoras en rendimiento, seguridad, confidencialidad. Versión 3: Entre sus mejoras con respecto a las versiones anteriores del protocolo incluye importantes medidas de seguridad, como la confidencialidad, integridad y autenticación. SNMP utiliza segmentos UDP y los puertos 161(agente) y 162(NMS) para las comunicaciones no seguras. Las comunicaciones seguras TLS emplean los puertos 10161(agente) y 10162(NMS) (Guerra Soto, 2016).

En cuando a las herramientas de gestión existen un amplio abanico de herramientas para la gestión y mantenimiento de la red al igual que un amplio de rango de precios, que va desde las que son libres hasta las que valen miles de dólares. Tales como capturador de paquetes, es un programa que solicita una copia a una NIC de todos los paquetes que entran y salen por ella. Analizadores de paquetes, vienen integrados con un software que permite analizar los paquetes capturados. Monitorización del flujo de paquetes, que consiste en analizar el tráfico de red que fluye entre determinados dispositivos origen y destino. Este concepto fue desarrollado por cisco, que lo incluyó en routers y switches, esta herramienta se llama netflow, que se basa en el concepto de flujos definidos por el administrador de red para poder monitorizar el tipo de tráfico deseado. Monitor de interfaz, permite determinar la robustez de la red en la que conecta, permite medir el ancho de banda y utilización de una o más interfaces de red de uno o más dispositivos, tales como velocidad y utilización de canal, ancho de banda consumido, paquetes descartados, errores, descartes, reinicio de interfaz. Monitor de rendimiento, mide el rendimiento de algún aspecto de un sistema en función del tiempo, permitiendo de este modo al administrador de red conocer cuando se está produciendo una anomalía (Guerra Soto, 2016).

Los monitores de rendimiento utilizan los ficheros de registro de eventos del sistema(log) para medir el rendimiento en función del tiempo. Los log almacenan la información relativa al rendimiento de un aspecto específico del sistema. Algunos ejemplos de los aspectos que pueden ser monitorizados son el porcentaje de utilización de un puerto ethernet especifico o el rendimiento a través de una conexión de red (Guerra Soto, 2016).

Figura 11

Monitorización de red con Zabbix

Fuente: (Zabbix, 2020)

Zabbix es un Sistema de Monitorización de Redes. Que está diseñado para monitorizar y registrar el estado de varios servicios de red, Servidores, y hardware de red. Ofrece múltiples opciones para monitorear: inspecciones simples que pueden validar la disponibilidad y el nivel de respuesta de servicios estándar como HTTP, sin la necesidad de instalar ningún aplicativo sobre el dispositivo a monitorear. Un agente Zabbix puede ser instalado sobre distintas maquinas como Linux y Windows para monitorizar estadísticas como carga de CPU, utilización de red, espacio en disco, entre otras opciones (Zabbix, 2020).

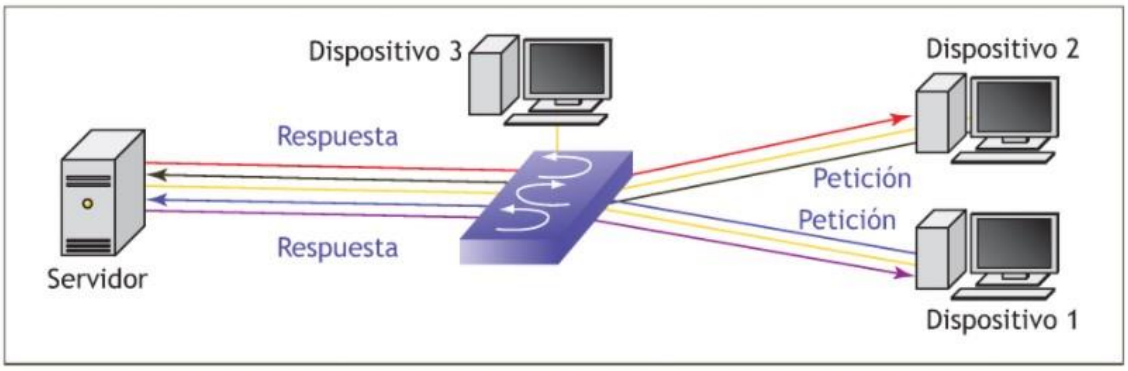
Grafana es un software libre utilizado para el análisis y visualización de datos. Esta herramienta nos permite consultar, visualizar, alertar y explorar sus métricas independientemente en dónde se estén almacenadas. En un lenguaje sencillo, que nos proporciona herramientas para ver reportes en gráficos y visualizaciones detallados que nos ayudará a una mejor monitorización de la red.(Grafana, 2020).

Grafana se ha convertido en la tecnología más popular del mundo que se utiliza para componer paneles de visualización desde métricas, gráficos y hasta registros y datos de aplicaciones.(Grafana, 2020)

Para montar el sistema de monitoreo se requiere un servidor de red, para ello se va a utilizar la estructura de red cliente servidor, en donde un equipo denominado servidor equipado con un hardware especial va a ejecutar el software de monitoreo que va a interactuar simultáneamente con dispositivos clientes de forma eficiente

Figura 12

Estructura de red cliente-servidor



Fuente: (Molina Robles & Polo Ortega, 2014)

Para este proyecto, utilizaremos CentOS 7 como servidor de red, CentOS Linux es un sistema operativo utilizada para servidores, es de distribución gratuita de Red Hat, como tal, CentOS Linux es funcionalmente compatible con RHEL. El Proyecto CentOS lo que cambia principalmente son los paquetes para eliminar la marca y el material gráfico de los proveedores. Cada versión de CentOS se mantiene hasta que la versión RHEL equivalente deja de ser compatible. Una nueva versión de CentOS está disponible una vez que se reconstruye una nueva versión de RHEL, aproximadamente cada 6-12 meses para versiones de puntos menores y varios años para cambios de versiones principales. El tiempo que lleva la reconstrucción varía desde semanas para lanzamientos puntuales hasta meses para cambios de versiones principales. Esto da como resultado un entorno Linux seguro, de bajo mantenimiento, confiable, predecible y reproducible. (CentOS, 2014).

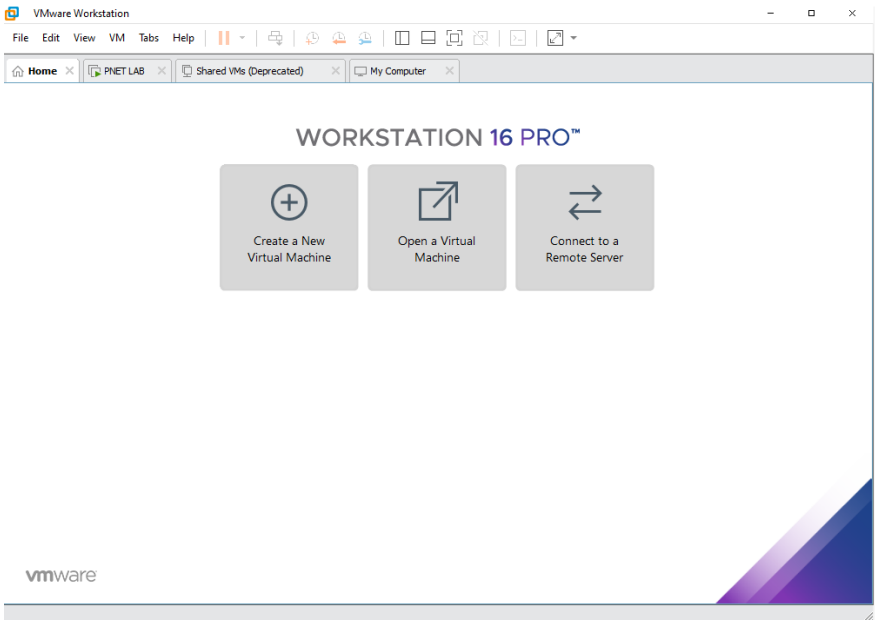
El servidor CentOS se puede instalar en una maquina física, máquina virtual o en la nube (Armazón, Google Cloud, Azure). Para instalar en una maquina física los requisitos mínimos son: procesador basado en arquitectura x86_x64,

memoria RAM mínimo de 1GB recomendado 2GB, disco duro mínimo 20GB recomendado 40GB.

Para instalar en una máquina virtual se puede utilizar los distintos softwares de virtualización que existen en el mercado tanto de pago como gratis tales como VMWare, Virtual Box.

Figura 13

Software de virtualización VMWare



Fuente: Elaboración propia

Figura 14

Software de virtualización Virtual Box

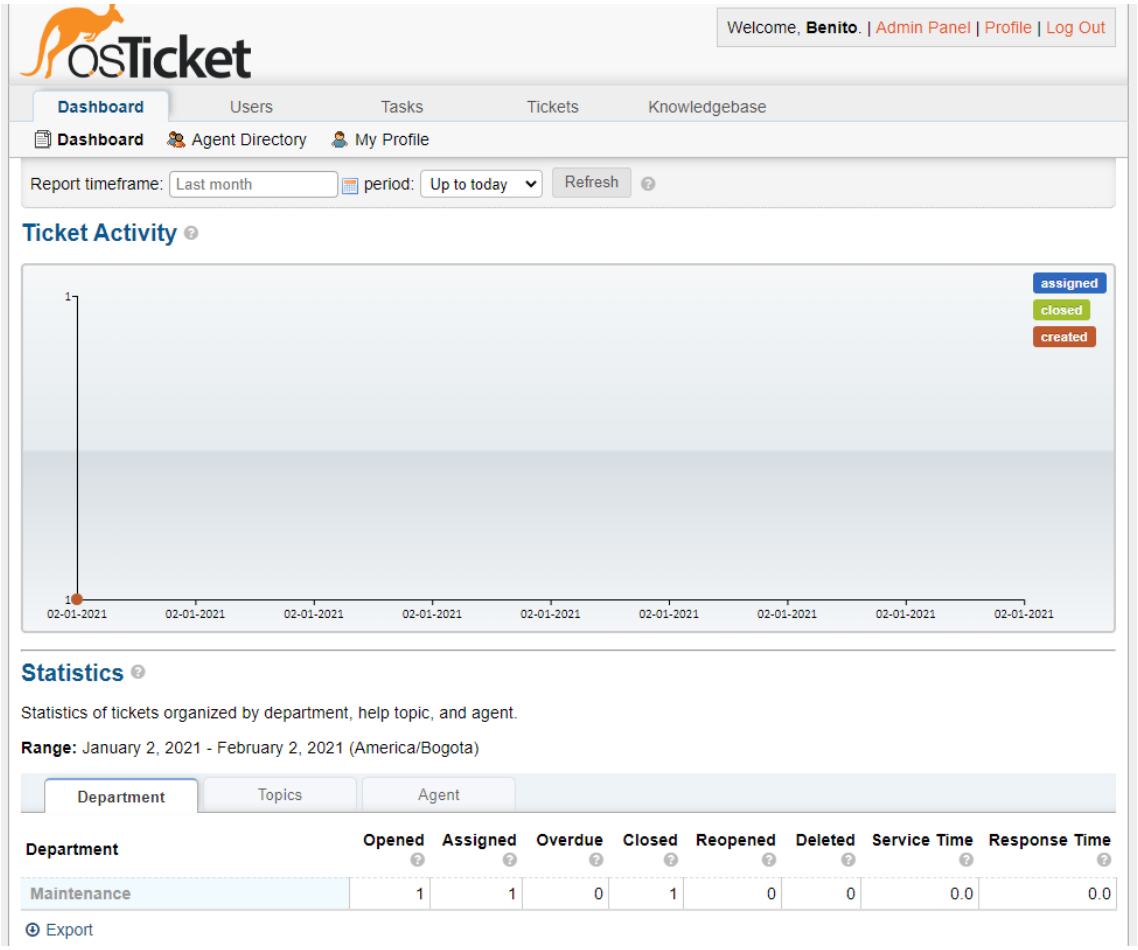
Fuente: Elaboración propia

Para el registro y control de los requerimientos e incidencias utilizaremos la herramienta osTicket, que es una herramienta de tiques para soporte de código abierto muy utilizado. Integra consultas a través de correo electrónico, teléfono y formularios basados en una interfaz web multiusuario. Nos permite administrar, organizar y archivar todas las solicitudes y respuestas de soporte en un mismo lugar.

Además de los correos electrónicos, los clientes y usuarios también pueden utilizar un formulario en línea para crear ticket. Los temas de ayuda permiten mapear consultas en línea a un departamento y asignan prioridad sin la necesidad de que el usuario seleccione un departamento o prioridad de ticket.(osTicket, 2020)

Figura 15

Herramienta de registro de tique osTicket



Fuente: Elaboración propia

Los dispositivos de red a monitorear en la empresa Interconexiones Ocaney son routers y Switches de la marca cisco, Los routers son utilizados en la red Backbone para salida a Internet, y los Switches para separar el tráfico por VLAN´s. Entre los diferentes modelos tenemos los Catalyst 2950, Catalyst 3750X-24T-S y router ISR 4331.

Figura 16

Imagen de Switch Cisco Catalyst 3750X-24T-S

Fuente: (CISCO, 2020)

Respecto a los dispositivos de red en los enlaces troncales tenemos la marca Mikrotik, los modelos SXT SA5AC, BaseBox 6, LDF 5AC que son dispositivos de alta velocidad y bajo costo.

Figura 17

Imagen de enlace inalámbrico Mikrotik

Fuente:(Mikrotik, 2020)

1.12. Definición y Operacionalización de Variables

Variable Independiente: Implementación de un centro de operaciones de red

Variable Dependiente: Monitoreo de Servicios Inalámbricos

Variables	Definición conceptual	Dimensiones	Indicadores
VI: Implementación de un centro de operaciones de red	Es el área que se encarga de monitorizar la disponibilidad y el estado de salud de los sistemas informáticos de una empresa en tiempo real, con el fin de prevenir incidentes que puedan poner en riesgo la disponibilidad de las operaciones del negocio y de esta manera asegurar su funcionamiento adecuado, en el caso de que sucedan, ofrecer una respuesta rápida y oportuna (Think networks, 2020).	Recursos informáticos	• Estado de los dispositivos de red • Configuración de los equipos de red
		Disponibilidad	• Operación y acceso a la red • Redundancia ante caída de los equipos de red
		Escalabilidad	• Cantidad de equipos informáticos • Servicios implementados
VD.: Monitoreo de Servicios Inalámbricos	Monitorizar la red significa supervisar de forma periódica con el fin de garantizar que el estado de salud de los dispositivos de red se encuentre dentro de los parámetros	Gestión	• Configuración de los servicios inalámbricos • Incidencias de los servicios inalámbricos

	establecidos previamente. Cuando se detecte que la red opera fuera de los límites establecidos, se registrara el suceso y se activara una alarma (Guerra Soto, 2016).		• Seguridad de los servicios inalámbricos • Capacidad de los servicios inalámbricos • Registro de los servicios inalámbricos
		Monitoreo	• Control de ancho de banda. • Estado de los equipos inalámbricos. • Respaldo de la información • Documentación de los dispositivos de red

CAPITULO II

2. Métodos y Materiales

2.1. Diseño de contrastación de hipótesis

La investigación fue de tipo aplicada, debido a sé que busca resolver un determinado planteamiento especifico o problema particular teniendo como propósito enfocarse en la búsqueda y consolidación del conocimiento científico, lo cual contribuye en nuestro caso a una solución de innovación tecnología (Biblioteca DUOC UC, 2018).

Se utilizó el enfoque cuantitativo, teniendo un alcance explicativo. El presente estudio tuvo un diseño pre experimental en donde se manipuló la variable independiente para obtener un efecto en la variable dependiente (Hernandez Sampieri et al., 2014).

2.2. Población y muestra

La población en estudio estuvo conformada por el personal administrativo y soporte de la empresa interconexiones Ocaney, lo que hizo un total de 12 empleados. Al estar la población significativamente pequeña, la muestra fue también igual a 12 sujetos.

2.3. Técnicas, instrumentos, equipos y materiales

La técnica utilizada fue la encuesta y se tuvo como instrumento el cuestionario con el cual se recolectó los datos y a su vez se recabó información referente al monitoreo de servicios inalámbricos en la empresa en estudio. Así mismo se hizo uso del software de monitoreo Zabbix con lo cual se permitió obtener el estado clínico de los dispositivos de red.

El instrumento estuvo conformado por 8 ítems y 3 dimensiones (Recursos informáticos, Disponibilidad, Escalabilidad) para la variable independiente (Implementación de un centro de operaciones de red); por su parte la variable dependiente (Monitoreo de Servicios Inalámbricos) contiene 9 ítems y 2 dimensiones (Gestión, Monitoreo).

La confiabilidad del instrumento se determinó por medio del alfa de Cronbach para lo cual se utilizó el software estadístico Jamovi v.1.2.27.0. El resultado obtenido indica que el instrumento es altamente confiable, según se muestra en la tabla 1.

Tabla 1

Confiabilidad del instrumento de recolección de datos

Scale Reliability Statistics	
	Cronbach's α
scale	0.958

Fuente: Elaboración propia

Entro los equipos y materiales utilizados se tiene:

Hardware

- Servidor con procesador Intel Core i3 de 2.0 GHZ, memoria RAM 8 GB, Disco duro 500 GB, puerto de red Realtek PCIe GBE.
- Routers
- Switches
- Antenas inalámbricas MikroTik

Software

- Sistema Operativo CentOS Linux 7 (Core) con kernel Linux 3.10.0-1160.15.2.el7.x86_64
- Zabbix versión 5.0.8
- PHP versión 7.4.15
- Apache versión 2.4.6
- MySQL versión 15.1
- Grafana versión 7.4.2
- OsTicket versión 1.14.5
- VMWare versión 16.1.0 build-17198959

Materiales

- Laptop
- Teléfono

CAPITULO III

3. Resultados y Discusión.

3.1. Resultados descriptivos.

Tabla 2

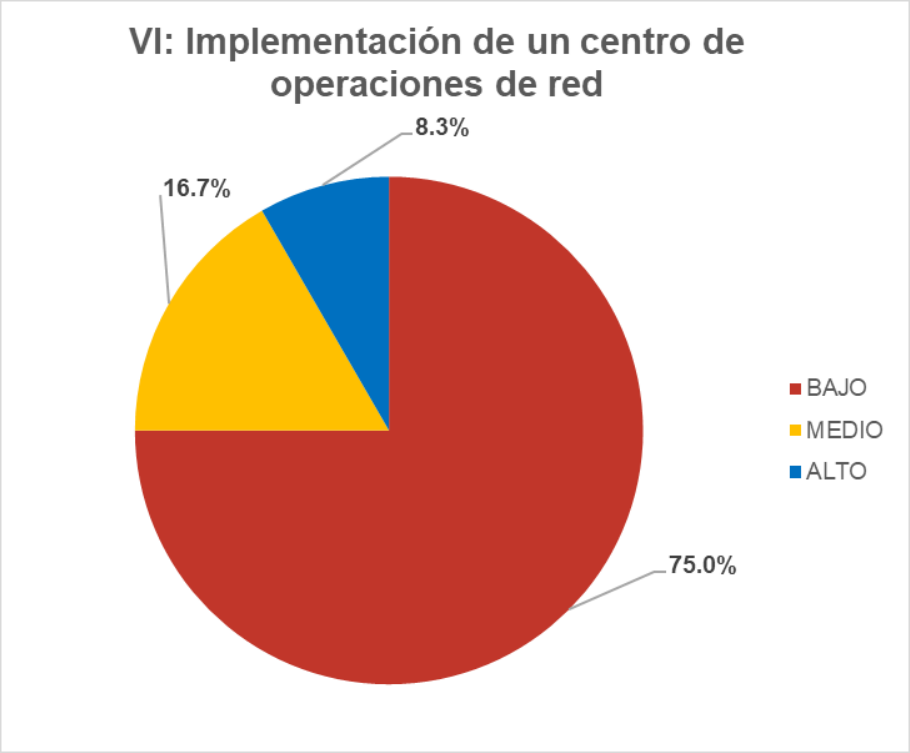
Calificación de la variable VI: Implementación de un centro de operaciones de red

Calificación	VI: Implementación de un centro de operaciones de red	
	Frecuencia (fi)	Porcentaje (%)
BAJO	9	75.0%
MEDIO	2	16.7%
ALTO	1	8.3%
TOTAL	12	100.0%

Fuente: Elaboración propia

Figura 18

Gráfico de la variable VI: Implementación de un centro de operaciones de red



Fuente: Elaboración propia

Interpretación: Tal como se observa en la tabla 2, figura 11, la variable independiente: Implementación de un centro de operaciones de red es calificada por los encuestados por el 75.0% como un nivel bajo, el 16.7% la califica como nivel medio y el 8.3% la califica como un nivel alto.

Tabla 3

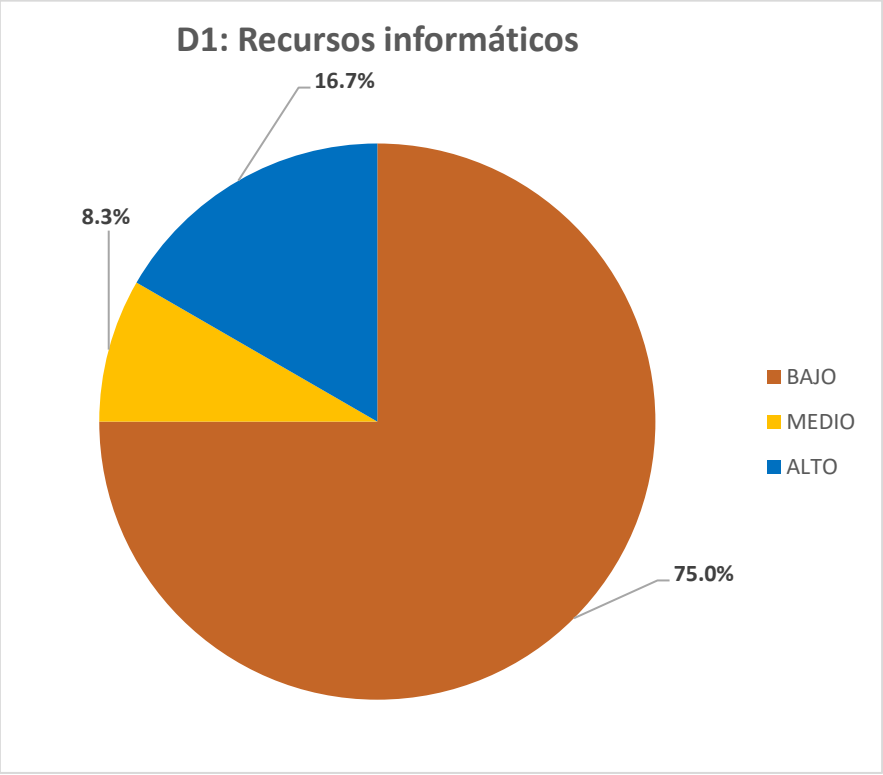
Calificación de la dimensión D1: Recursos informáticos

Calificación	D1: Recursos informáticos	
	Frecuencia (fi)	Porcentaje (%)
BAJO	9	75.0%
MEDIO	1	8.3%
ALTO	2	16.7%
TOTAL	12	100.0%

Fuente: Elaboración propia

Figure 19

Gráfico de la dimensión D1: Recursos informáticos



Fuente: Elaboración propia

Interpretación: Así como se observa en la tabla 3, figura 12, la dimensión: recursos informáticos es calificada por los encuestados por el 75.0% como un nivel bajo, el 16.7% la califica como nivel medio y el 8.3% la califica como un nivel alto.

Tabla 4

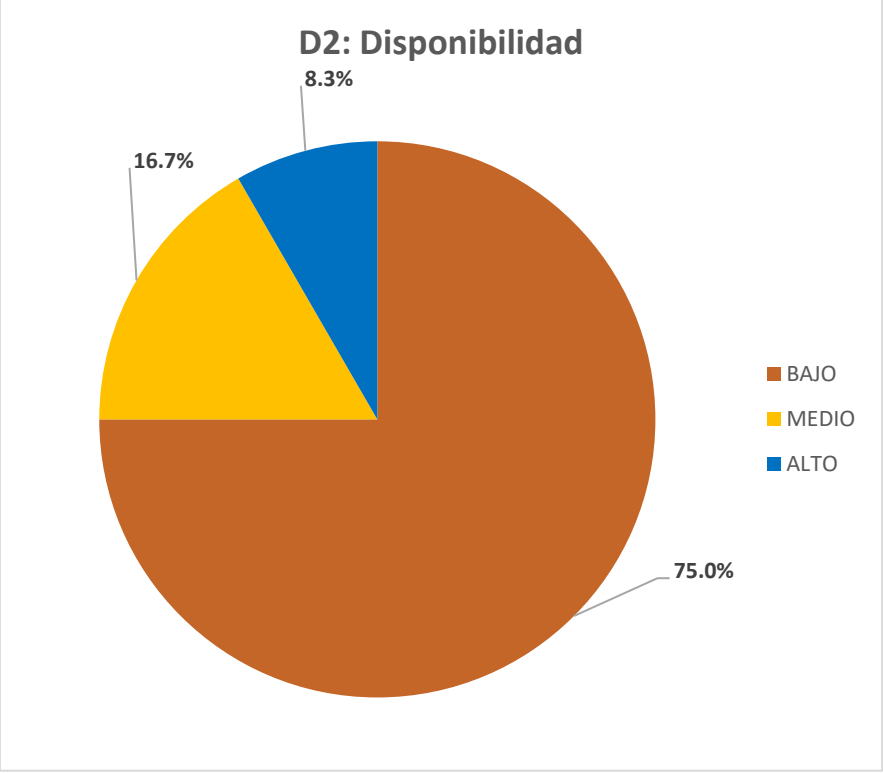
Calificación de la dimensión D2: Disponibilidad

Calificación	**D2: Disponibilidad**	
	Frecuencia (fi)	Porcentaje (%)
BAJO	9	75.0%
MEDIO	2	16.7%
ALTO	1	8.3%
TOTAL	12	100.0%

Fuente: Elaboración propia

Figura 20

Gráfico de la dimensión D2: Disponibilidad



Fuente: Elaboración propia

Interpretación: Lo que se observa en la tabla 4, figura 13, la dimensión: disponibilidad es calificada por los encuestados por el 75.0% como un nivel bajo, el 16.7% la califica como nivel medio y el 8.3% la califica como un nivel alto.

Tabla 5

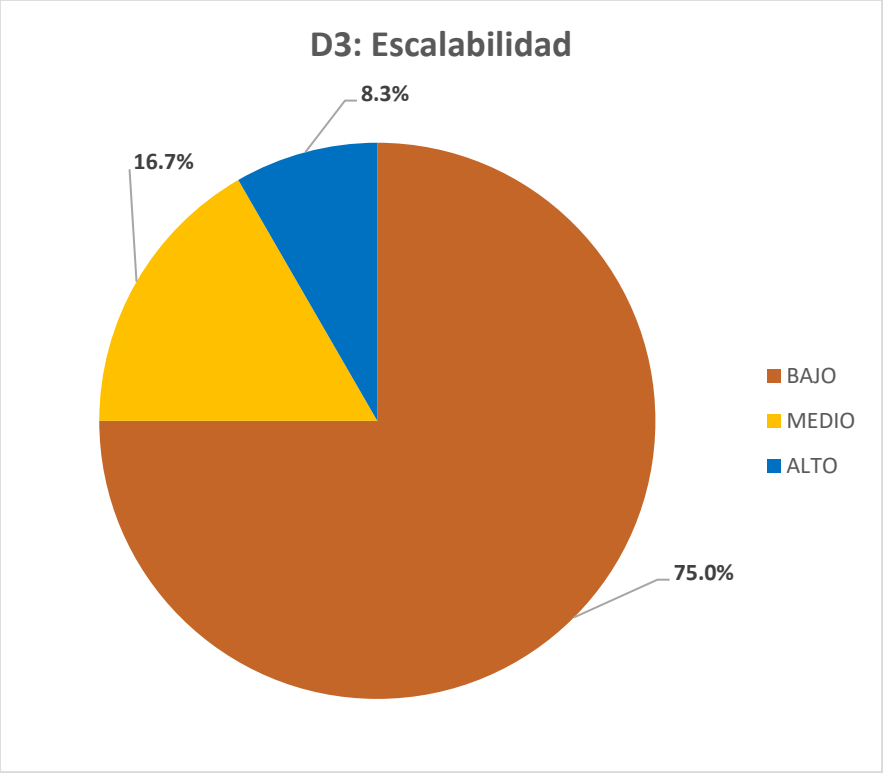
Calificación de la dimensión D3: Estabilidad

Calificación	**D3: Escalabilidad**	
	Frecuencia (fi)	Porcentaje (%)
BAJO	9	75.0%
MEDIO	2	16.7%
ALTO	1	8.3%
TOTAL	12	100.0%

Fuente: Elaboración propia.

Figura 21

Gráfico de la dimensión D3: Escalabilidad



Fuente: Elaboración propia

Interpretación: Lo que se observa en la tabla 5, figura 14, la dimensión: disponibilidad es calificada por los encuestados por el 75.0% como un nivel bajo, el 16.7% la califica como nivel medio y el 8.3% la califica como un nivel alto.

Tabla 6

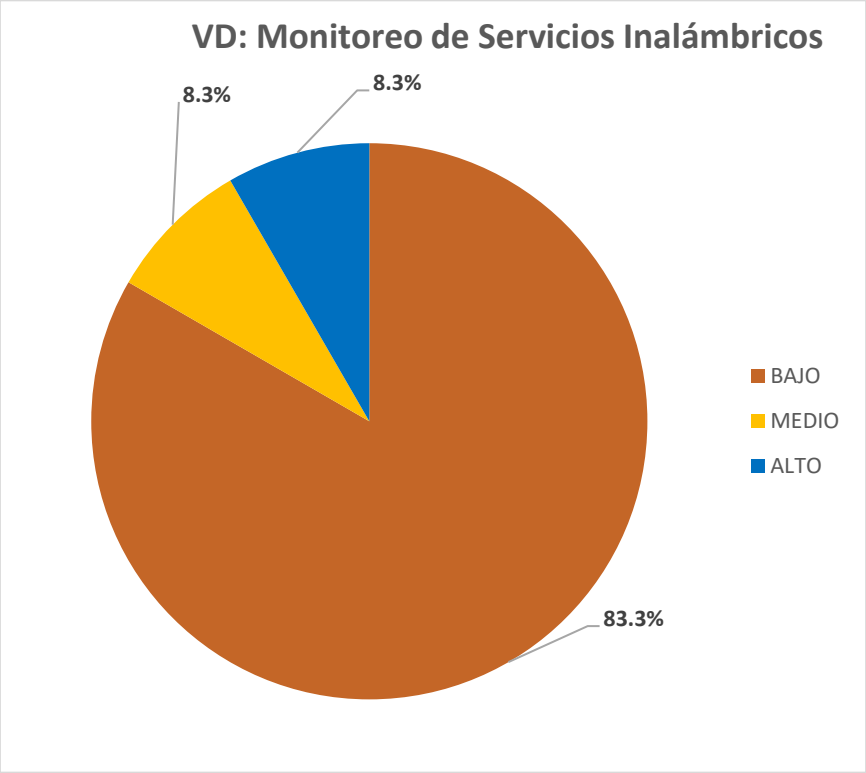
Calificación de la variable VD: Monitoreo de Servicios Inalámbricos

Calificación	VD: Monitoreo de Servicios Inalámbricos	
	Frecuencia (fi)	Porcentaje (%)
BAJO	10	83.3%
MEDIO	1	8.3%
ALTO	1	8.3%
TOTAL	12	100.0%

Fuente: Elaboración propia.

Figura 22

Gráfico de la variable VD: Monitoreo de servicios inalámbricos



Fuente: Elaboración propia

Interpretación: tal como se observa en la tabla 6, figura 15, la variable dependiente: monitoreo de servicios inalámbricos es calificada por los encuestados por el 83.3% como un nivel bajo, el 8.3.7% la califica como nivel medio y el 8.3% la califica como un nivel alto.

