UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES

CARRERA DE INGENIERÍA EN INFORMÁTICA

Tema: "Implementación del sistema de monitoreo y mejora del rendimiento de la red de datos en la Universidad Politécnica Estatal del Carchi"

Trabajo de titulación previa la obtención del
título de Ingeniero en Informática

AUTORES: Casanova Imbaquingo Edi Santiago
Chulde Molina Anderson Xavier
TUTOR: Ing. Milton del Hierro. Msc

Tulcán, 2021

CERTIFICADO JURADO EXAMINADOR

Certificamos que el estudiante Casanova Imbaquingo Edi Santiago con el número de cédula 0401587050 ha elaborado el trabajo de titulación: “Implementación del sistema de monitoreo y mejora del rendimiento de la red de datos en la Universidad Politécnica Estatal del Carchi”

Este trabajo se sujeta a las normas y metodología dispuesta en el Reglamento de Titulación, Sustentación e Incorporación de la UPEC, por lo tanto, autorizamos la presentación de la sustentación para la calificación respectiva.

MILTON GABRIEL DEL HIERRO MOSQUERA
Firmado digitalmente por MILTON GABRIEL DEL HIERRO MOSQUERA
Fecha: 2021.05.11 14:44:16 -05'00'

f.....

Msc. Milton del Hierro

TUTOR

Firmado electrónicamente por:
JAIRO VLADIMIR HIDALGO GUIJARRO

f.....

Msc. Jairo Hidalgo

LECTOR

Tulcán, mayo de 2021

CERTIFICADO JURADO EXAMINADOR

Certificamos que el estudiante Chulde Molina Anderson Xavier con el número de cédula 0401995154 ha elaborado el trabajo de titulación: “Implementación del sistema de monitoreo y mejora del rendimiento de la red de datos en la Universidad Politécnica Estatal del Carchi”

Este trabajo se sujeta a las normas y metodología dispuesta en el Reglamento de Titulación, Sustentación e Incorporación de la UPEC, por lo tanto, autorizamos la presentación de la sustentación para la calificación respectiva.

MILTON GABRIEL DEL HIERRO MOSQUERA
Firmado digitalmente por MILTON GABRIEL DEL HIERRO MOSQUERA
Fecha: 2021.05.11 14:44:41 -05'00'

f.....

MSc. Milton del Hierro

TUTOR

Firmado electrónicamente por:
JAIRO VLADIMIR HIDALGO GUIJARRO

f.....

MSc. Jairo Hidalgo

LECTOR

Tulcán, mayo de 2021

AUTORÍA DE TRABAJO

El presente trabajo de titulación constituye requisito previo para la obtención del título de Ingeniero en la Carrera de ingeniería en informática de la Facultad de Industrias Agropecuarias y Ciencias Ambientales

Yo, Casanova Imbaquingo Edi Santiago con cédula de identidad número 0401587050 declaro: que la investigación es absolutamente original, auténtica, personal y los resultados y conclusiones a los que he llegado son de mi absoluta responsabilidad.

f.....

Casanova Imbaquingo Edi Santiago

AUTOR

Tulcán, mayo de 2021

AUTORÍA DE TRABAJO

El presente trabajo de titulación constituye requisito previo para la obtención del título de Ingeniero en la Carrera de ingeniería en informática de la Facultad de Industrias Agropecuarias y Ciencias Ambientales

Yo, Chulde Molina Anderson Xavier con cédula de identidad número 0401995154 declaro: que la investigación es absolutamente original, auténtica, personal y los resultados y conclusiones a los que he llegado son de mi absoluta responsabilidad.

f.....

Chulde Molina Anderson Xavier

AUTOR

Tulcán, mayo de 2021

ACTA DE CESIÓN DE DERECHOS DEL TRABAJO DE TITULACIÓN

Yo, Casanova Imbaquingo Edi Santiago declaro ser autor/a de los criterios emitidos en el trabajo de investigación: "Implementación del sistema de Monitoreo y mejora del rendimiento de la red de datos en la Universidad Politécnica Estatal del Carchi" y eximo expresamente a la Universidad Politécnica Estatal del Carchi y a sus representantes legales de posibles reclamos o acciones legales.

f.....

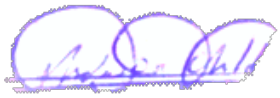
Casanova Imbaquingo Edi Santiago

AUTOR(A)

Tulcán, mayo de 2021

ACTA DE CESIÓN DE DERECHOS DEL TRABAJO DE TITULACIÓN

Yo, Chulde Molina Anderson Xavier declaro ser autor/a de los criterios emitidos en el trabajo de investigación: “Implementación del sistema de Monitoreo y mejora del rendimiento de la red de datos en la Universidad Politécnica Estatal del Carchi” y eximo expresamente a la Universidad Politécnica Estatal del Carchi y a sus representantes legales de posibles reclamos o acciones legales.



f.....

Chulde Molina Anderson Xavier

AUTOR

Tulcán, mayo de 2021

DEDICATORIA

A mis padres Leopoldo y Aura por brindarme su apoyo incondicional y sus consejos.
A mis hermanos quienes han sido mi fuente de inspiración para lograr esta meta.
Y a toda mi familia agradecerles ya que con sus palabras de aliento en los duros momentos he logrado salir adelante y formarme así profesionalmente.

Edi Santiago Casanova Imbaquingo

A mi madre, por estas siempre presente apoyándome en todos mis proyectos de vida y sus consejos que me ayudaron a ser la persona que soy hoy.

A mis hermanos por su cariño y palabras de aliento para lograr esta meta.

Anderson Xavier Chulde Molina

AGRADECIMIENTO

A mis padres por su cariño, comprensión, consejos y sobre todo por ser mi pilar principal para lograr mis metas.
A las personas incondicionales en mi vida que me han dado estabilidad, confianza y firmeza para salir siempre adelante.
A mi tutor por brindarme la confianza y apoyo durante todo este proceso.

Edi Santiago Casanova Imbaquingo

A mis padres y hermanos quienes han sido pilar fundamental para mi crecimiento personal y apoyo incondicional a fin de finalización de este proyecto.
A mi tutor por su asesoría en el desarrollo y culminación de este proceso.

Anderson Xavier Chulde Molina

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

RESUMEN

El presente proyecto de investigación tiene como objetivo implementar un sistema de monitoreo basado en el protocolo SNMP, por medio de herramientas de software libre, disminuyendo la intermitencia y mejorando el rendimiento de la red de datos en la Universidad Politécnica Estatal del Carchi en la ciudad de Tulcán, con la intención de monitorear los elementos de hardware (equipos de comunicación) y software (servicios disponibles) dentro de la infraestructura interna, facilitando a los administradores de red la detección de fallas o sobrecarga del sistema, notificándose de manera oportuna, permitiendo la obtención de reportes a través de gráficos de cientos de dispositivos y equipos de manera casi inmediata, dando a conocer la disponibilidad de cada uno y verificando que funcionen correctamente. De esta forma se obtiene información real y fidedigna sobre la situación actual de la red de datos y sus respectivos servicios que esta brinda, se ha realizado una investigación basada principalmente en la observación directa, investigación de campo y como técnicas de recopilación de información la encuesta y la entrevista a los principales actores en este caso estudiantes y el administrador de la red de datos de la institución, los cuales luego de ser analizadas han permitido plantear una solución factible y viable como lo es zabbix el cual permite cumplir con el presente objetivo de la investigación. De modo que se obtiene las conclusiones y recomendaciones, las cuales abarcan los temas de éxito en la investigación, observaciones que se ponen a disposición y aspectos que permitirán mejorar los siguientes estudios.

Palabras clave: Monitoreo de red, software libre, zabbix.

ABSTRACT

The present research project aims to implement a monitoring system based on the SNMP protocol, by means of free software tools, reducing intermittency and improving the performance of the data network at the Politécnica Estatal del Carchi University in Tulcán city, with the intention of monitoring hardware elements (communication equipment) and software (available services) within the internal infrastructure, making it easier for network administrators to detect failures or system overloads, notifying themselves in a timely manner. Allowing the obtaining of reports through graphs of hundreds of devices and equipment almost immediately, making known the availability of each one and verifying that they work correctly. In this way, real and reliable information is obtained on the current situation of the data network and its respective services that it offers, an investigation has been carried out based mainly on direct observation, field research and as information gathering techniques the survey and the interview with the main actors, in this case students and the administrator of the institution's data network, which after being analyzed have allowed to propose a feasible and viable solution which allows meeting the present objective of the research. Based on the research carried out, the conclusions and recommendations are obtained, which cover the topics of success in the research, observations that are made available and aspects that will allow to improve the following studies.

Keywords: Network monitoring, free software, zabbix.

INTRODUCCIÓN

La administración de redes se ha convertido en parte esencial dentro de una institución educativa, por la gran afluencia de usuarios que se conectan a esta, de modo que se vuelve complejo conocer el comportamiento general de la infraestructura de comunicaciones, por ende la demora en la identificación de problemas, por consiguiente la implementación de un sistema de monitoreo enfocado en mantener la red operativa, segura, disponible y constantemente gestionada llevando consigo la documentación debida, mejorando el rendimiento dentro de toda la red, teniendo consigo una continuidad en las operaciones de control y monitoreo dando un uso eficiente de todos los recursos y servicios de esta.

El presente proyecto está enfocado en una metodología mixta basada en la investigación acción debido a que permiten resolver problemas cotidianos que se presentan en nuestro entorno, por tanto, es de manera directa tomando en cuenta los problemas con la conexión a la red de datos, la cual es inestable y con mucha intermitencia, esto influye en el trabajo diario de los usuarios, además, esto provoca gran cantidad de insatisfacción al no tener un buen rendimiento de esta.

La importancia de este trabajo de investigación se ve reflejada cuando la disponibilidad de los recursos y servicios de TI presentan intermitencias, ya que cada día cientos de usuarios se encuentran conectados a la misma y dependen de una buena conexión para el trabajo diario. Es así como, al suscitarse un problema, este no se notifica, siendo necesaria la intervención del administrador de red y su equipo de trabajo para que verifiquen de forma personal el funcionamiento de todos los equipos buscando encontrar la falla.

Es muy importante contar con una buena infraestructura de red en instituciones de educación superior, puesto que en ellas se maneja una gran cantidad de información y usuarios conectados en diversos servicios que proveen estas. Hoy en día no es una tarea fácil manejar, supervisar y controlar manualmente todos los equipos que integran la red, menos si se cuenta con gran cantidad de estos, para lo cual se propone la utilización de las herramientas de monitoreo continuo, las cuales nos permiten conocer en tiempo real el estado de disponibilidad que estos brindan a los usuarios y en caso de haber alguna falla poder fácilmente solucionarla, su objetivo final es brindar la información requerida para una toma de decisiones ágiles con el fin de garantizar un óptimo funcionamiento de la red de datos.

En la actualidad la UPEC no cuenta con una herramienta especializada dentro de su infraestructura que les permita monitorear la red de todos sus equipos de manera continua y confiable a fin de mantener la disponibilidad del uso de dispositivos, servicios o aplicaciones, tales como correo electrónico, base de datos, sitio web, etc. Uno de los objetivos del área de TIC's y su administrador, es tener a disposición la información confiable del estado general de la infraestructura de comunicaciones, para que la toma decisiones sea inmediata.

Para brindar la solución a esta problemática, se definió como objetivo general "Implementar un sistema de monitoreo basado en el protocolo SNMP, utilizando herramientas de Software Libre, disminuyendo la intermitencia y mejorando el rendimiento de la red de datos" con la finalidad de solucionar los problemas con equipos de comunicación y transmisión de datos. Surgiendo la siguiente hipótesis "El Sistema de monitoreo influye positivamente en la intermitencia y mejora el rendimiento de la red de datos que utilizan los usuarios en la Universidad Politécnica Estatal del Carchi". Determinando la factibilidad del proyecto, el cual permitirá la detección de fallas y su resolución inmediata por parte del departamento de TIC's, esta implementación permite conocer el estado de todos los equipos y su disponibilidad hacia los usuarios en tiempo real y con información detallada y fiable.

I. PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

La gestión de redes a nivel de América del Sur es aplicada en las instituciones públicas y empresas, con el objetivo de garantizar la calidad de servicios, asegurando la disponibilidad de los sistemas de redes, obteniendo un resultado adecuado y eficiente. "El término gestión de redes es determinado por la suma de las políticas, procedimientos de diseño o planeación, configuración, intervención y monitoreo de elementos que forman parte de una red garantizando el uso adecuado de los recursos" (Terán, 2017, p.1). El tema de disponibilidad de los servicios de datos en la red es un problema frecuente, pues el incremento de dispositivos conectados a esta sin un control adecuado de la misma provoca una insatisfacción a las necesidades de comunicación del usuario.

Dentro de las características de las herramientas del monitoreo de redes está la posibilidad de tomar decisiones en tiempo real y así mismo la optimización de los procesos convirtiéndose en situaciones clave ante posibles contratiempos. Porro (2018) afirma: "Las soluciones de gestión de TI de ip switch brindan a los equipos de TI de todo el mundo las capacidades tecnológicas necesarias para satisfacer todos los desafíos complejos vinculados al monitoreo de redes y la transferencia segura de archivos" (p.2). El monitorear una red permite aprovechar al máximo los recursos de software y hardware, previniendo incidencias y detectando problemas con anterioridad ahorrando costos y tiempo.

Durante los últimos años las empresas privadas y entidades públicas se han visto obligados a llevar un registro del funcionamiento de la red de datos, para conocer el estado de la infraestructura física y lógica de estas, comprobando los equipos con mayor prioridad con el fin de detectar problemas anticipadamente evitando la degradación del servicio de red. Cadena, Dulce, y Toledo (2016) expresan que, en el área de tecnología de la Universidad Mariana, Colombia, tiene implementado un sistema para la administración de redes llamado HP Intelligent Management Center, el cual es un software propietario que reconoce todas las bondades, mientras se esté trabajando en dispositivos de marca Hewlett-Packard, actualmente esta herramienta tiene limitación en relación con el número de equipos a gestionar, debido a su licencia de tipo propietario, a lo cual implica que en la red de datos existan nodos que no están siendo gestionados por el sistema. Muchas de las entidades públicas mantienen políticas de prevención las cuales les generan ahorros significativos en términos económicos y tiempo,

mediante la planificación e inversión se puede evitar las caídas de los sistemas y garantizar un buen funcionamiento.

Por otra parte, en el Ecuador, el uso de herramientas de sistema de monitoreo es indispensable en las instituciones educativas, puesto que manejan gran cantidad de datos que deben estar en constante monitoreo y esto impliquen la degradación del rendimiento de la red de datos. García (como se citó en Estado Digital Ecuador, 2020) publicado en el periódico El Universo del Ecuador, de acuerdo con estadísticas del informe presentado en enero indica que en el país el 80% de personas tiene acceso a la web el cual el 33% corresponde a Quito y Guayaquil y el 63% del total de usuarios tiene más de 24 años los cuales registran mayor acceso a redes sociales como Facebook, WhatsApp, Instagram y Messenger manteniendo un consumo alto de estas. Además, el 92.3% de los usuarios en el ecuador interactúan con contenido en la web 24/7 consumiendo gran cantidad de datos en los cuales se considera de mayor demanda como videos, fotos, mensajería, redes sociales, gestión de consultas y tramites en línea entre otros.

Toda esta demanda de consumo de ancho de banda puede traer consecuencias en instituciones educativas públicas y privadas en el Ecuador, pues el congestionamiento de los datos en la red en horas pico es muy frecuente sean estos por voz, texto o video, generando grandes cargas a los servidores, dando como resultado una baja calidad del servicio, estos problemas se ven diariamente en laboratorios y a nivel administrativo, por tanto, este flujo de información debe ser monitorizada y controlada diariamente por los administradores de la red de datos. Las instituciones educativas muy poco toman en cuenta el estado de la infraestructura de comunicación, en su mayoría no disponen de herramientas especializadas en el monitoreo de sus recursos de red que permitan mejorar el rendimiento y mantengan una mejor gestión de estos, por tanto, a la hora de la identificación de fallos se complica el llevar una buena administración y control de la red. Estas limitaciones traen como resultado respuestas tardías a problemas o eventos que se presentan en la red provocando saturaciones y evitando un correcto funcionamiento de esta.

En la provincia del Carchi, en la ciudad de Tulcán, en la Universidad Politécnica Estatal del Carchi existe un incremento de dispositivos conectados en la red sin restricción alguna lo cual se ha convertido en un problema puesto que inciden en el rendimiento de los servicios de la red informática, perjudicando a equipos e incluso comprometiendo la seguridad de la información. A mayor cantidad de equipos conectados mayor tráfico a medida que aumenta las colisiones,

provocando ralentizar la red de modo que se vuelve un método de acceso lento. Uno de los principales problemas que afectan al servicio de navegación se presenta en diferentes departamentos y en horarios distintos siendo difícil determinar el problema que se está produciendo, además presenta también inconvenientes en la red de datos general, dando como consecuencia la necesidad de reiniciar el servicio de internet provocando insatisfacción al usuario cuando se restablece el servicio para que pueda continuar con el trabajo.

Estos problemas son más a menudo cuando se requiere realizar trabajos que implican un gran consumo de la red, produciéndose sobrecarga o lentitud en la misma para los demás usuarios. La principal preocupación del personal de TIC's es identificar donde se producen los cuellos de botella, con el objetivo de realizar los cambios respectivos o las configuraciones correspondientes, pero al no disponer de herramientas especializadas, el analizar, controlar y monitorear el comportamiento de la infraestructura de comunicación no es posible, resultando así con soluciones tardías no logrando asegurar la disponibilidad de los servicios.

Sin herramientas especializadas no es posible las alertas de la presencia de un problema o fallo, sin posibilidades de reaccionar a tiempo ante la caída de los servicios produciendo insatisfacción a los usuarios, por lo cual el centro de TIC's de la Universidad Politécnica Estatal del Carchi necesita una herramienta para el monitoreo constante de los servidores, los enlaces de comunicaciones, información del estado del ancho de banda que provee el mismo centro.

1.2. FORMULACIÓN DEL PROBLEMA

El precario sistema de monitoreo de la red de datos genera la intermitencia en el rendimiento de esta, ocasionando insatisfacción en los usuarios que hacen uso de los servicios de la red en la Universidad Politécnica Estatal del Carchi en el periodo 2019-2020.

1.3. JUSTIFICACIÓN

La presente investigación como parte de finalización de carrera, hace referencia al uso y aplicación de herramientas especializadas en el monitoreo, estas brindan un control centralizado de la red de datos, aumentando la operatividad y uso eficiente de los recursos de la infraestructura de comunicación, dado que al suscitarse un problema en alguno de los componentes de red este nos notifique de forma automática, por ende ayudara a el encargado del mantenimiento de la misma a determinar, analizar y mitigar los errores con mayor rapidez

generando registros de eventos aplicando medidas preventivas para actuar de manera inmediata a posibles errores futuros.

El estado actualmente establece el uso de herramientas de software libre dentro de instituciones públicas según el Artículo 1 del decreto ejecutivo 1014 publicado en registro oficial el 10 de abril del 2008 que dice. “Establecer como política pública para las entidades de la Administración Pública Central la utilización de software libre en sus sistemas y equipamientos informáticos” (Decreto Ejecutivo 1014, 2008). Para el beneficio de las instituciones públicas por tal motivo el uso de estas herramientas. Las aplicaciones y la concurrencia de los usuarios en la red de datos actualmente provocan que los recursos sean totalmente consumidos y la mayoría de las veces sin garantías del servicio, haciéndose de esta forma indispensable la provisión del rendimiento en este tipo de redes. Actualmente el exceso de usuarios conectados a la red en la Universidad Politécnica Estatal del Carchi provoca un deficiente rendimiento e incluso pueden comprometer la seguridad de la información puesto que no existe una herramienta especializada en el control adecuado que nos permita monitorear el consumo del ancho de banda. El sistema de monitoreo permitirá un control centralizado sobre los equipos conectados a la misma, además permitirá la notificación de posibles errores que pueda afectar el rendimiento de la red, reduciendo la cantidad de errores posibles aprovechando al máximo la infraestructura de comunicación.

Por lo tanto, la presente investigación tiene como finalidad implementar una herramienta que más se ajuste a los requerimientos de funcionalidad del departamento de TIC’s permitiendo monitorear, diagnosticar y establecer soluciones para controlar las anomalías propias de la red, gestionando de una manera eficiente el tráfico de datos y el consumo del ancho de banda de cada uno de los equipos pertenecientes a esta, permitiendo de forma notable el incremento de conectividad a los servicios, convirtiéndose así en una solución indispensable para los usuarios que necesitan del servicio a diario, es así que se propone soluciones innovadoras que favorezcan el crecimiento de la red.

1.4. OBJETIVOS Y PREGUNTAS DE INVESTIGACIÓN

1.4.1. Objetivo General

Implementar un sistema de monitoreo basado en el protocolo SNMP, por medio de herramientas de Software Libre, disminuyendo la intermitencia y mejorando el rendimiento de la red de datos en la Universidad Politécnica Estatal del Carchi.

1.4.2. Objetivos Específicos

- Fundamentar bibliográficamente las variables de estudio a través de medios tecnológicos y físicos, para la sustentación de la investigación.
- Analizar el estado actual de la infraestructura física y lógica de la red de datos, para conocer los requerimientos de gestión de esta.
- Determinar las herramientas de monitoreo de software libre a través de técnicas de investigación, identificando la más idónea de acuerdo con los requerimientos del departamento de TIC's.
- Implementar la herramienta de monitoreo de la red de datos a través del software seleccionado, gestionando los recursos de la red y permitiendo la identificación de los problemas presentes.

1.4.3. Preguntas de Investigación

- ¿Cómo la fundamentación bibliográfica acerca de las variables de estudio sustento la investigación?
- ¿Cuál es la factibilidad de implementar herramientas de monitoreo de Software Libre dentro de la red de datos?
- ¿Cómo la implementación de la herramienta de monitoreo mejorará la disponibilidad de los recursos de la red?
- ¿Cómo mejorará el rendimiento de la red con la detección oportuna de fallos mediante el análisis de la infraestructura?

II. FUNDAMENTACIÓN TEÓRICA

2.1. ANTECEDENTES INVESTIGATIVOS

Para la presente investigación se ha considerado los siguientes antecedentes de investigación nacionales e internacionales, debido a la gran importancia en el proceso de investigación.

Jessica Estefanía Báez en el año 2017 realiza la tesis de pregrado denominada: "Diseño e Implementación de un Modelo de Gestión de red para la red de Área Local del Edificio Central de la Universidad Técnica del Norte en base al modelo de gestión OSI con el protocolo SNMP", en Ibarra, UTN, el objetivo de la investigación es plantear un modelo de administración y gestión de la red del Edificio Central de la Universidad Técnica del Norte, a través de la implementación de una herramienta de gestión, en función del modelo de gestión OSI mediante el protocolo SNMP, para mejorar el rendimiento de la red. El cual permite administrar, supervisar el rendimiento de la red de datos, el análisis de la información referente a la gestión de red y en especial al modelo de gestión ISO/OSI es útil para conocer los criterios que deben tomarse en cuenta para la implementación del modelo basado en las cinco áreas funcionales de gestión: configuraciones, fallos, rendimiento, contabilidad y seguridad. Las políticas de gestión del modelo ISO/OSI constituyen una guía para una gestión de red organizada. El análisis costo-beneficio evidencia la factibilidad del proyecto, se destaca el gasto ahorrado al utilizar herramientas de distribución libre y los beneficios que genera este proyecto tanto para el administrador de red como para los usuarios. La gestión de red en la red de datos del Edificio Central de la Universidad Técnica del Norte es fundamental, ya que permite al administrador de la red supervisar el rendimiento de esta, de manera que se detecte con prontitud los problemas que se presentan y puedan ser resueltos a tiempo. El análisis costo-beneficio evidencia la factibilidad del proyecto, se destaca el gasto ahorrado al utilizar herramientas de distribución libre y los beneficios que genera este proyecto tanto para el administrador de red como para los usuarios.

Con la implementación del modelo de gestión de la red de datos de este proyecto se comprobó el funcionamiento en las áreas funcionales que comprende el modelo ISO, permitiendo tener una red operativa y continuamente monitoreada, presentado alarmas ante diferentes problemas que se susciten en la red. Además, evidenciando la factibilidad del proyecto puesto que hace uso de software libre generando beneficios tanto como al administrador como a los usuarios.

Jorge Stteven García y Camilo Andrés Roa en el año 2020 en la Universidad Cooperativa de Colombia en la Facultad de Ingeniería, Bogotá D.C realizan como parte de Monografía de Grado "Diseño de una herramienta de monitoreo y control de servidores utilizando como eje principal Cacti aplicado a una Pyme Mediana." Los objetivos planteados de su investigación es diseñar una herramienta de monitoreo y control de servidores utilizando principalmente Cacti la cual se encarga de monitorear los elementos de hardware y software dentro de la infraestructura de datacenter facilitando a los administradores de red la detección problemas y notificando de manera oportuna vía correo electrónico, SMS, y otros medios. Todo evento presentado en la red, también el software brinda la facilidad de generar un reporte de disponibilidad en los equipos. La herramienta CACTI es una herramienta de control histórico de consumo de interfaces de red ya sean estas de enlaces internos o externos, la cual facilitará gráficamente detectar comportamientos anómalos en la red y en los consumos de CPU y memoria RAM de los equipos de datacenter. La propuesta se ha implementado bajo LINUX/WINDOWS lo cual brinda a las pymes medianas grandes beneficios en cuanto a costo del proyecto, resultados esperados y en personalización del monitoreo. La metodología para utilizar en el presente trabajo se trata de forma en cascada ya que es un proceso secuencial en cual consta de un conjunto de etapas que se ejecutan un tras de otra, este modelo está diseñado para llevar a cabo una revisión final, que se encarga de determinar si el proyecto está listo para avanzar a la siguiente fase y así hasta llegar al objetivo principal del proyecto. Se ha construido un software de open source capaz de monitorear los diferentes dispositivos, enlaces y servicios que servirán de manera eficaz en cualquier empresa que tenga a su disposición un datacenter porque el equipo de redes tendrá información sobre los parámetros SLA, equipos en cuanto a tiempos de respuesta y en porcentaje de rendimiento en cuanto a CPU, memoria y consumo de red.

Por otra parte, este proyecto de investigación permitió monitorear los diferentes dispositivos, enlaces y servicios de la red de datos, como también tiempos de respuesta y rendimiento en cuanto a la CP, memoria y tráfico de la red. Además, se evidencia lo necesario de clasificar los equipos críticos con los no tan críticos, teniendo así identificados los equipos con más prioridad a ser monitorizados y a la vez su respectiva configuración de alertas de acuerdo con su nivel de criticidad.