Tabla 7

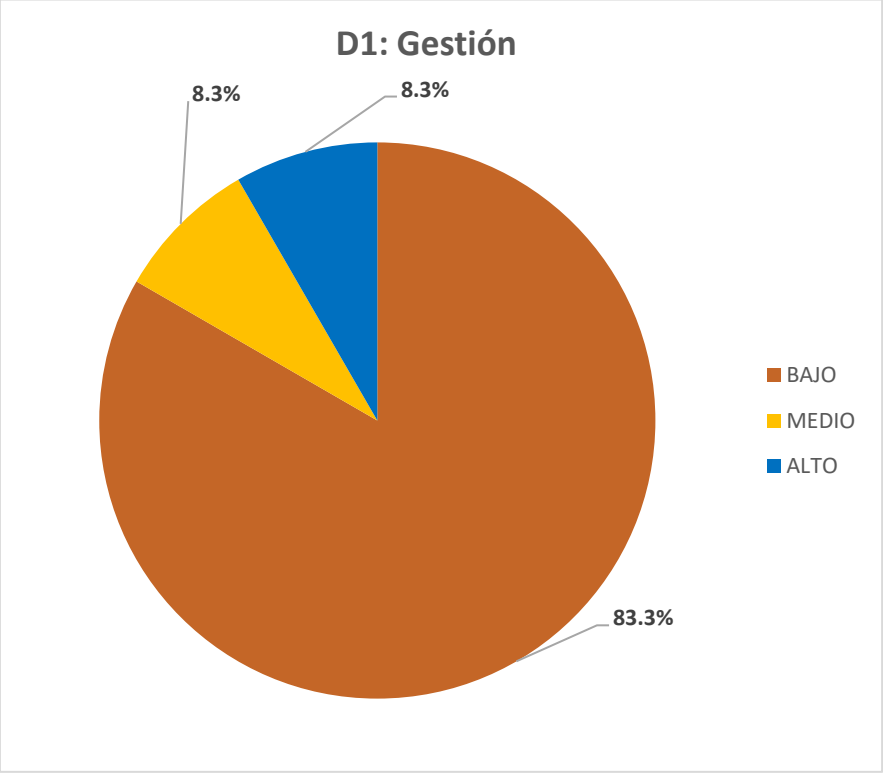
Calificación de la dimensión D1: Gestión

Calificación	D1: Gestión	
	Frecuencia (fi)	Porcentaje (%)
BAJO	10	83.3%
MEDIO	1	8.3%
ALTO	1	8.3%
TOTAL	12	100.0%

Fuente: Elaboración propia.

Figura 23

Gráfica de la dimensión D1: Gestión



Fuente: Elaboración propia

Interpretación: Como se observa en la tabla 7, figura 16, la dimensión: Gestión es calificada por los encuestados por el 83.3% como un nivel bajo, el 8.3.7% la califica como nivel medio y el 8.3% la califica como un nivel alto.

Tabla 8

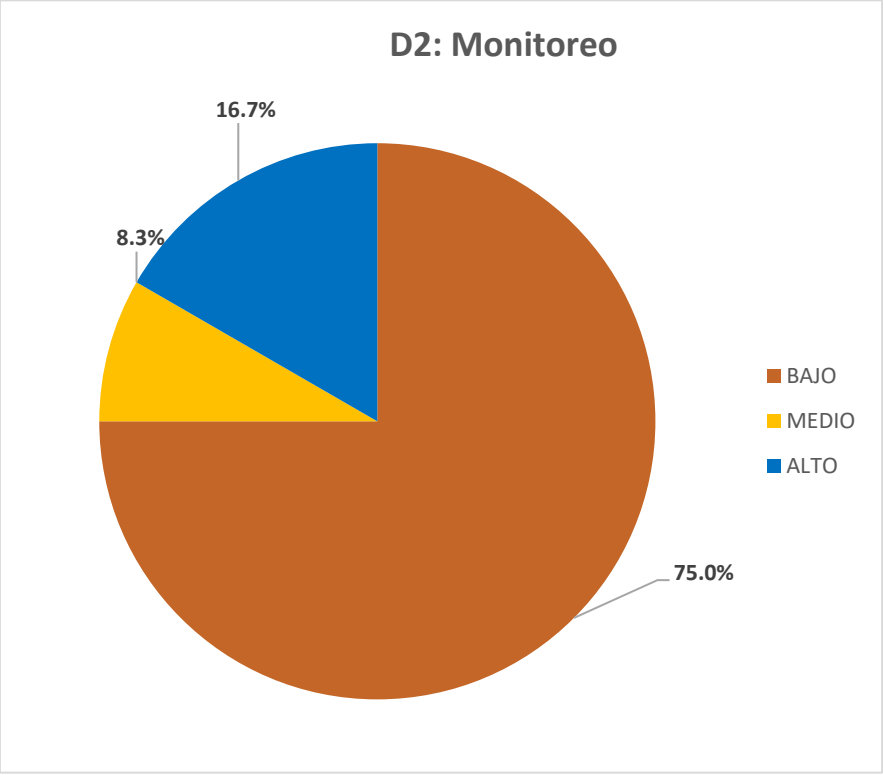
Calificación de la dimensión D2: Monitoreo

Calificación	D2: Monitoreo	
	Frecuencia (fi)	Porcentaje (%)
BAJO	9	75.0%
MEDIO	1	8.3%
ALTO	2	16.7%
TOTAL	12	100.0%

Fuente: Elaboración propia.

Figura 24

Gráfica de la dimensión D2: Monitoreo



Fuente: Elaboración propia

Interpretación: Así como se observa en la tabla 8, figura 17, la dimensión: Gestión es calificada por los encuestados por el 83.3% como un nivel bajo, el 8.3.7% la califica como nivel medio y el 8.3% la califica como un nivel alto

3.2. Comprobación de la Hipótesis.

Una forma de comprobar la hipótesis se detalla a continuación:
La empresa Interconexiones Ocaney que es un proveedor de servicio de Internet que no cuenta con una correcta gestión y administración de sus dispositivos de red, que es fundamental para ofrecer un servicio eficiente y de calidad. Esto ocasiona demora en la atención de las incidencias y requerimientos, generando malestar en sus suscriptores. Por lo que se propone implementar un centro de operación de red, lo cual va a resolver los problemas de gestión y administración de los equipos de telecomunicaciones tal como se demuestra en los anexos 3, 4, y 6, en lo cual mediante el uso del servidor de red centos7, se procede a instalar y configurar el sistema de monitoreo de red Zabbix, integrando con la aplicación Grafana para monitorear en tiempo real los dispositivos de red de la empresa Interconexiones Ocaney, y gestionar adecuadamente las diferentes solicitudes de requerimientos e incidencias con la aplicación osTicket (ver anexo 5).

3.3. Gestionar el centro de operaciones de red

Frente a los resultados obtenidos en las encuestas se evidencia que la empresa Interconexiones Ocaney cuenta con un sistema de monitoreo para ver estado de salud de sus equipos de red muy limitado, la plataforma de acceso a los equipos de telecomunicaciones es deficiente, tiene retrasos en restablecer el servicio cuando se presentan averías en los enlaces troncales y los dispositivos finales.

Debido a los muchos problemas presentados en la red de la empresa Interconexiones Ocaney, se propuso instalar el servidor CentOS 7, en la cual se implementó el sistema de monitoreo de red Zabbix. Dicho sistema está diseñado para monitorizar y registrar el estado de salud de los distintos servicios de red, Servidores, y hardware de red.

3.3.1. Configuración de los servicios inalámbricos

CentOS Linux es una un sistema operativo para servidores, de distribución gratuita. Cada versión de CentOS se mantiene hasta que la versión RHEL equivalente deja de ser compatible. (CentOS, 2014).

Antes de comenzar a instalar CentOS, debemos descargar una imagen ISO de instalación. Las imágenes están disponibles en el sitio web de CentOS en https://www.centos.org/download/. Están disponibles los siguientes tipos básicos de medios:

DVD ISO: Esta imagen contiene el instalador, así como un conjunto de todos los paquetes que se pueden instalar durante una instalación interactiva. Esta es la descarga recomendada para la mayoría de los usuarios.

Everything ISO: Contiene el instalador y todos los paquetes disponibles para CentOS. Esta imagen ISO se puede usar para instalar el sistema con paquetes adicionales, también se puede utilizar para configurar un espejo local para descargar paquetes. Tener en cuenta que esta imagen es muy grande y requiere una unidad flash de al menos 16 GB u otro almacenamiento.

Minimal ISO: Contiene el instalador y un conjunto mínimo de paquetes que se pueden usar para instalar un sistema CentOS muy básico. Luego, puede usar yum para descargar paquetes adicionales de los repositorios de actualización.

Para la siguiente investigación utilizaremos la versión Minimal, y luego iremos instalando los paquetes de acuerdo con nuestras necesidades. Una vez que haya descargado un archivo de imagen ISO del Portal, lo podemos montar en una máquina virtual, en el presente proyecto se implementará sobre VMWare Player. Una vez que lo tengamos montando, editamos las interfaces de acuerdo con nuestras preferencias y automáticamente se ejecutará el instalador de CentOS que previamente descargamos.

La configuración detallada del servidor CentOS se encuentra en el Anexo 2 (Instalación de servidor CentOS 7).

Finalizada la instalación del servidor CentOS, se procederá a instalar el sistema de monitorización de redes Zabbix. Brinda soluciones para cualquier tipo de infraestructura, servicios, aplicaciones, recursos de TI. En redes supervisa cualquier posible métrica de rendimiento e incidentes en su red (performance, salud, cambios de configuración) (Zabbix, 2020).

Los beneficios de utilizar Zabbix: Recopilación de datos flexible, autodescubrimiento, monitoreo de red proactivo, niveles de gravedad del problema, integración con software de terceros, optimizado para alto rendimiento, alta disponibilidad, seguridad y autenticación (Zabbix, 2020).

Los requerimientos para instalar Zabbix a nivel de hardware son:

- **Memoria:** La cantidad de memoria de disco requerida dependen de la cantidad de dispositivos y los parámetros a monitorean. El requisito mínimo es 128 MB de memoria física y 256 MB de espacio libre en disco podrían ser un buen punto de partida.
- **CPU:** La base de datos Zabbix utiliza recursos de CPU significativamente altos por lo que va a depender de la cantidad de parámetros a monitorear y el motor de base de datos elegido**.**

Figura 25

Requisitos de configuración de hardware.

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

Fuente: (Zabbix, 2020).

Zabbix se basa en servidores web modernos, motores de bases de datos líderes y lenguaje de programación PHP.

- **MySQL:** Un software que brinda un servidor de base de datos SQL (lenguaje de consulta estructurado) ligero, multiproceso, multiusuario y sólido. Diseñado para sistemas de producción de carga pesada de misión crítica, así como para integrarse en software implementado en

masa.(MySQL, 2020). Zabbix lo utiliza como base de datos backend. Versión recomendada 5.5.62 o superior.

- **Apache:** Es un servidor web HTTP de código abierto, que implementa el protocolo HTTP/1.1 y la noción de sitio virtual según la normativa RFC 2616. Versión requerida para Zabbix es 1.3.12 o superior.
- **PHP:** Es un lenguaje de código abierto para el desarrollo web y que puede ser incrustado en HTML.(PHP, 2020). Versión a utilizar 7.2.0 o superior.

La configuración detallada del sistema de monitorización se encuentra en el anexo 3 (instalación del sistema de monitoreo Zabbix).

Una vez culminada con la configuración de Zabbix, procedemos a integrar Grafana al sistema de monitorización. Grafana nos ofrece poder consultar, visualizar, alertar y comprender sus métricas independientemente dónde estén almacenadas. Ofrece 2 ediciones para utilizar: Edición Open Source que puede utilizar de manera gratuita y Enterprise que incluye complementos exclusivos de fuentes de datos, funciones de seguridad, autenticación, y soporte (Grafana, 2020).

Utilizaremos la versión Open Source, la configuración se encuentra en el anexo 4 (Integración de Grafana a Zabbix).

Para gestionar los registros de las incidencias y los requerimientos se va a implementar y configurar el sistema de ticketera osTicket, que es un sistema automatizado de soporte al usuario final, fácil de administrar y de utilizar mediante interface web que, guarda todos registros de las solicitudes de soporte.

La finalidad de utilizar OsTicket es tener un registro detallado de las incidencias y los requerimientos que se presentan en los servicios prestados en la empresa Interconexiones Ocaney, de esta manera brindar una respuesta oportuna, eficiente y en el menor tiempo posible a los clientes.

Entre las principales características de OsTicket tenemos

- Campos personalizados: se pueden agregar campos, formularios y listas a cada tique creado.
- Búsqueda avanzada: se puede guardar los criterios seleccionados para facilitar búsquedas futuras.

- Auto respuesta: Envío de mensaje de la creación de ticket al cliente y al NOC para ser atendido.
- Acuerdo de nivel de servicio: se puede recibir alertas y avisos vencidos sobre fecha de vencimientos incumplidas y escalamiento de prioridades.
- Filtro de tiques: permite automatizar la creación de los tiques, se puede establecer acciones como rechazar tique, asignar a un área o agente.
- Multiplataforma: se puede utilizar desde cualquier dispositivo y que cuente con cualquier navegador (osTicket, 2020).

La configuración de OsTicket se encuentra en el anexo 5 (Implementación de OsTicket)

3.4. Gestión de Incidencias de los servicios inalámbricos

Monitorear eficientemente la conectividad y operatividad de los enlaces, así como gestionar configuración, eventos, alarmas y gráficas conforme al estados de los casos. Atender eficientemente cada una de las incidencias pendientes en relación con los equipos de seguridad detectadas proactivamente, realizando un correcto diagnóstico, solución y garantizar la trazabilidad de la gestión de los casos conforme al estado de los casos.

Para ver el diagrama de flujo y descripción de las actividades de las incidencias de los servicios inalámbricos ver la figura N° 26 y tabla la N° 9.

3.4.1. Procedimiento de incidencias de los dispositivos de red.

La incidencia de red puede iniciarse por los siguientes motivos:

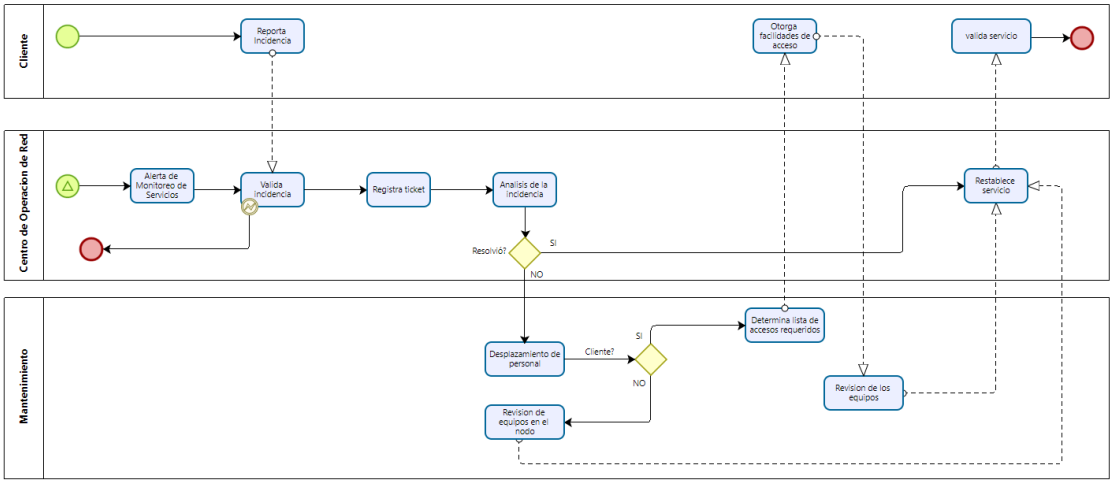
- Incidencias reportadas por el cliente
- Monitoreo realizado por el centro de operaciones de red.

Durante el transcurso del incidente de red, la comunicación hacia el cliente interesado es a través del operador de red (NOC) que abre el tique en la plataforma osTicket.

Diagrama de flujo

Figura 26

Procedimiento de incidencias de los servicios inalámbricos



Fuente: Elaboración propia.

Descripción de actividades.

Tabla 9

Tabla de procedimiento de incidencias de los servicios inalámbricos

Actividad	Descripción	Responsable
Basado en el proceso de gestión de incidencia de ITIL		
Reporta incidencia	El cliente puede reportar incidentes de red a través de llamada telefónica	Cliente
Valida incidencia	Recibida la notificación del probable incidente, el operador de red valida si efectivamente se trata de un incidente de red. De ser una falsa alarma se da por finalizada.	Centro de operación de red
Alerta de Monitoreo de Servicios	Una incidencia de red, también se puede reportar como resultado del monitoreo de red que se realiza a los clientes. Para ello se apoya en la herramienta de monitoreo de salud Zabbix	Centro de operación de red
Registro de ticket	El operador de red crea un tique de atención por incidencia reportada en la plataforma osTicket.	Centro de operación de red

Análisis de la incidencia	Con la información disponible hasta este punto, se realiza el análisis respectivo y la solución	Centro de operación de red
Desplazamiento de personal	El operador de red solicita al personal de mantenimiento desplazarse a sitio para revisión de los dispositivos de telecomunicaciones.	Mantenimiento
Determinar lista de accesos requeridos	El operador de red puede solicitar accesos adicionales, si está contemplado como parte del servicio con el cliente afectado.	Mantenimiento
Revisión de los equipos en el cliente	Personal de mantenimiento, en la sede del cliente revisa los equipos de telecomunicaciones.	Mantenimiento
Revisión de los equipos en el nodo	Personal de mantenimiento, en el nodo revisa los equipos de telecomunicaciones	Mantenimiento
Restablece servicio	El operador de red valida que se restablece el servicio.	Centro de operación de red
Valida servicio	Cliente brinda conformidad del servicio	Cliente

Fuente: Elaboración propia.

Con lo descrito en el punto anterior, el operador NOC al recibir un ticket de atención, seguirá un procedimiento para atender de manera más rápida las incidencias que van reportando los clientes de la empresa Interconexiones Ocaney. Al seguir un orden en las atenciones, ya no se tendrá tiempos muertos que puedan ocasionar demora en la resolución de incidencias y generar quejas del cliente.

3.5. Gestión de registro de los servicios inalámbricos

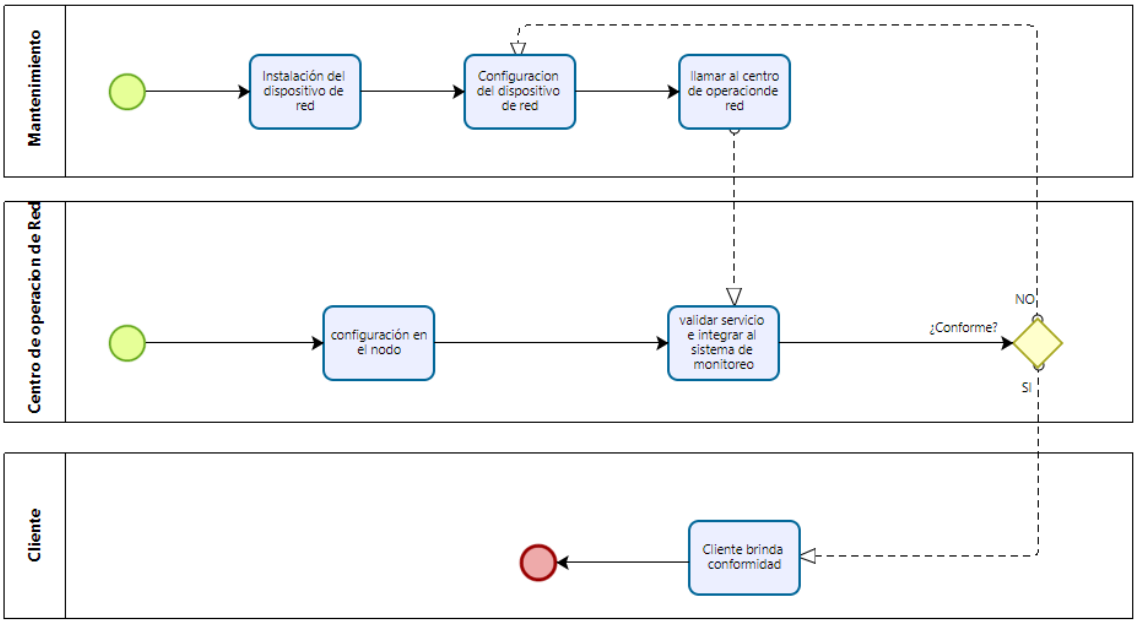
Integrar los nuevos dispositivos de red al sistema de monitoreo con la herramienta Zabbix.

Para ver el diagrama de flujo y descripción de las actividades de la gestión de registro de los servicios inalámbricos ver la figura N° 27 y la tabla N° 10.

Diagrama de flujo

Figura 27

Procedimiento de registro de los servicios inalámbricos



Fuente: Elaboración propia.

Descripción de actividades.

Tabla 10

Tabla de procedimiento de registro de los servicios inalámbricos

Actividad	Descripción	Responsable
Instalación del dispositivo de red	Personal de mantenimiento instala los equipos de telecomunicaciones en el cliente	Mantenimiento
Configuración del dispositivo de red	El Personal de mantenimiento, una vez instalado, realiza las configuraciones en los dispositivos	Mantenimiento

llamar al centro de operaciones red	El personal de mantenimiento, una vez finalizado las configuraciones llama al operador de red para validar servicio	Mantenimiento
configuración en el nodo	El operador de red realiza las configuraciones en los enlaces troncales	Centro de operación de red
validar servicio e integrar al sistema de monitoreo	Cuando personal de mantenimiento se comunica, el operador de red valida conectividad e integra el nuevo dispositivo al sistema de monitoreo Zabbix	Centro de operación de red
Cliente brinda conformidad	Cliente valida servicio y brinda su conformidad.	Cliente

Fuente: Elaboración propia.

Con el procedimiento de registro de los servicios inalámbricos, se detalla los pasos a seguir para registrar un nuevo servicio a la red de la empresa Interconexiones Ocaney. De esta manera el operador del NOC, procederá a integrar de manera rápida y efectiva los nuevos servicios al sistema de monitoreo. El monitoreo detallado se encuentra en el anexo 6: Configuración de SNMP.

3.6. Gestión de seguridad de los servicios inalámbricos

Otro punto importante en la gestión de los dispositivos de red es la seguridad de acceso a los equipos de telecomunicaciones, es decir aplicar barreras y procedimientos que resguarden el acceso a los datos y sólo permitan acceder a ellos a las personas autorizadas para hacerlo. Al implementarse estos controles de acceso constituyen una importante ayuda para proteger la red contra ingresos y modificaciones no autorizadas; mantener la integridad de la información restringiendo la cantidad de usuarios y resguardar la información confidencial de accesos no autorizados (Costas Santos, 2014).

Para ellos se va a utilizar un servidor de autenticación sobre el cual los usuarios se van a identificar, y que se encargará luego de autenticar al usuario sobre los restantes equipos a lo que éste pueda acceder. Para este proyecto utilizaremos

TACACS+ que es una aplicación de seguridad que proporciona una validación centralizada de los usuarios que intentan obtener acceso a un enrutador o servidor de acceso a la red. TACACS+ proporciona funciones de autenticación, autorización y contabilidad independientes y modulares. El objetivo es proporcionar una metodología para administrar múltiples puntos de acceso a la red desde un servicio de gestión única. La autenticación entre los equipos de acceso de red y el servidor garantiza la confidencialidad porque todos los intercambios de protocolo están encriptados.

Las ventajas de usar TACACS+, respecto otros servidores de autenticación como por ejemplo radius, es el uso del protocolo TCP para la conexión y cifra la contraseña durante toda la sesión, además separa la autenticación al dispositivo y la autorización del usuario. En resumen, TACACS+ es más seguro que radius.

A continuación, se muestra un cuadro comparativo entre los protocolos Tacacs y Radius.

Tabla 11

Tabla de procedimiento de gestión de la seguridad de los servicios inalámbricos

TACACS +	RADIUS
Utiliza TCP	Utiliza UDP
Cifrado de todo el paquete	cifrado solo la contraseña
Permite separar autenticación y autorización	combina autenticación y autorización
Proporciona dos métodos para controlar la autorización de los comandos del enrutador por usuario o por grupo	No permite a los usuarios controlar qué comandos se pueden ejecutar en un enrutador y cuáles no
Soporte multiprotocolo	No soportar protocolos ARA, NetBIOS, NASI

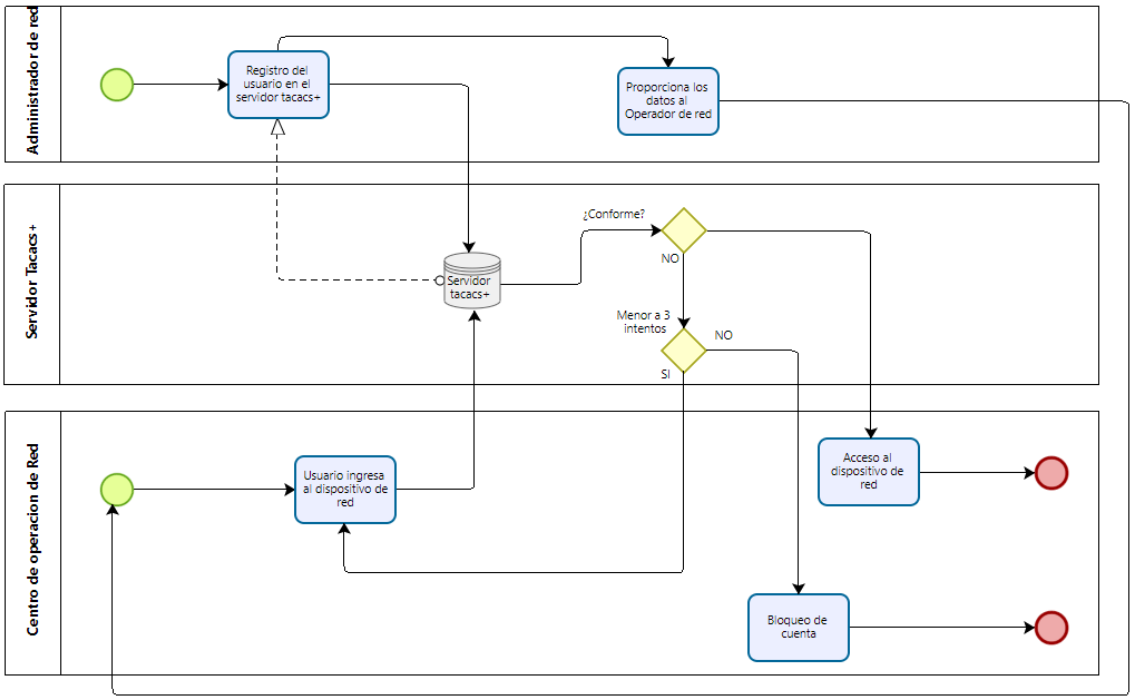
Fuente: (Cisco, 2021).

Para ver el diagrama de flujo y descripción de las actividades de la gestión de seguridad de los servicios inalámbricos ver la figura N° 28 y la tabla N°11.

Diagrama de flujo

Figura 28

Procedimiento de gestión de la seguridad de los servicios inalámbricos



Fuente: Elaboración propia.

Descripción de actividades.

Tabla 12

Tabla de procedimiento de gestión de la seguridad de los servicios inalámbricos

Actividad	Descripción	Responsable
Basado en el proceso de gestión de seguridad de ITIL		
Registro del usuario en el servidor tacacs+	Un administrador autorizado procede a registrar al usuario en el servidor.	Administrador de red
Usuario ingresa al dispositivo de red	Operador accede mediante SSH por la IP de gestión al dispositivo de red, luego le solicitará usuario y clave.	Operador de red
Validación en el servidor	El servidor tacacs+ valida si el usuario y clave coinciden con los datos registrados.	Servidor Tacacs+
Acceso al dispositivo de red	Si los datos ingresados coindicen con los datos guardados en el servidor, el operador accede exitosamente al dispositivo de red, sino coinciden le volverá a solicitar ingresar sus datos hasta 3 intentos, luego de ello se desconectará.	Operador de red
Bloqueo de cuenta	Si un operador intenta acceder a un dispositivo de red y se equivoca con su clave en 3 intentos, el usuario	Operador de red

	automáticamente se bloqueará, hasta que un administrador de red lo vuelva a reactivar.	

Fuente: Elaboración propia.

Con la Gestión de seguridad de los servicios inalámbricos, se detalla el procedimiento para integrar los equipos de red de la empresa Interconexiones Ocaney al servidor de seguridad, con ello garantizar la seguridad en toda la red, solo personal autorizado y registrado en el servidor de seguridad podrá autenticarse en los diferentes dispositivos de la red.

La configuración detallada se encuentra en el anexo 7: Configuración de seguridad en los dispositivos de red.

3.7. Gestión de la Capacidad de los servicios inalámbricos

El proceso de gestión de la capacidad se encarga de asegurar que todos los servicios TI corresponda con las necesidades del negocio en términos de coste y de tiempo, caso contrario los recursos no se utilizarán apropiadamente y se efectuaran inversiones innecesarias que ocasionen gastos extras de mantenimiento y administración (ITIL, 2011).

La gestión de capacidad cuenta con tres subprocesos: gestión de la capacidad del negocio encargado de necesidades futuras del negocio, gestión de la capacidad de los servicios asegura que los servicios operen conforme a los acuerdos de niveles de servicio, gestión de la capacidad de los recursos que gestiona los recursos de bajo nivel de las infraestructuras.

La empresa Interconexiones Ocaney no cuenta con una gestión de capacidad que pueda controlar el rendimiento de su infraestructura TI y pueda implementar planes de capacidad asociados a los niveles de servicio. Por lo que se propone elaborar un conjunto de sugerencias y recomendaciones para gestionar la capacidad de los servicios.

Para ver a mayor detalle la descripción de las actividades de la gestión de la capacidad de los servicios inalámbricos ver la tabla N° 12.

Descripción de actividades.

Tabla 13

Tabla de gestión de la capacidad de los servicios inalámbricos

Procedimiento	Gestión de Capacidad				
Objetivo	Asegurar que los servicios y recursos de TI se vean respaldados por una capacidad de procesamiento y almacenamiento suficiente y correctamente dimensionada, que garantice ofrecer un servicio de calidad a los clientes				
Alcance	Inicia desde monitorear los dispositivos de red de la empresa Interconexiones Ocaney y termina en proponer mejoras, para que todos los servicios TI se vean respaldados por una capacidad de proceso y almacenamiento suficiente que tenga en cuenta las proyecciones y planes de la organización				
Referencia	Basado en subprocesos de gestión de capacidad de ITIL				
Responsable	Administrador de Red				
Proceso Asociado	Centro de Operación de Red				
Nro.	Actividad	Tarea	Responsable	Registro	Tiempo
1	Monitorear los dispositivos de red	Capacidad de procesamiento	Centro de Operación de Red	Plan de Capacidad	Semanal
		tiempo de respuesta			
		ancho de banda			
2	Modelar y simular escenarios de capacidad	Diseñar planes que permitan predecir el comportamiento del consumo/uso de la	Centro de Operación de Red	Plan de Capacidad	Mensual

3	Realizar evaluación	Evaluar las cargas y consumos de los elementos de capacidad que definen los niveles de servicio	Centro de Operación de Red	Plan de Capacidad	Mensual
4	Realizar informes sobre el estado de los enlaces inalámbricos	Realizar informes sobre el estado de los dispositivos de red y los servicios ofrecidos	Centro de Operación de Red	Plan de Capacidad	Mensual
5	Proponer mejoras a la capacidad del servicio	Realizar mejoras de los servicios ofrecidos de acuerdo a la evaluación realizada en el punto 3.	Centro de Operación de Red	Plan de Capacidad	Mensual
		Realizar seguimiento de las mejoras propuestas			

Con la gestión de capacidad de los servicios inalámbricos, se intenta realizar un seguimiento periódico del estado de los servicios de la empresa Interconexiones Ocaney, para revisar el procesamiento de CPU, memoria, latencia, cantidad de tráfico que pasan por los enlaces troncales y los equipos de acceso, para luego evaluar y proponer mejorar en el servicio. De esta manera no se creará un cuello de botella cuando la red crezca en tamaño y aumente el tráfico de los diferentes servicios que ofrece la empresa a sus clientes.

3.8. Monitorear el centro de operaciones de red

Para realizar el monitoreo de los dispositivos de red utilizaremos El Protocolo simple de administración de red (SNMP) que es un protocolo de transferencia de información de gestión en redes. Su importancia en la administración de redes es que nos permite recopilar información sobre dispositivos conectados a la red de forma estandarizada en una gran variedad de tipos de hardware y software.

- **SNMP mánager:** Un sistema de gestión de red que utiliza SNMP para sondear y recibir datos de los dispositivos de red. En SNMP mánager generalmente es una aplicación que se ejecuta en una ubicación central.
- **SNMP agente:** Es un módulo de software de administración de red que se encuentra en un dispositivo administrado**.** posee información del dispositivo donde se aloja tales como memoria libre, número de paquetes IP recibidos, rutas, entre otros.

Cada dispositivo recoge información automáticamente los datos acerca de sí mismo, de sus recursos, y de cada uno de sus interfaces y son almacenados en el MIB (Managament Information Base). Para comunicación entre el mánager y el agente se utiliza los siguientes mecanismos: get request, get next request, get bulk request y set request. (Ariganello & Barrientos Sevilla, 2015).

Los agentes pueden enviar alertas no solicitadas para notificar al mánager de eventos en tiempo real en cualquier momento utilizando los siguientes mecanismos:

- **Trap:** notificaciones de eventos tales como fallos en los dispositivos, interfaces.
- **Inform request:** son enviados y espera respuesta de que se ha recibido.

Desde su creación, SNMP ha ido evolucionando en distintas versiones. Entre los cuales tenemos: la versión SNMP v1 y v2c que son las versiones más implementadas de SNMP. La versión SNMP v3 ha comenzado a implementarse recientemente, ya que es más segura en comparación con sus versiones anteriores, pero aún no ha alcanzado una cuota de mercado considerable.(ManageEngine, 2020) .

La configuración detallada se encuentra en el anexo 6: Configuración de SNMP.