Edward Fernando Rodríguez (2017), desarrolla la tesis de pregrado denominada "Análisis de tráfico y gestión del rendimiento en las redes de datos" desarrollada en la ciudad de Jipijapa

menciona que: En esta investigación el objetivo es realizar un análisis de tráfico y gestión del rendimiento en las redes de datos para las Carreras de Ingeniería en Sistemas Computacionales y Tecnología de la Información de la Universidad Estatal del Sur de Manabí. Se realizó el monitoreo de todos los servicios captados en la red de datos. La carrera cuenta con un enlace de red se distribuye por laboratorios de cómputo, salas de docentes y redes inalámbricas. detectados problemas que aquejan la conectividad de los usuarios y no satisface la necesidad de cada uno para esto se ha evaluado con un estudio, para mejorar el servicio, permitiendo describir las principales falencias por sus defectos a esto nos conlleva a un mal funcionamiento, se da como propuesta la implementación de un sistema de control de tráfico y para gestión de rendimiento de las redes de datos con el propósito de lograr que la red sea más eficiente, rápida y segura. la investigación busca alternativas para la mejor conectividad en la carrera de sistema computacionales y tecnología de información logrando tener el control total en el momento que todos los usuarios arranquen con sus actividades así poder satisfacer sus necesidades y obtener mejor servicio. La carrera de ingeniería en sistemas computacionales y tecnología de información cuenta con un total de 362 usuarios que les dan usos a las redes de datos, se aplicó la fórmula para obtener la muestra con 190 usuarios encuestados el resultado sobre la investigación encontraremos la factibilidad del sistema de tráfico y rendimiento en las redes de datos.

Por otra parte, este proyecto de investigación cumple con todos los requisitos previsto permitiendo mejorar la conectividad en la carrera de sistemas computacionales y tecnología de la información, el control de tráfico dentro de la universidad es un despliegue, integración y unión de hardware y software el cual permite a los elementos humanos la monitorización de los equipos, la prueba de diferentes configuraciones, el sondeo de los paquetes en la red además analiza, evalúa y controla todos los recursos que la entidad posee.

David Fernando Sánchez 2017 realiza la tesis de grado en la Universidad Técnica de Ambato denominada “Implementación de un Sistema de monitoreo y Protección de datos en la red de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.” en Ambato, UTA cuyo objetivo es la implementación de un sistemas de monitoreo y protección de datos, el cual analizará el tráfico de red, en la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato para conocer el estado de la infraestructura física y lógica de la red de datos que incida en el congestionamiento de la red y esta produzca cuellos de botella ocasionando la degradación del el servicio de red, recalcando la importancia que tiene el

proyecto de investigación en instituciones públicas al identificar todas las actividades no autorizadas dentro de la red de datos que provocan de manera directa el congestionamiento de la red además existen conflictos de IP de alerta de intrusos que pretenden colapsar la red de datos, eso determina la importancia de un sistema de monitoreo con protección de la red para la detección de intrusos externos e internos dentro de la misma y la generación de alertas inmediatas de cualquier tipo de congestionamiento para su mitigación.

Para conclusión de este proyecto, en el cual es implementa un sistema de monitoreo y protección de datos en la red de la facultad de ingeniería en sistemas, electrónica e industrial, tiene como resultado eficaz en cuando a la detección y congestionamiento de la red, evidenciando el comportamiento de los equipos de la red alertado sobre los paquetes perdidos, ataques a la red y deteriores de esta, además, se determinó que al establecer mecanismos de control y protección de la red mejora el rendimiento de esta.

2.2. MARCO TEÓRICO

El presente capitulo aborda conceptos generales sobre la administración y gestión de una red de datos en función del modelo OSI, como también los protocolos que intervienen al gestionar dichas redes, además se analiza herramientas de monitoreo de software libre que mejor se ajusten a los equipos de la institución.

2.2.1. Red de datos

Una red de datos es un conjunto de equipos de interconexión que permiten la conmutación de paquetes y se clasifican de acuerdo con su tamaño. “Se denomina red de datos a aquellas infraestructuras o redes de comunicación que se ha diseñado específicamente a la transmisión de información mediante el intercambio de datos” (Ochoa, 2017, p.29). Generalmente se comunica a través del envío de paquetes cubriendo la arquitectura física que esta tenga, posibilitando la comunicación electrónica que permite la transmisión ordenada y la percepción de datos así también el compartir recursos y ofrecer servicios. En una red de datos se puede distinguir cuatro elementos importantes para su funcionamiento:

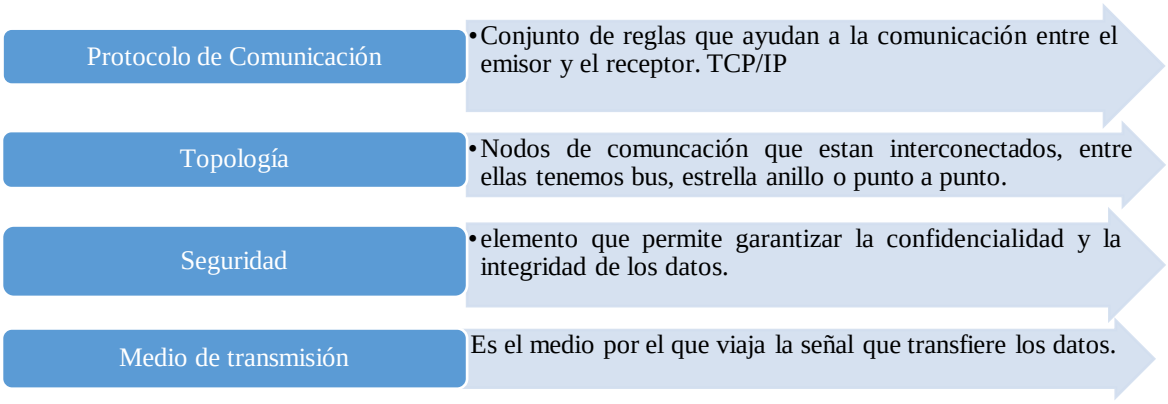


Figura 1. Características de una Red de Datos

2.2.1.1 Tipo de redes

Las redes de datos se diseñan y construyen en distintas arquitecturas para el servicio y uso específico, basándose en la conmutación de paquetes y se clasifican de acuerdo con su tamaño, la distancia que cubre y su arquitectura física. Se puede clasificar las diferentes dimensiones de red entre las más importantes como son:

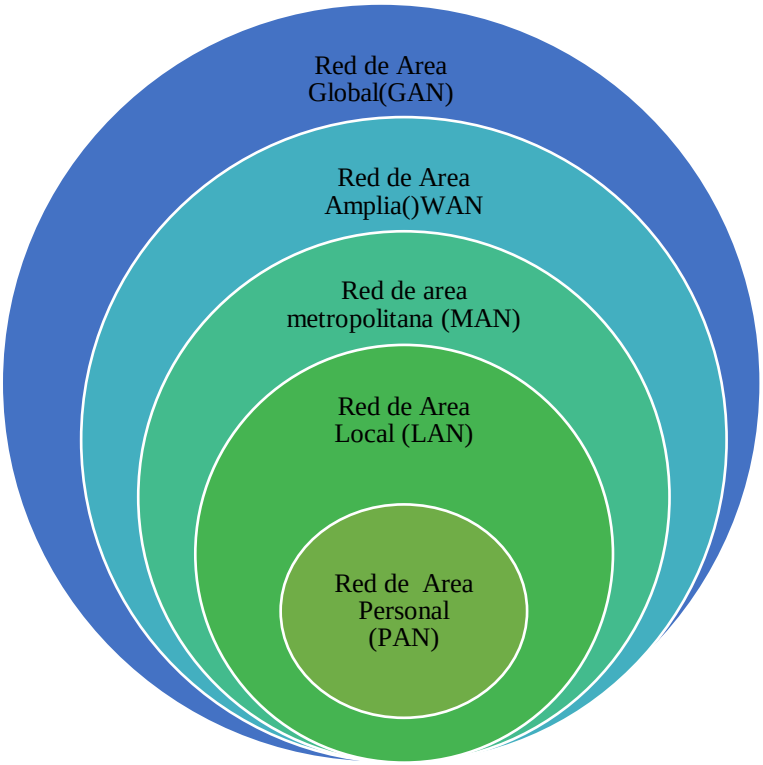


Figura 2. Tipos de Redes

> La conexión física en la que se basan estos tipos de redes puede presentarse por medio de cables o llevarse a cabo con tecnología inalámbrica. A menudo, las redes físicas conforman la base para varias redes de comunicación lógicas, las llamadas Virtual Private Networks (VPN). Para la transmisión de datos, estas emplean un medio de transmisión físico común como puede ser la fibra óptica y se vinculan de forma lógica a diferentes tipos de redes virtuales por medio de un software de tunelización. (IONOS, 2019, p.2)

Estos tipos de redes antes mencionados permiten que los dispositivos puedan intercambiar datos en la red, permitiendo el transporte de información entre nodos de manera rápida, segura y confiable, manteniendo así la disponibilidad para los usuarios.

2.2.1.2 Trafico de red

En el tráfico de la red de datos se analiza todos los paquetes que se envían dentro y fuera de la red recopilando datos que pueden usarse para la toma de decisiones.

Ríos y La Red Martínez (2018) Manifiestan que:

> En el tráfico de redes es necesario que los nodos deban tomar decisiones basados en acuerdos respecto del acceso a rutas disponibles; las decisiones pueden estar relacionadas con el estado de los nodos de acuerdo con, por ejemplo, el porcentaje de CPU usado, la memoria disponible y el número de paquetes encolados para ser distribuidos, como así también el estado de los tramos entre nodos. (p.1)

En muchas redes, la gestión se da perfectamente en situaciones de tráfico intenso en la red, sin embargo, en otras redes ethernet existe la sobrecarga de esta con lo cual es de suma importancia la observación periódica del tráfico de red, así como los parámetros por los que se regula e incluso medir el nivel de las colisiones existentes frente a un volumen de datos transferidos. El análisis de tráfico de la red es un proceso de control permanente que está enfocado en mejorar el desempeño de los servicios de una red, donde se captura los datos de diferentes entornos que operan simultáneamente mediante ese análisis y control se evalúa el comportamiento y establece políticas de acceso óptimas para que la red funcione eficientemente.

2.2.1.3. Intercambio de información en la red de datos

Para el intercambio de información, el administrador debe de subir la información al servidor FTP y el cliente deberá conectarse al mismo servidor y buscar los elementos que quiera descargar o visualizar, es así como se puede construir una red de comunicaciones.

Soret (2017) afirma:

> Con la globalización y la aparición de los dispositivos móviles, el mundo empresarial está geográficamente disperso a lo largo y ancho del planeta y requiere que los equipos estén permanentemente conectados entre sí para compartir información de forma rápida, fiable y segura, razón por la que las líneas punto a punto prácticamente han desaparecido. En su lugar, todos los nodos de una red utilizan una única infraestructura: la "red de redes" o Internet. (p.3)

Así, con la globalización el mayor inconveniente que se dio en este servicio es que las velocidades de transferencia son más bien lentas, no dependiendo únicamente de tu tipo de conexión, sino también del tipo de archivo el cual se desea descargar.

2.2.2. Seguridad en la red de datos

La seguridad de los datos en la red se puede implementar mediante diferentes tareas y herramientas para evitar que usuarios sin autorización entren en las redes.

Fruhlinger (2018) afirma:

> La seguridad de la red es la práctica de prevenir y proteger contra la intrusión no autorizada en redes corporativas. Como filosofía, complementa la seguridad del punto final, que se centra en dispositivos individuales; la seguridad de la red se centra en cómo interactúan esos dispositivos y en el tejido conectivo entre ellos. (p.1)

Como una buena estrategia de defensa siempre debemos tener en cuenta que la protección de la información es primordial y se debe hacer lo más correctamente posible; en la detección una buena configuración juega un papel importante el poder identificar algún tráfico de red inusual y en la reacción lo cual convierte al usuario en primera defensa el poder responder lo más seguro posible ante cualquier altercado.

2.2.3. Modelo OSI

El modelo OSI esté compuesto por 7 capas con funciones individuales que en conjunto permiten la comunicación entre protocolos, cuando fue creado perseguía el ambicioso objetivo de interconectar sistemas de procedencia distinta para darse el intercambio de información sin ningún tipo de impedimento. “El modelo de interconexión de sistemas abiertos (OSI) es un modelo de referencia para los protocolos de red la arquitectura en capas, creado en el año 1980 por la Organización Internacional de Normalización (ISO, International Organization for Standardization)” (Becerra, 2016, p.11). En el modelo OSI se pude destacar el modelo de referencia para los protocolos de la red en la arquitectura de capas las cuales tienen como objetivo el descomponer dichos problemas complejos de comunicación a las distintas capas, formando así problemas más sencillos distribuyendo el trabajo.

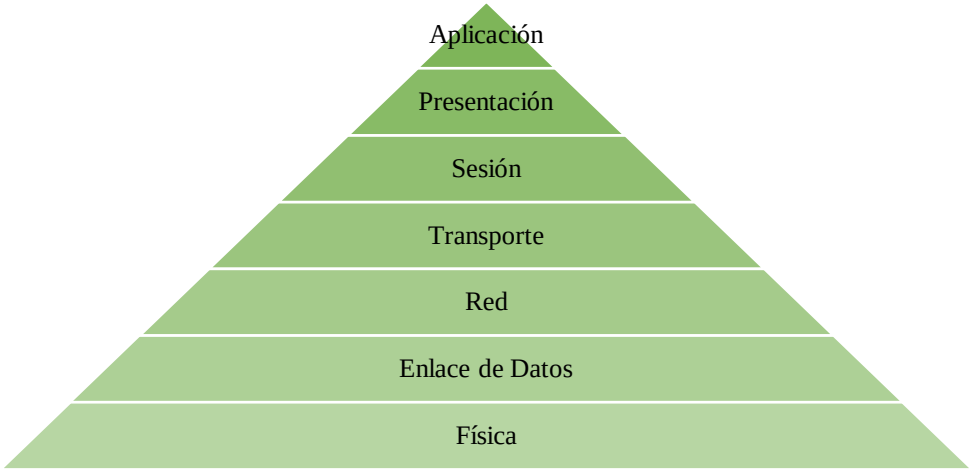


Figura 3. Capas del Modelo OSI

2.2.4. Modelo TCP/IP

El TCP/IP es la base de internet y este sirve para la comunicación de todo tipo de dispositivos con sus diferentes sistemas operativos sea que trabajen en una red de área local o LAN (Local Área Network en inglés) o en una red de área amplia, o WAN (Wide Área Network en inglés). Así, su nombre proviene de sus dos protocolos más importantes, que a la vez dan nombre a su capa. El protocolo de internet, que da nombre a la capa de red, y el protocolo de control de transmisión, que da nombre a la capa de Transporte (Juncosa, 2019). Este modelo está compuesto por cuatro capas o niveles: la capa de aplicación, transporte, internet y acceso a la

red, cada una de estas capas se encarga de determinados aspectos de la comunicación y a la vez brinda un servicio específico a la capa superior.

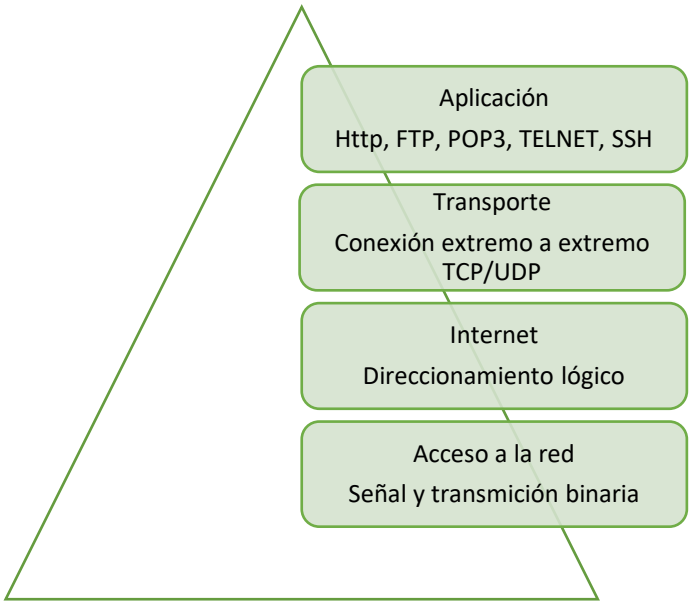


Figura 4. Modelo TCP/IP

2.2.5. Software Libre

Se refiere a un software de código abierto el cual puede ser analizado, estudiado y modificado libremente con el fin de contribuir con el conocimiento a diferentes comunidades de desarrolladores permitiendo mejorar el software a través de la colaboración.

> El software libre (free software) hace referencia al programa que una vez puesto a disposición del público (publicado o entregado), da libertad al usuario de este sobre tal producto y por tanto este programa puede ser usado, copiado, estudiado, cambiado y redistribuido libremente. Esta es la definición más aceptada por la comunidad de desarrolladores de software y ha sido establecida por la Free Software Foundation. El concepto de software libre es universal. (Gómez y Arteaga, 2010, p.2)

Actualmente el estado promueve el uso de herramientas de software libre en instituciones que permitan mejorar la educación y el acceso libre a herramientas se relacionen al progreso y desarrollo de las personas.

2.2.6 Protocolos de gestión

De acuerdo con Martínez (2015), los protocolos de gestión de red más importantes son SNMP, NetFlow, CDP y Syslog, la utilización de más de un protocolo de gestión implementado en una red no se recomienda, ya que tales combinaciones son perjudiciales e incrementan notoriamente la complejidad de la red.

2.2.6.1. NetFlow

Es un protocolo de código abierto el cual mediante estadísticas sobre el tráfico de red y una maquina recolectora permite conocer toda la información que se crea en los dispositivos.

> El protocolo abierto NetFlow, desarrollado por CISCO System, ha demostrado ser muy útil en el trabajo diario de los técnicos de red, ya que permite monitorizar y representar el tráfico de red en tiempo real, pero también es una herramienta esencial para los técnicos de seguridad que pueden utilizar la información de los registros NetFlow recibidos de los dispositivos capaces de exportar esta información para analizar y detectar ataques y anomalías de seguridad, aumentando así su proactividad y su capacidad de operación y respuesta.(Malagón, 2009, p.1)

Toda la información que obtiene y con la cual trabaja para el análisis mediante el protocolo NetFlow es de suma importancia y así mismo confidencial por lo cual no obtiene datos del usuario, únicamente datos de sus conexiones, permitiendo visiones detalladas del comportamiento de toda la red.

2.2.6.2. CDP

Cisco Discovery Protocol (CDP) es un protocolo de gestión de red del cual es propietario Cisco utilizado específicamente para el descubrimiento de los dispositivos.

> El CDP es un protocolo propietario de Cisco, destinado al descubrimiento de vecinos y es independiente de los medios y del protocolo de enrutamiento. Aunque el CDP solamente mostrará información sobre los vecinos conectados de forma directa, este constituye una herramienta de gran utilidad. El Protocolo CDP es un protocolo de Capa 2 que conecta los medios físicos inferiores con los protocolos de red de las capas superiores. (Ariganello,2020, p.2).

Este tipo de protocolo permite encontrar información acerca de las conexiones entre los dispositivos, además de útil es fácil de usar debiendo así dividir la red y especificar que equipos que desea monitorear.

2.2.6.3. Syslog

El protocolo SysLog es muy sencillo y tiene problemas con su seguridad, pero el hecho de fácil uso hace que muchos dispositivos lo implementen integrando mensajes de varios tipos de sistemas en un solo repositorio central. Méndez (2016) afirma: "El protocolo y servicios Syslog proveen un transporte y funcionalidades para el envío de mensajes a través de redes IP con el objetivo de centralizar servicios de log" (p.3). Además, se presenta un formato para mensajes y el mapeo del transporte, describiendo los elementos de datos estructurados sin incluir formatos y almacenamiento.

2.2.6.4. SNMP

Simple Network Mangement Protocol (SNMP), fue el primer protocolo de gestión de la red creado en 1988, tratándose de un protocolo de aplicación IP que se ha convertido en el estándar para el intercambio de información y administración entre diversos dispositivos de red. Martínez (2015) afirma que: "SNMP se ejecuta sobre User Datagram Protocol (UDP) y por lo tanto no proporciona inherentemente secuenciación y reconocimiento de los paquetes, pero aun así se reduce la cantidad de sobrecarga usado para la información de gestión" (p.1). Permitiendo a los administradores de red supervisar el correcto funcionamiento de los equipos, rastreando, identificando y resolviendo el problema.

2.2.7. Protocolo SNMP

Protocolo SNMP es un protocolo base en la administración o gestión de la red que permite monitorear el tráfico de datos y equipos que se encuentran dentro de la red el cual opera a nivel de la capa de aplicación permitiendo la facilidad de intercambio de información sobre la gestión de los equipos de red.

> Se puede usar SNMP para monitorizar el estado de los routers, servidores y otros componentes de red, pero también se usa para controlar dispositivos de red o tomar acciones de forma automática en caso de que se presente un problema. Se puede monitorizar información, ésta puede ser simple, como la cantidad de tráfico que entra o

sale en una interfaz, o puede ser algo más complejo como la temperatura del aire dentro de un router. También puede verificar la velocidad a la cual opera una interfaz de red. (Naranjo, 2016, p.20)

Con la herramienta de monitoreo y en base a el protocolo SNMP se puede decir que con la implementación se mejora el control y uso eficiente de los recursos de red de la institución, por ende, habrá una mejor prestación de servicios al usuario.

2.2.6.1. Mensajes SNMP

Los mensajes SNMP son los encargados en recopilar la información entre el gestor y el equipo administrado de manera asincrónica según los eventos que ocurran dentro de este.

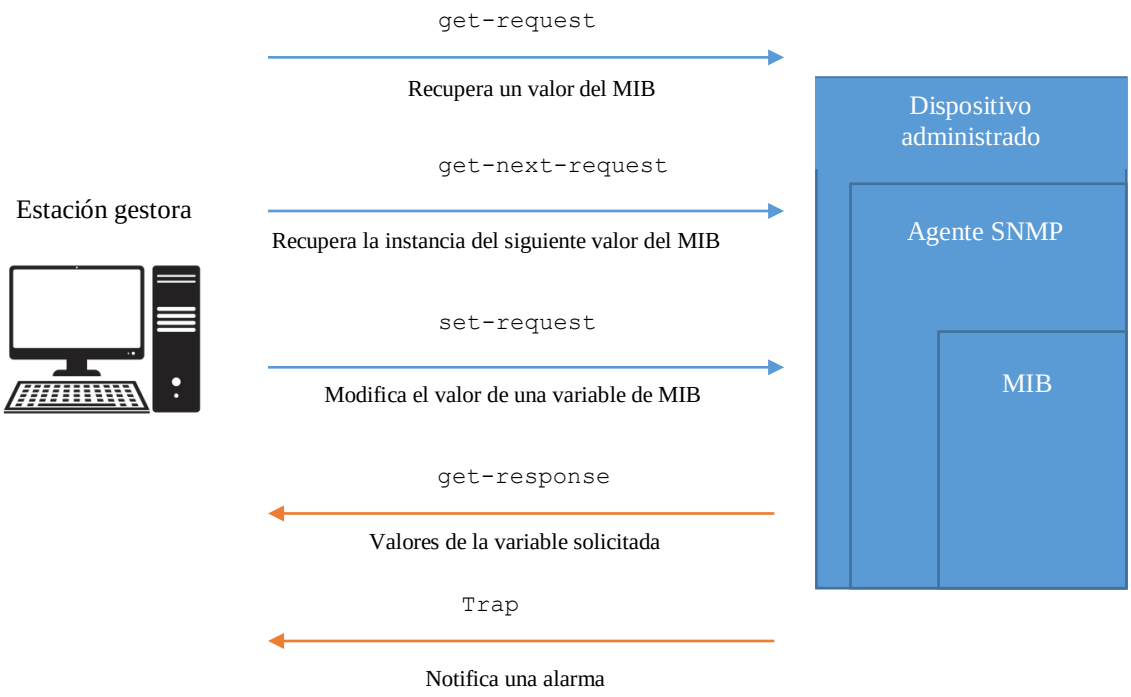


Figura 5. Mensajes SNMP

2.2.6.2. Versiones SNMP

Hoy en día, el hablar de una red administrada por SNMP es símbolo de seguridad y cada administrador o estudiantes que interactúen constantemente con redes en algún momento de su vida tendrán que toparse con el protocolo SNMP el cual ayudara a garantizar la disponibilidad, el funcionamiento y la resolución rápida de problemas.

> Los orígenes de SNMP también se remontan a finales de los 80, cuando la administración de red carecía de herramientas de administración de red adecuadas que no dependieran de los fabricantes de hardware. En estos tiempos surgieron dos protocolos importantes. El CMISE / CMIP (Common Management Information Services Element / Common Management Information Protocol) y SNMP (Simple Network Management Protocol), que tiene sus raíces en el SGMP (Simple Gateway Monitoring Protocol) alias RFC 1028. (Wittmann,2017, p.3)

Con la activación del protocolo SNMP sea en switches, servidores, APs u otro dispositivo de conexión de redes, se puede supervisar casi todo, esto incluye carga de cpu, estado de ventiladores, el tráfico en un conmutador, enrutador o concentrador. Además, la obtención de respuestas ante eventos programados o no programados es vital dentro de una monitorización.

- **SNMPv1**

Es la versión de SNMP más antigua, la cual incorpora una seguridad precaria debido a que usa una contraseña limitada, actualmente esta versión no se distribuye en los equipos de telecomunicación. Esta versión de SNMP propone un modelo "gestor-agente" y ha sido la base para la comunicación entre la estación del gestor y cada agente operando a nivel de aplicación.

- **SNMPv2c**

Es la evolución del protocolo SNMP, a diferencia de la primera versión cuenta con mayor número de mejoras las cuales incluyen el manejo mejorado de errores, la comunicación de administrador con administrador y comandos set más potentes.

- **SNMPv3**

Es la última versión de SNMP en la cual se incorpora seguridad para mantener una comunicación más privada entre entidades administrativas, integrando seguridad de acceso a los dispositivos de interconexión mediante una autentificación y cifrado de paquetes que transitan por la red de datos.

Tabla 1. Versiones SNMP

	SNMPv1	**SNMPv2**	**SNMPv3**
Estándares	RFC-1155.1157.1212	RFC-1441,1452 RFC-1909.1910 RFC- 1901 a 1908	RFC-1902 a 1908, RFC-2271 a 2275
Seguridad	Ninguna seguridad	No mejoró la seguridad	Su principal característica es la mejora en la seguridad
Complejidad	Limitaciones en rendimiento y seguridad	Más potente pero más complejo que en la primera versión	Se centra en mejorar el aspecto de la seguridad
Tipos de paquetes	- Get-Request - Get-Next-Request - Set Request - Get Response	- Get-Request - Get-Bulk-Request - Get-Next-Request - Set Request - Inform-Response SNMP v2 Trap	Las funciones básicas de v3 son de v1 y v2. La versión 3 tiene un nuevo formato de mensaje SNMP

2.2.7 Agente SNMP

Dentro de los dispositivos a monitorizar se encuentran los llamados agentes los cuales permiten la administración.