3.8.1. Monitoreo del control de ancho de banda

Mediante el uso de la herramienta Zabbix, el operador NOC debe identificar que enlaces troncales están consumiendo tráfico de datos mayor al umbral permitido y registrar un histórico del consumo mensual, para luego informar al administrador de red, quien debe tomar las medidas adecuadas, como por ejemplo implementar un nuevo enlace, aumentar el ancho de banda del enlace actual o cambiar el dispositivo de red a uno de mayor capacidad.

El monitoreo detallado se encuentra en el anexo 6: Configuración de SNMP.

3.8.2. Monitoreo de respaldo de la información

El operador de red debe realizar una copia de seguridad de la configuración de los dispositivos de red de la empresa Interconexiones Ocaney semanalmente, o cada vez que realice algún cambio en la configuración y proceder a guardar en el servidor, en caso de que se requiera volver a configurar o cambiar por otro equipo de red por alguna avería, el tiempo de respuesta sea en el corto plazo posible y no afectar el servicio prestado al cliente, de esta manera cumplir con los SLA acordados entre el operador y el cliente.

3.8.3. Monitoreo de la documentación de los dispositivos de red

Cada vez que el operador de red agrega, cambia o da de baja algún equipo o enlace en la red, debe actualizar la topología de red, tanto lógica en la herramienta de monitoreo Zabbix, como física, y a su vez actualizar en la lista de dispositivos de telecomunicaciones. De esta manera llevar un mejor control del inventario de todos los equipos informáticos que tiene la empresa Interconexiones Ocaney. Se creará una carpeta en el servidor, donde el operador deberá guardar la topología física por versiones y además la lista de equipos de todos los enlaces inalámbricos e ir actualizando cada vez que se va a realizar algún cambio de equipo de red. A su

vez, se tendrá una copia de respaldo de toda la documentación antes menciona en la nube, ya sea en mega, Google drive u OneDrive. De esta manera, si por alguna razón se tiene problemas con el servidor físico, tener siempre a mano la documentación. El operador de red será el encargado de actualizar dichos documentos tanto en el servidor como en la nube.

3.8.4. Monitoreo del estado de salud de los servicios inalámbricos

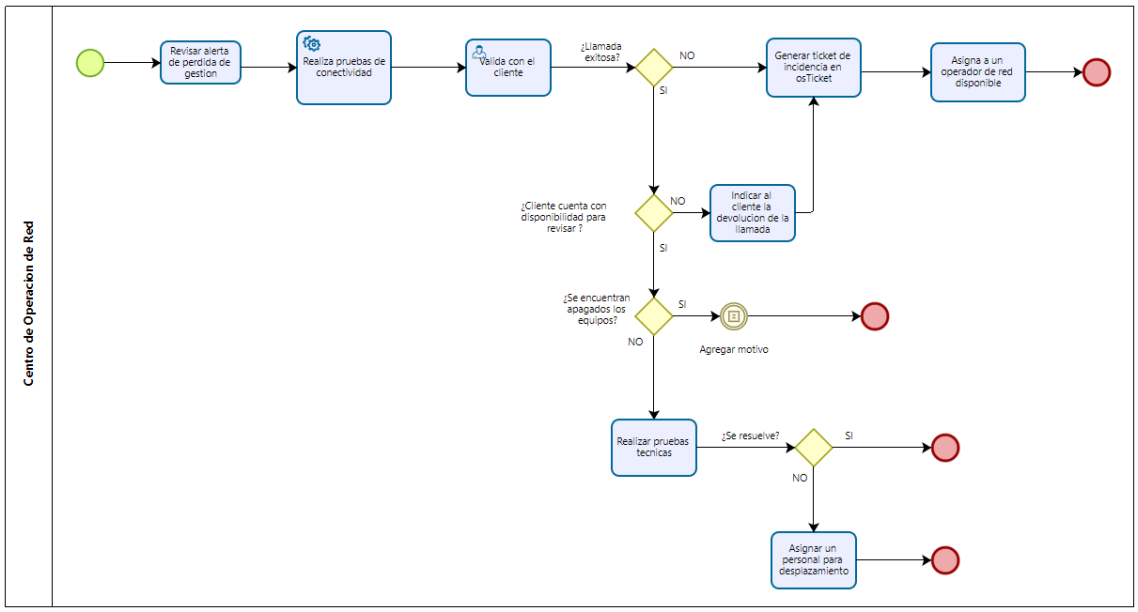
Identificar las alarmas proactivamente en la herramienta Zabbix, el cliente alarmado y posteriormente poder comunicarse con éste para las pruebas y/o validaciones correspondientes. Cuando el dispositivo se encuentre apagado se deberá de indicar los siguientes motivos:

- Corte de energía de la zona
- Trabajo de mantenimiento de los equipos
- Corte por falta de pagos
- Otro motivo que no tenga relación con el equipo de telecomunicaciones

Diagrama de flujo

Figura 29

Procedimiento de monitoreo del estado de salud de los servicios inalámbricos



Fuente: Elaboración propia.

Descripción de actividades.

Tabla 14

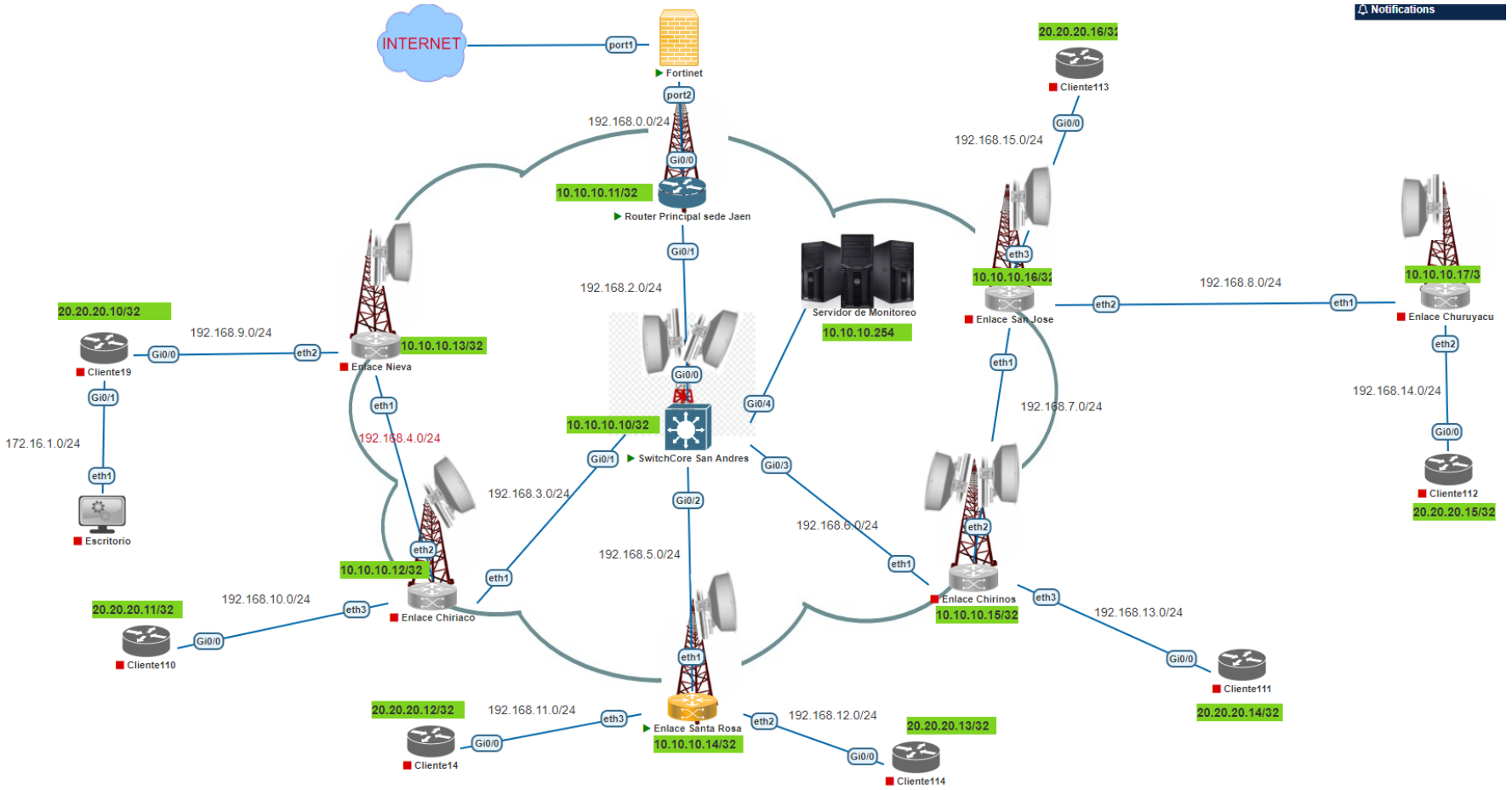
Tabla de procedimiento de monitoreo del estado de salud de los servicios inalámbricos

Actividad	Descripción	Responsable
Revisar alerta de perdida de gestión	El operador de red revisa las alertas en la plataforma de monitoreo Zabbix	Centro de operación de red
Realiza pruebas de conectividad	El operador de red realiza pruebas de conectividad y revisa que los enlaces troncales se encuentren operativos	Centro de operación de red
Valida con el cliente	El operador de red se comunica con el cliente para realizar descartes a nivel físico	Centro de operación de red
Generar tique de incidencia en osTicket	En caso no tener respuesta del cliente, el operador de red genera un tique proactivo para mantener en monitoreo.	Centro de operación de red
Enviar correo al cliente	Enviar correo al cliente indicado que no se tiene conexión con sus equipos en su sede y dejar constancia del monitoreo.	Centro de operación de red
Indicar al cliente la devolución de la llamada	En caso de que cliente indique no contar con disponibilidad para revisiones en línea, solicitar comunicarse con nosotros en caso no cuente con servicio.	Centro de operación de red
Realizar pruebas técnicas	Con el apoyo del cliente, solicitar reinicio de los dispositivos de red.	Centro de operación de red
Asignar un personal para desplazamiento	En caso no se restablezca el servicio, solicitar al personal de mantenimiento desplazarse a la sede del cliente para las revisiones.	Centro de operación de red

Fuente: Elaboración propia.

Con el procedimiento de monitoreo del estado de salud de los servicios inalámbricos, el operador NOC realizará un monitoreo óptimo de los dispositivos de red, tomar decisiones de manera oportuna en el menor tiempo posible y de esta manera resolver tanto las incidencias que reporte el cliente y las alertas que se presente en la plataforma de monitoreo y dejar un registro de cada una de las atenciones realizadas.

Figura 30
Topología de red a monitorear



Fuente: Elaboración propia.

3.9. Discusión.

Como lo indica Think networks (2020) el NOC es el encargado de monitorizar las actividades, la disponibilidad y el estado de salud de los sistemas informáticos de una empresa en tiempo real, con el fin de prever incidentes que pongan en riesgo la disponibilidad de las operaciones del negocio. Lo cual tiene similitud con el objetivo, implementar el centro de operaciones de red mediante el uso de tecnologías de monitorización, en donde la monitorización es una parte fundamental de un proveedor de servicio, ayuda a optimizar la resolución de inconvenientes que se presente en el día a día, a mejorar los procedimientos de atención respecto al cliente, a centralizar la gestión de todos los dispositivos de red. Con la implementación de un centro de operación de red en la empresa Interconexiones Ocaney se va lograr reducir el tiempo de atención a una o dos horas las incidencias bajas y medias, lo que antes tomaba más de 4 horas. Debido a que no se contaba con un procedimiento de atención definida y las incidencias altas que requieran desplazamiento a sitio, entre 4 horas a un día dependiendo de la distancia geográfica. Con lo dicho anteriormente, todas las empresas deben contar con un sistema de monitoreo de red.

Como lo hace notar Hegde et al. (2015) a medida que una empresa crece en tamaño, su red de enrutadores, conmutadores y servidores se vuelve compleja y poder operarlo y administrarlo se convierte en una tarea abrumadora. Para ello es necesario realizar una planificación y tener un control de todos los dispositivos de la red. Lo mencionado en el punto anterior coincide con el objetivo, monitorear los dispositivos de red haciendo uso del protocolo simple de administración de red, que brinda a los administradores la capacidad de gestionar todos los dispositivos de su red y asegurarse de que no solo estén en funcionamiento, sino que también tengan un rendimiento óptimo. De esta manera, la red de la empresa Interconexiones Ocaney va crecer de manera ordenada.

Considerando a Becerra Orrala (2016) propone la instalación del sistema de monitorización Cacti, para ver en estado de salud de los dispositivos de red, si bien es cierto que Cacti es un software libre, que ofrece generación de gráficos y reportes, no tiene la versatilidad de otros sistemas de monitoreo; como la integración con mesa de ayuda, reporte de sistema, gestión de inventarios, sistema de mensajería. Por lo mencionado en el punto anterior, y según lo

mencionado en las bases teóricas, se sugiere el uso de Zabbix como sistema de monitorización, un software de código abierto, con soporte a precio razonable, la interfaz web es mejor que la mayoría de los programas de monitorización de redes disponibles en el mercado. Debido a las características versátiles, el seguimiento de los sitios web se puede realizar de forma muy exhaustiva. Además, se puede integrar con el sistema de Ticket y Help Desk tales como Jira, BMC Remedy, ServiceNow, Bugzilla. Con sistemas de mensajería como HipChat, Slack, PagerDuty, Skype. La empresa Interconexiones Ocaney no cuenta con un sistema de monitoreo de red, por lo que se propone instalar el sistema de monitorización Zabbix, con lo cual se va tener un control centralizado de toda la red, el cual nos alertará de posibles fallos, saturación de ancho de banda, alto consumo de CPU y memoria. Y el operador de red, realizará las correcciones necesarias de acuerdo al tipo de alerta que muestre el sistema de monitoreo de red.

En el caso de Quispe Bustincio (2018) implementa un sistema de monitoreo y control de red, pero no menciona la implementación de un sistema de mesa de ayuda para registro de todas las incidencias y solicitudes que se presente durante la monitorización. A diferencia del punto anterior, en el objetivo implementar el centro de operaciones de red mediante el uso de tecnologías de monitorización, se ejecuta un sistema de registro de incidencias, de esa manera se tendrá un reporte de todas las actividades que se presente durante el periodo de monitorización y tomar acciones de mejora si fuera necesario. Se recomienda implementar OsTicket como plataforma de manejo de tiques de incidencias de soporte y servicio al cliente. Permite facilidad de uso. Ayuda a lleva un registro detallado de las solicitudes de los usuarios para dar respuesta y dar solución a la brevedad posible. La empresa Interconexiones Ocaney no cuenta con un registro de las incidencias atendidas que le pueda ayudar a realizar reportes de las atenciones realizadas durante el mes. Al usar la plataforma OsTicket, se va lograr un registro de todas las atenciones, el tiempo de duración de una incidencia o requerimiento. Con dichos datos se puede realizar reportes de la cantidad de incidencias al mes y tomar medidas correctivas en caso se requiera.

Entre tanto Bravo & Lucero (2017) diseña una red de telemedicina para unir remotamente la sede remota con la sede central, en la cual propone la implementación de un enlace inalámbrico con equipos de la marca albentia systems, equipos con mecanismos anti interferencias que mejoran la sensibilidad y facilitan encontrar espectro disponible y con dispositivos inalámbricos de la marca radwin modelo RAD2011. Haciendo hincapié en el punto anterior, son equipos inalámbricos con precios elevados con respecto a otras marcas existentes en el marcado y que pueden ofrecer las mismas funcionalidades. Como lo mencionado en las bases teóricas, Mikrotik es una empresa que desarrolla amplia gama de soluciones en enrutadores y sistemas ISP inalámbricos a precios accesibles y que son dispositivos diseñado para soportar grandes cantidades de tráfico, y que tiene buena performance en la implementación de enlaces inalámbricos en zonas rurales y con climas con extremo calor o lluvia. La empresa Interconexiones Ocaney cuenta con enlaces inalámbricos Mikrotik para sus enlaces punto a punto con sus clientes finales y equipos cisco como Core para salida a Internet.

De la misma manera que Campos Bances (2015) plantea la implementación de sistema de monitorización de una central de datos utilizando sensores de temperatura y humedad, utilizando IDE Arduino y con ayuda de herramientas de software libre tales como Lubuntu, apache, MySQL y PHP. Lo propuesto en el punto anterior, se recomienda realizar mejoras. Haciendo referencias a lo indicado en las bases teóricas, se sugiere integrar con el sistema de monitorización Zabbix y con ello tener un punto central de gestión y control, no solo de la salud de los dispositivos de red, sino también de la temperatura y la humedad del medio ambiente en donde se encuentra los equipos de telecomunicaciones, ya sea en un centro de datos o una estación en un punto determinado. Es importante saber dichos parámetros debido a que los dispositivos de red trabajan a una cierta temperatura y humedad, en caso de que dichos valores no se encuentren en el umbral indicado en su ficha técnica, son propensos a malograrse o presentar anomalías inesperadas y causar problemas en la red de transporte.

CAPITULO IV

Conclusiones

En la presente investigación se propuso establecer un sistema de monitoreo para los servicios inalámbricos en la empresa Interconexiones Ocaney mediante la implementación de un Centro de Operaciones de Red para la gestión y administración centralizada de los equipos de telecomunicaciones, la cual se simuló y se realizó las pruebas con plena satisfacción el monitoreo de los enlaces inalámbricos.

1. Para poder caracterizar el monitoreo de los servicios inalámbricos se recurrió a la revisión de la literatura en fuentes primarias como artículos obtenidos de Google académico, Ebsco, Scopus, IEEE Xplore, entre otras y fuentes secundarias como libros, tesis, revistas de la industria y sitios web.
2. Se realizó el diagnóstico del estado actual de los servicios inalámbricos proporcionados por la empresa Interconexiones Ocaney mediante la utilización de instrumentos de recolección de datos como el cuestionario y la guía de observación.
3. Se implementó el centro de operaciones de red mediante el uso del sistema de monitorización Zabbix y se integró con la herramienta Grafana para mejorar la visualización de los gráficos del estado de salud de los dispositivos de red. Para lo cual fue necesario la instalación del servidor de red, en este caso se usó CentOS 7, sobre el cual se implementó el sistema de monitorización.
4. Para poder gestionar el centro de operaciones de red en concordancia a los estándares de servicios de TI, se elaboraron un conjunto de reglas y buenas prácticas, que el operador de red utilizará de acuerdo con la situación que se presente en el monitoreo de los servicios inalámbricos.
5. Para realizar la monitorización de los equipos de telecomunicaciones, se utilizó el protocolo simple de administración de red. Se instaló el agente SNMP en cada uno de los equipos de red en la empresa Interconexiones Ocaney, para recopilar información del estado de salud de los dispositivos y enviar al administrador SNMP.

CAPITULO V

Recomendaciones

- Se recomienda implementar el sistema de monitoreo de red en la empresa Interconexiones Ocaney, con ello tener un control y una gestión centralizada de su red, debido que a medida que su red crece se vuelve compleja y difícil de administrar.
- En el mercado tecnológico existen variadas herramientas de monitorización, muchos de ellos software libre y gran versatilidad, por lo que se sugiere a todas las empresas pequeñas o medianas tener un sistema de monitoreo de red, que le será de gran utilidad en cuando se presente algún problema de red.
- En cuando a la implementación del sistema de monitorización Zabbix, se recomienda siempre integrarlo con la herramienta Grafana y con ello obtener una mejor visualización de los gráficos del estado de salud de los dispositivos de red.
- Se sugiere contar siempre con un personal en el centro de monitoreo de red, para estar al tanto de alguna alerta que se presente en los equipos de red. Además de un personal en campo para cuando no sea posible la solución remota por parte del personal del NOC.
- Al mismo tiempo se recomienda brindarle capacitación adecuada en el uso del sistema de monitoreo de red, tanto al personal que va a realizar el trabajo en el NOC y al personal de campo que va a brindar la solución de las averías en sitio.
- Se recomienda crear un usuario y clave para acceder a los dispositivos de red, a cada uno de los empleados que va a realizar el monitoreo de los equipos de telecomunicaciones. Dicho usuario y clave debe ser personal e intransferible.
- Cada vez que un nuevo equipo de telecomunicaciones se integre al sistema de monitorización, es recomendable realizar una actualización de la topología física y lógica de la red.
- Como mejora al sistema de monitoreo de red, se recomienda la implementación de un sistema de control de temperatura y humedad con ayuda de IDE Arduino e integrar al sistema de monitorización Zabbix y

con ello monitorear no solo el estado de salud de los dispositivos de red sino además del medio ambiente en donde se encuentran.

- Respecto al uso de herramientas para el registro de tique de incidencias y requerimientos, si la empresa cuenta con presupuesto, se sugiere el uso de software de pago como es el caso de BMC Remedy ISTM.
- Finalmente, la implementación de un centro de operación de red diseñada en la presente investigación no acarrea ningún costo, por lo que se recomienda implantar en cualquier empresa del rubro de telecomunicaciones que desee tener un centro de operación de red, y que no cuente con los recursos suficientes para contratar un sistema de monitorización de pago.

Referencias

Andreu, J. (2011). Redes inalámbricas (Servicios en red) . In *Editex*. https://books.google.com.pe/books?hl=es&lr=&id=98_TAwAAQBAJ&oi=fnd&pg=PA209&dq=redes+inalámbricas&ots=toJkdltlBR&sig=Lw4TfOwY6S87AZ1fgrQS_92N5qc&redir_esc=y#v=onepage&q=redes inalámbricas&f=false

Anytech. (2019). *Importancia de un Network Operations Center (NOC)*. Anytech. https://www.aynitech.com/articulo/importancia-de-un-network-operations-center-noc

Ariganello, E., & Barrientos Sevilla, E. (2015). *unprg - Redes Cisco: guía de estudio para la certificación CCNP Routing y Switching (3a. ed.)*. https://elibro.net/es/lc/unprg/titulos/106474?as_all=netflow__en__cisco&as_all_op=unaccent__icontains&prev=as

Becerra Orrala, E. D. R. (2016). IMPLEMENTACIÓN DE MONITOREO DE RED UTILIZANDO LOS PROTOCOLOS ICMP Y SNMP. In *Universidad Estatal Peninsula Santa Elena* (Issue 7047). https://repositorio.upse.edu.ec/handle/46000/2583

Biblioteca DUOC UC. (2018). Definición y propósito de la Investigación Aplicada | Biblioteca DUOC UC. *CRAI*. http://www.duoc.cl/biblioteca/crai/definicion-y-proposito-de-la-investigacion-aplicada

Bravo, W., & Lucero, R. (2017). Diseño de una red de telemedicina para monitoreo de pacientes en el centro poblado de Huayrul del distrito de Incahuasi, provincia de Ferreñafe, región Lambayeque. *Universidad Nnacional Pedro Ruiz Gallo*, 95. http://repositorio.unprg.edu.pe/handle/UNPRG/1240

Campos Bances, C. A. (2015). Sistema de monitoreo de seguridad física en plataforma libre de componentes electrónicos para asegurar la gestión de los niveles de continuidad de los servicios. In *Universidad Católica Santo Toribio de Mogrovejo*. http://54.165.197.99/jspui/handle/123456789/382

Castano Ribes, R. J. (2013). Redes locales. *Macmillan Iberia*, 322.

https://elibro.net/es/lc/unprg/titulos/43257

CentOS. (2014). *FrontPage - CentOS Wiki*. CentOS. https://wiki.centos.org/FrontPage

Cisco. (2021). *TACACS+ and RADIUS Comparison - Cisco*. Cisco. https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html#comparing

CISCO. (2020). *Switch Cisco Catalyst 3750X-24T-S - Cisco*. CISCO. https://www.cisco.com/c/es_mx/support/switches/catalyst-3750x-24t-s-switch/model.html

Costas Santos, J. (2014). Seguridad Informáctica. In *RA-MA Editorial*. https://elibro.net/es/ereader/unprg/62452?page=86

Flickenger, R. (2008). Redes Inalámbricas en los Países en Desarrollo. *Creative Commons*.

Grafana. (2020). *Grafana: The open observability platform | Grafana Labs*. Grafana. https://grafana.com/

Guerra Soto, M. (2016). *Interconexión de redes privadas y redes públicas*. RA-MA Editorial. https://elibro.net/es/lc/unprg/titulos/106399?as_all=%22monitoreo__de__red%22&as_all_op=unaccent__icontains&fs_page=4&prev=as

Hegde, M., Narana, M., & Kumar, A. (2015). netmon: An SNMP Based Network Performance Monitoring Tool for Packet Data Networks. *IETE Journal of Research*, *46*(1–2), 15–25. https://doi.org/10.1080/03772063.2000.11416131

Hernandez Sampieri, R., Fernandez Collado, C., & Baptista Lucio, M. del P. (2014). Metodología de la Investigacion. In *MC Graw Hill*.

Internet Paso a Paso. (2018). *【RED WLAN】Qué es + Tipos + Cómo crear ▷ 2020*. Internet Paso a Paso. https://internetpasoapaso.com/red-wlan/

Interpolados. (2017). *COMPARACIÓN ENTRE EL MODELO OSI Y EL MODELO TCP/IP – Interpolados*. Interpolados.

https://interpolados.wordpress.com/2017/03/01/comparacion-entre-el-modelo-osi-y-el-modelo-tcpip/

ITIL. (2011). ITIL Service Design. *Information & Publishing Solutions*. http://www.itrs.net/Links/2011ITRS/2011Chapters/

López Pérez, M., Padilla de la Torre, P., & Padilla de la Torre, J. L. (2013). Redes e infraestructuras de telecomunicación. In *Pearson Educación*. https://elibro.net/es/lc/unprg/titulos/57162?as_all=redes&as_all_op=unaccent__icontains&fs_page=2&prev=as

ManageEngine. (2020). *Software de monitoreo de Cisco | Administración de redes Cisco - ManageEngine OpManager*. ManageEngine. https://www.manageengine.com/latam/network-monitoring/software-monitoreo-redes-cisco.html

Mikrotik. (2020). *MikroTik Routers and Wireless - Products: SXT SA5 ac*. Mikrotik. https://mikrotik.com/product/RBSXTG-5HPacD-SAr2#fndtn-gallery

Molina Robles, F. J., & Polo Ortega, E. (2014). Servicios en red. In *RA-MA*. https://elibro.net/es/lc/unprg/titulos/62455?as_all=redes&as_all_op=unaccent__icontains&prev=as

MySQL. (2020). *MySQL*. MySQL. https://www.mysql.com/

osTicket. (2020). *osTicket | Support Ticketing System*. OsTicket. https://osticket.com/

PandoraFMS. (2017). *Monitoreo de red que debemos saber: características necesarias*. PandoraFMS. https://web.archive.org/web/20181107223812/https://blog.pandorafms.org/es/monitoreo-de-red-que-debemos-saber/#

PayScale. (2020). *Network Operations Center (NOC) Engineer with Cisco Networking Skills Salary | PayScale*. PayScale. https://www.payscale.com/research/US/Job=Network_Operations_Center_(NOC)_Engineer/Salary/e52cae8c/Cisco-Networking

PHP. (2020). *PHP: ¿Qué es PHP? - Manual*. PHP. https://www.php.net/manual/es/intro-whatis.php

Quispe Bustincio, J. W. (2018). Implementación De Un Sistema De Monitoreo Y Control De Red, Para Un Canal De Televisión, Basado En Herramientas Open Source Y Software Libre, Lima- 2017. In *Universidad Nacional del Altiplano*. http://tesis.unap.edu.pe/bitstream/handle/UNAP/9019/Quispe_Bustincio_Jhon_Watson.pdf?sequence=1&isAllowed=y

Reid, A., Lorenz, J., & Schmidt, C. (2009). Introducción al enrutamiento y la conmutación de la empresa. In *Pearson Edutation*. https://elibro.net/es/ereader/unprg/53862?fs_q=ccna&prev=fs&page=11

Salazar, J. (2016). Redes Inalámbricas. In *TechPedia* (Vol. 2). http://www3.uah.es/vivatacademia/ficheros/n54/redesinalam.PDF

Sánchez Rubio, M., Barchino Plata, R., & Martinez Herraiz, J. J. (2020). Redes de Computadores. In *Universidad de Alcalá*. https://elibro.net/es/ereader/unprg/131606?as_all=redes&as_all_op=unaccent__icontains&prev=as&page=18

Think networks. (2020). *Centro de operaciones de Red (NOC) - Think Networks Perú*. Think Networks. https://www.thinknetworks.pe/noc/

Tipos de redes. (2017). *Tipos de redes: RED WMAN*. Tiposderessac. http://tiposderedessac.blogspot.com/2017/04/red-wman.html

Wilson, J. D., & Stevens, N. T. (2020). Quality Engineering special issue on Network Monitoring. *Quality Engineering*, *32*(2), 263–263. https://doi.org/10.1080/08982112.2020.1731279

Zabbix. (2020). *Zabbix*. Zabbix. https://www.zabbix.com/manuals

Zhao, L., & Yu, H. (2020). A wireless network remote monitoring method driven by artificial intelligence. *International Journal of Computers and Applications*. https://doi.org/10.1080/1206212X.2019.1710664

Anexos

Anexo 1: Instrumento de recolección de datos

Cuestionario dirigido al personal de sistemas y administrativo de la empresa interconexiones Ocaney.

Estimado colaborador: Lea atentamente cada pregunta, valore y elija la respuesta que mejor describa acerca de monitoreo y gestión de la red en la empresa interconexiones Ocaney. Por favor exprese su opinión que le merece marcando en cada ítem solo una de las opciones en cualquiera de las 5 posibles alternativas, considerando que:

1 = Nunca, 2 = Casi nunca, 3: A veces 4 = Casi siempre, 5 = Siempre

Cabe indicar que esta encuesta es completamente ANÓNIMO.

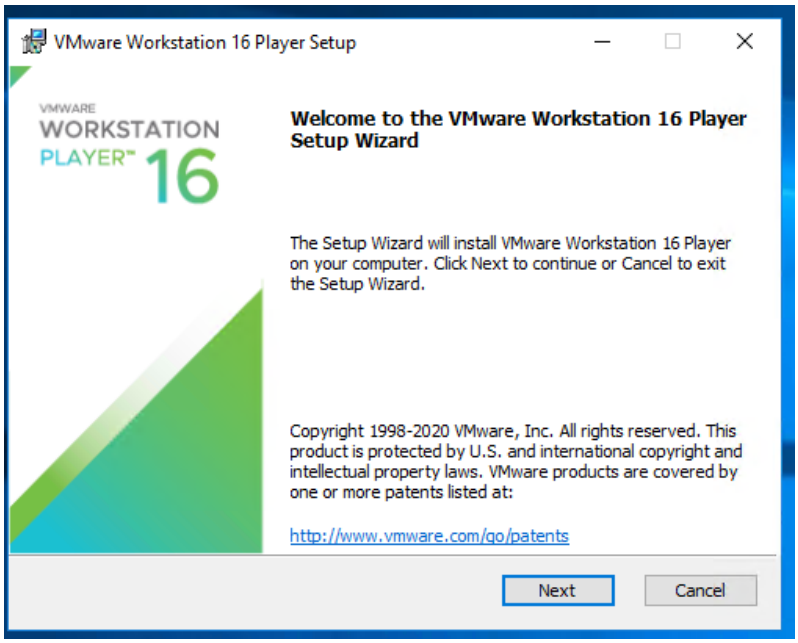
Variable Dependiente: Implementación de un centro de operaciones de red								
		Dimensión 1: Recursos informáticos	**Alternativas**					
N°	**Indicador**	**Ítems**	**1**	**2**	**3**	**4**	**5**
1	Estado de los dispositivos de red	¿La empresa Interconexiones Ocaney cuenta con un sistema de monitoreo para ver el estado de los dispositivos de red?					
2		¿La empresa Interconexiones Ocaney dispone de equipos para brindar continuidad del servicio las 24hrs del día?					
3	Configuración de los equipos de red	¿La empresa Interconexiones Ocaney cuenta con sistema automatizado para la configuración de los equipos de red?					
		Dimensión 2: Disponibilidad	**1**	**2**	**3**	**4**	**5**
4	Operación y acceso a la red	¿La empresa interconexiones Ocaney cuenta con una plataforma de fácil acceso a los dispositivos de red?					
5	Redundancia ante caída de los equipos de red	¿La empresa interconexiones Ocaney cuenta con respaldo ante caídas de los equipos de red?					