> El agente es un programa que está empaquetado dentro del elemento de red. La habilitación del agente le permite recopilar la base de datos de información de administración del dispositivo localmente y la pone a disposición del administrador SNMP, cuando se le solicita. (ManageEngine, 2020, p.2)

Estos agentes SNMP ayuda a administrar y exponen los datos de la gestión a las estaciones desde donde se administra o monitoriza la información permitiendo la actuación rápida de los administradores de red.

2.2.7.1. Funciones del agente SNMP

- Recopila toda la información de administración del entorno local.
- Almacena, recupera y permite el análisis de la información de gestión según se define en la MIB.
- Señala un evento al administrador mediante notificaciones.
- Actúa como proxy para algunos nodos de red administrables que no son SNMP.

2.7.1.2. Funcionamiento

Dentro del funcionamiento SNMP se destaca la administración donde se recopila la información mediante diversas acciones, reflejando los recursos de los dispositivos monitoreados, así como sus actividades.

> Los agentes SNMP que residen en los dispositivos administrados recopilan y almacenan información sobre los dispositivos y su funcionamiento. El agente almacena esta información localmente en la MIB. El administrador SNMP luego usa el agente SNMP para tener acceso a la información dentro de la MIB. (CCNA, 2018, p.3)

Además, de destacar la administración y recopilación, también puede recuperar información valiosa activando dentro de los dispositivos mediante herramientas de monitoreo distintos umbrales de notificaciones de acciones o disparadores.

2.2.7. Monitoreo

Es un proceso de recolección y utilización de la información que permite hacer el seguimiento y análisis sobre el progreso de un programa, permitiendo tomar decisiones de gestión, generalmente el monitoreo tiene lugar en actividades que desarrolla una entidad.

2.2.7.1. Sistema de monitoreo

Es un conjunto de procesos que permite analizar constantemente una red de computadoras en busca de fallos, para luego informar al administrador de la red y a la vez mitigar el problema. “Un sistema de monitoreo es aquel que permite realizar un análisis cuantitativo y cualitativo del tráfico en una red local o global, el cual puede generar reportes en tiempo real o en intervalos de tiempo, con la capacidad de proveer al usuario consultas, alertas que muestren el estado en que se encuentre un servicio” (Gonzales y Carrasco, 2015, pp.12-13). Por tanto, el uso de un sistema de monitoreo es indispensable en una entidad dado que permite mantener una red de datos operativa y disponible a los usuarios conectados a la misma.

2.2.8. Tipos de sistema de monitoreo de red

2.2.8.1. Monitoreo activo

El monitoreo activo está orientado a medir el rendimiento de una red de datos puesto que determinar la calidad de servicio que esta presenta. “Este tipo de monitoreo se realiza inyectando paquetes de prueba en la red, o enviando paquetes a determinadas aplicaciones midiendo sus tiempos de respuesta. Este enfoque tiene la característica de agregar tráfico en la red” (Sánchez, 2017, p.10). Además, este tipo de monitoreo es de gran importancia dentro de una entidad puesto que permite a el encargado en el manejo de la red tomar mejores decisiones para que la red de datos sea más operativa y brinde mejor servicio a los usuarios que hagan uso de esta.

2.2.8.2. Monitoreo pasivo

Este tipo de monitoreo está orientado a la recolección de información dentro de una red de datos y a partir de esta hacer un análisis que determine el tráfico que circula dentro de la misma. “Este enfoque se basa en la obtención de datos a partir de recolectar y analizar el tráfico que circula por la red. Emplean diversas herramientas como sniffers, software de análisis de tráfico y en general dispositivos con soporte para SNMP” (Sánchez, 2017, p.10). El monitoreo activo y pasivo son mecanismos de relevancia dentro de una red de datos puesto que al relacionarse permite un análisis más completo de la red permitiendo determinar problemas que se presentan dentro de la misma en un gestor de eventos ayudando a el departamento de red tomar mejores decisiones.

2.2.8.3. Monitoreo basado en SNMP

Actualmente existen dos métodos para la gestión de la red de datos los cuales implementan protocolos diferentes entre estos esta (CMIP/ CMIS) propuesto por la organización OSI y el otro SNMP propuesto por IETF. “SNMP se ha convertido en el protocolo de gestión de red más popular por su simplicidad y escalabilidad. Casi todos los fabricantes de equipos de red admiten SNMP” (Zeng y Wang, 2009, p.680). Mediante el uso de protocolo SNMP dentro de la infraestructura interna de la institución se podrá determinar aspectos básicos en la gestión de equipos de red, permitiendo determinar problemas presentados dentro de la red de datos, para ello el uso del protocolo SNMP con implementación de una herramienta de monitoreo permitirá un análisis más profundo de la misma manteniendo una red más operativa.

2.2.8. Elemento de la gestión de red

La arquitectura de administración en una red está distribuida por: Gestor, agente y dispositivos administrados con los cuales se pretende recopilar información sobre el estado en el que se encuentre cada equipo que cuente configurado el agente.

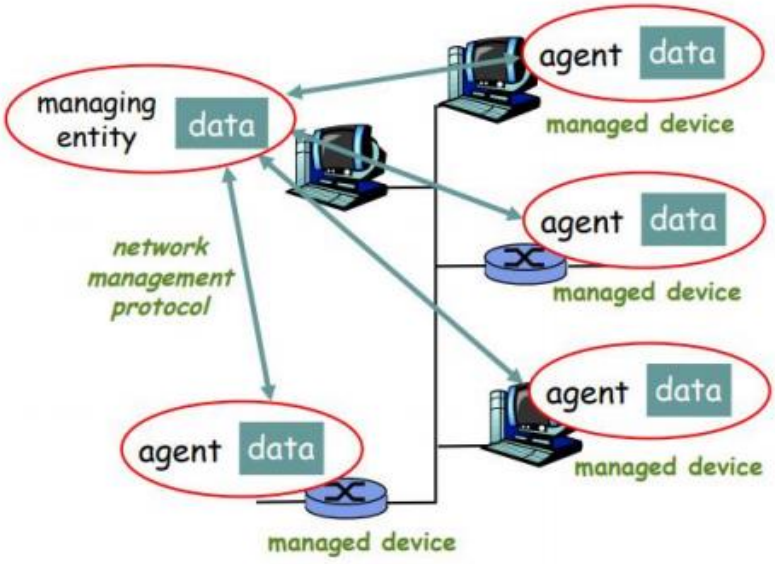


Figura 6. Esquema de Elementos de Gestión de Red.

Fuente: Protocolo SNMP, por Lorge, (2020).

2.2.8.1 Gestor

Es la persona encargada de administrar la infraestructura de la red de la entidad también denominado Network Management Station (NMS). Este gestor tiene la responsabilidad de la supervisión y control de todos los dispositivos que se encuentran en la red.

2.2.8.2. Agente

El agente en la gestión de una red es el software de administración que se encuentra en los dispositivos para ser gestionados en estos se encuentran los MIB (base de datos local de información de administración) los cuales permiten tomar la información necesaria sobre el estado en el que se encuentran los dispositivos mediante el protocolo SNMP indicando cuando se produce un evento al administrador.

2.2.8.3. Dispositivos administrados

Los dispositivos administrados son los equipos en los cuales se encuentra activado el agente SNMP para ser monitorizado estos pueden ser: routers, switch, servidores, hubs, computadoras entre otros dispositivos de interconexión.

2.2.9. Calidad de servicio

La calidad de servicio dentro de las redes de datos se caracteriza por la priorización de tráfico y garantía de ancho de banda para un rendimiento óptimo para los usuarios.

Narváez (2015) Indica que:

> La convergencia hoy en día es una de las características primordiales de las redes de comunicación, actualmente través de las infraestructuras de redes ya sea por medios como: fibra óptica, inalámbrico o cobre no solo se transmite datos, sino que también tráfico de voz, video, multimedia, en general aplicaciones críticas y en tiempo real. Estos diferentes tipos de tráfico no tienen los mismos requerimientos en cuanto a: delay, jitter, descarte de paquetes y consumo de ancho de banda y por lo tanto la implementación de estos requiere de calidad de servicio, es decir mecanismos que garanticen su transmisión y recepción con parámetros aceptables y a satisfacción de los usuarios. (p.53)

Es la característica que le da el usuario al hacer uso de ese servicio por tanto quien puede calificar viene siendo únicamente quien haga uso, evidenciando que cumpla con ciertos requerimientos garantizando siempre la eficiencia e integridad del servicio.

2.2.10. Seguridad en sistemas de monitoreo

Los sistemas de monitoreo de red permiten alertar a los administradores de la red cuando haya algún problema o surja algún error, ayudando a mantener una buena disponibilidad.

Motadata (2019) afirma:

> Una herramienta de monitoreo de red le permite luchar contra las brechas de datos para proteger sus datos críticos para el negocio. El mayor beneficio que obtiene es una imagen aparente de cómo se ve el rendimiento de red "óptimo" para la infraestructura

de su empresa. Esta transparencia simplifica la identificación de cualquier desconfianza que surja en su red.

El tener definido el monitoreo dentro de la red y los controles que se van a utilizar, ya que de esta forma se incrementa la efectividad y disponibilidad de todo el sistema.

2.2.11. Gestión de red

La gestión de red permite un control adecuado de los equipos y recursos de la red de datos con el fin de garantizar la disponibilidad de los servicios que esta provea, mejorando el rendimiento de esta.

> Esto permite optimizar el uso. recursos disponibles y reduce el tiempo de inactividad del equipo y / o servicio red, principalmente ayudando a los gerentes en la toma de decisiones, por ejemplo, clúster de servidores de archivos, en caso de que un equipo deje de funcionar, los gerentes son Se le pedirá que defina una estrategia rápida para resolver el incidente. (Benicio, 2015, p.21)

Dentro de la gestión de la red en la institución se incluye el rendimiento, parte fundamental que se pretende medir y controlar gestionando mejor los recursos utilizados en cada uno de los equipos de red, además se prevé gestionar los fallos presentados en la red de datos como también cada una de las configuraciones tanto de software como de hardware permitiendo tener una red más operativa.

> La gestión de red está basada en el paradigma gestor-agente, en el cual el primero ejecuta aplicaciones que supervisan y controlan permanentemente los elementos administrados de la red, y el segundo, se encuentra ubicado en los elementos de red y ejecuta las acciones invocadas por el gestor. (Trujillo,2019, p.6)

Por lo tanto, su principal objetivo es el de mejorar el rendimiento y disponibilidad de los recursos de la red garantizando un nivel adecuado del servicio que se provea.

2.2.12. Herramientas de monitoreo

2.2.12.1. NAGIOS

Nagios es un sistema de monitorización de código abierto ampliamente utilizado en la vigilancia de los equipos (hardware) y servicios (software) que se encuentran en constante expansión de información. Así, nagios siendo un software de código abierto ha sido diseñado para la supervisión continua y automática en sistemas informáticos o tecnologías de infraestructura de comunicaciones escrito bajo General Public License (GNU) enfocándose principalmente en vigilar el comportamiento de hosts y servicios de red. (Nagios, 2012).
Las características principales de nagios son:

Tabla 2. Características Principales de Nagios

Características
• Monitoreo de servicios de red • Monitoreo de recursos (CPU, Memoria, Discos, etc.) • Definición de contacto para envío de notificaciones • Manejo de eventos • Logs de eventos • Interfaz web • Multiplataforma

Nagios puede ser utilizado de manera gratuita con todos sus componentes los cuales permiten que este sea más interactivo y de fácil manejo mostrando todos los análisis que permite hacer tanto a hardware como software.

2.2.12.2. PRTG Network Monitor

PRTG Network Monitor es una herramienta de gratuidad durante 3 meses y permite durante este tiempo una versión ilimitada supervisando toda la infraestructura de TI dentro del monitoreo de la red. Así, esta solución unificada para el monitoreo de una infraestructura de red elaborada por Paessler AG. PRTG funciona en equipos con windows, recopilando información sobre equipos de interconexión generando datos estadísticos sobre estos. También permite recopilar datos históricos. Incluyendo gráficas en tiempo real y reportes (Paessler, 2018).

Algunas de las características de PRTG son:

Tabla 3. Características Principales de PRTG

Características
• Monitoreo de ancho de banda, tiempo de actividades y SLA • Monitoreo de ubicaciones con una sola licencia • Ideal para redes de distintos tamaños • API basado en HTTP para comunicación con otras apps • Descubrimiento automático de red (IPv4/IPv6)

Estas características han permitido la comprensión y entendimiento de los datos al ser recopilados y analizados de forma exhaustiva por los administradores de la red, siendo esto de gran beneficio para las instituciones.

2.2.12.3. CACTI

Es una herramienta de código abierto con la cual se puede verificar toda la información necesaria gracias a su pantalla grafica la cual se puede modificar de acuerdo con las necesidades del administrador. “Cacti es una solución gráfica que permite monitorizar dispositivos conectados a una red que tengan activado el protocolo SNMP. Cacti provee un modelo avanzado de plantillas, múltiples métodos de adquisición de datos y funciones de gestión de usuarios” (Cacti, 2015). Puede monitorear redes complejas con miles de dispositivos y se distribuye bajo licencia GPL, y con su solución grafica se puede aprovechar todas sus funcionalidades como la adquisición de datos y las funciones de administración.

Algunas de sus características son:

Tabla 4. Características Principales de CACTI

Características
• Uso de PHP, Mysql, RRDTOOL • Ilimitado número de elementos para cada gráfico • Scripts personalizados • Organización jerárquica de la información • Soporte SNMP • Admite creación de usuarios y permisos

CACTI se caracteriza por su solución gratuita grafica la cual permite monitorizar los dispositivos conectados a la red con la gran amplitud, recopilando datos y manteniendo su propia configuración.