6		¿En caso de caída de los equipos intermediarios, la empresa Interconexiones Ocaney cuenta con equipos de respaldo?					
		Dimensión 3: Escalabilidad	**1**	**2**	**3**	**4**	**5**
7	Cantidad de equipos informáticos	¿La empresa interconexiones Ocaney cuenta con la cantidad suficiente de equipos para abastecer de servicio a sus suscriptores?					
8	Servicios implementados	¿La empresa interconexiones Ocaney ofrece diversos servicios (Internet, Datos, VPN, Telefonía, Seguridad, servicio por cable) a sus clientes?					
Variable Independiente: Monitoreo de Servicios Inalámbricos							
		Dimensión 2: Gestión	**1**	**2**	**3**	**4**	**5**
9	Configuración de los servicios inalámbricos	¿Consideras que la empresa interconexiones Ocaney configura adecuadamente los servicios de los enlaces inalámbricos?					
10	Incidencias de los servicios inalámbricos	¿Con que frecuencia, la calidad del servicio inalámbrico que brinda la empresa interconexiones Ocaney se ve afectado?					
11	Capacidad de los servicios inalámbricos	¿Cuándo se interrumpen los servicios inalámbricos, la empresa interconexiones Ocaney responde de una manera rápida y eficiente?					
12	Seguridad de los servicios inalámbricos	¿La empresa interconexiones Ocaney cuenta con una política de acceso seguro a su dispositivo de red inalámbricos?					
13	Registro de servicios inalámbricos	¿La empresa interconexiones Ocaney cuenta con un registro adecuado de sus dispositivos de red inalámbricos?					
		Dimensión 2: Monitoreo	**1**	**2**	**3**	**4**	**5**

14	Control de ancho de banda.	¿La empresa interconexiones Ocaney cuenta con un control adecuado del ancho de banda de su red?					
15	Estado de los equipos inalámbricos.	¿La empresa interconexiones Ocaney cuenta con una plataforma donde se pueda ver en tiempo real el estado de los equipos de red inalámbricos?					
16	Respaldo de la información	¿La empresa interconexiones Ocaney cuenta con un respaldo de la configuración de los dispositivos de red en caso de una avería de un dispositivo de red?					
17	Documentación de los dispositivos de red	¿La empresa interconexiones Ocaney cuenta con la documentación actualizada de los dispositivos de red inalámbricos?					

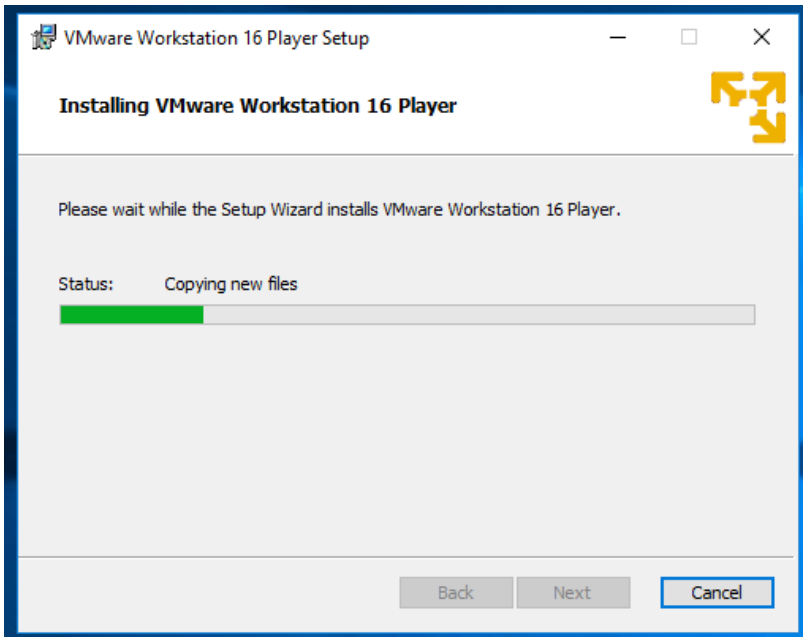
Anexo 2: Instalación de servidor CentOS 7.

Procedemos a descargar VMWare, desde la página web oficial de VMWare https://www.vmware.com/latam/products/workstation-player/workstation-player-evaluation.html, una vez descargado iniciamos a instalar



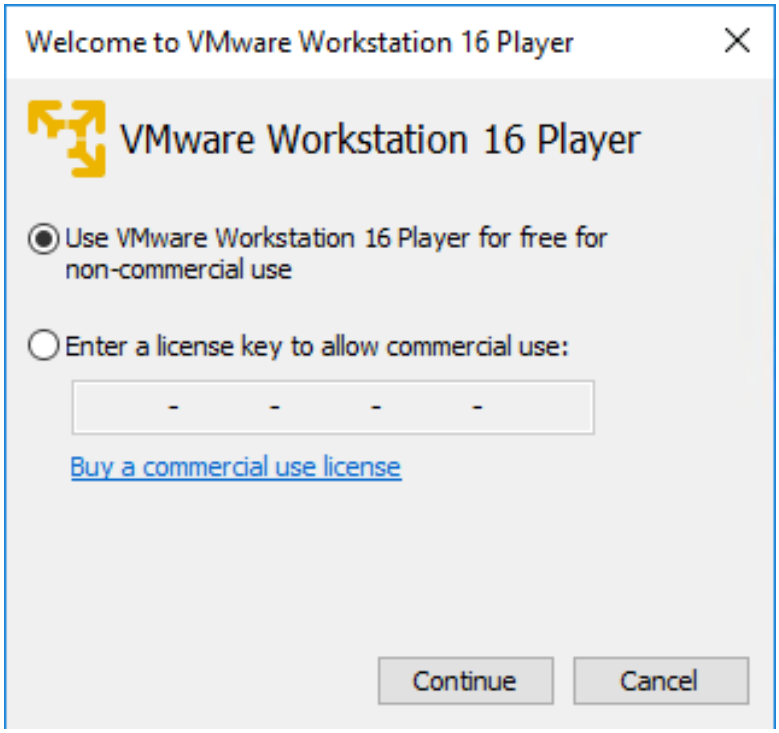
Fuente: Elaboración propia.

Seleccionamos en siguiente y le damos a instalar



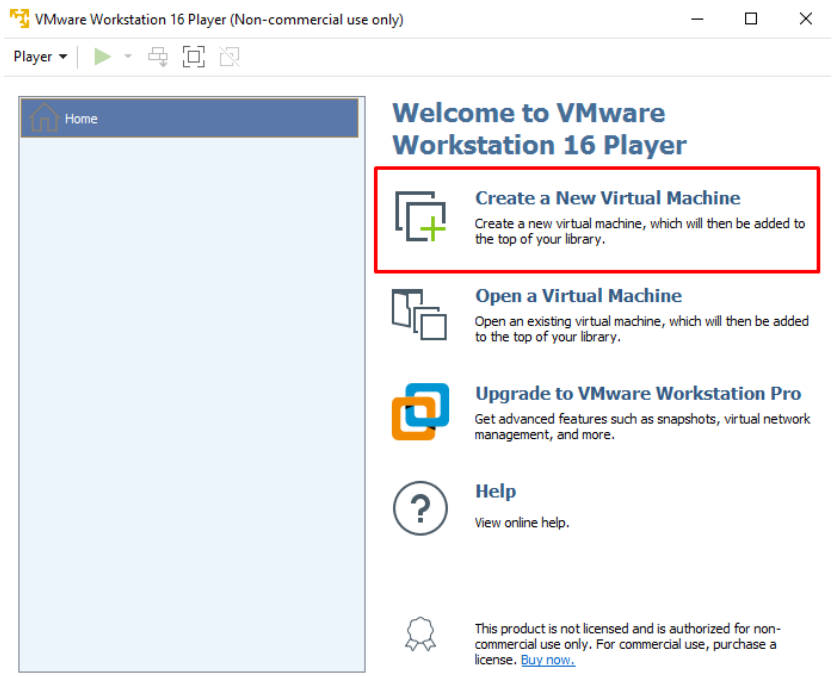
Fuente: Elaboración propia.

Seleccionamos el uso no comercial



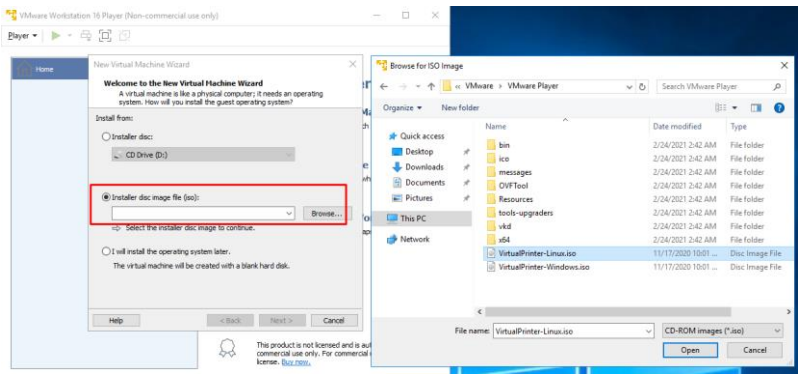
Fuente: Elaboración propia.

Elegimos crear una nueva máquina virtual



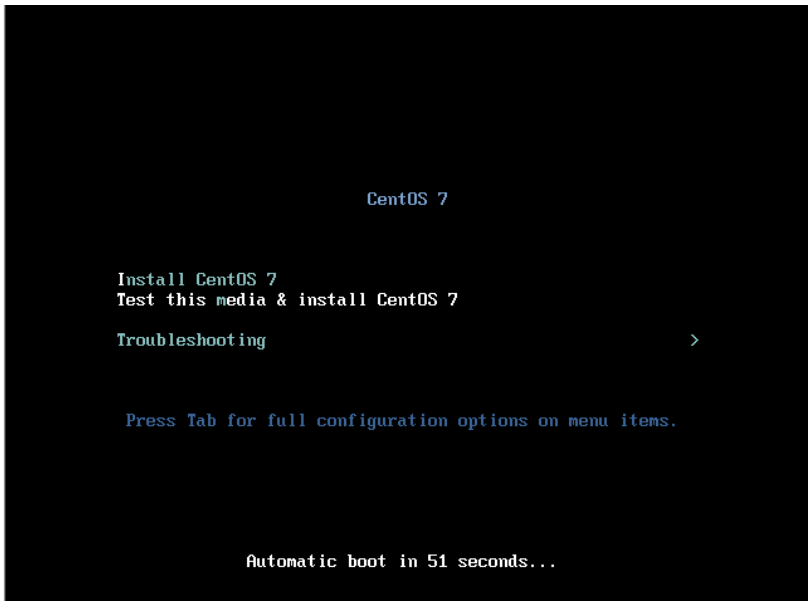
Fuente: Elaboración propia.

Seleccionamos instalar imagen y elegimos el sistema operativo que queremos montar en la máquina virtual.



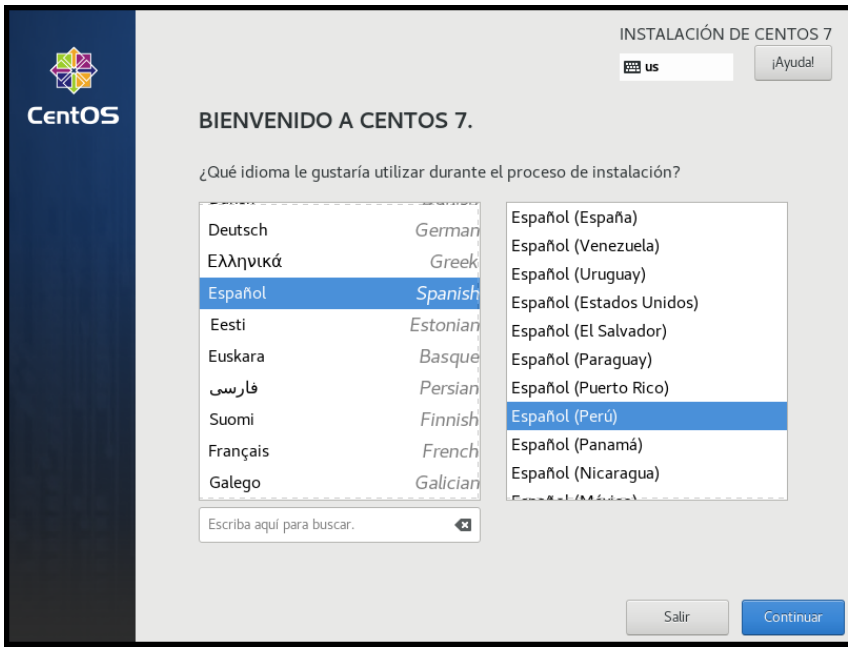
Fuente: Elaboración propia.

Una vez montado el sistema operativo sobre la máquina virtual, Iniciamos a instalar CentOS 7, la primera pantalla que nos aparece debemos seleccionar *“Install CentOS 7”.*



Fuente: Elaboración propia.

Automáticamente se iniciará el proceso de instalación, una vez iniciado nos solicitará seleccionar idioma, seleccionamos *“español (Perú)”*.



Fuente: Elaboración propia.

A continuación, nos aparece un menú donde debemos ir seleccionando los iconos en función de lo que queramos hacer a la hora de instalar CentOS 7. En la parte de regionalización seleccionamos "*Fecha & hora*".

Fuente: Elaboración propia.

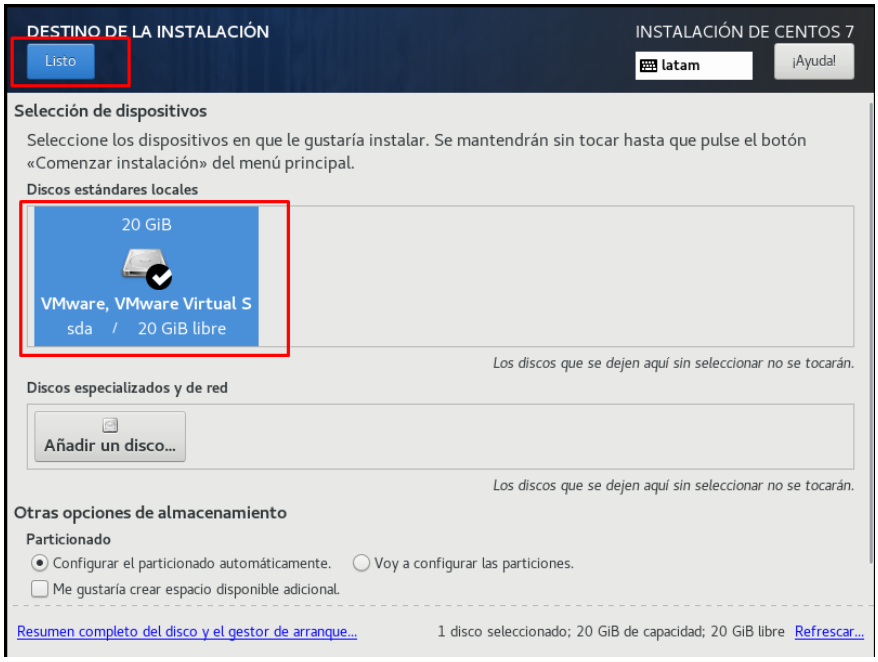
Personalizamos la Región y ponemos la hora y fecha actual y seleccionamos "*Listo*".

Fuente: Elaboración propia.

En la parte de Sistema, seleccionamos "*Destino de la instalación*".

Fuente: Elaboración propia.

Seleccionamos el disco duro donde vamos a instalar el sistema operativo CentOS y seleccionamos listo.

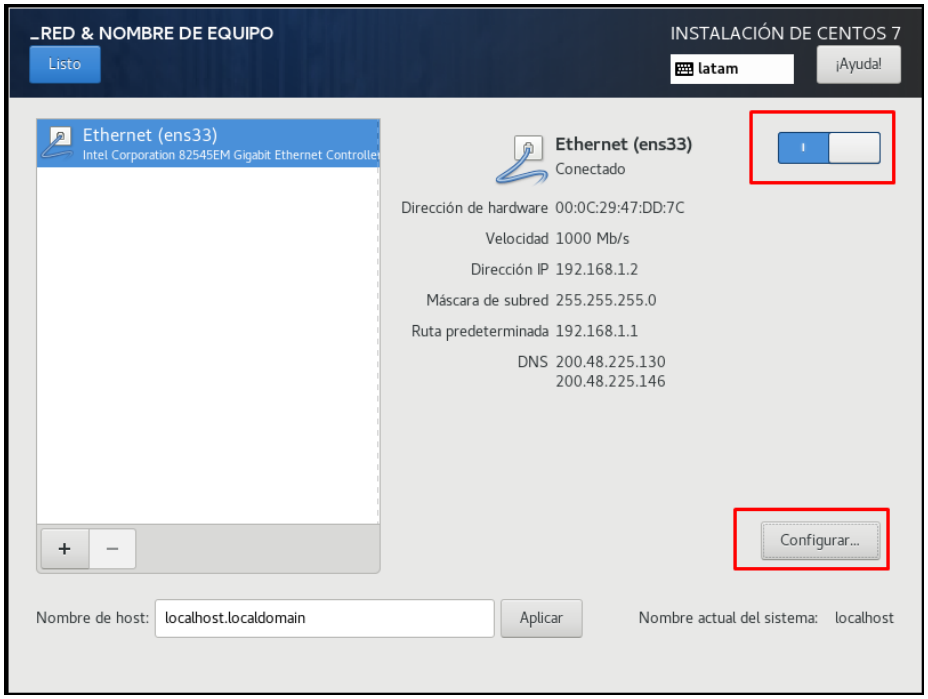


Fuente: Elaboración propia.

En la parte de Sistema, seleccionamos "*Red & nombre de equipo*".

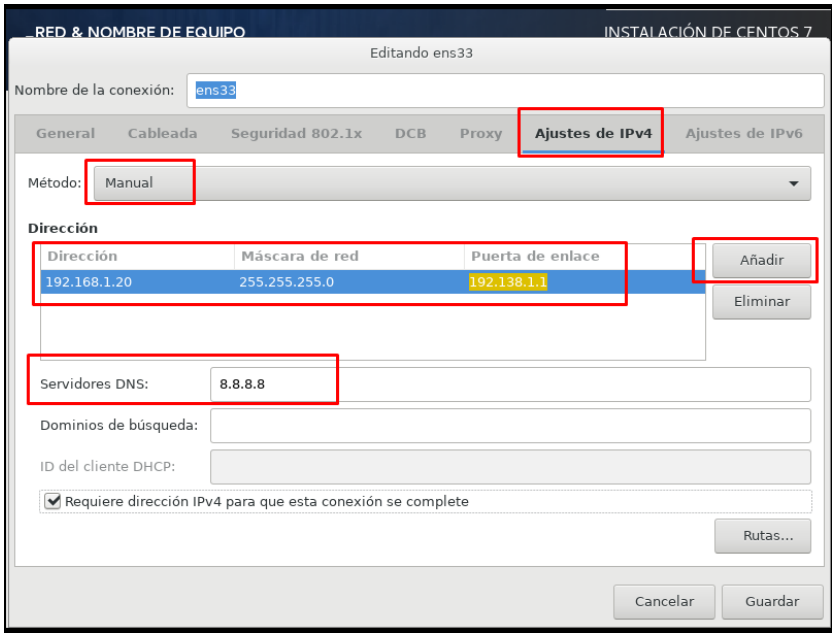
Fuente: Elaboración propia.

Encendemos la tarjeta de red y vamos a la opción configurar.



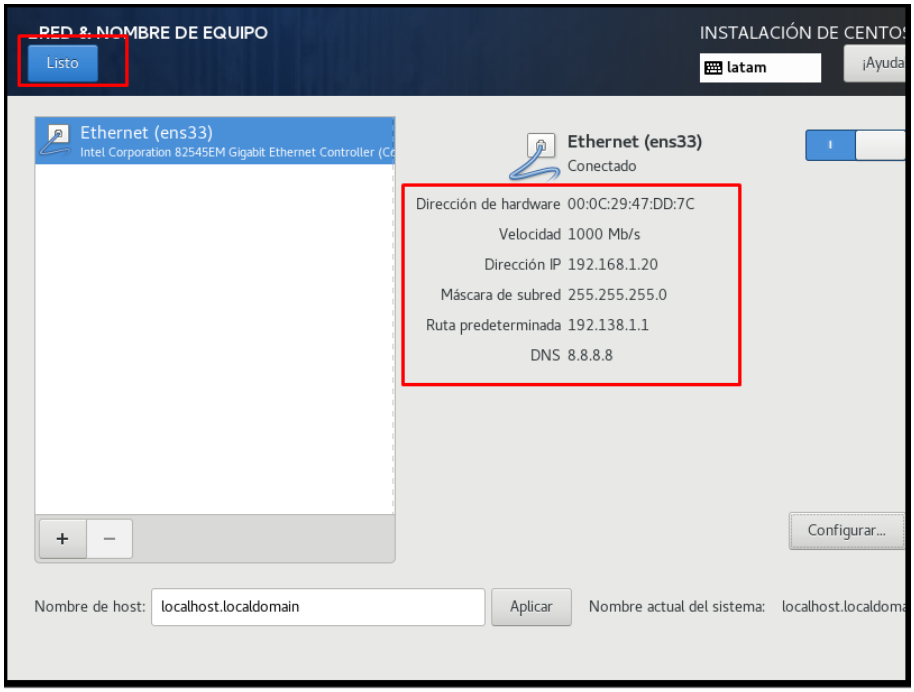
Fuente: Elaboración propia.

Vamos a la opcion "*Ajustes de IPV4",* luego metodo *"Manual"* y seleccionamos *"añadir"* y ponemos nuestra IP, máscara de red y puerta de enlace, ademas de los servidores DNS y finalmente seleccionamos *"guardar".*



Fuente: Elaboración propia.

Finalmente seleccionamos “*listo*”.



Fuente: Elaboración propia.

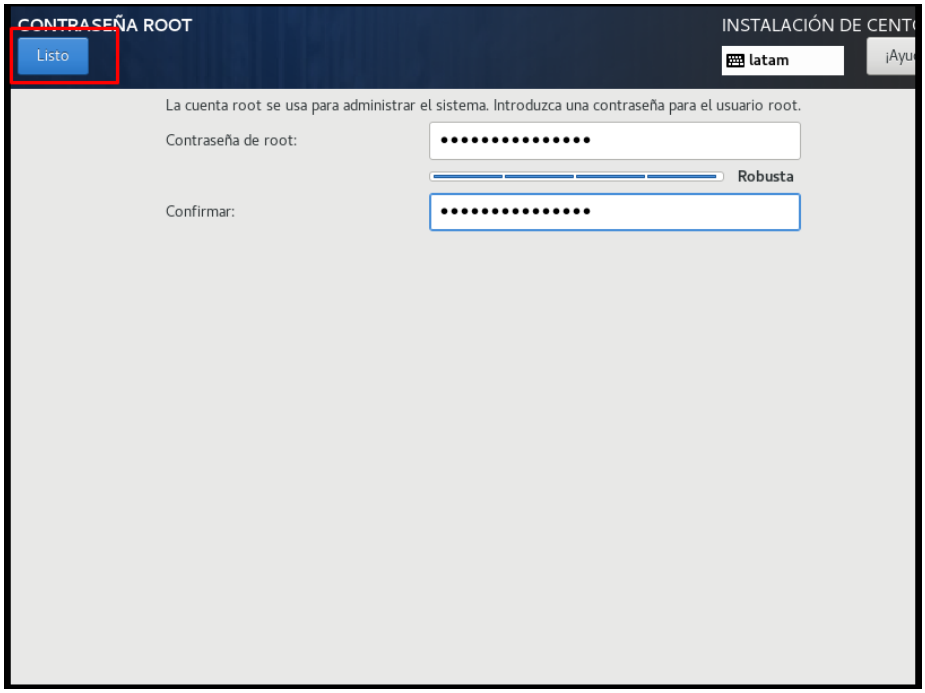
Una vez terminado las personalizaciones, seleccionamos *“Empezar instalacion”.*

Fuente: Elaboración propia.

En la opción Ajustes de Usuario “*Contraseña de root*”.

Fuente: Elaboración propia.

Asiganos una contraseña y seleccionamos *“Listo”.*

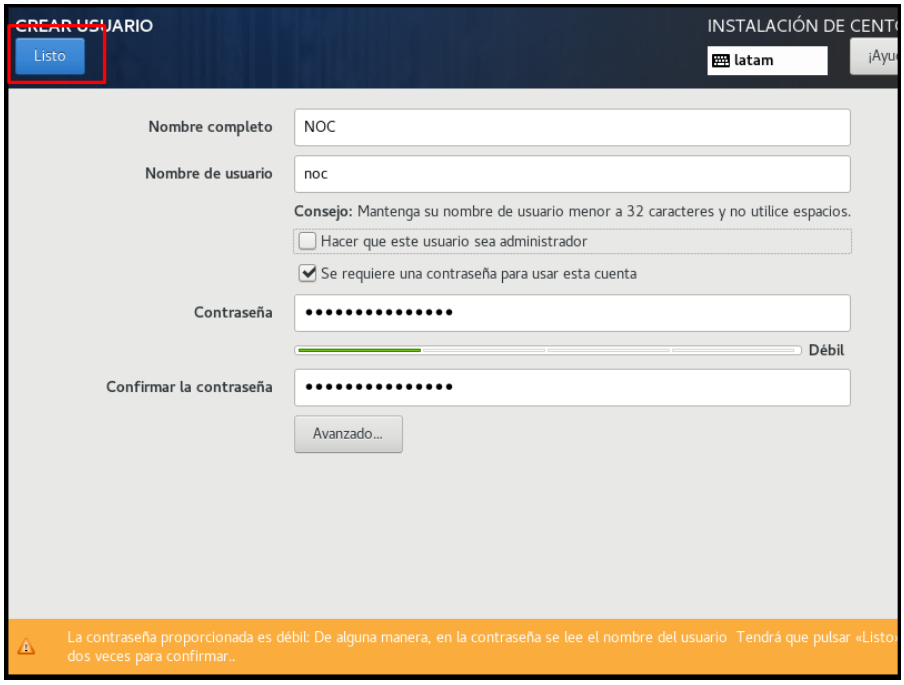


Fuente: Elaboración propia.

Luego seleccionamos “*Creación de usuario” y creamos un usuario*

Fuente: Elaboración propia.

Creamos un usuario y le asignamos una clave y seleccionamos “*Listo*”.



Fuente: Elaboración propia.

Finalmente, seleccionamos *"Finalizar configuración"*

Fuente: Elaboración propia.

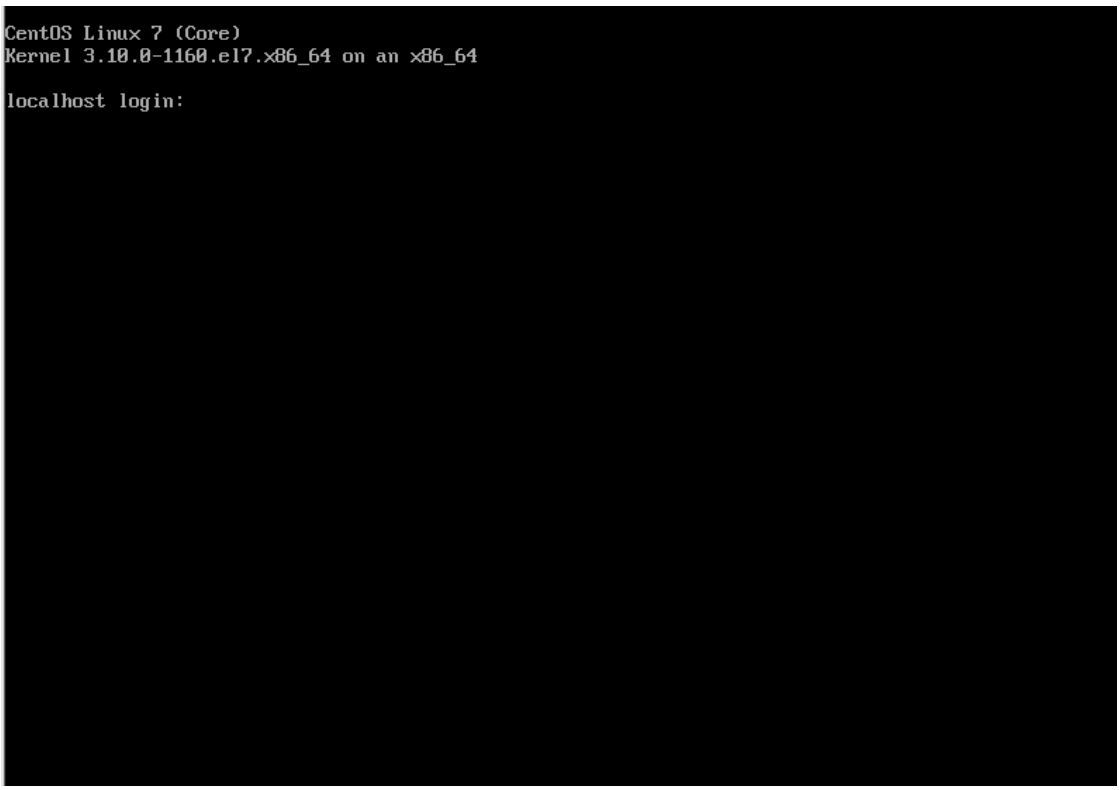
Esperemos a que termine el proceso de instalación.

Fuente: Elaboración propia.

Ahora le damos “*reiniciar*”

Fuente: Elaboración propia.

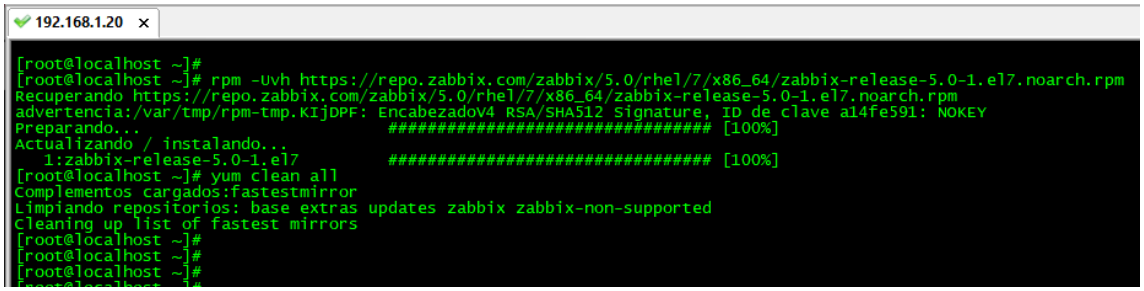
Una vez reiniciado nos aparecerá una pantalla pidiendo contraseñas del usuario que hemos creado en la instalación.



Fuente: Elaboración propia.

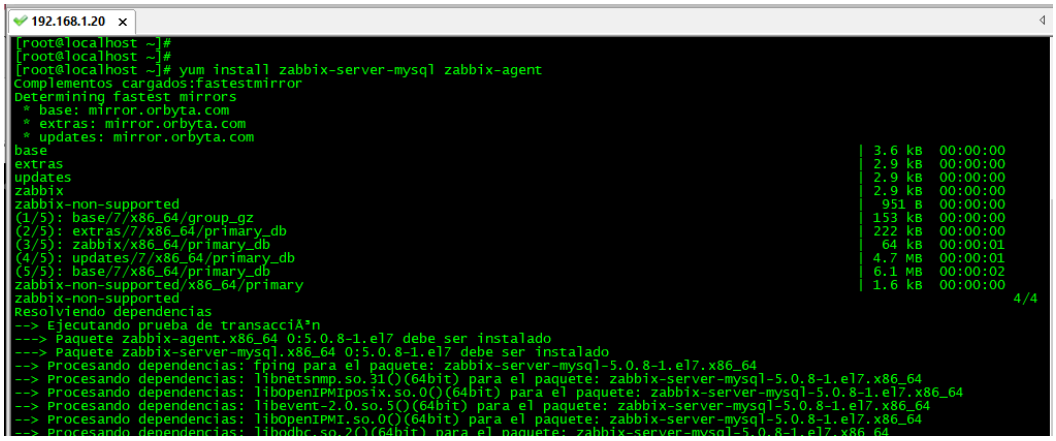
Anexo 3: Instalación del sistema de monitoreo Zabbix.

Procedemos a instalar el repositorio de Zabbix sobre el servidor CentOS.



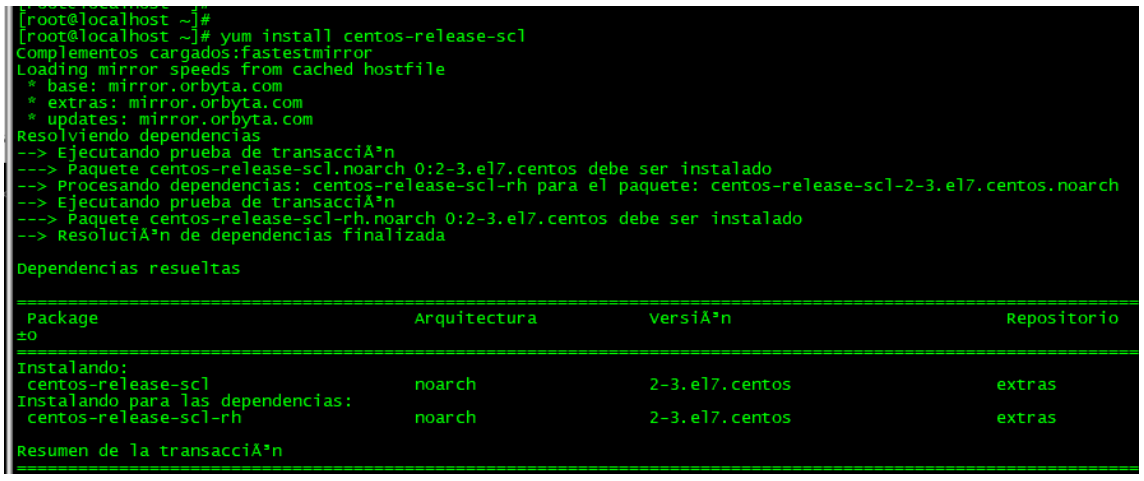
Fuente: Elaboración propia.

Luego se procede a instalar el servidor y el agente Zabbix



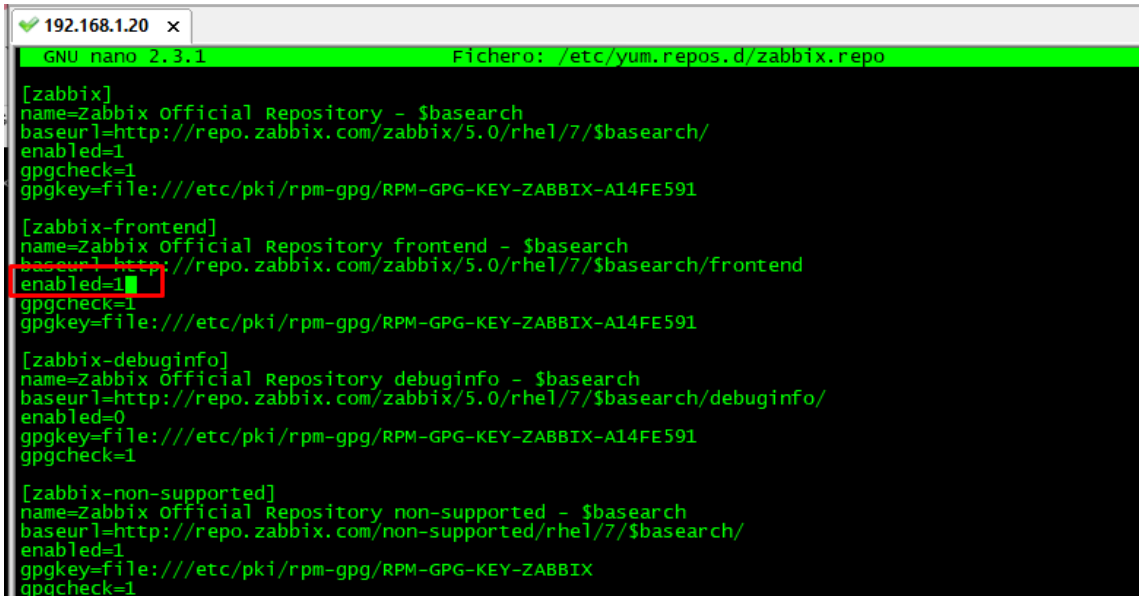
Fuente: Elaboración propia.

Ahora se va a instalar la interfaz de Zabbix



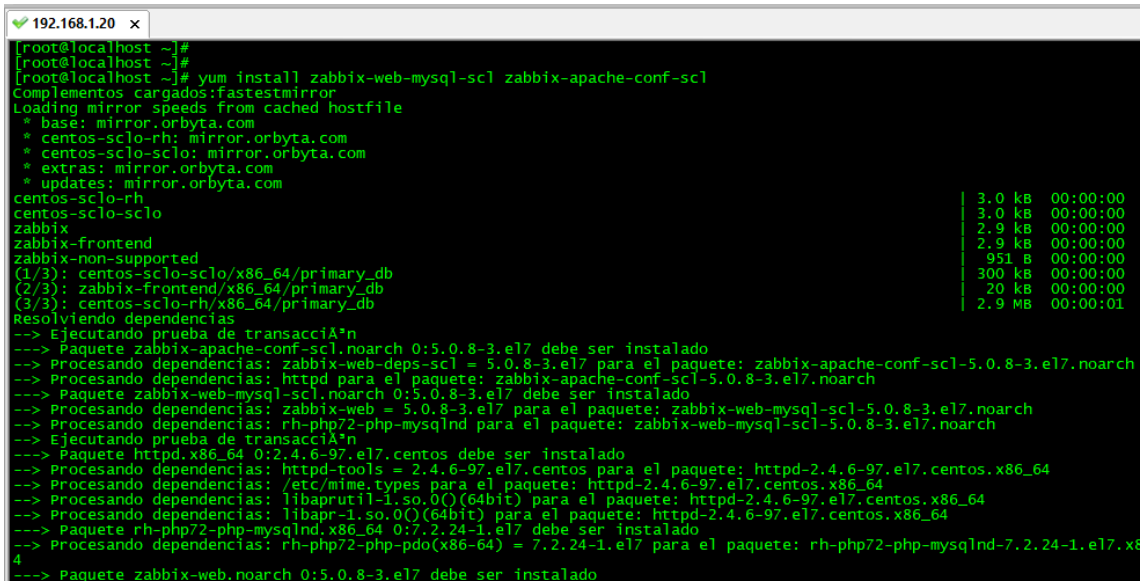
Fuente: Elaboración propia.

Habilitar el repositorio de frontend de Zabbix



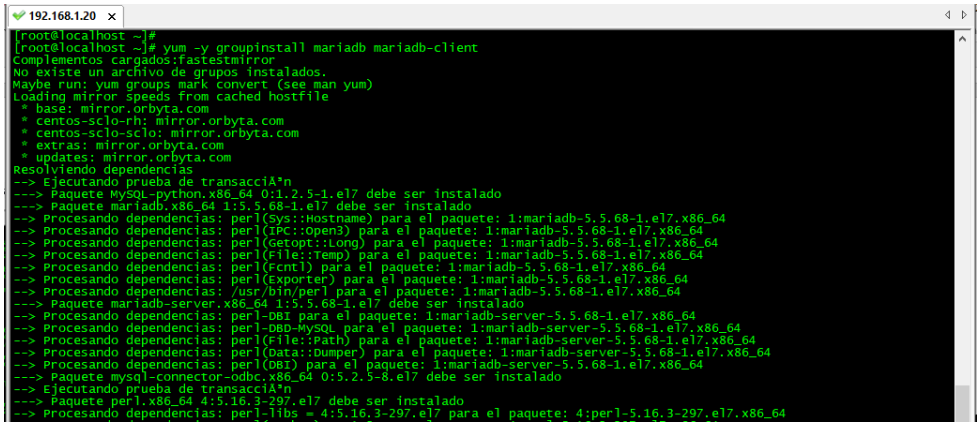
Fuente: Elaboración propia.

Luego se Instala los paquetes frontend de Zabbix.



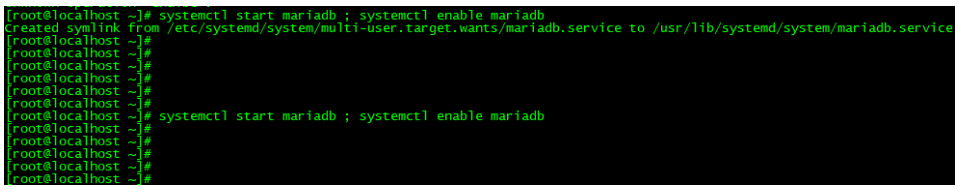
Fuente: Elaboración propia.

Ahora procedemos a instalar la base de datos MariaDB.



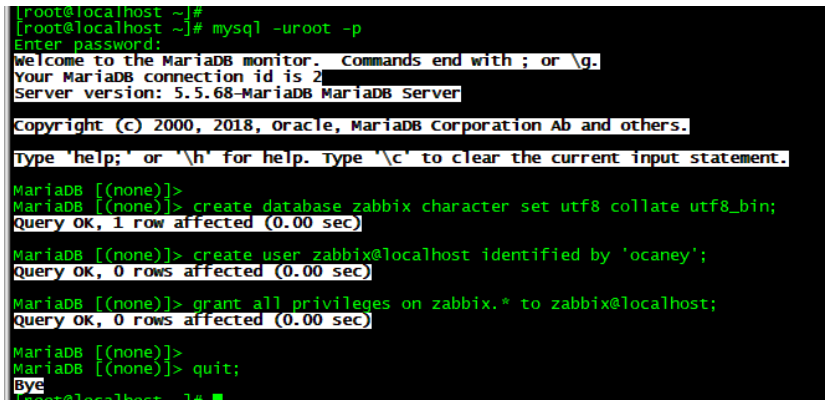
Fuente: Elaboración propia.

Una vez instalado MariaDB se procede a iniciar.



Fuente: Elaboración propia.

Ahora vamos a crear la base de datos inicial, con nombre de prueba de prueba Zabbix, y usuario: zabbix y clave ocaney.

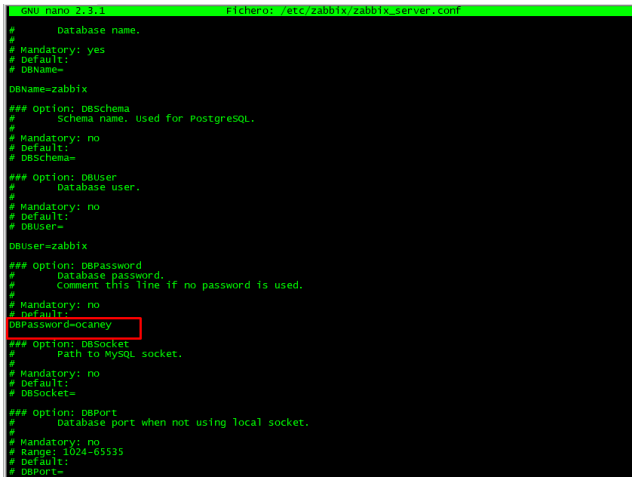


Fuente: Elaboración propia.

En el servidor Zabbix, importamos el esquema y los datos iniciales. Nos solicitará que ingresemos la contraseña recién creada.

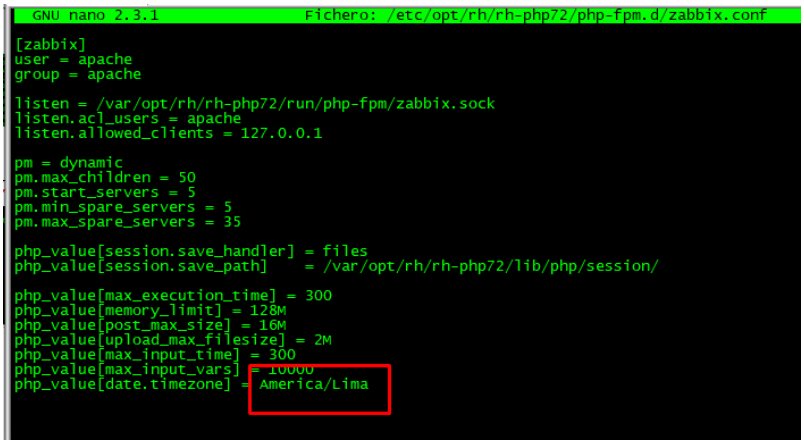
Fuente: Elaboración propia.

Luego Configuramos la base de datos para el servidor Zabbix, editamos archivo /etc/zabbix/zabbix_server.conf en la línea DBPassword ponemos la clave que creamos en la creación de la base de datos.



Fuente: Elaboración propia.

Ahora configuramos el horario del servidor para la interfaz de Zabbix, editar archivo /etc/opt/rh/rh-php72/php-fpm.d/zabbix.conf.



Fuente: Elaboración propia.

Finalmente, Inicia los procesos del agente y del servidor Zabbix con los comandos:

Fuente: Elaboración propia.

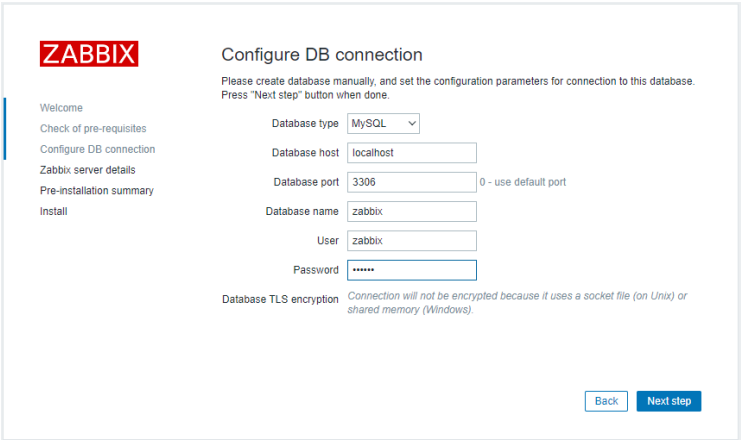
Para acceder a Zabbix por web es necesario habilitar http en el servidor CentOS.

Fuente: Elaboración propia.

Acceso a Zabbix por web.

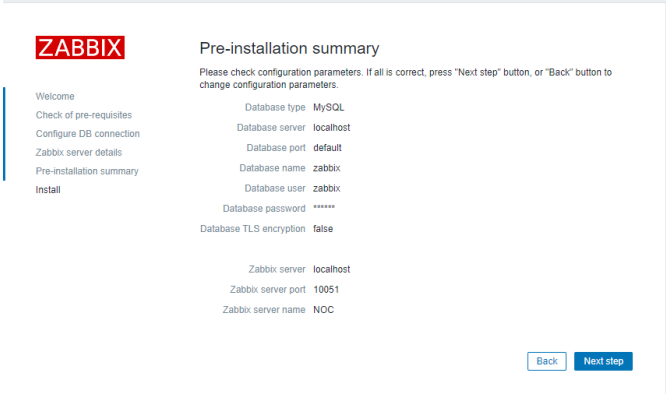
Fuente: Elaboración propia.

Configurar los parámetros de Zabbix.



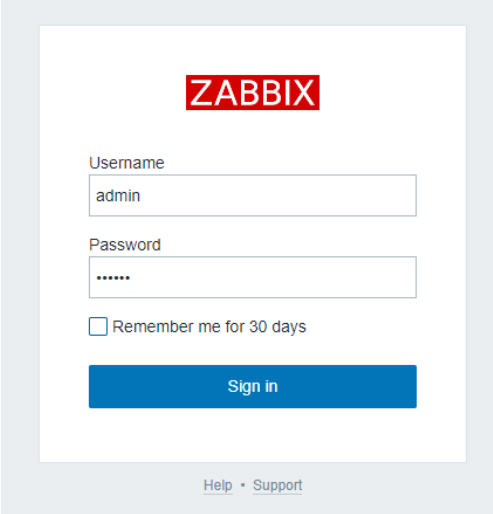
Fuente: Elaboración propia.

Vista de la configuración previa de Zabbix.



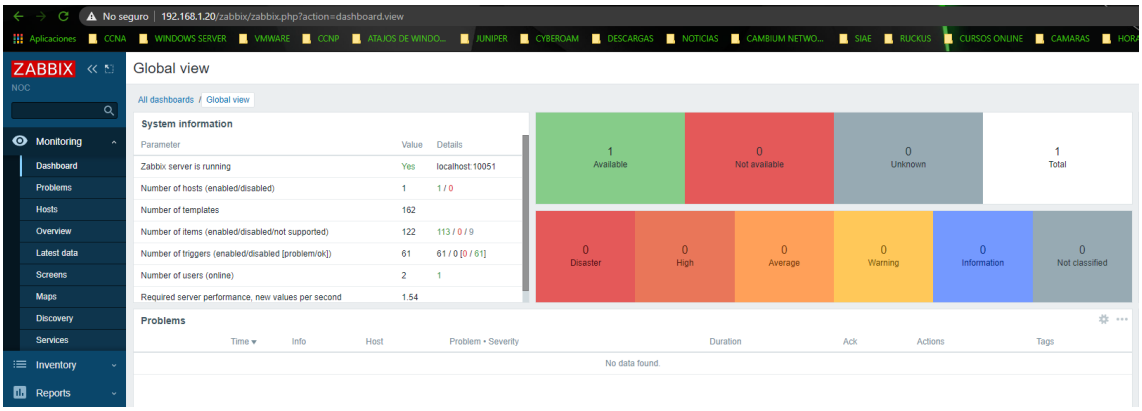
Fuente: Elaboración propia.

Inicio de sesión de Zabbix.



Fuente: Elaboración propia.

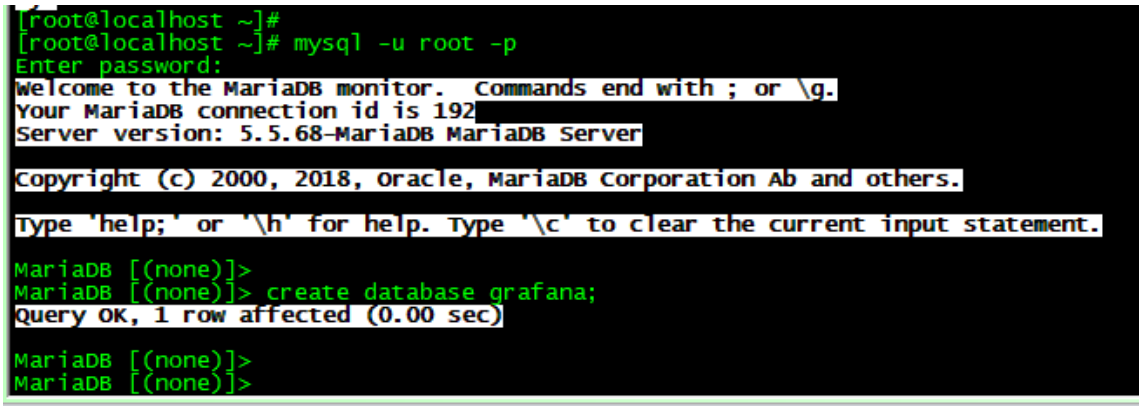
Página de inicio de Zabbix.



Fuente: Elaboración propia.

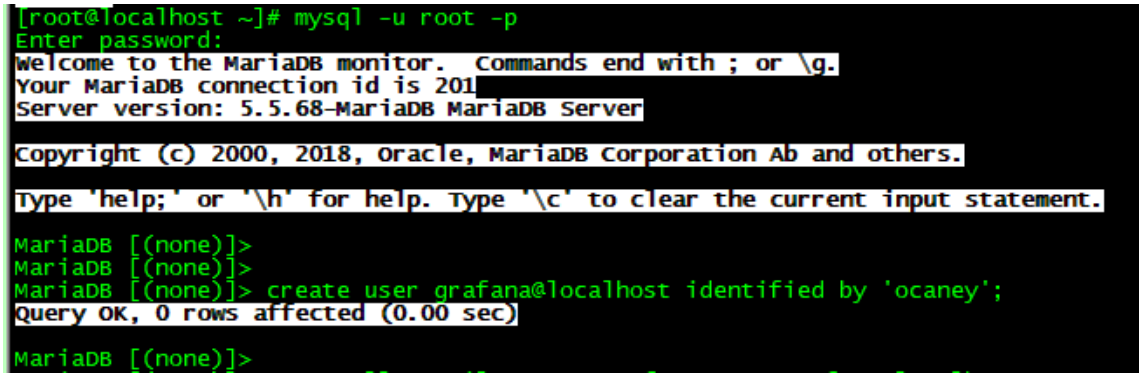
Anexo 4: Integración de Grafana a Zabbix

Para integrar Grafana al sistema de monitorización Zabbix, lo primeros que haremos es crear una base de datos en el servidor CentOS. Ejecutar los siguientes comandos para crear la base de datos en el servidor.



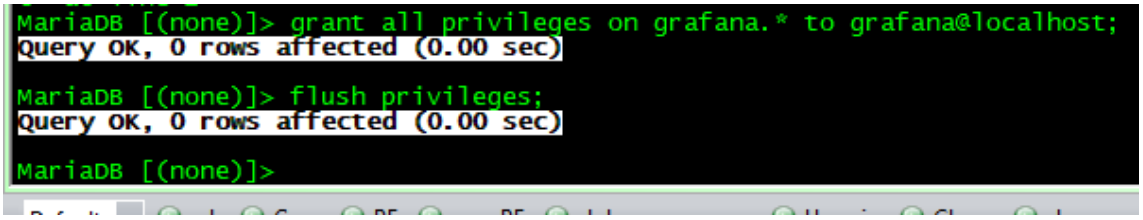
Fuente: Elaboración propia.

Luego creamos un usuario y una clave para la nueva base de datos creado. El usuario de prueba será Grafana y una clave de prueba ocaney.



Fuente: Elaboración propia.

Una vez creado la base de datos y los usuarios, le damos los privilegios y luego actualizados.



Fuente: Elaboración propia.

Ahora, procedemos a instalar Grafana en el servidor CentOS.

```
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# yum install https://dl.grafana.com/oss/release/grafana-7.4.2-1.x86_64.rpm
Complementos cargados:fastestmirror
grafana-7.4.2-1.x86_64.rpm                                  |  49 MB  00:00:10
Examinando /var/tmp/yum-root-VSUG68/grafana-7.4.2-1.x86_64.rpm: grafana-7.4.2-1.x86_64
Marcando /var/tmp/yum-root-VSUG68/grafana-7.4.2-1.x86_64.rpm para ser instalado
Resolviendo dependencias
--> Ejecutando prueba de transacciÃ³n
---> Paquete grafana.x86_64 0:7.4.2-1 debe ser instalado
--> Procesando dependencias: urw-fonts para el paquete: grafana-7.4.2-1.x86_64
Determining fastest mirrors
epel/x86_64/metalink                                        |  55 kB  00:00:00
```

Fuente: Elaboración propia.

Luego de instalar Grafana, ejecutar el comando nano /etc/grafana/grafana.ini y editamos las siguientes líneas según la base de datos que creamos al inicio del anexo 4.

```
#################################### Database ####################################
[database]
# You can configure the database connection by specifying type, host, name, user and password
# as separate properties or as on string using the url properties.

# Either "mysql", "postgres" or "sqlite3", it's your choice
type = mysql
host = 127.0.0.1:3306
name = grafana
user = grafana
# If the password contains # or ; you have to wrap it with triple quotes. Ex """#password;"""
password = ocaney

# Use either URL or the previous fields to configure the database
# Example: mysql://user:secret@host:port/database
;url =

# For "postgres" only, either "disable", "require" or "verify-full"
;ssl_mode = disable

;ca_cert_path =
;client_key_path =
;client_cert_path =
;server_cert_name =

# For "sqlite3" only, path relative to data_path setting
;path = grafana.db

# Max idle conn setting default is 2
;max_idle_conn = 2

# Max conn setting default is 0 (mean not set)
;max_open_conn =
```

Fuente: Elaboración propia.

Una vez configurado la base de datos, habilitar e iniciar Grafana con los siguientes comandos.

```
[root@localhost grafana]#
[root@localhost grafana]# systemctl enable grafana-server
Created symlink from /etc/systemd/system/multi-user.target.wants/grafana-server.s
systemd/system/grafana-server.service.
[root@localhost grafana]#
[root@localhost grafana]# systemctl deamon-reload
Unknown operation 'deamon-reload'.
[root@localhost grafana]#
[root@localhost grafana]# systemctl daemon-reload
[root@localhost grafana]#
[root@localhost grafana]# systemctl start grafana-server
[root@localhost grafana]#
[root@localhost grafana]#
```

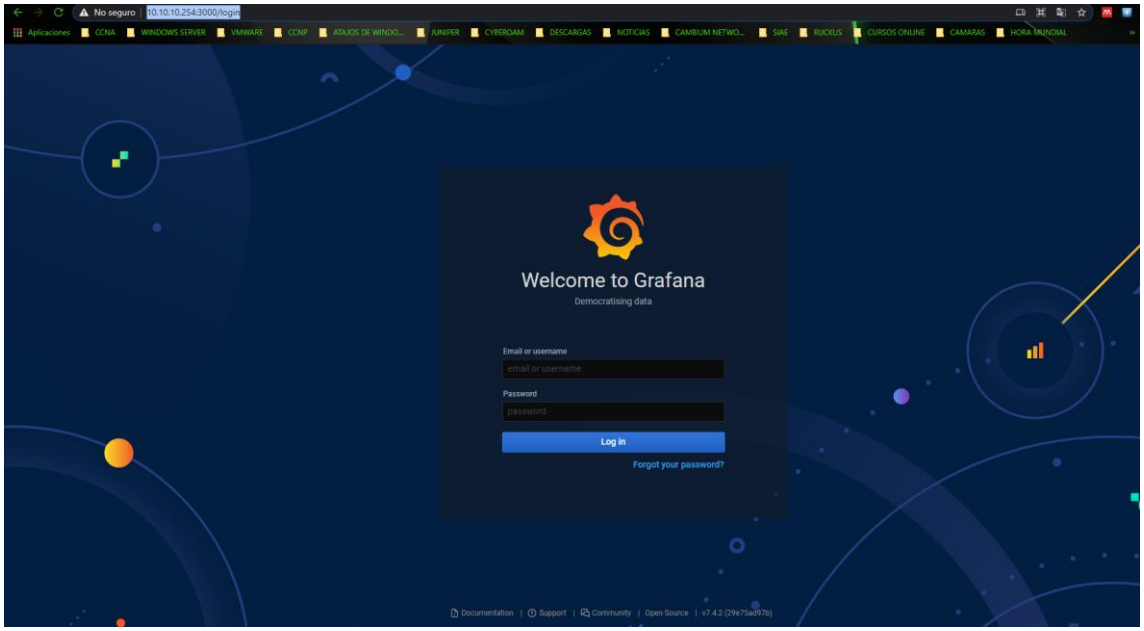
Fuente: Elaboración propia.

Ahora habilitamos el puerto 3000 que utiliza Grafana en el firewall del servidor CentOS y luego reiniciamos el firewall.

```
[root@localhost grafana]#
[root@localhost grafana]#
[root@localhost grafana]# firewall-cmd --permanent --add-port=3000/tcp
success
[root@localhost grafana]#
[root@localhost grafana]# firewall-cmd --reload
success
[root@localhost grafana]#
[root@localhost grafana]#
```

Fuente: Elaboración propia.

Finalmente, ingresamos por navegador por web http://ip_servidor/3000, usuario y clave por default admin/admin. Una vez ingresado solicitará cambiar clave.



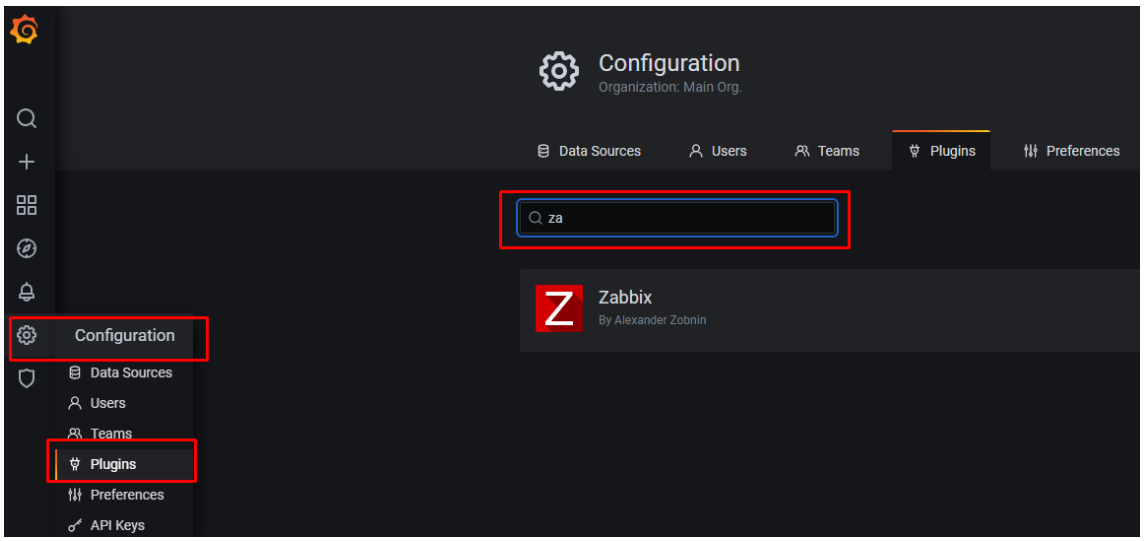
Fuente: Elaboración propia.

Hasta el momento solo se instaló Grafana, el siguiente paso es integrarlo con Zabbix, para ello ejecutamos el siguiente comando en el servidor CentOS y reiniciamos nuevamente Grafana.

```
[root@localhost grafana]#
[root@localhost grafana]# grafana-cli plugins install alexanderzobnin-zabbix-app
installing alexanderzobnin-zabbix-app @ 4.1.2
from: https://grafana.com/api/plugins/alexanderzobnin-zabbix-app/versions/4.1.2/download
into: /var/lib/grafana/plugins

âœ" Installed alexanderzobnin-zabbix-app successfully

Restart grafana after installing plugins . <service grafana-server restart>

[root@localhost grafana]# service grafana-server restart
Restarting grafana-server (via systemctl):                 [  OK  ]
[root@localhost grafana]#
[root@localhost grafana]#
```

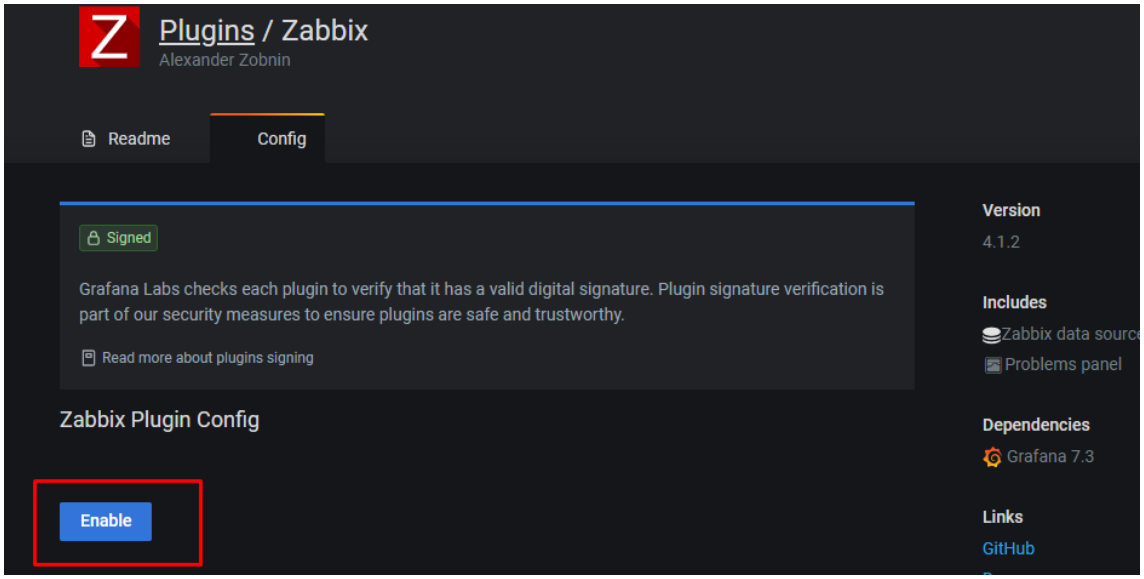
Fuente: Elaboración propia.

Luego ingresamos por web a Grafana y buscamos Zabbix, con se detalla en la siguiente imagen.



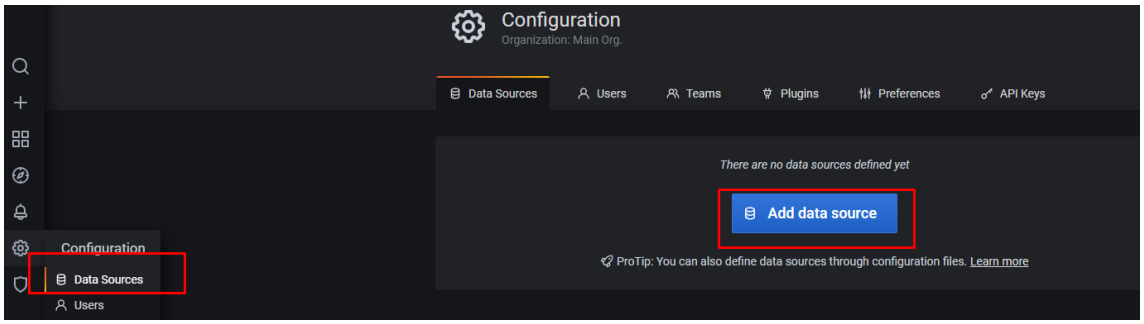
Fuente: Elaboración propia.

Una vez seleccionado, habilitamos el plugin de Zabbix.



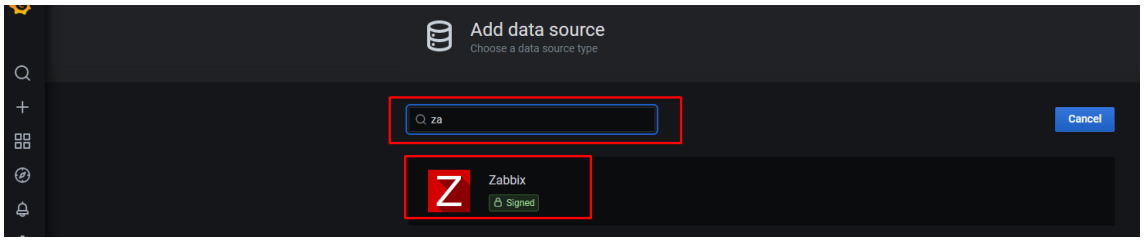
Fuente: Elaboración propia.

Luego de habilitar el plugin de Zabbix, agregamos la fuente de los datos siguiendo los pasos de la siguiente imagen.