2.2.12.4. ZABBIX

ZABBIX es una herramienta de código abierto la cual nos permite la monitorización de diferentes componentes de la red, logrando gran amplitud en la recepción de información y paquetes de datos. Así, siendo un software de código abierto diseñado para la monitorización de red, esta herramienta tiene la posibilidad de recopilar una amplia gama de datos de miles de servidores, máquinas virtuales y dispositivos de red simultáneamente, contando con almacenamiento de datos, características flexibles de visualización y análisis, así como formas muy variadas de evaluar los datos con el fin de alertar los problemas que aparecen (Zabbix, 2016). Además, de vigilar numerosos dispositivos permite mantener la integridad de los servidores con mecanismos flexibles dando prioridad a los usuarios y permitiendo alertar rápidamente a los administradores, los cuales pueden reaccionar a los distintos problemas que se pueden suscitar.

Algunas de las características de ZABBIX son:

Tabla 5. Características Principales de ZABBIX

Características
• Detección automática de servidores y dispositivos en la red • Software de servidores para Linux • Autentificación de usuarios • Permiso de usuarios flexibles • Interfaz web • Notificación por email • Auto descubrimiento

ZABBIX es software de nivel empresarial, código abierto y viene sin costo, diseñado específicamente para el monitoreo en tiempo real de millones de métricas recopiladas dentro de los servidores, máquinas virtuales y dispositivos de red.

2.2.12.5. ZENOSS

ZENOSS es una plataforma inteligente de gestión de operaciones que transmite y normaliza todos los datos de la máquina, permitiendo de forma única la aparición de contexto para evitar interrupciones del servicio en entornos modernos y complejos. Así, la herramienta de monitoreo de red proporciona funcionalidades necesarias para el control eficaz de la red de datos como también estabilidad y rendimiento de los equipos de interconexión que se encuentran monitorizados. Esta herramienta cuenta con una versión libre y dos versiones comerciales (Zenoss,2019). Zenoss ha sido desarrollada como un software hibrido el cual puede trabajar en infraestructuras físicas, virtuales y basadas en la nube.

Sus principales características son:

Tabla 6. Características Principales de ZENOSS

Características
• Detección automática de dispositivos • Interfaz web • Generación automática de eventos • Envío de correo electrónico y sms • Dashboard personalizado • Generación de informes multigráfico

La herramienta ZENOSS debido a su sistema integrado proporciona estabilidad, fácil configuración y un rendimiento de los servicios eficiente.

2.2.13. Comparativa de herramientas de monitoreo

Para la comparación se tomó en cuenta cinco herramientas de gestión de red. De acuerdo con PANDORAFMS (2016), algunas de las mejores herramientas de monitoreo de redes (gratis y de pago) que existen actualmente en el mercado son: NAGIOS, ZABBIX, ZENOSS, PRTG NETWORK MONITOR, CACTI.

Tabla 7. Comparativa de Herramientas de Monitoreo

REQUISITOS	**Requisitos funcionales**				**Requisitos de Usabilidad**	**Atributos del sistema**				**CUMPLIMIENTO TOTAL DE REQUISITOS**	
DESCRIPCIÓN	Monitorización de manera remota	Autodescubrimiento de la red	Notificaciones y alertas	Generación de reportes	Visualización gráfica	Fácil instalación, configuración y uso	Ingreso al sistema con usuario y contraseña	Funcionamiento del sistema las 24h del día	Cambios de configuración	Rendimiento	
NAGIOS	SI	SI	SI	SI	SI	NO	SI	SI	SI	SI	88,80%
ZABBIX	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	100%
ZENOSS	SI	SI	SI	SI	SI	NO	SI	SI	SI	SI	88,80%
PRTG NETWORK MONITOR	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	100%
CACTI	SI	NO	SI	NO	SI	SI	SI	SI	SI	SI	77,70%

III. METODOLOGÍA

3.1. ENFOQUE METODOLÓGICO

3.1.1. Enfoque

Para efecto de esta investigación se toma en cuenta un enfoque mixto, dado a que se va a medir las variables de estudio tales como sistema de monitoreo y rendimiento de la red de datos, en el caso de la variable sistema de monitoreo será del enfoque cuantitativo discreta. Ortega (2018) define que la investigación cuantitativa: "Utiliza la observación del proceso en forma de recolección de datos y los analiza para llegar a responder sus preguntas de investigación. Este enfoque utiliza los análisis estadísticos" (p.3). Por tanto, permite establecer el número de eventos que ocurren internamente en la red de datos como también el número de equipos monitorizados diariamente por parte del administrador de red esta información permitirá conocer como es el funcionamiento ante posibles problemas que presente la red, los datos se estarán manejando con encuestas para un análisis estadístico sobre que eventos producen más cuellos de botella dentro de la infraestructura de red de la institución. Para la variable del rendimiento de la red de datos se utilizará el enfoque cualitativo ordinal con el cual se podrá contextualizar las experiencias que tienen los usuarios de la red de datos de la UPEC. "Es escogido cuando se busca comprender la perspectiva de individuos o grupos de personas a los que se investigará, acerca de los sucesos que los rodean, ahondar en sus experiencias, opiniones, conociendo de esta forma cómo subjetivamente perciben su realidad (Guerrero, 2016, p.3). Este tipo de enfoque permite conocer la satisfacción de los usuarios en el uso de los mismos servicios.

Por tanto, se puede concluir que el proyecto de investigación utilizara el enfoque mixto para la recolección de información utilizando sus técnicas e instrumentos permitiendo obtener resultados pertinentes a la investigación.

3.1.2. Tipo de Investigación

Para esta investigación se consideró el enfoque metodológico mixto, permitiendo obtener mejores resultados en la resolución de problemas además se considera la investigación descriptiva, bibliografía y la investigación acción, basándose en una investigación acción la cual permite actuar directamente con los problemas que ocurren en nuestro entorno, por tanto,

la investigación es de manera directa, en este caso mediante la implementación de un sistema de monitoreo que permita determinar los problemas de red que se suscitan en intervalos de tiempo y a la vez mitigarlos evitando el congestionamiento de los servicios de la red de datos de la UPEC.

3.1.2.1. Investigación bibliográfica

Se hace uso de este tipo de investigación para ayudar la obtención de información fidedigna de fuentes confiables que permitan conocer sobre los conceptos y ventajas de las herramientas de monitoreo de la red de datos además de cómo es el funcionamiento de cada una de estas permitiendo seleccionar la más idónea e iniciar la implementación de esta herramienta.

3.1.2.2. Investigación descriptiva

Por otra parte, la investigación descriptiva hace uso de preguntas planteadas hacia problemas precisos, además se describe problemas relacionados con fenómenos sociales y educativos, con lo cual se puede decir que se trabajaría con el problema específico encontrado dentro de la investigación.

Cauas (2015) afirma:

> Este estudio se dirige fundamentalmente a la descripción de fenómenos sociales o educativos en una circunstancia temporal y especial determinada. Los diferentes niveles de investigación difieren en el tipo de pregunta que pueden formular. Mientras en las investigaciones exploratorias no se plantean preguntas que conduzcan a problemas precisos, sino que se exploran áreas problemáticas, en este nivel las preguntas están guiadas por esquemas descriptivos y taxonomías; sus preguntas se enfocan hacia las variables de los sujetos o de la situación. (p. 6)

Esta investigación se centra en describir cual es el motivo en este caso "el que" utilizando técnicas como la observación y la encuesta entre otras, y esta no altera o manipula ninguna de las variables de estudio y se limita a la medición y descripción de esta.

3.2. IDEA A DEFENDER

El sistema de monitoreo influye positivamente en la intermitencia y mejora el rendimiento de la red de datos que utilizan los usuarios en la Universidad Politécnica Estatal del Carchi.

3.3. DEFINICIÓN Y OPERACIONALIZACIÓN DE VARIABLES

3.3.1 Definición de variables

- **Sistema de monitoreo:** "Un sistema de monitoreo es aquel que permite realizar un análisis cuantitativo y cualitativo del tráfico en una red local o global, el cual puede generar reportes en tiempo real o en intervalos de tiempo, con la capacidad de proveer al usuario consultas, alertas que muestren el estado en que se encuentre un servicio." (Gonzales y Carrasco, 2015, pp.12-13).
- **Rendimiento de la red de datos:** "Se denomina red de datos a aquellas infraestructuras o redes de comunicación que se ha diseñado específicamente a la transmisión de información mediante el intercambio de datos." (Ochoa, 2017, p.29).

3.3.2. Operacionalización de variables

Tabla 8. Operacionalización de Variables

Variable	Dimensión	Indicadores	Técnica	Instrumento
Sistema de monitoreo (Independiente-Cuantitativa-Discreta)	Red de datos	Número de herramientas especializadas en el monitoreo Número de nodos	Encuesta: Entrevista	Cuestionario
	Dispositivos de interconexión	Número equipos conectados al sistema de monitoreo en la red de datos		
	Servidores	Número de servidores utilizando el sistema de monitoreo		
	Vlan's	Número de vlan's		
	Métodos de Acceso	Número de megas por derivación o troncal		
	Agentes SNMP	Número de procesos ejecutados		
	Calidad de servicio	Nivel de calidad del servicio QoS	Encuesta Entrevista	

		Nivel de configuración Tiempo de respuesta del servicio	Cuestionario
Rendimiento de la red de datos (Dependiente-Cualitativa-Ordinal)	Dispositivos conectados a la red	Características de dispositivos conectados a la red.	
	Ancho de banda	Nivel de dispersión de ancho de banda	
	Latencia	Grado de calidad del ancho de banda	
	Envió de paquetes	Nivel de latencia en la red	
	Tasas de error	Nivel de errores presentes en la red de datos	
	Tráfico en la red	Factor del tráfico de datos en la red	
	Disponibilidad	Nivel de satisfacción del usuario	

3.4. MÉTODOS UTILIZADOS

3.4.1. Métodos

Para el análisis de esta investigación se ha enfocado en el método analítico y lógico deductivo permitiendo el método analítico identificar el funcionamiento de la infraestructura física y lógica de la institución determinando problemas que inciden en el rendimiento de la red de datos lo cual corvella una insatisfacción por parte de la comunidad universitaria, por otra parte, el método lógico deductivo permitirá la identificación de una herramienta de monitoreo que mayor se ajuste a los requerimientos de los equipos de la institución permitiendo mitigar problemas como cuellos de botella mejorando los servicios de la red de datos.

3.4.2. Análisis estadístico

- **Población y Muestra**

Al conocer la población de estudio se determina que la investigación es finita, de acuerdo a el departamento de dirección académica de la UPEC del año 2020, se tiene un total de 3301 estudiantes que integran la comunidad universitaria, por ende, se ve necesario sacar una muestra debido a que el número de estudiantes es alto para la aplicación de la encuesta, se toma en cuenta a los estudiantes de la institución puesto que son quienes dependen del buen funcionamiento de la red de datos para desempeñar sus actividades estudiantiles. Para visualizar el número de estudiantes matriculados véase en el "Anexo 4".

El nivel de confianza es el valor obtenido mediante niveles de confianza. Su valor es una constante, el valor mínimo aceptado para considerar la investigación como confiable es de 1.96, equivalente al 95%.

Para determinar el tamaño de la muestra, es decir, el número de sujetos necesarios para que los datos obtenidos de la encuesta sean representativos de la población se utiliza la ecuación 1:

$$n = \frac{NZ^2S^2}{d^2(N-1) + Z^2S^2}$$

Donde:

n= Muestra número de personas a ser encuestadas

N= Población total (3301)

Z= Nivel de confianza de los encuestados (1,96)

S= Desviación estándar

d= precisión absoluta

$$n = \frac{3301(1.96)^2(0.05 * 0.95)}{(0.05)^2(3301 - 1) + (1.96)^2(0.05 * 0.95)} = 71$$

- **Técnicas**

Como parte del proceso de extracción de datos se consideran las siguientes técnicas de recopilación de información.

- **Entrevista**

Para la obtención de la información del funcionamiento de la infraestructura de la red datos de la Universidad Politécnica Estatal del Carchi se aplicó una entrevista semiestructurada dirigida a el ingeniero Javier Torres quien desempeña la función de administrador de la red del departamento de TIC´s, en donde se determinó sobre los requerimientos de funcionalidad de la herramienta de monitoreo a implementar, permitiendo mitigar los problemas recurrentes que aquejan a la red de datos de la institución.

- **Encuesta**

Se establece como técnica una encuesta estructurada ya que tiene como función primordial la recolección de datos por medio de un instrumento y al cual se le denomina cuestionario, además, cuyo objetivo es conocer la satisfacción de los usuarios sobre la red interna de datos de la UPEC en el año 2020, siendo los usuarios encuestados estudiantes para la obtención de los resultados de la investigación.

IV. RESULTADOS Y DISCUSIÓN

4.1. RESULTADOS

A continuación, se presentan los resultados de esta investigación sobre la implementación de una herramienta de monitoreo en la Universidad Politécnica Estatal del Carchi, en el cual se formularon 5 objetivos que se lograron alcanzar, para el análisis y procesamiento de este capítulo se aplicó una entrevista semiestructurada y una encuesta estructurada como técnicas de recopilación de información, permitiendo mejorar los tiempos de respuesta al suscitarse un problema interno de la red de datos de la institución. La información obtenida es vital para el mejoramiento del servicio de red de la Universidad Politécnica Estatal del Carchi.

Implementar un sistema de monitoreo basado en el protocolo SNMP, por medio de herramientas de Software Libre, disminuyendo la intermitencia y mejorando el rendimiento de la red de datos en la Universidad Politécnica Estatal del Carchi.