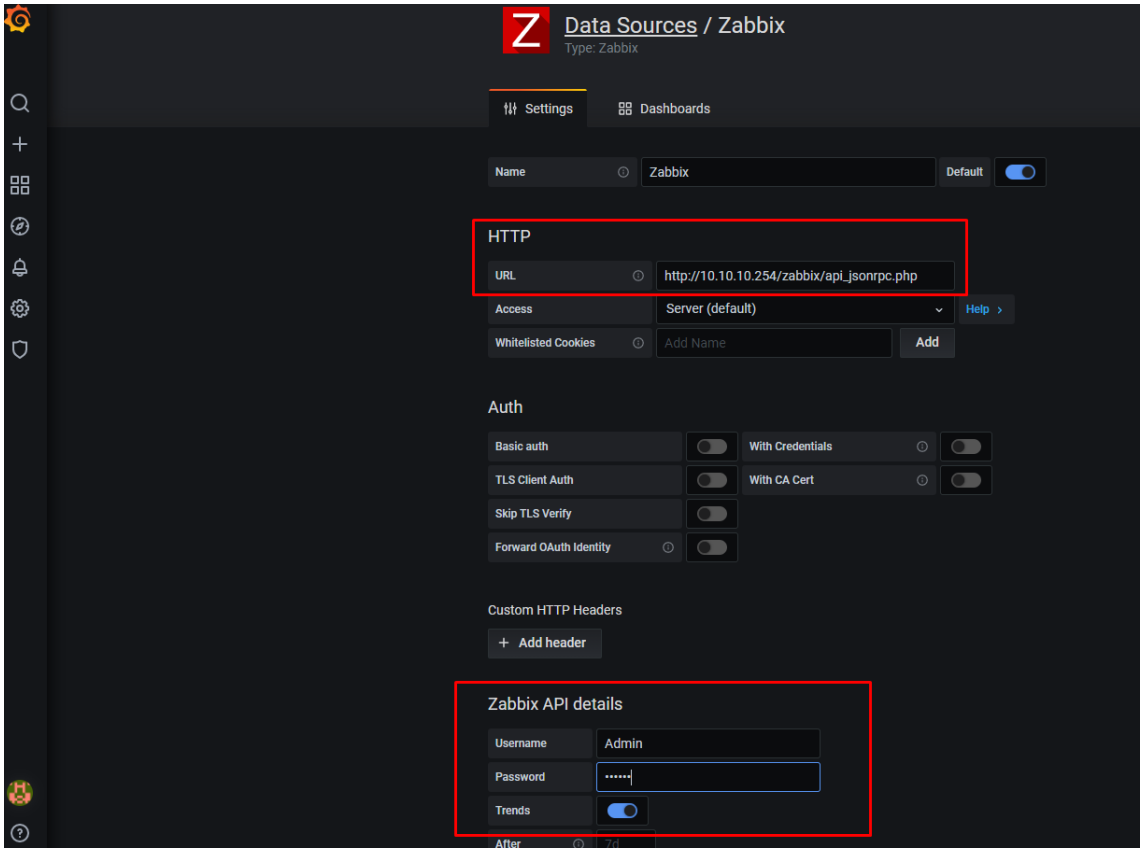


Fuente: Elaboración propia.

Buscamos Zabbix y lo seleccionamos

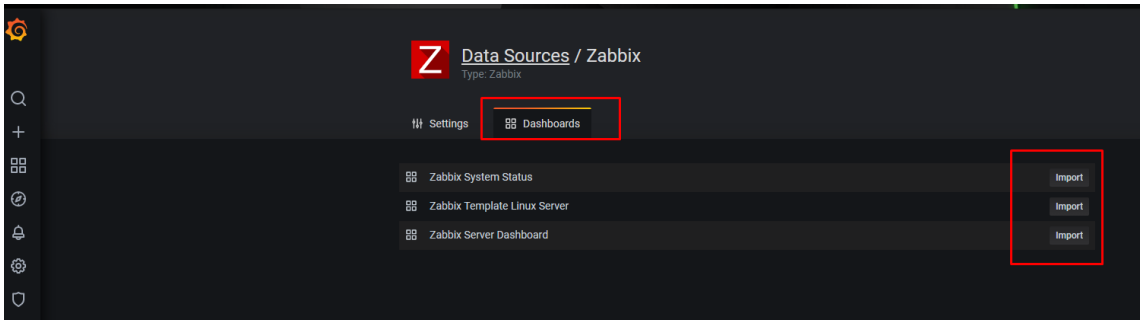


En ajustes, agregamos a dirección del sistema de monitorización Zabbix y le agregamos la extensión /api_jsonrpc.php y en la sección de detalles de la API de Zabbix, ingresamos el usuario y clave que usamos para ingresar a Zabbix.



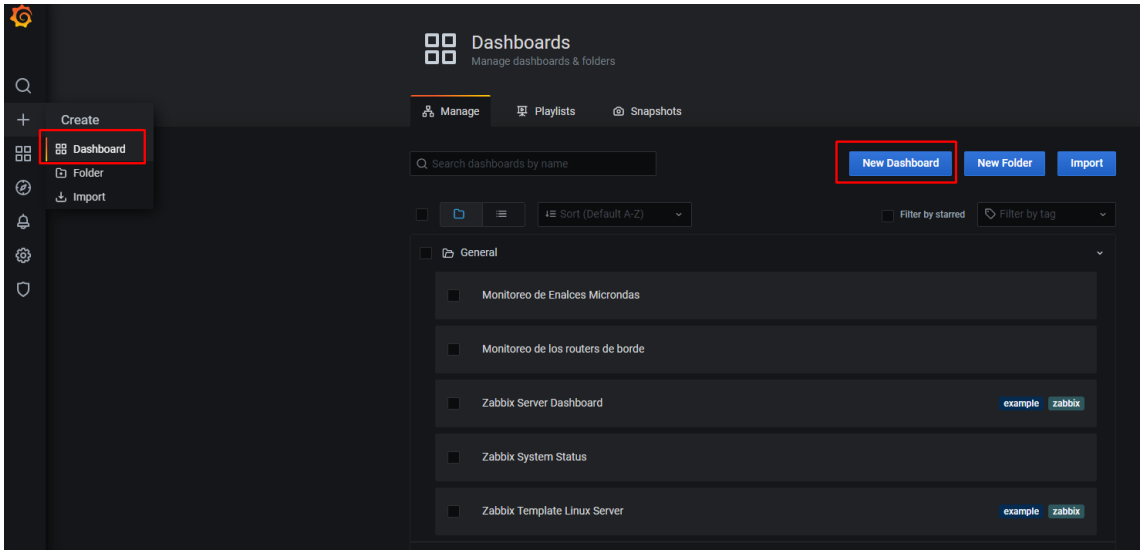
Fuente: Elaboración propia.

Una vez integrado Grafana con Zabbix, importamos los templates por default.



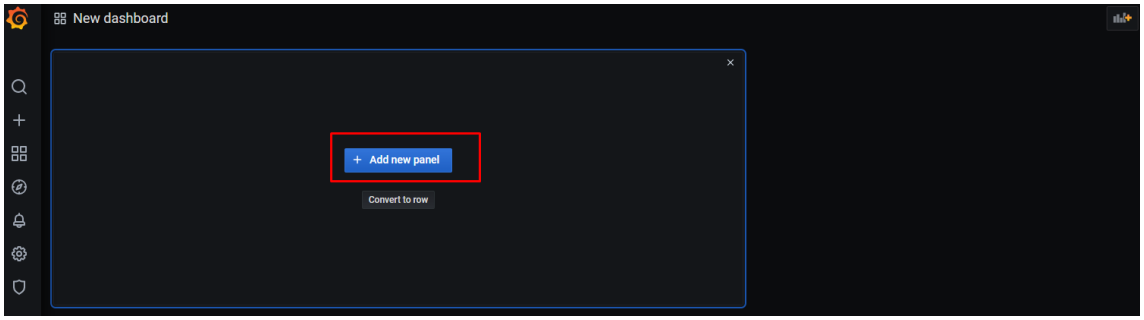
Fuente: Elaboración propia.

Finalmente, ahora podemos personalizar los paneles para empezar a monitorear la red.



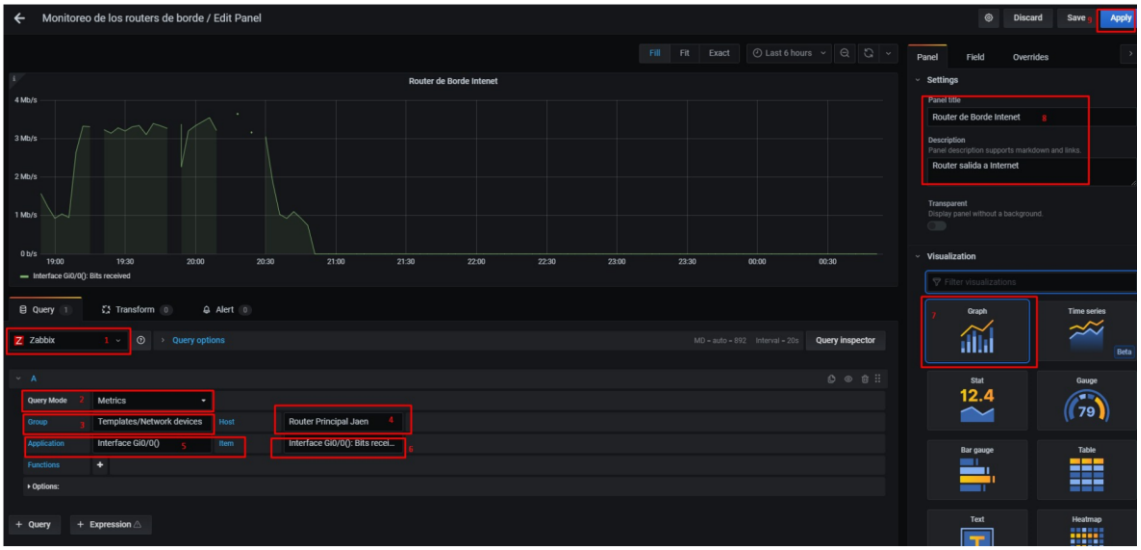
Fuente: Elaboración propia.

Agregamos un nuevo panel



Fuente: Elaboración propia.

Personalizamos el panel de acuerdo con nuestros requerimientos, siguiendo los pasos de acuerdo con la siguiente imagen.



Fuente: Elaboración propia.

Vista general de monitoreo de redes, luego de personalizar los paneles

Fuente: Elaboración propia.

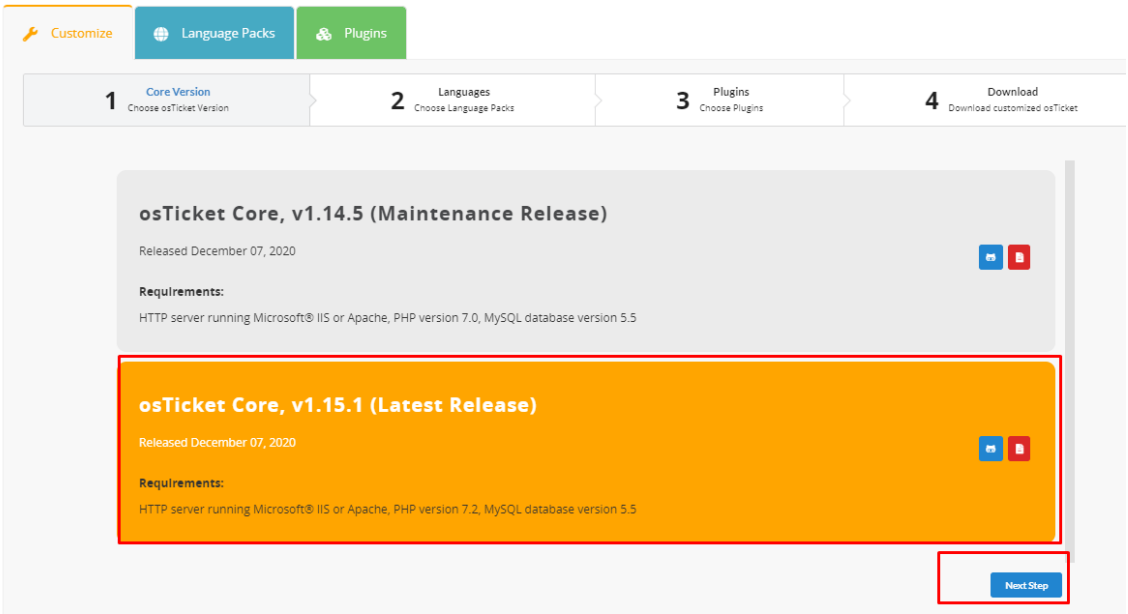
Anexo 5: Implementación de OsTicket

Creamos BD en el servidor CentOS con el nombre de prueba osTicket y usuario osTicket y clave ost-TICK5w%6d. Luego le brindamos el privilegio al usuario creado anteriormente.

```
mysql>
mysql> create database osTicket;
Query OK, 1 row affected (0.01 sec)

mysql>
mysql> create user osTicket@localhost identified by 'ocaney';
ERROR 1819 (HY000): Your password does not satisfy the current policy requirements
mysql>
mysql> create user osTicket@localhost identified by 'ost-TICK5w%6d';
Query OK, 0 rows affected (0.00 sec)

mysql>
mysql> grant all privileges on osTicket.* to osTicket@localhost;
Query OK, 0 rows affected (0.01 sec)

mysql> flush privileges;
Query OK, 0 rows affected (0.00 sec)

mysql>
```

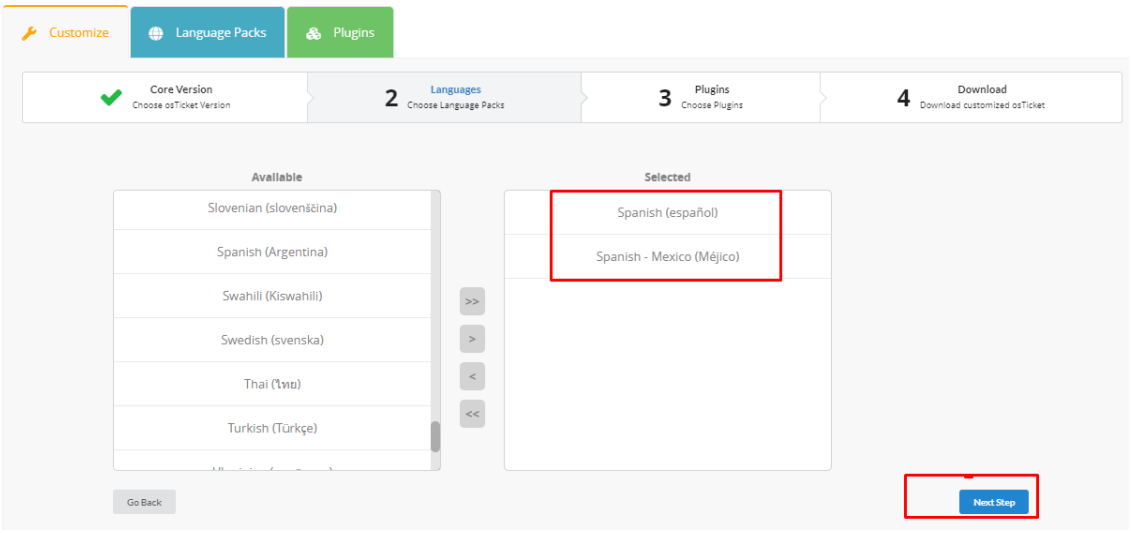
Fuente: Elaboración propia.

Luego desde la página web oficial de osTicket https://osticket.com/download/ descargar la versión v1.15.1



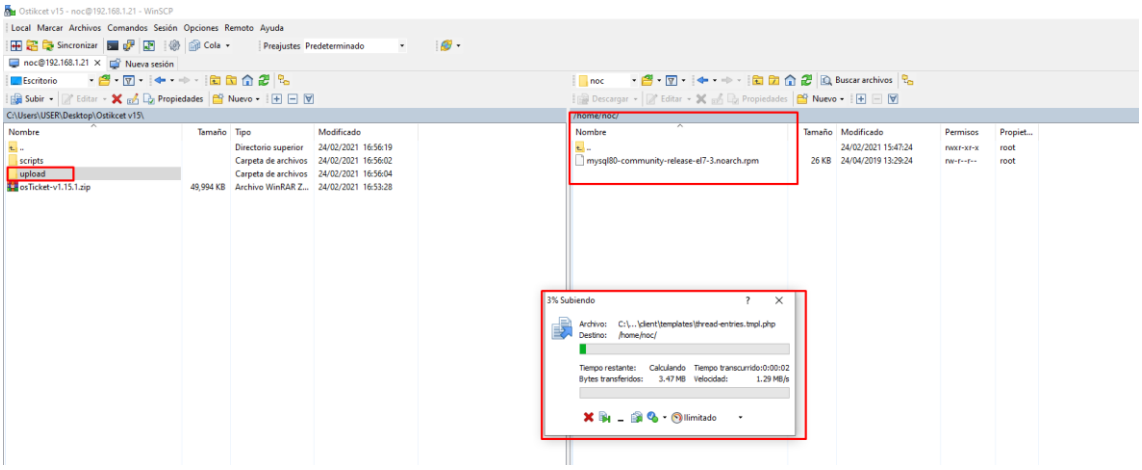
Fuente: (osTicket, 2020)

Seleccionamos el idioma español y le damos en continuar y descargar.



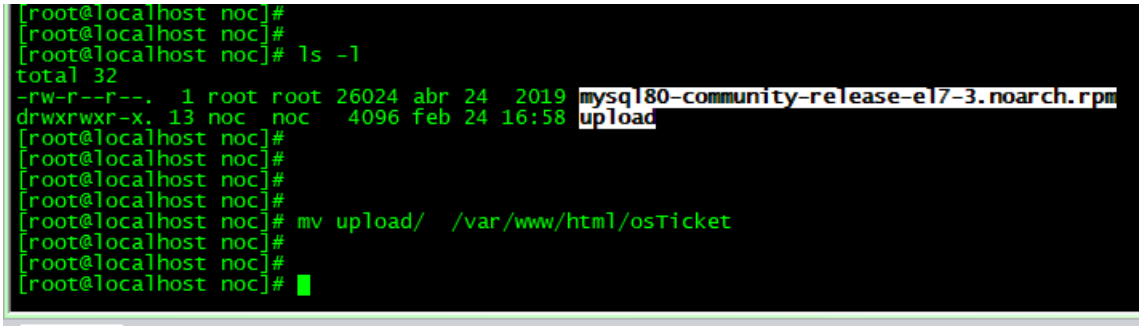
Fuente: (osTicket, 2020)

Con la ayuda de un cliente SFP, transferir el archivo descargado al servidor CentOS.



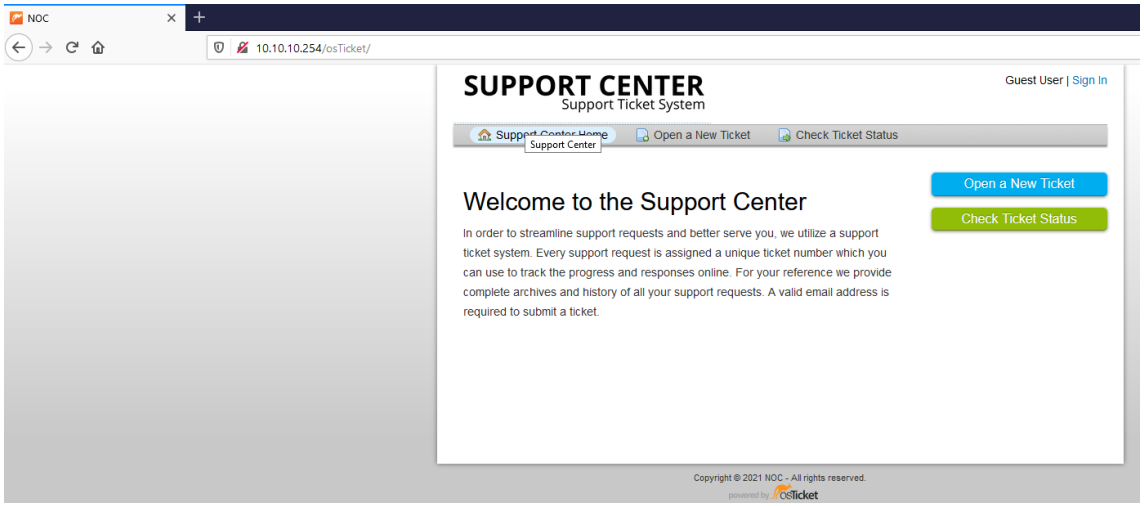
Fuente: Elaboración propia.

Luego de copiar el archivo descargado, mover al directorio de osTicket.



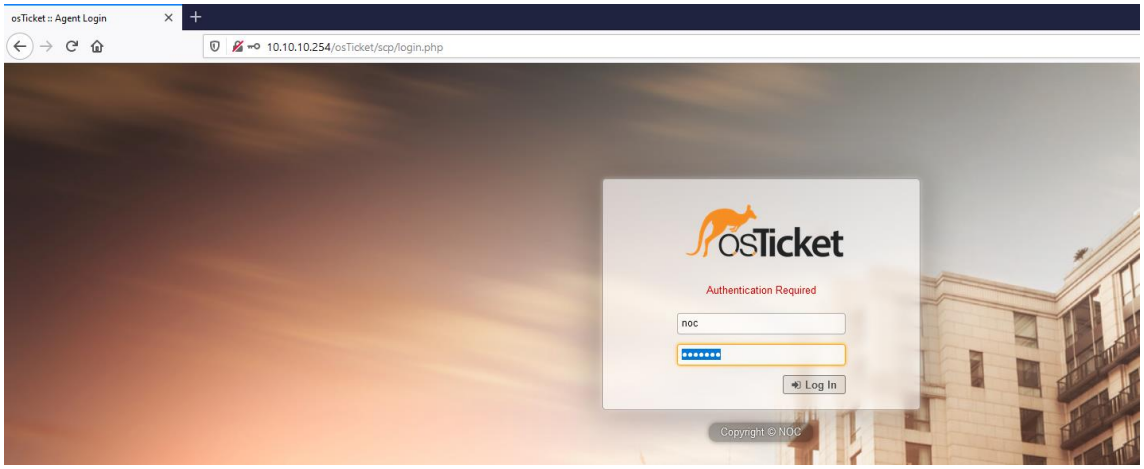
Fuente: Elaboración propia.

Una vez configurado, ingresado por navegador a la dirección del servidor /osTicket



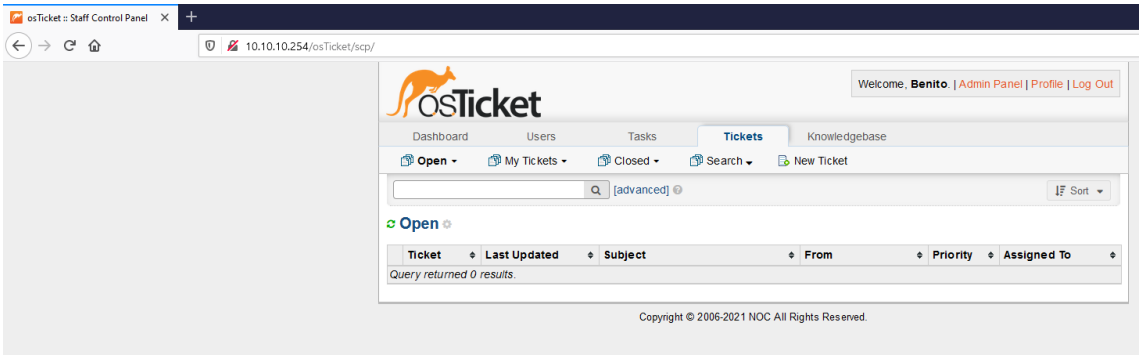
Fuente: Elaboración propia.

Para revisión de tique por parte del NOC, ir a la opción registro e ingresar con las credenciales creados al momento de la instalación.



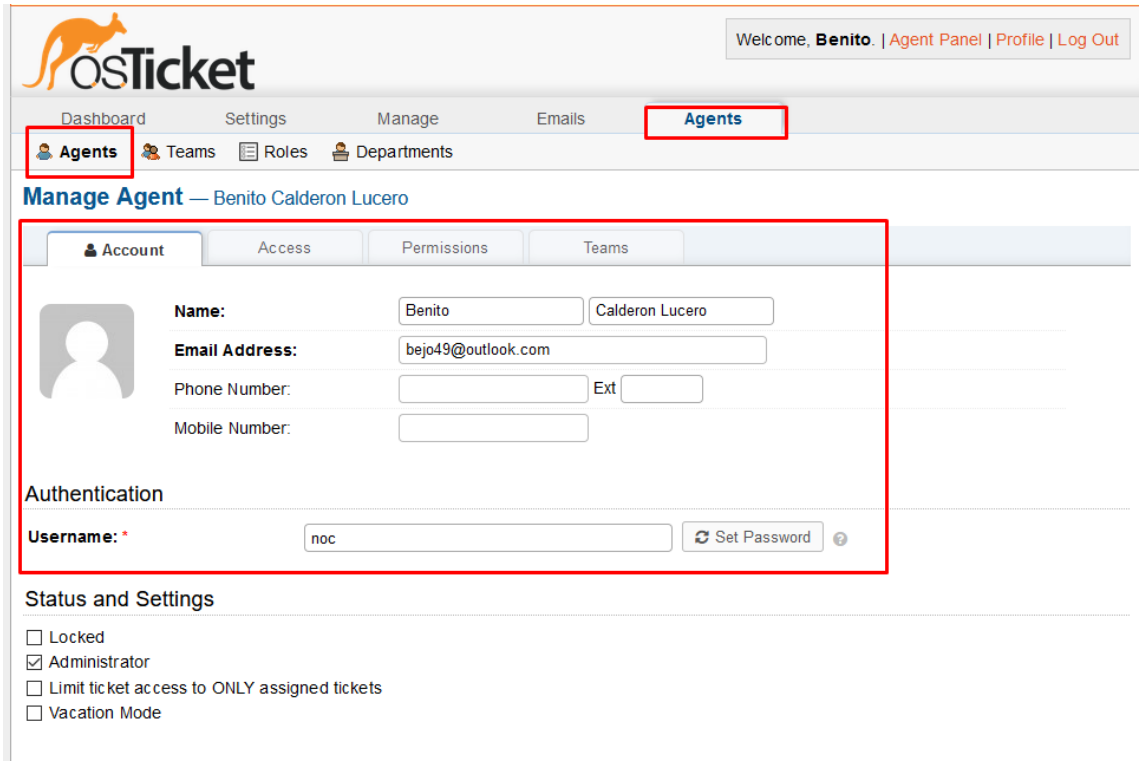
Fuente: Elaboración propia.

Pantalla principal, para gestionar los tiques por parte del personal del NOC en la empresa Interconexiones Ocaney.



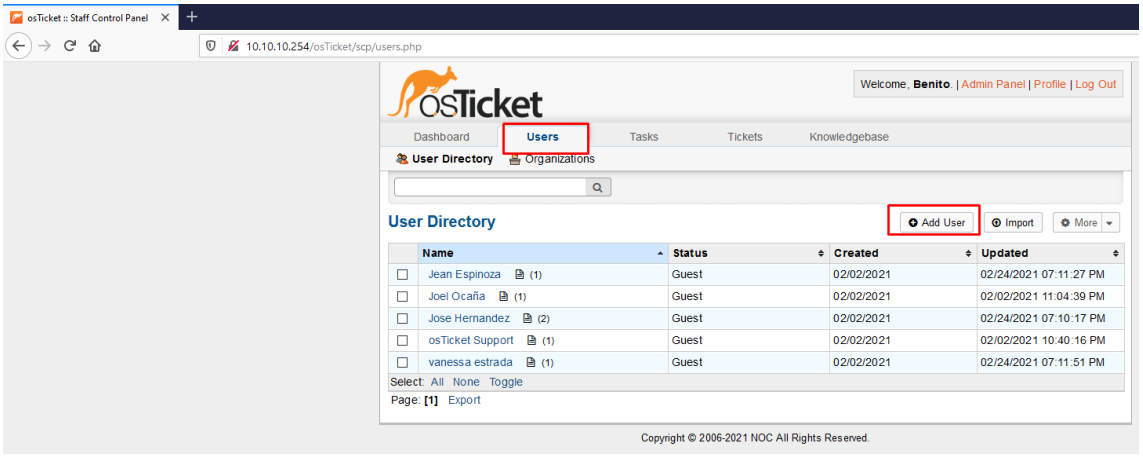
Fuente: Elaboración propia.

Para crear un nuevo agente para la atención de las incidencias y requerimientos ir a la pestaña agentes y llenar el formulario como se observa en la imagen.



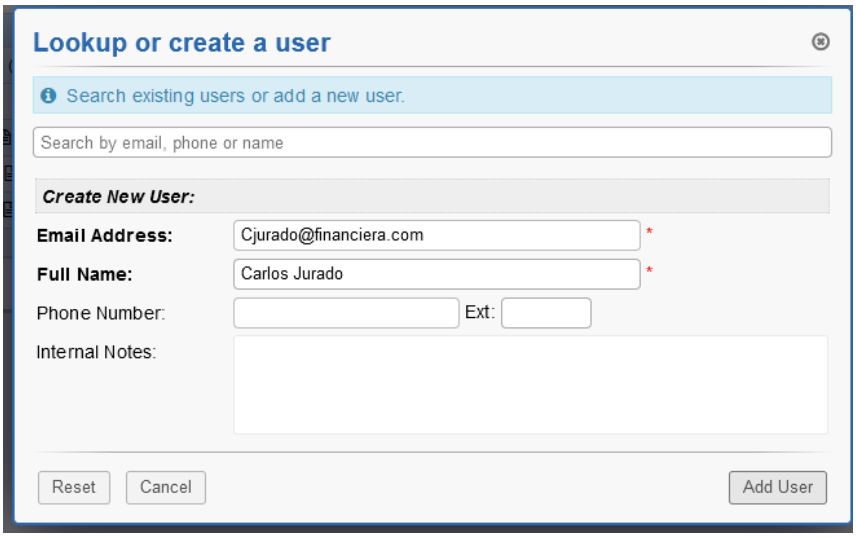
Fuente: Elaboración propia.

Para registrar un nuevo usuario y a que empresa pertenece, ir a user y agregar el nuevo usuario.



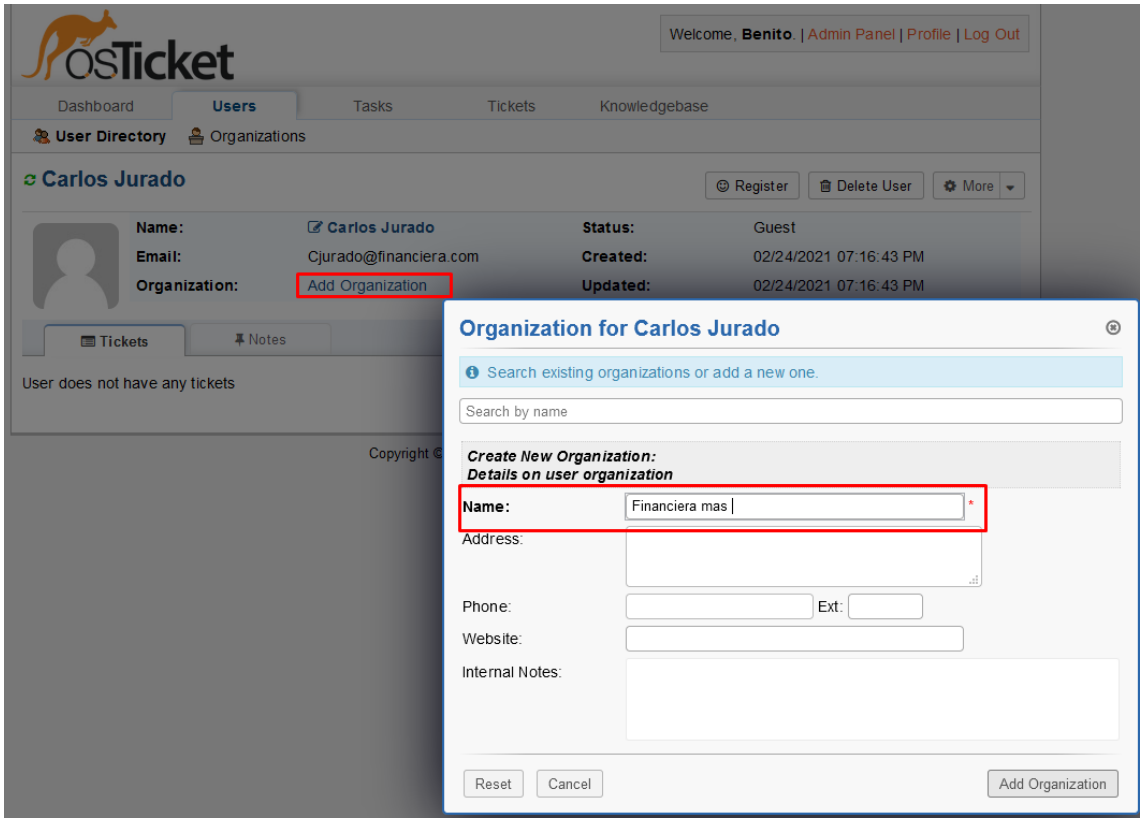
Fuente: Elaboración propia.

Rellenamos los datos del nuevo usuario y le damos a agregar.



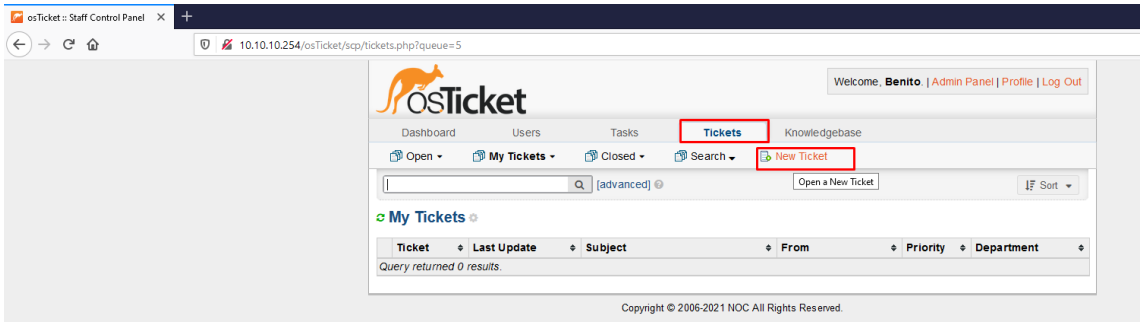
Fuente: Elaboración propia.

En la sección organización, ingresamos a la empresa que pertenece dicho usuario.



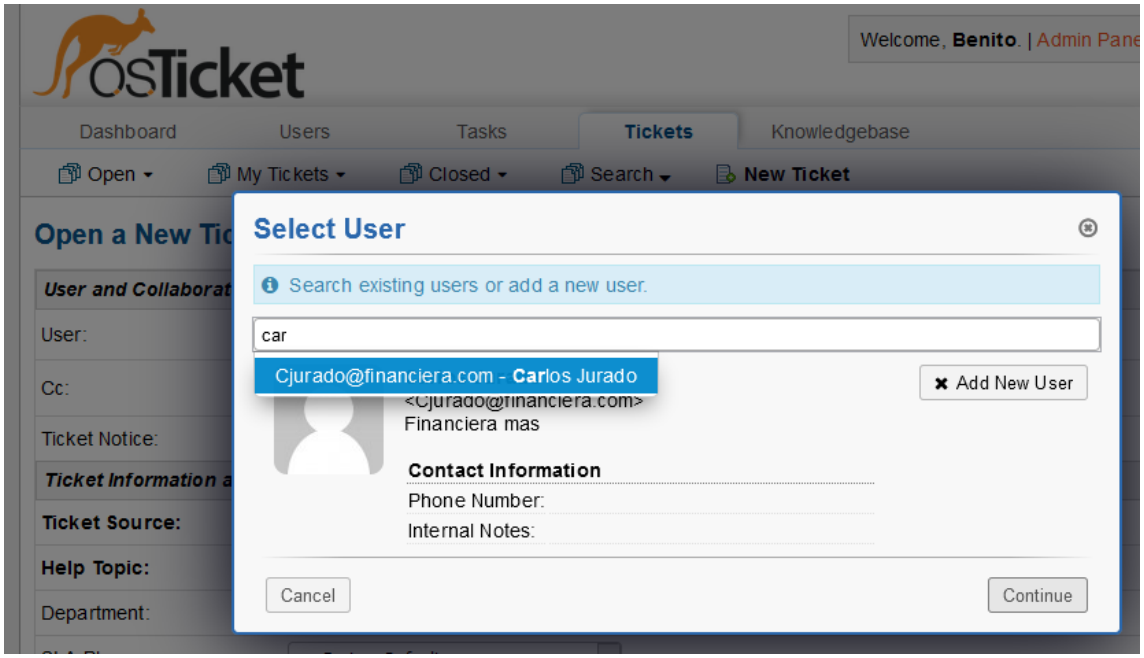
Fuente: Elaboración propia.

Para registrar un tique por incidencia o requerimiento, ir a la pestaña tique y seleccionar new tique.



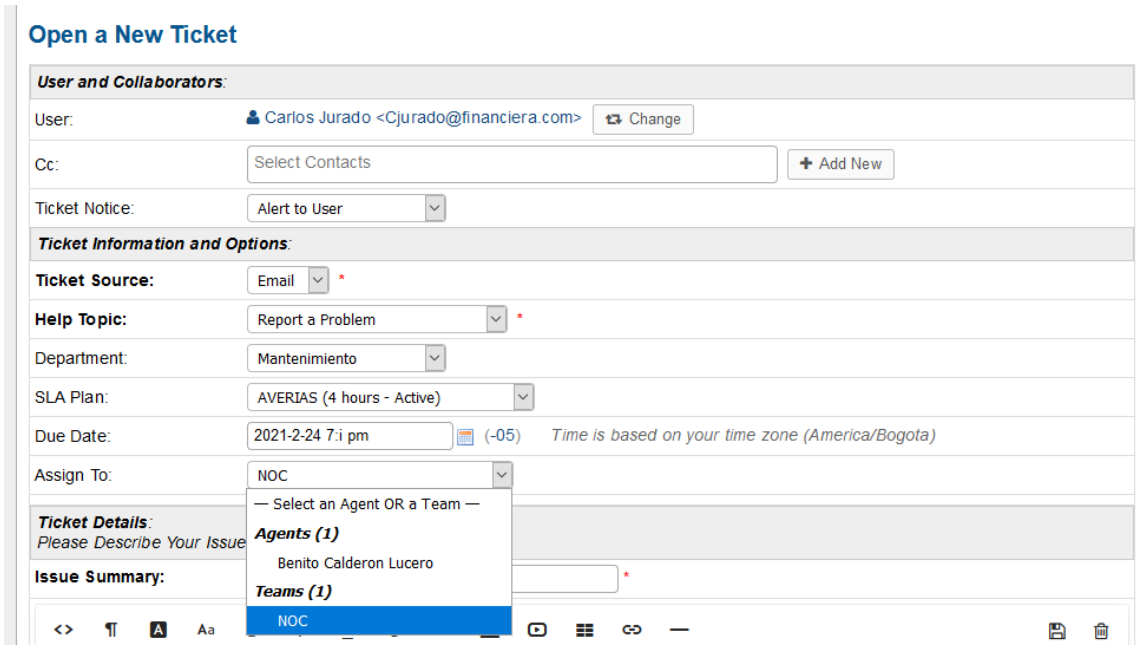
Fuente: Elaboración propia.

Luego en la ventana emergente, buscamos el nombre del usuario que está reportando la incidencia o requerimiento, en caso de que no esté registrado aún, seleccionamos add new user.



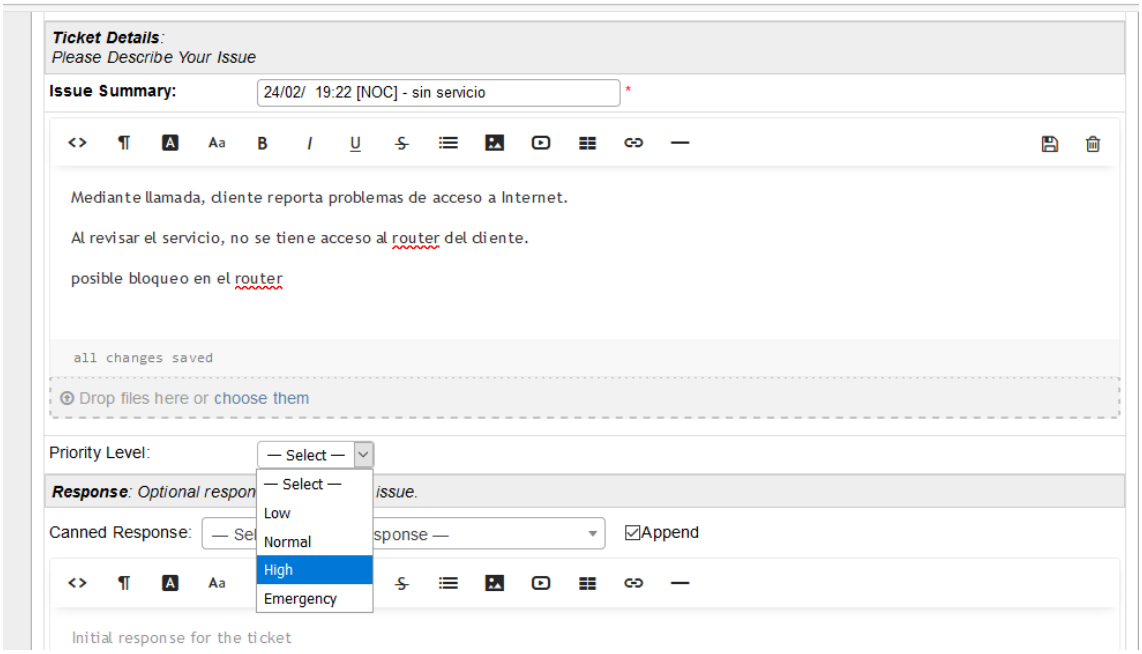
Fuente: Elaboración propia.

Una vez que seleccionamos el usuario que reporta el problema, llenar los siguientes campos como se observa en la imagen. Seleccionamos el departamento que lo va a atender, el SLA según sea el caso, avería (4 horas), requerimiento (24horas), la hora de vencimiento del tique y el agente que lo va a atender.



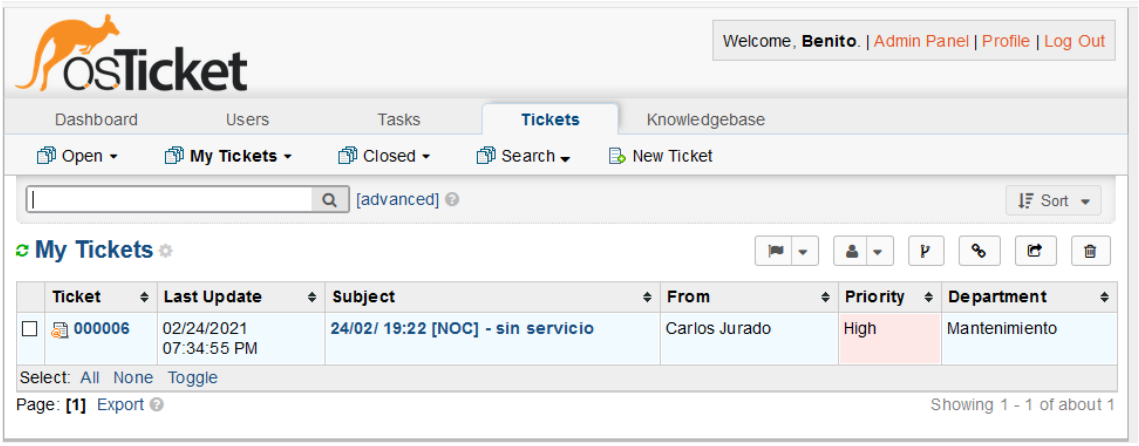
Fuente: Elaboración propia.

Seguidamente, se debe de llenar resumen del problema en el formato hora/estado/problema y luego detallar el problema que está reportando el cliente tal como se observa en la siguiente imagen.



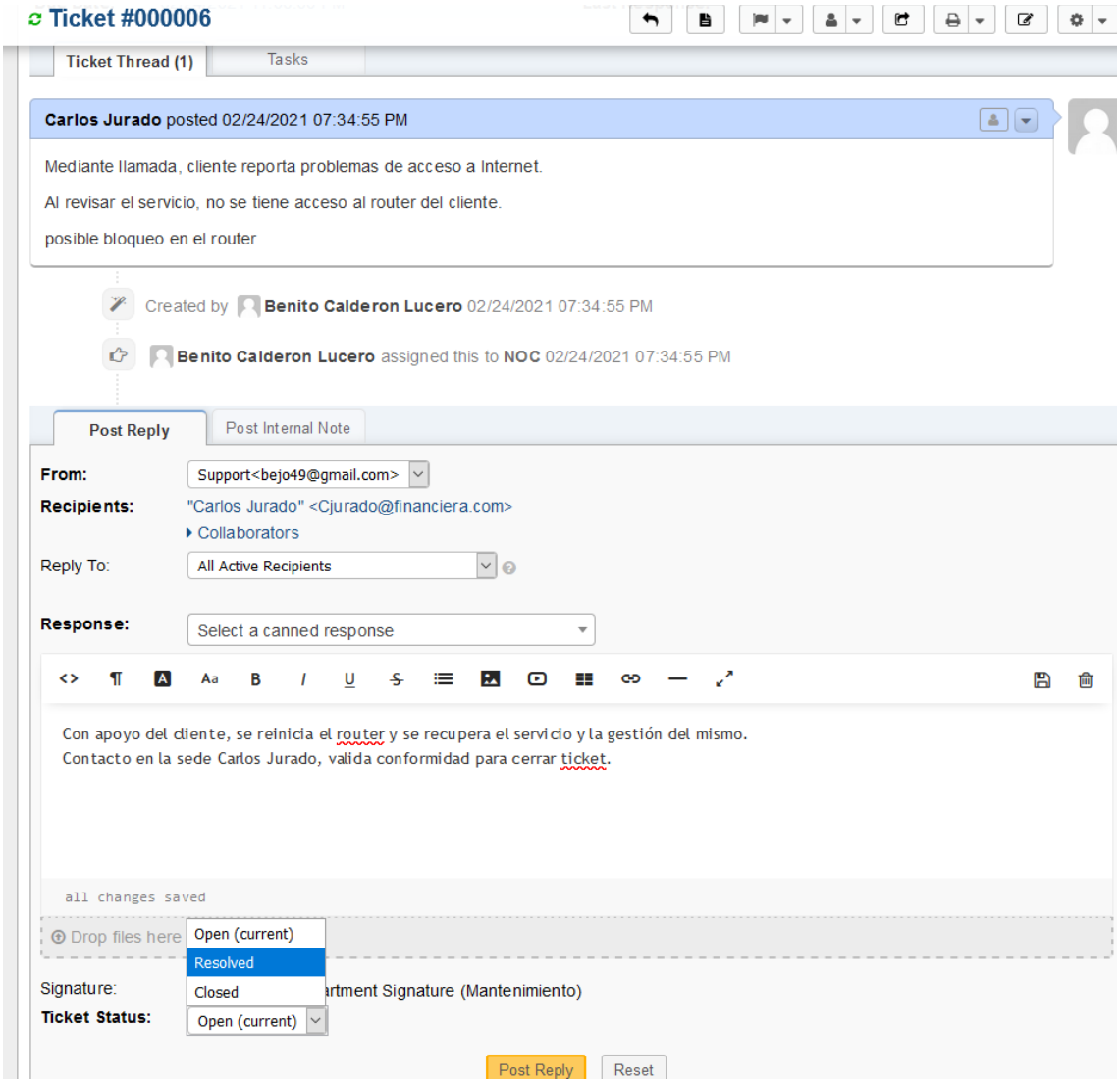
Fuente: Elaboración propia.

Resumen del tique creado para la atención y asignado a un agente.



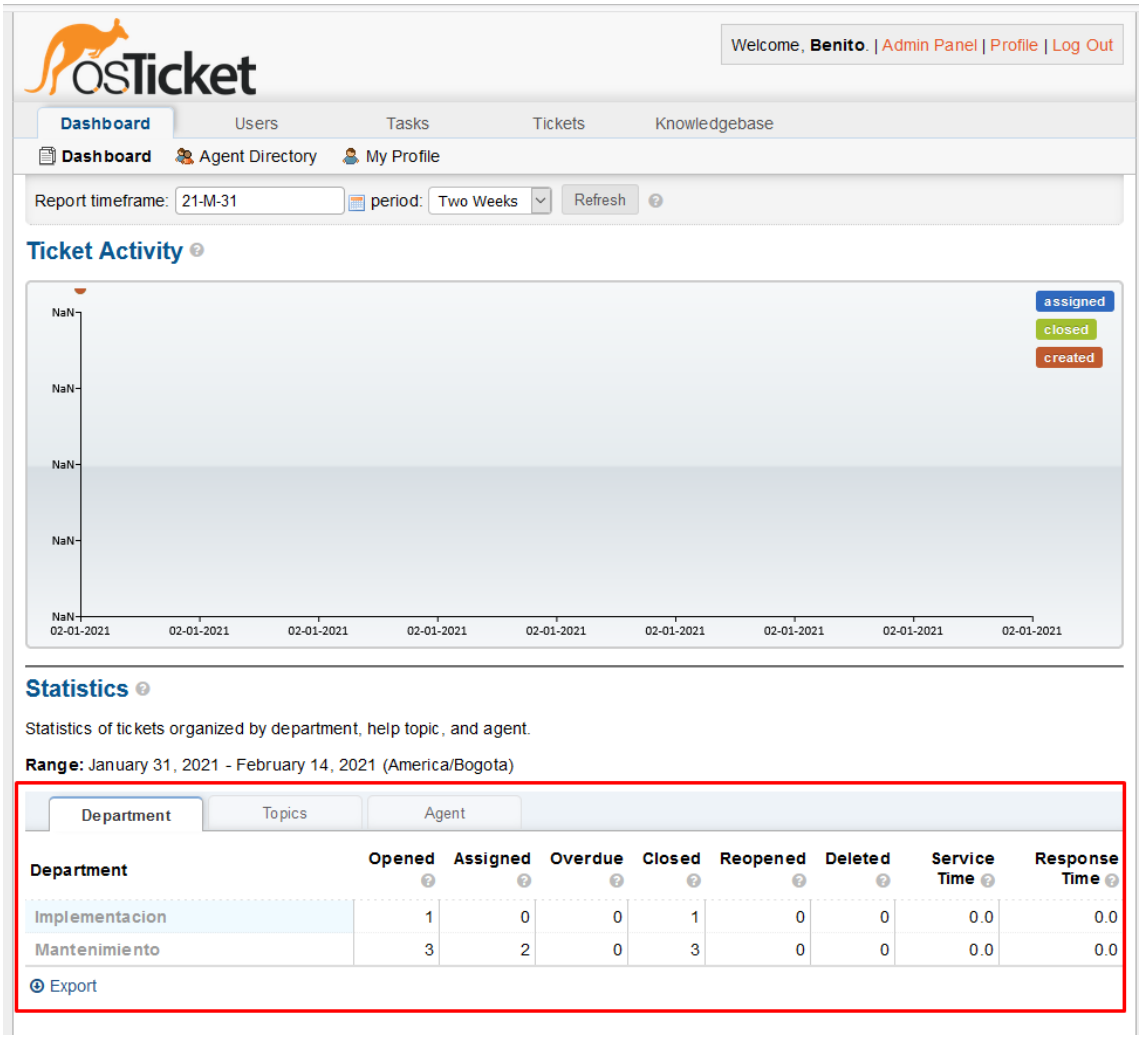
Fuente: Elaboración propia.

Finalmente, una vez que se resuelve el problema, se debe poner estado del tique en resuelto, tal como se observa en la imagen.



Fuente: Elaboración propia.

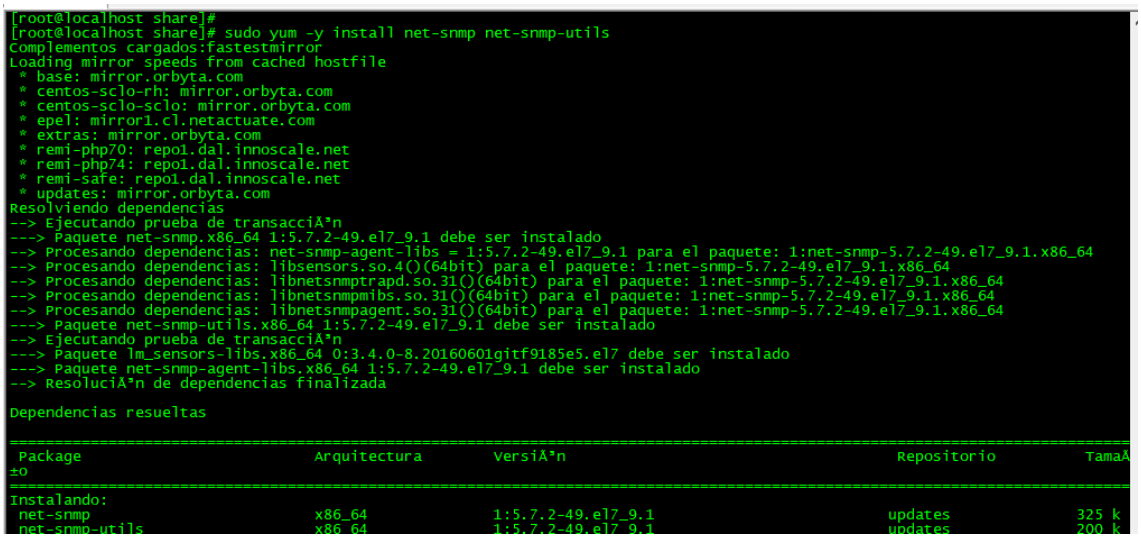
La aplicación osTicket nos permite sacar reportes del historial de las incidencias y requerimientos por departamento, agentes o tipo de problema y exportar en Excel para medir las métricas de las atenciones y tomar acciones de mejoras si fuera necesario.



Fuente: Elaboración propia.

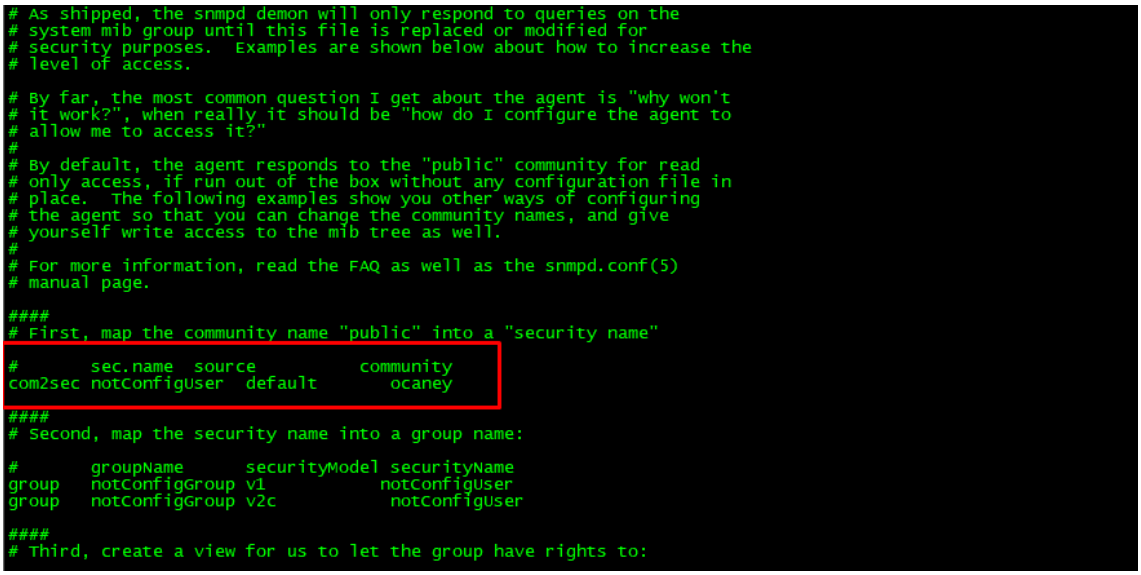
Anexo 6: Configuración de SNMP

Habilitamos y configuramos SNMP en los dispositivos de red a monitorear, se requiere una comunidad (clave) y la IP del servidor donde se encuentra alojado la herramienta de monitoreo (Zabbix). Procedemos a instalar SNMP en el servidor con el comando yum -y install net-snmp net-snmp-utils



Fuente: Elaboración propia.

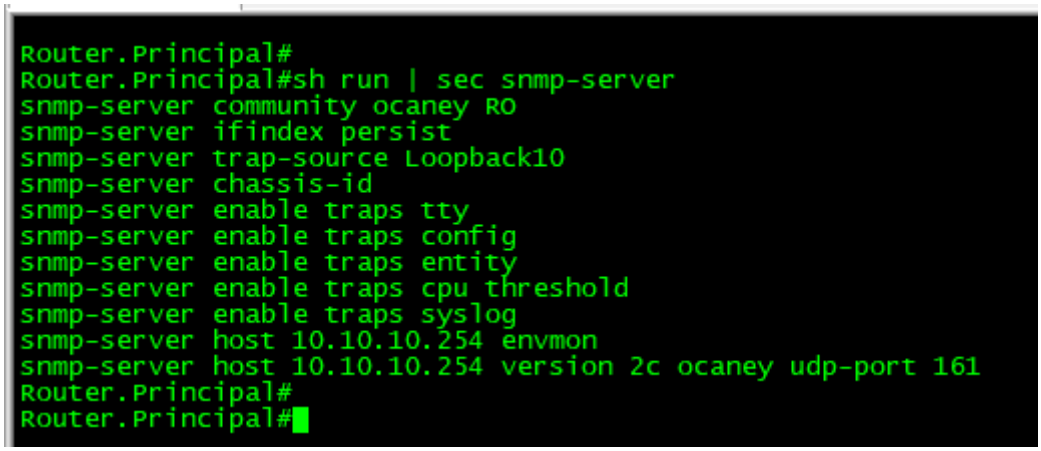
Una vez instalado SNMP, procedemos a instalar y configurar la comunidad que nosotros elijamos, ejecutando el comando nano /etc/snmp/snmpd.conf guardamos y salimos.



Fuente: Elaboración propia.

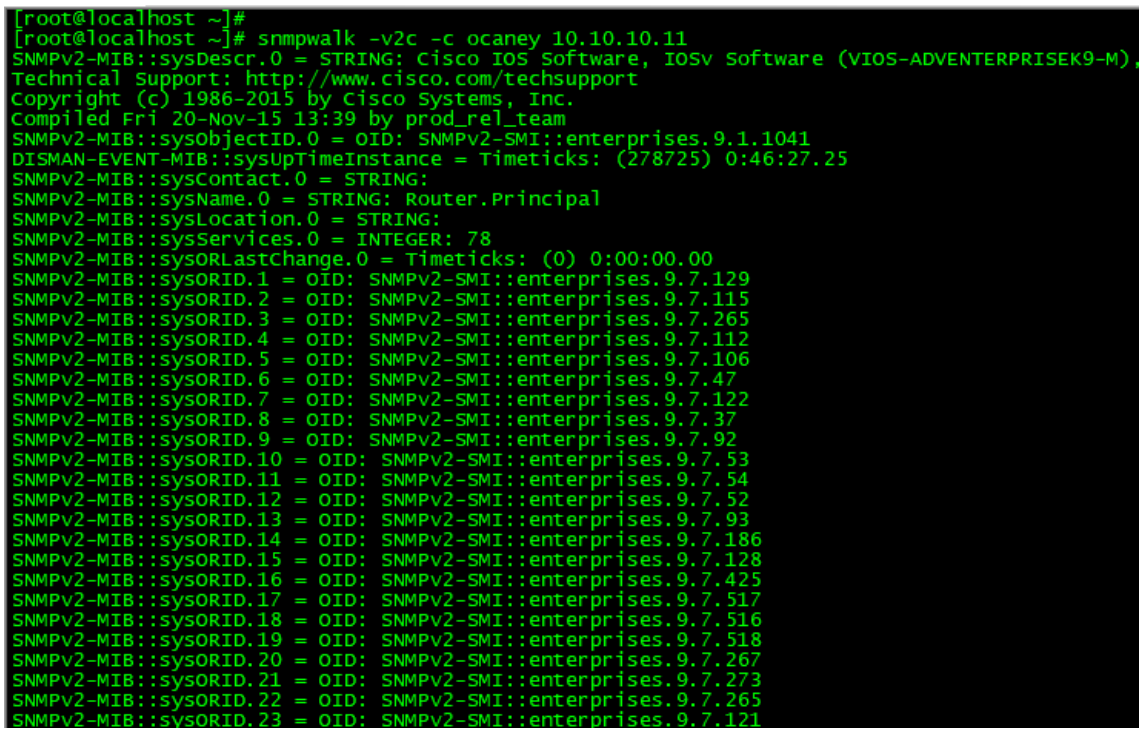
Configuración de SNMP en dispositivos cisco

Para habilitar SNMP en los dispositivos cisco se requiere la comunidad, interface que se va a utilizar para el envío de los mensajes, IP del servidor y el puerto que se va a utilizar, por default es 161.



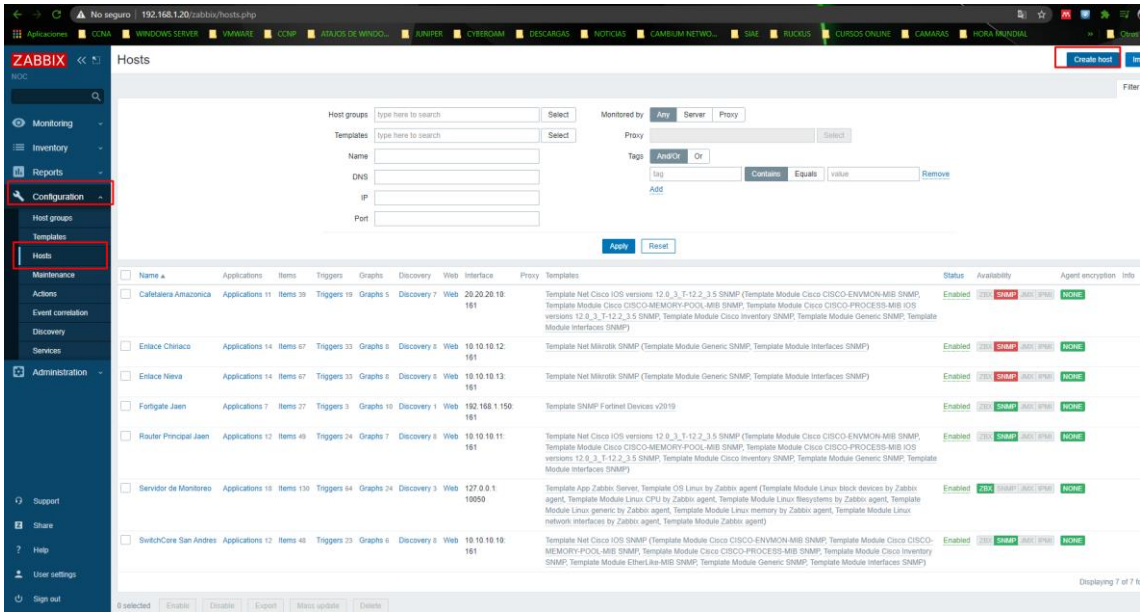
Fuente: Elaboración propia.

Una vez configurado en el router, ejecutar le comando snmpwalk -v2c -c ocaney 10.10.10.11 en el servidor para validar la conectividad SNMP entre el dispositivo a monitorear y el servidor.



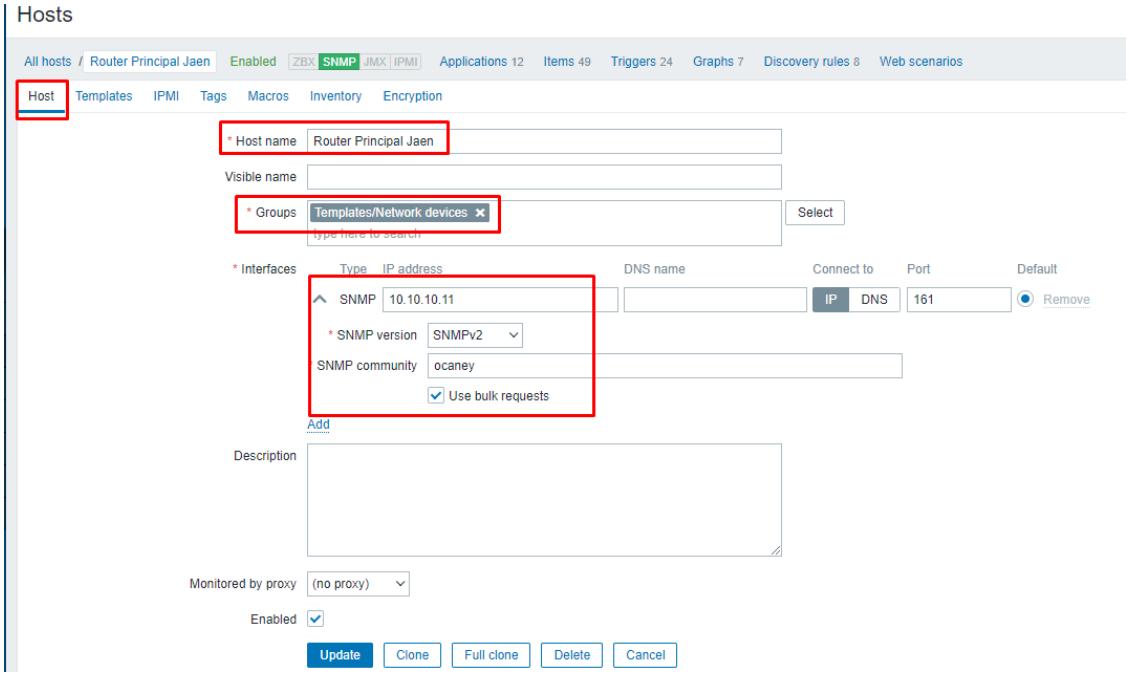
Fuente: Elaboración propia.