Para lograr este objetivo, se implementa la herramienta de monitoreo de Software Libre capaz de alertar sobre los problemas que se suscitan dentro de la red de datos de la institución, además, evidenciando que el uso del sistema de monitoreo de red mejora la calidad de servicio en la institución, disminuyendo la intermitencia y mejorando la experiencia de uso del servicio por parte de los usuarios.

Para este objetivo se toman en cuenta las siguientes preguntas de la entrevista que se detallan en la Tabla 9, para más detalle en el "Anexo 2".

Tabla 9. Resultados del Objetivo General

Ítem	Pregunta	Respuesta
3	¿Qué herramientas utilizan para la detección de fallos en la red?	Al momento no poseemos ningún Hardware ni Software que nos permita detectar los fallos en la red institucional.
11	¿La universidad cuenta con una herramienta de sistema de monitoreo?	La universidad no cuenta con herramientas de monitoreo de la red.

Como se observa en la Tabla 9, se evidencia que la institución no cuenta con herramientas especializadas en el monitoreo de la infraestructura de la red de datos, de tal modo que existe una demora en la identificación de los problemas, a través de la implementación de un sistema de monitoreo se puede decir que influye positivamente en el mejoramiento de la red, pudiendo

tener mayor eficacia en la búsqueda y solución de problemas y a su vez mejore la calidad del servicio de red para los usuarios de la universidad, garantizando así un mejor entorno de trabajo.

Fundamentar bibliográficamente las variables de estudio a través de medios tecnológicos y físicos, para la sustentación de la investigación.

Para evidenciar este objetivo se realizó una revisión bibliográfica en medios digitales como libros, artículos, revistas entre otras fuentes acerca de la gestión de red y protocolos que intervienen en ello, pudiendo conocer los temas relacionados a las variables investigativas presentes en el estudio con las cuales permitan crear argumentos sólidos y fundamentados para la investigación.

Analizar el estado actual de la infraestructura física y lógica de la red de datos, para conocer los requerimientos de gestión de esta.

Para cumplir este objetivo se elaboró una entrevista semiestructura dirigida a la persona encargada de la administración de la red, permitiendo conocer el estado actual de la infraestructura de la red y equipos que esta integra. A continuación, se muestra las preguntas favorables para el alcance del objetivo, detallándose en la Tabla 10.

Tabla 10. Resultados del Segundo Objetivo Específico de la Entrevista

Ítem	Pregunta	Respuesta
1	¿Se establece algún procedimiento para mitigar una falla en la red, al conocerse de alguna?	Básicamente los procedimientos son resolver de manera inmediata las fallas al momento de ser detectadas, ya que pueden existir diferentes fallas no existe un procedimiento preestablecido.
2	¿Mantienen evidencia sobre los diferentes eventos de fallos en la red y de las configuraciones respectivas sobre los equipos y cuál es su proceso para hacerlo?	No se guarda evidencia de los diferentes eventos de fallos, pero de las configuraciones de los equipos si se tiene un respaldo, esto se lo realiza 1 vez al mes de los equipos principales.
4	¿Qué tiempo lleva detectar una falla en la red?	Los fallos en la red son comunicados por aquellas personas que lo detectan, por ejemplo, si no existe conectividad de un teléfono IP, el usuario es quien inmediatamente lo comunica al área de Redes y Telecomunicaciones.
5	¿Cuál es el proceso para la solución del problema en caso de ser detectado?	El proceso es muy simple, aunque no poseemos un esquema que nos indique el procedimiento para cada

		uno de los eventos de fallas, solo se detecta la falla analizar la solución y aplicarla. Existen eventos de fallas que son muy comunes dentro de la red los cuales su solución ya es conocida y reparar esta falla no lleva mucho tiempo.
6	¿Se generan periódicamente registros acerca del rendimiento de los dispositivos de red?	No se han generado registros del rendimiento de ninguno de los equipos activos de la red institucional.
7	¿Cómo calificaría la disponibilidad de los servicios que provee la red de datos de la UPEC?	Dentro de una escala del 1 al 10, lo calificaría con un 8 ya que, debido a la obsolescencia de algunos de los equipos, hay períodos cortos en los que los equipos no responden y es necesario su reinicio.
8	¿Cuál es el proceso de gestión de acceso a los dispositivos de red de la Universidad?	Para la gestión de acceso a los dispositivos, se lo hace vía remota y solamente el administrador de redes y telecomunicaciones conoce y hace uso de las direcciones IP, usuarios y claves para acceder y realizar las configuraciones necesarias en los equipos.
9	¿Cuántos son los equipos con los cuales cuenta la red actual de la Universidad?	Dentro de la red institucional, contamos con más de 200 equipos activos de red, entre los que tenemos, Switch de Core, Firewall, Servidores, Switch de acceso, Access Point, entre otros.
10	¿Se ha levantado la topología actual de la infraestructura física de la UPEC?	Dentro de nuestros esquemas tenemos diseñado una topología física de la red, aunque no se encuentra actualizada por los cambios constantes que se producen. Además, y de igual forma, la topología física se la tiene documentada.

Como se evidencia en las preguntas de la entrevista, se puede deducir que dentro del departamento de TIC’s al momento de la detección de alguna falla en la infraestructura de la institución no se presentan procedimientos adecuados para la mitigación de estas, además, se aprecia que la evidencia de registros de inconvenientes presentados no es almacenada periódicamente por lo que al momento de la toma de decisiones sobre la solución de un problema no es de manera inmediata. Así mismo, estos problemas son comunicados por las personas que se aquejan ante la intermitencia de los servicios. Consecuentemente al ser notificados del problema se toma acciones de manera inmediata, debido a que los problemas recurrentes son conocidos y no llevan mucho tiempo en su respectiva reparación.

La disponibilidad de los servicios dentro de la red de datos de la institución es valorada como buena de acuerdo con el administrador de la red, pero existe deficiencias en periodos de tiempo al contar con equipos obsoletos los cuales no poseen soporte desde hace años atrás siendo para ello muchas veces necesario el reinicio de los equipos.

Para la verificación del funcionamiento de los equipos es necesario contar con la gestión de acceso a los dispositivos siendo las más conveniente hacerlo vía remota a lo cual únicamente el administrador de la red tiene acceso a dichas configuraciones. Además, la institución cuenta actualmente con un aproximando de 200 equipos activos en la red y distribuidos pertinentemente.

De la misma manera se tiene preguntas favorables a el objetivo por medio de la encuesta dirigida hacia nuestro público objetivo, para ello se definen las siguientes preguntas detalladas en la Tabla 11.

Tabla 11. Resultados del Segundo Objetivo Específico de la Encuesta

Pregunta	Nivel	Resultado
¿Con que frecuencia tiene usted problemas de conexión con la red de datos inalámbrica (WIFI) en la institución?	Una vez por día	21,10%
	Más de una vez por día	53,50%
	Una vez por semana	15,50%
	Más de una vez por semana	9,90%
¿Ha experimentado usted problemas con las plataformas (Aulas virtuales, Portafolio académico, Correo electrónico, Pagina Web) institucional?	Siempre	8.5%
	Regularmente	45.1%
	Ocasionalmente	43.7%
	Nunca	2.8%
¿Cuáles han sido los problemas más comunes al utilizar las plataformas (Aulas virtuales, Portafolio académico, Correo electrónico, Pagina Web) de la institución?	Restricciones Ingreso	18.3%
	Demora del Servicio	74.6%
	Indisponibilidad del Servicio	39.4%
	Ninguno	2.8%

Adicionalmente, Los datos obtenidos por medio de la encuesta, se puede apreciar que los usuarios encuestados manifiestan tener problemas de conectividad en la comunidad universitaria, que se dan frecuentemente a lo largo de la jornada educativa al acceder a los servicios que ofrece la institución como son las aulas virtuales, portafolios académicos y repositorio virtual para acceso a documentación para investigaciones. Estos se ven arruinados por una demora en estos servicios, generando inconformidad en los usuarios, y en base a estos datos, se puede considerar la implementación de un sistema de monitoreo, que tenga la capacidad de alertar adecuadamente los problemas en la red para atenderlos rápidamente beneficiando a toda la comunidad universitaria.

- **Infraestructura física de la red de datos**

Actualmente el campus de la UPEC cuenta con un espacio de 5 hectáreas en las cuales consta de un edificio principal administrativo, cuatro edificios de aulas, un edificio de laboratorios, un ágora, una plaza central, canchas deportivas, espacios de recreación, un centro infantil y un coliseo.

La Universidad Politécnica Estatal del Carchi cuenta con una red de datos interconectada entre edificios por medio de enlaces fibra óptica, la cual provee un servicio de internet con un ancho de banda simétrico de 600Mbps contratado con CEDIA, distribuido mediante un router de borde el cual está conectado a un firewall cisco asa 5520 el cual tiene la función de dar seguridad a la red interna de la institución, también tiene la funcionalidad de conectar a la red privada con la pública, este firewall se encuentra conectado con controlador Mikrotik encargado de asignar el ancho de banda a las Vlan’s que se encuentran creadas en la institución.

Posteriormente, se encuentra un switch principal de core catalys 4506-e de capa 3 administrable, en el cual concentra las Vlan’s principales de la institución, es aquí donde se conectan los diferentes enlaces de fibra de las diferentes dependencias de la institución entre una velocidad de 1Gbps y a 10Gbps.

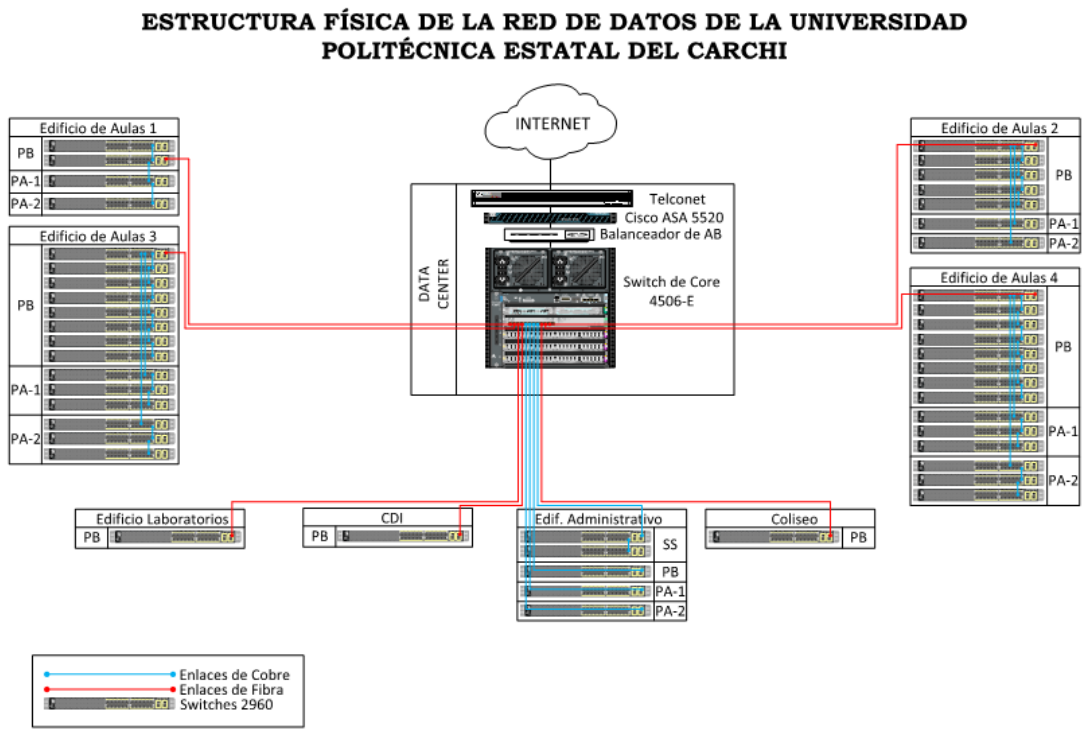


Figura 7. Diseño Físico de la Red de Datos de la UPEC

Fuente: DDTI

➢ Edificio administrativo

El edificio principal administrativo incorpora la mayor parte de actividades administrativas de la UPEC, ubicado en la parte principal del campus universitario, el cual está distribuido en las dependencias como son: contabilidad, tesorería, biblioteca, procuraduría, control cctv, dirección administrativa, talento humano, centro de TIC's, rectorado y vicerrectorado por nombrar las más importantes, se toma mucho en cuenta las dependencias debido a que estás están distribuidas acorde a los equipos y distribución de lo que se refiere a los 5 switch ubicados respectivamente de acuerdo a sus plantas, al igual que los APs, para su detalle véase en el ("Anexo 17 y 18").

- ✓ Planta de subsuelo
- ✓ Planta baja
- ✓ Planta 1
- ✓ Planta 2
- ✓ Planta 3

- **Edificio de aulas 1**

El edificio de aulas 1 conectada con un enlace de fibra óptica principal al switch de la planta baja con el switch de capa core con una velocidad de 1Gbps del enlace troncal, consta de 4 switch administrables y 15 APs ubicados de acuerdo con sus diferentes plantas. (véase el "Anexo 17 y 18")

- ✓ Planta baja
- ✓ Planta 1
- ✓ Planta 2

- **Edificio de aulas 2**

El edificio de aulas 2 se conecta con un enlace de fibra óptica al switch de la planta baja principal con el switch de capa core con una velocidad de 1Gbps del enlace troncal, consta de 8 switches administrables y 15 APs distribuidos en las distintas plantas. (véase el "Anexo 17 y 18").