Una vez configurado y validado conectividad, registramos el dispositivo de red a la herramienta de monitoreo. Ingresamos a Zabbix mediante navegador web, vamos al a opción configuración, luego host y elegimos crear nuevo host.



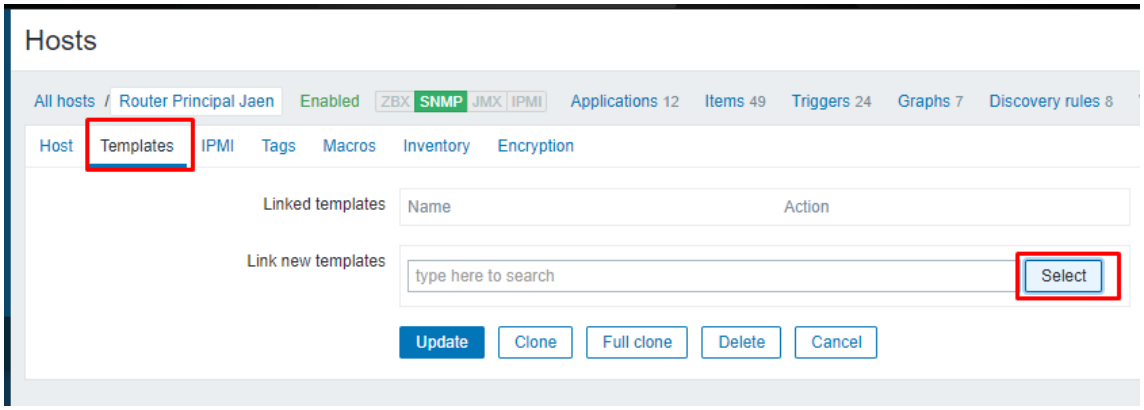
Fuente: Elaboración propia.

En la pestaña host, elegimos un nombre, seleccionamos el tamplate y en la opción interfaces ponemos la IP el dispositivo a monitorear y la comunidad.



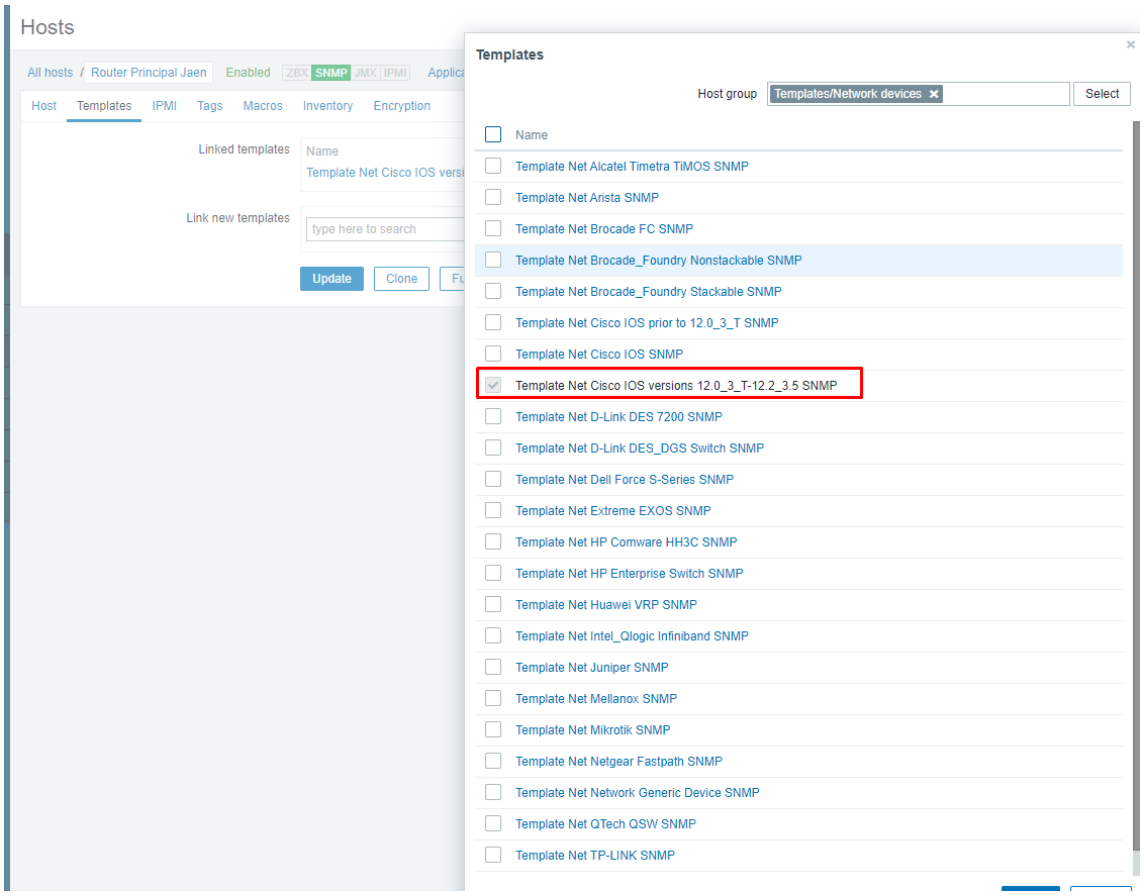
Fuente: Elaboración propia.

En la pestaña template, seleccionamos select



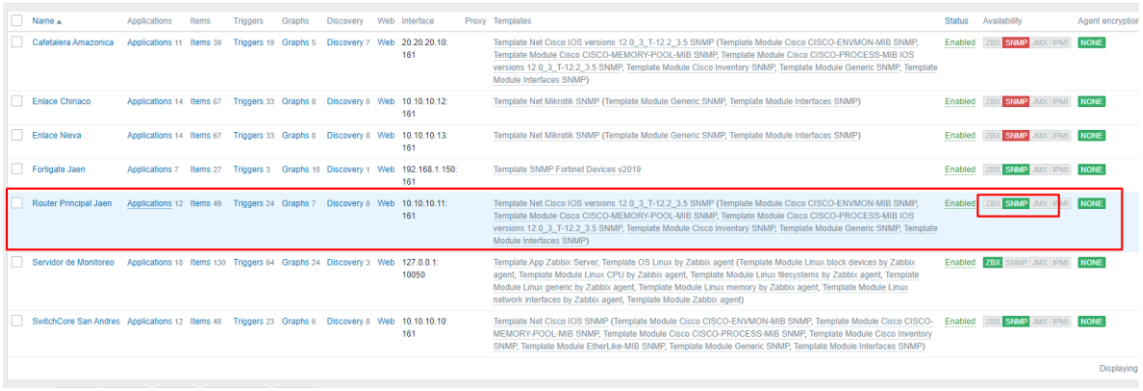
Fuente: Elaboración propia.

Elegimos el template para cisco y agregamos el dispositivo.



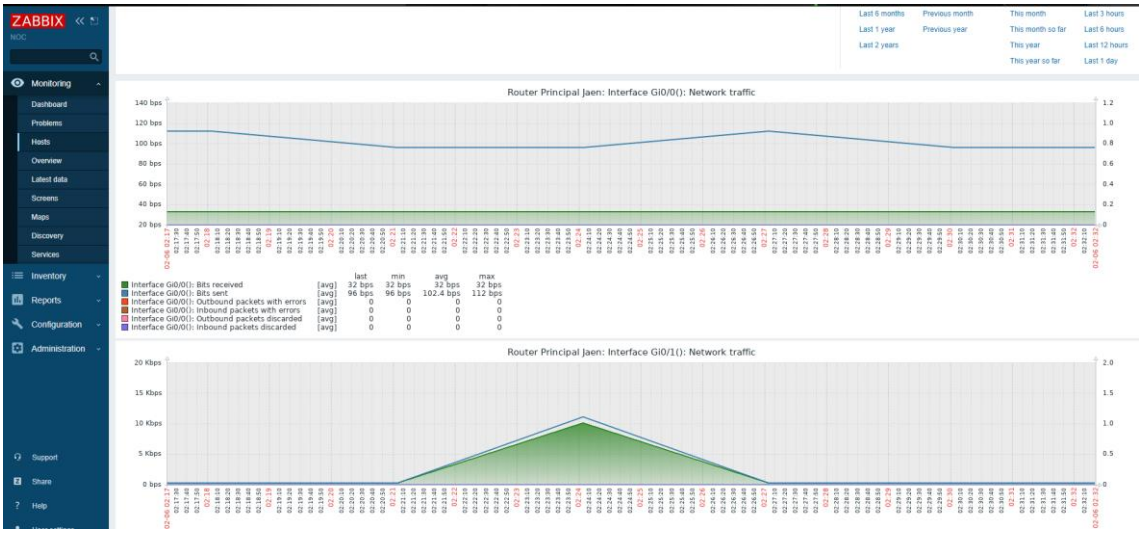
Fuente: Elaboración propia.

Una vez que agregado, debe aparecer la opción SNMP en verde, lo cual indica que ya lo registramos correctamente.



Fuente: Elaboración propia.

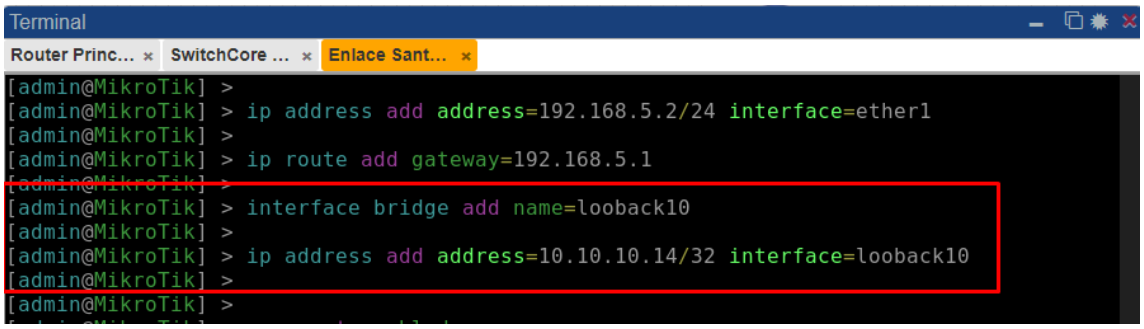
Una vez registrado ya nos graficará el estado de salud del dispositivo de red cisco.



Fuente: Elaboración propia.

Configuración de SNMP en los enlaces microondas MikroTik

Para habilitar SNMP en los enlaces microondas Mikrotik, se requiere la comunidad, una interface Loopback. Creamos una interface lógica para el monitoreo de los dispositivos Mikrotik y le asignamos una IP.

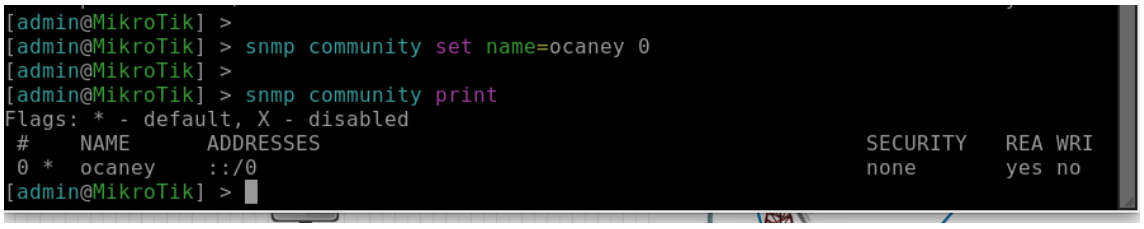


Fuente: Elaboración propia.

Con el siguiente comando habilitamos el servicio SNMP en el dispositivo MikroTik. Y luego ejecutamos el comando print para enumerar las comunidades SNMP disponibles.

Fuente: Elaboración propia.

Luego usamos el siguiente comando para cambiar el nombre de la comunidad PUBLIC SNMP por la comunidad que vamos a utilizar nosotros.



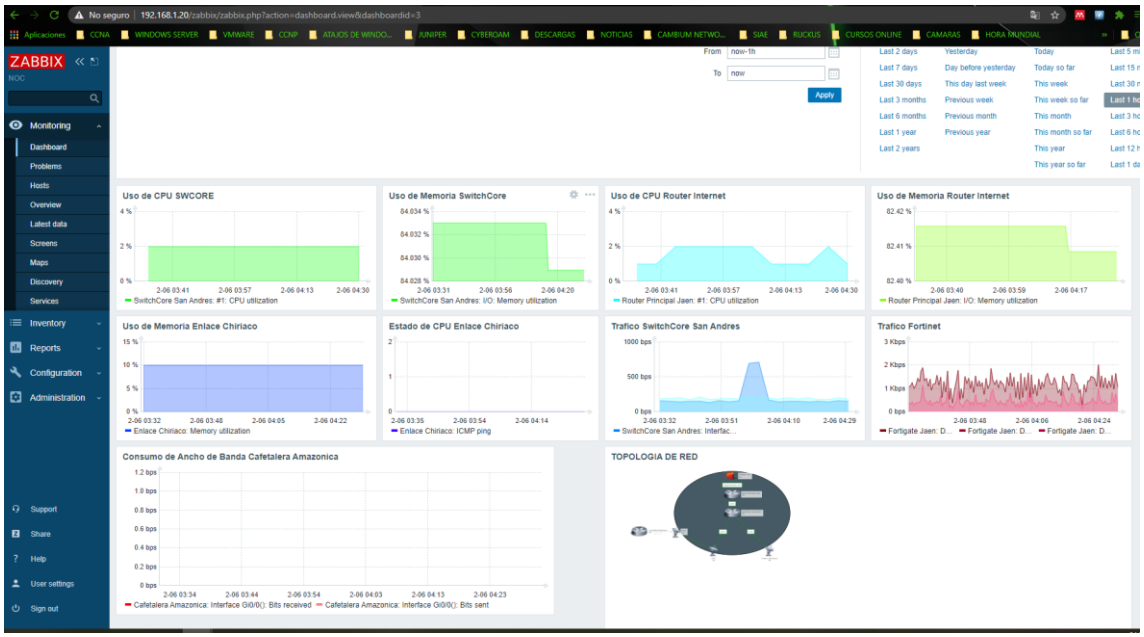
Fuente: Elaboración propia.

Una vez configurado en el dispositivo, ejecutar el comando snmpwalk -v2c -c ocaney 10.10.10.14 en el servidor para validar la conectividad SNMP entre el dispositivo a monitorear y el servidor. Y finalmente para registrar en el servidor seguimos los mismos pasos que en la figura 68.

```
[root@localhost ~]# snmpwalk -v2c -c ocaney 10.10.10.14
SNMPv2-MIB::sysDescr.0 = STRING: RouterOS CHR
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.14988.1
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (268900) 0:44:49.00
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: MikroTik
SNMPv2-MIB::sysLocation.0 = STRING:
SNMPv2-MIB::sysServices.0 = INTEGER: 78
IF-MIB::ifNumber.0 = INTEGER: 5
IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifIndex.2 = INTEGER: 2
IF-MIB::ifIndex.3 = INTEGER: 3
IF-MIB::ifIndex.4 = INTEGER: 4
IF-MIB::ifIndex.5 = INTEGER: 5
IF-MIB::ifDescr.1 = STRING: ether1
IF-MIB::ifDescr.2 = STRING: ether2
IF-MIB::ifDescr.3 = STRING: ether3
IF-MIB::ifDescr.4 = STRING: ether4
IF-MIB::ifDescr.5 = STRING: looback10
IF-MIB::ifType.1 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.2 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.3 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.4 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.5 = INTEGER: bridge(209)
```

Fuente: Elaboración propia.

Vista de los dispositivos de red en monitoreo.

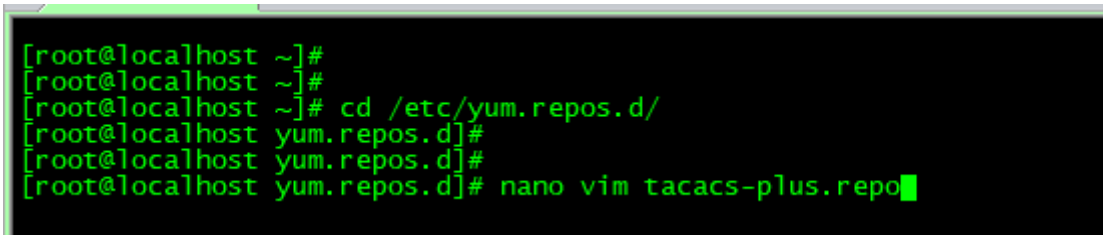


Fuente: Elaboración propia.

Anexo 7: Configuración de seguridad en los dispositivos de red

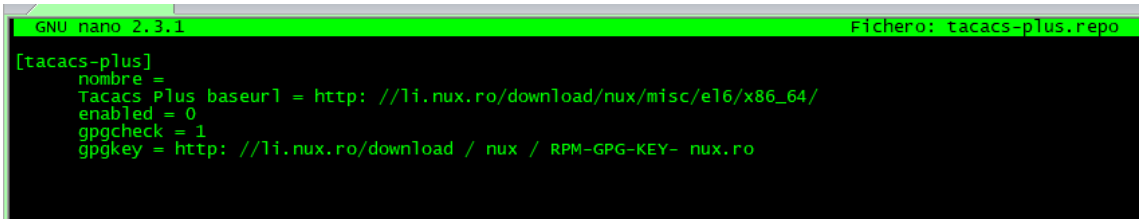
Habilitamos y configuramos tacacs en los dispositivos de red a monitorear, se requiere una clave y la IP del servidor tacacs se configurará en los dispositivos de red.

En primer lugar, necesitamos crear un nuevo archivo de repositorio donde podamos tomar el paquete tac_plus de las soluciones de administración de identidad y acceso Tacac +. Creamos el repositorio con el siguiente comando.



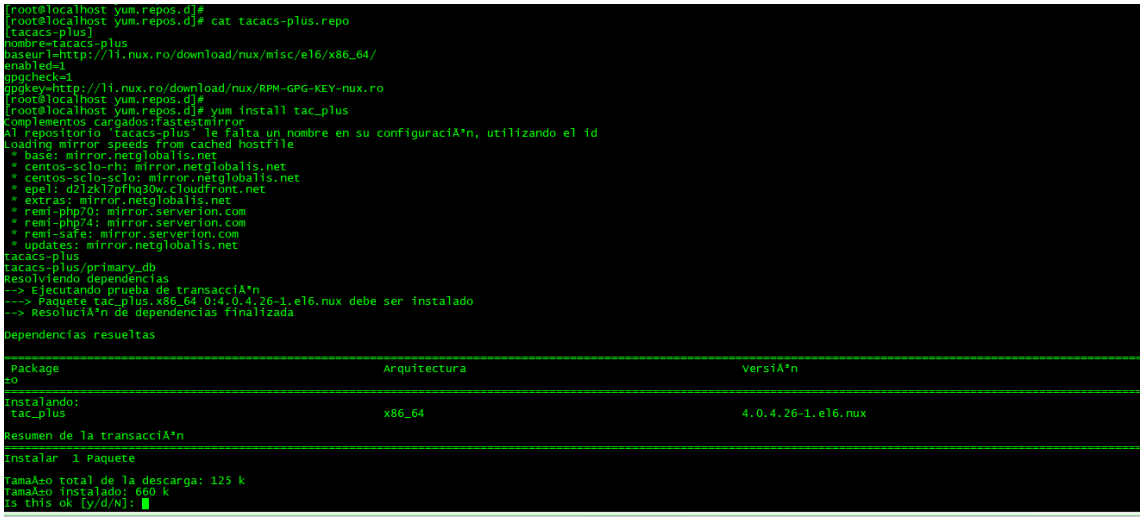
Fuente: Elaboración propia.

Editamos el repositorio donde podemos tomar tac_plus



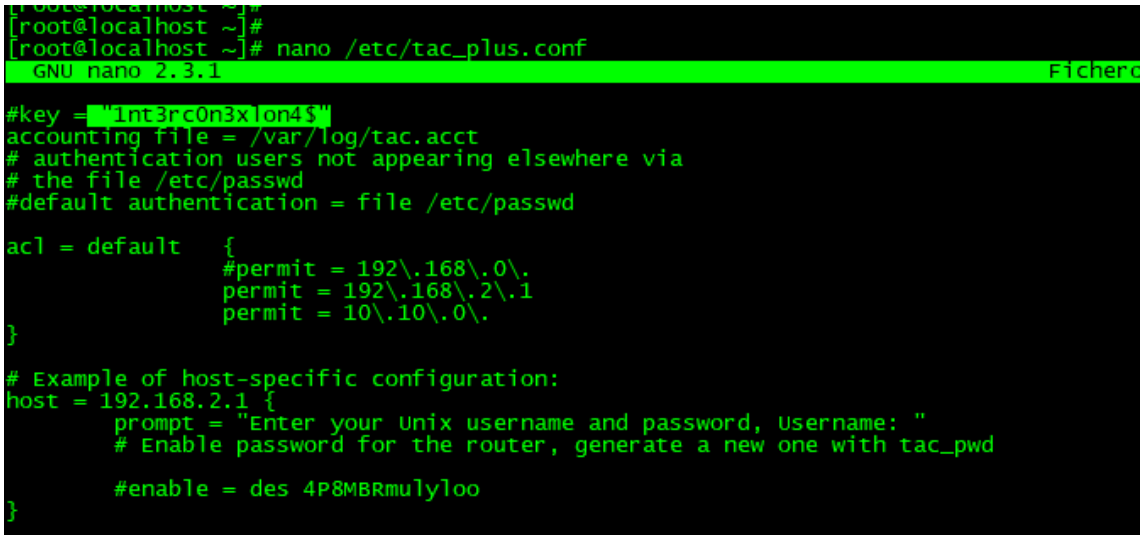
Fuente: Elaboración propia.

Ahora podemos comenzar a instalar las soluciones de administración de identidad y acceso Tacac + instalando el paquete tac_plus usando el siguiente comando.



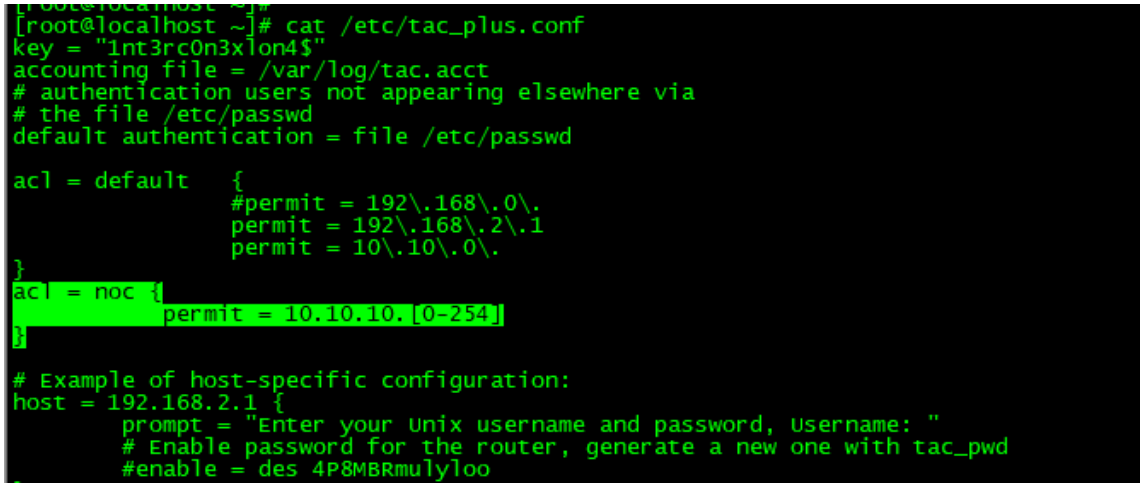
Fuente: Elaboración propia.

Podemos comenzar a editar el archivo de configuración de las soluciones de administración de identidad y acceso Tacacs de la siguiente manera. Primeramente, se requiere compartir una clave entre el servidor y el dispositivo de red.



Fuente: Elaboración propia.

Luego se procede a restringir acceso solo a la red 10.10.10.0/24 que pertenece al rango de dispositivos de red.



Fuente: Elaboración propia.

Se procede a crear grupos y permitir privilegios, se crea el grupo admin y los permisos que pueda realizar en el router.

```
# Group that is allowed to do most configuration on all interfaces etc.
group = admin {
        # group members who don't have their own login password will be
        # looked up in /etc/passwd
        login = file /etc/passwd
        #login = PAM

        # group members who have no expiry date set will use this one
        #expires = "Jan 1 1997"

        # only allow access to specific routers
        acl = noc


        # Needed for the router to make commands available to user (subject
        # to authorization if so configured on the router
        service = exec {
                priv-lvl = 15
                #default service = permit
        }

        cmd = username {
                permit .*
        }
        cmd = enable {
                permit .*
        }
        cmd = show {
                permit .*
        }
        cmd = exit {
                permit .*
        }
        cmd = configure {
                permit .*
        }
        cmd = interface {
                permit .*
        }
        cmd =  switchport  {
                permit .*
        }
        cmd = description {
                permit .*
        }
        cmd = no {
                permit shutdown
        }
        cmd = write {
                permit .*
        }
```

Fuente: Elaboración propia.

Crear usuarios y asociarlos a al grupo creado anteriormente.

```
user = joe {
        login = PAM
        #member = sysadmin
        member = admin
}

user = fred {
        login = PAM
        member = sysadmin
}
user = noc {
        login = file /etc/passwd
        #member = sysadmin
        enable = file /etc/passwd
        member = admin
}
```

Fuente: Elaboración propia.

Luego de editar el archivo tacacs_plus, se procede a iniciar el servidor tacacs con el siguiente comando.

```
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# service tac_plus start
Starting tac_plus (via systemctl):                         [  OK  ]
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]#
```

Una vez configurado el servidor tacacs, se procede a configurar el dispositivo de red, como se observa en la siguiente imagen.

```
aaa new-model
!
!
aaa authentication login default group tacacs+ enable
aaa authentication enable default group tacacs+ enable
aaa authorization commands 1 default group tacacs+ none
aaa authorization commands 15 default group tacacs+ none
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting network default start-stop group tacacs+
aaa accounting connection default start-stop group tacacs+
!
```

```
ip tacacs source-interface GigabitEthernet0/0
!
logging source-interface GigabitEthernet0/0
!
!
tacacs-server host 10.10.10.254
tacacs-server directed-request
tacacs-server key 1nt3rc0n3xlon4$
!
```

Fuente: Elaboración propia.

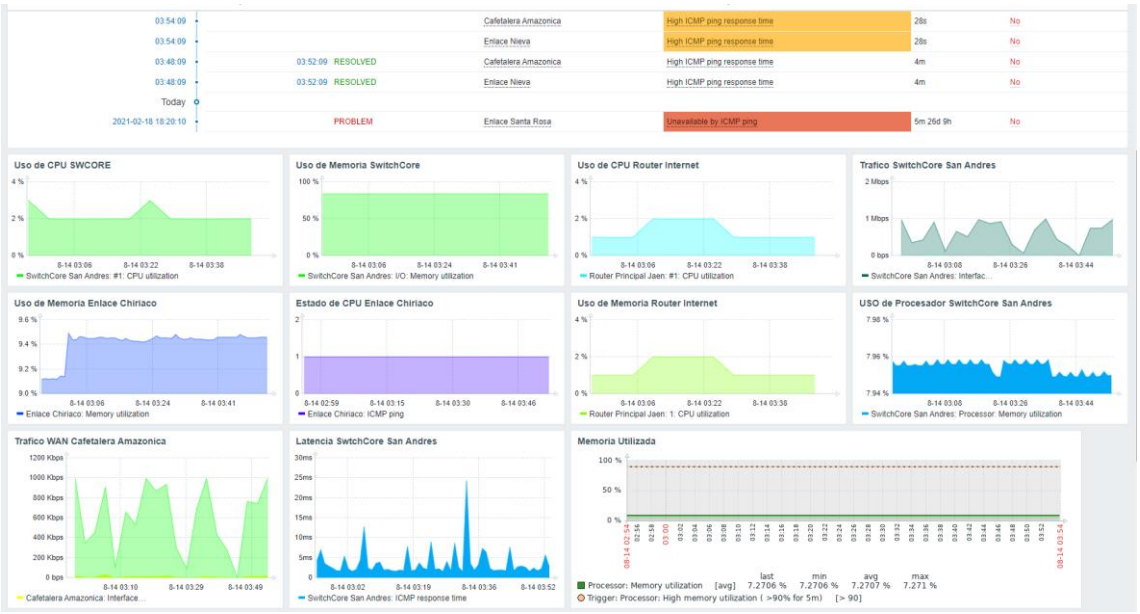
Una vez configurado, en los dispositivos de red, nos aparece el mensaje para ingresar usuario y clave.

```
CC
**************************************************************
*                                                            *
*------------------------------------------------------------*
*                  INTERCONEXIONES OCANEy                    *
*------------------------------------------------------------*
*                                                            *
*                     |          |                           *
*                   |||          |||                         *
*                 |||||          |||||                       *
*              .:|||||||:..:|||||||:.                        *
*------------------------------------------------------------*
**************************************************************
Usuario: noc
Password:

SwitchCore2>
```

Fuente: Elaboración propia.

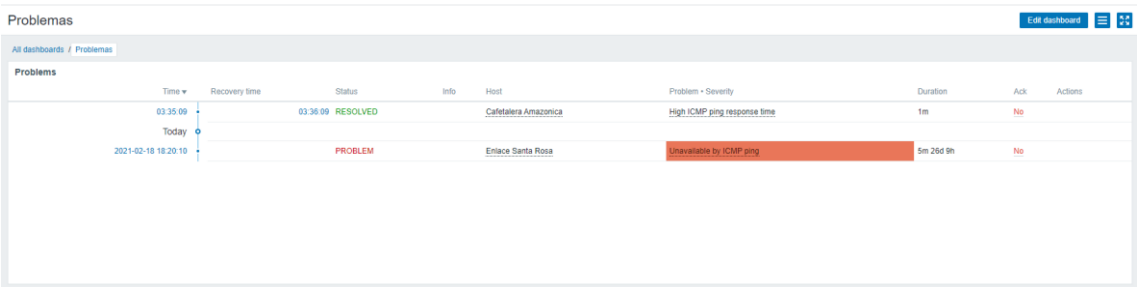
Anexo 8: Resultado del monitoreo de los dispositivos de red

Dashboard de monitoreo de los servicios inalámbricos



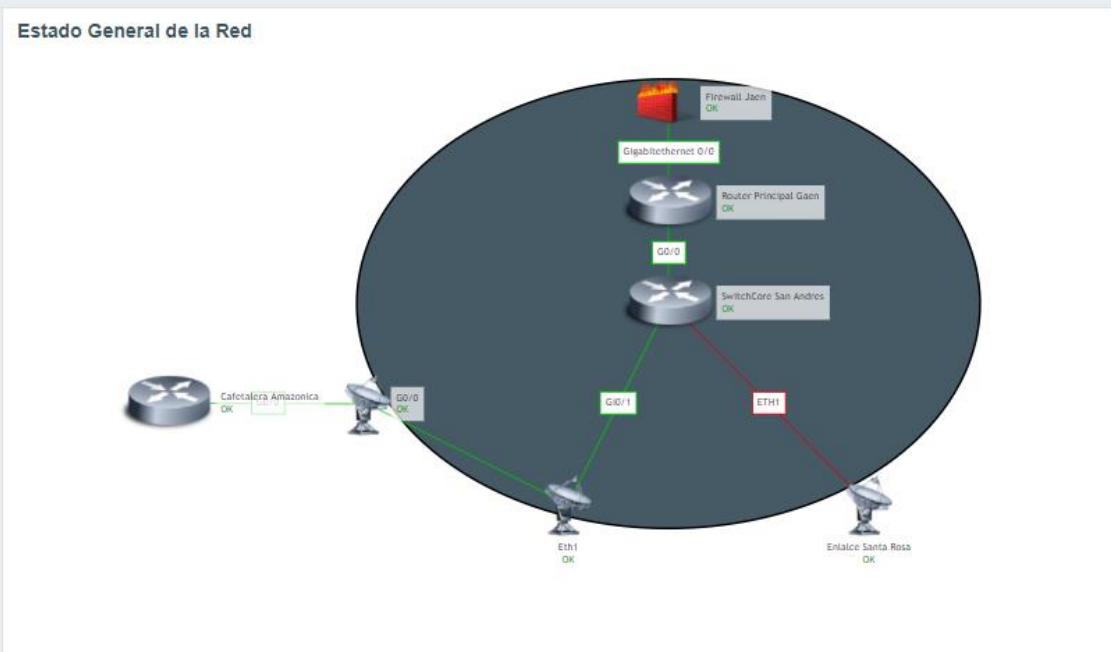
Fuente: Elaboración propia.

Dashboard de problemas, en donde se visualiza los motivos de las alertas de los dispositivos de red



Fuente: Elaboración propia.

Topología de red, donde se puede visualizar el enlace caído de color rojo



Fuente: Elaboración propia.

Captura donde se puede visualizar tráfico de los enlaces troncales, y estado del procesador

Fuente: Elaboración propia.