- ✓ Planta baja
- ✓ Planta 1
- ✓ Planta 2

- **Edificio de aulas 3**

El edificio de aulas 3 se conecta con un enlace de fibra óptica al switch de la planta baja principal con el switch de capa core con una velocidad de 1Gbps del enlace troncal, consta de 14 switch administrables y 15 APs distribuidos en las siguientes plantas: (véase el "Anexo 17 y 18")

- ✓ Planta baja
- ✓ Planta 1
- ✓ Planta 2

- **Edificio de aulas 4**

El edificio de aulas 4 se conecta con un enlace de fibra óptica al switch de la planta baja principal con el switch de capa core con una velocidad de 1Gbps del enlace troncal, consta de 14 switch administrables y 15 APs distribuidos de la siguiente manera: (véase el "Anexo 17 y 18")

- ✓ Planta baja
- ✓ Planta 1
- ✓ Planta 2

- **Coliseo**

El coliseo se conecta con un enlace de fibra óptica al switch de la planta baja principal con el switch de capa core con una velocidad de 1Gbps del enlace troncal, consta de 1 switch administrable y 5 APs distribuidos de acuerdo con las necesidades del lugar. (véase el "Anexo 17 y 18")

- ✓ Planta baja

- **Centro de desarrollo infantil**

El centro de desarrollo infantil se conecta con un enlace de fibra óptica al switch de la planta baja principal con el switch de capa core con una velocidad de 1Gbps del enlace troncal, consta de 1 switch administrable y 1 AP. (véase el "Anexo 17 y 18").

- ✓ Planta baja

- **Edificio de laboratorios**

El edificio de laboratorios se conecta con un enlace de fibra óptica al switch de la planta baja principal con el switch de capa core con una velocidad de 1Gbps del enlace troncal, consta de 1 switch administrable y 6 APs distribuidos en todo el edificio. (véase el "Anexo 17 y 18").

- ✓ Planta baja
- ✓ Planta 1

- **Biblioteca**

La biblioteca se encuentra conectada con un enlace de cable de cobre con el switch de la planta baja con una velocidad de 1Gbs y consta de 4 APs distribuidos 2 en planta baja y dos en el primer piso.

- ✓ Planta baja
- ✓ Planta 1

- **Diseño de la estructura de seguridad lógica**

Dentro de la seguridad lógica de la UPEC se encuentra la interconexión de distintos dispositivos los cuales trabajan para brindar un servicio óptimo a sus usuarios. Como ya se conoce el router de borde encargado de conectar con el firewall cisco asa 5520 realiza distintas funciones, así como el firewall el cual se encarga de brindar la seguridad a toda la red principalmente de acciones mal intencionadas externas o internas, así como de enrutar a la red privada con la pública y la conexión con la DMZ la cual está encargada de proteger a los distintos servidores de ataques o virus (ver figura 8).

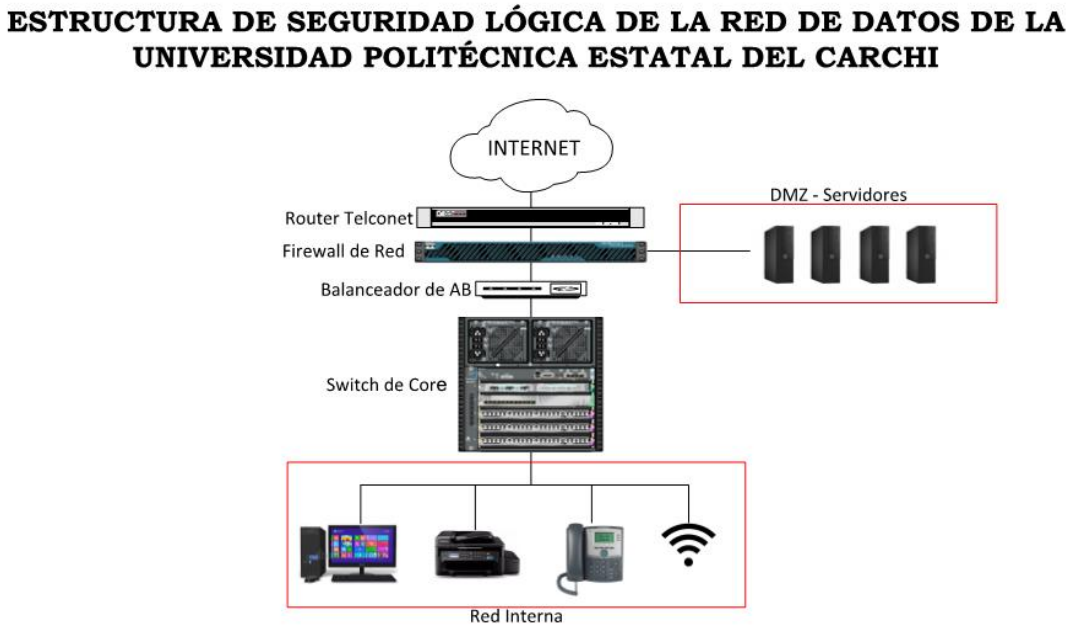


Figura 8. Estructura de Seguridad Lógica de la Red

Fuente: DDTI

- **Distribución de vlan’s**

En la estructura lógica se evidencia la distinta distribución de las vlan’s, las cuales están creadas en el switch cisco catalyst 4506-e, éste se encuentra conectado con el segmentador (Mikrotik) de ancho de banda concentrando los enlaces de fibra óptica de las diferentes dependencias a 1Gbps y a 10Gbps. Al switch cisco catalyst 4506-e también se encuentra el enlace a los distintos servidores de la red como el sistema Integrado, repositorio digital, aulas virtuales, telefonía ip entre otros los cuales se detallan en el “Anexo 22”.

Determinar las herramientas de monitoreo de software libre a través de revisión documental, identificando la más idónea de acuerdo con los requerimientos del departamento de TIC’s.

Para el cumplimiento de este objetivo, se estableció requerimientos de funcionalidad del sistema de monitoreo mediante la entrevista dirigida a el administrador de la red, permitiendo priorizar funcionalidades requeridas, para la comparación de las herramientas se hace una comparativa de los servicios que ofrece de cada una de estas herramientas, seleccionando la más idónea. A continuación, se muestra las preguntas que se establecieron en la entrevista para el cumplimiento de este objetivo, detallándose en la Tabla 12.

Tabla 12. Resultados del Tercer Objetivo Especifico

Ítem	Pregunta	Respuesta
13	¿Equipos o programa de monitoreo que conoce o maneja usted?	Bueno existen algunos, PRTG, Nagios, NTOP, entre otros que son free y licenciados. Y manejo Zabbix, para el monitoreo del enlace principal de internet el cual nos provee CEDIA.
14	¿Basado en su experiencia cuales serían los requerimientos mínimos para implementar un sistema de monitoreo?	Debido a que somos una institución pública y nos basamos en recursos estatales, nuestro principal requerimiento es que sea un software de plataforma libre, así no incurrir en gastos de licenciamiento. Que nos permita ver a cada uno de nuestros usuarios por IP, que nos indique las características físicas que son ocupadas por cada uno de nuestros equipos activos de red y que se pueda generar reportes para su análisis de datos.

Se evidencia en la Tabla 12 que el administrador de la red de datos de la institución conoce acerca de varias herramientas de monitoreo las cuales son de software libre y privatizado, además hacer referencia que utiliza la herramienta zabbix, para el monitoreo del enlace principal de internet el cual es brindado por CEDIA como un usuario normal. Así mismo, se determina que a base de la experiencia del administrador de la red los requerimientos mínimos de implementación es que sea de software libre, puesto que es una institución pública y no incurre en gastos de licenciamiento, para ello se determina los siguientes requisitos de funcionalidad evidenciados en él "Anexo 7".

Implementar la herramienta de monitoreo de la red de datos a través del software seleccionado, permitiendo la monitorización de los recursos de red e identificación de los problemas presentes en esta.

Para el cumplimiento de este objetivo, se implementó el sistema de monitoreo zabbix, herramienta que más se ajusta a los requerimientos del departamento de TIC's cumplimento con cada una de las funcionalidades presentadas por ellos, permitiendo monitorizar todos los recursos de la infraestructura de red de datos de la institución. Para ello se establece las siguientes preguntas de la entrevista.

Tabla 13. Resultados del Cuarto Objetivo Específico de la Entrevista

Ítems	Pregunta	Respuesta
12	¿Qué equipos tienen mayor necesidad de ser monitoreados?	Los equipos activos de red, es decir: Switch de Core, firewall, switch de acceso, servidores, Access points.

Se evidencia en la Tabla 13, sobre que equipos tienen mayor prioridad de ser monitorizados puesto que estos equipos desempeñan funciones de vital importancia, para el correcto funcionamiento de la red de datos de la institución. La implementación se ha realizado por que en las instituciones públicas promueven el uso de software libre.

Además, podemos incluir datos obtenidos gracias a la encuesta, lo cuales se evidencia en la Tabla 14.

Tabla 14. Resultados del Cuarto Objetivo Específico de la Encuesta

Ítem	Pregunta	Nivel	Resultados
9	¿Cree usted necesario que el departamento de TIC's monitoree el uso de los servicios de red para hacer cumplir las políticas y así mantener la calidad de los servicios?	Siempre	67.6%
		Solo cuando existan problemas	32.4%
		Nunca	0%

De acuerdo a la Tabla 14, de la pregunta 9 de la encuesta, el 67.7% de los encuestados están de acuerdo que el departamento de TIC's monitoree frecuentemente la red de datos para así hacer cumplir con las políticas de acceso a la red de modo que se provea un mejor servicio en la red de datos, con la realización de las pruebas correspondiente y determinando los requerimientos mínimos ante los equipos que dispone la institución, se optó por la herramienta de monitoreo zabbix la cual permite analizar durante los siete días de la semana por las 24 horas toda la infraestructura de la red de datos, evitando que el encargado de mantenimiento de la red verifique personalmente cada uno de los equipos hasta encontrar la falla.

En cuanto a las funcionalidades de la herramienta permite un análisis personalizado priorizando equipos de capa core, distribución y de acceso que presentan problemas frecuentes, generando así un registro de eventos, permitiendo aplicar medidas preventivas para mitigar posibles problemas futuros que se generen en la red, manteniendo siempre todos los servicios operativos que dispone la institución.

4.1.1. Implementación

Para la implementación del modelo de gestión de la red de la institución, conformada por la estación gestora, agentes y protocolo de gestión. El "Anexo 23" muestra cómo se encuentra implementado el sistema identificando la estación gestora y los dispositivos monitoreados mediante el protocolo SNMP, permitiendo obtener información acerca del estado en el que se encuentra cada uno de los equipos que pertenecen a cada una de las dependencias de la institución.

Una vez definido la herramienta de monitoreo de la infraestructura de la red de datos se define la arquitectura de funcionamiento de dicha herramienta.

- **Gestor o estación gestora.**

Este es el encargado de recibir toda la información de los equipos monitorizados, comprobando el estado en el que se encuentre el equipo enlazado, mediante alarmas definidas y estas se almacenaran en una base de datos.

Para el levantamiento del sistema de monitoreo de la red de datos de la institución, mediante la documentación oficial de la página de zabbix se evalúa los requerimientos necesarios para la selección del equipo que mejor se ajuste a los requerimientos de dicha herramienta, por otra parte, se detalla las características del equipo en el cual será implementado.

Tabla 15. Características del Servidor Zabbix

Características	**Descripción**
CPU	Intel(R) Xeon(R) Silver 4214R CPU @ 2.40GHz
Arquitectura	64 bits
Memoria	6 GB de memoria RAM
Disco	100GB
Cache	16KiB L1 cache
Video	SVGA II Adapter

De acuerdo con las características establecidas se procede a la instalación de la estación gestora, y para ello se selecciona el sistema operativo CentOS 7 para levantar el servidor zabbix, cumpliendo con los requerimientos del departamento de TIC´s y la herramienta de monitoreo para ello se establece realizar la instalación del sistema de monitoreo en su versión 5.0.

Para la instalación del servidor zabbix, se detalla su instalación en el "Anexo 9"**,** generalizando los siguientes pasos:

- Instalación del repositorio de epel y actualización del sistema.
- Descargar repositorio zabbix 5.0 desde página oficial.
- Instalación de zabbix 5.0 server, agente.
- Instalación de complementos reléase.
- Instalación de apache, mysql y zabbix-web.
- Instalar mariadb server, habilitarlo e iniciarlo.
- Crear base de datos y usuario zabbix.
- Configurar conexión de base de datos.

- Agregar reglas de selinux y firewall.
- Habilitar e iniciar el servidor zabbix, agente y servicio httpd.
- Finalizar con instalación a través de la interfaz web.

- **Agentes**

Dispositivos gestionados son aquellos que van a ser monitorizados con el fin de recopilar información en tiempo real, permitiendo generar alertas al momento de suscitarse un problema que afecte el rendimiento y caída del servicio que disponga la institución. Para ello es necesario que los dispositivos gestionados tengan habilitado el protocolo SNMP para que puedan ser monitorizados. La herramienta de monitoreo de la red soporta el protocolo en sus versiones SNMPv1, SNMPv2 y SNMPv3. La versión de SNMP a implementarse en cada uno de los dispositivos de interconexión es la SNMPv2 puesto que esta es la más soportada por la mayoría de los dispositivos que integra la institución además por su configuración es más simple, no se tomó en cuenta la versión de SNMPv3 debido a que los mecanismos de seguridad que esta integra generan más carga para el cpu provocando que el sistema degrade en su rendimiento.

- **Configuración de equipos**

Para la configuración de los equipos se habilito el protocolo SNMP de cada uno de los equipos de interconexión que integra la institución.

- **Switch serie catalyst**

Para el acceso de los dispositivos de interconexión de la institución es necesario utilizar una herramienta remota que permita la habilitación del protocolo SNMP, debido a que por defecto viene deshabilitado en este caso se hace uso de la herramienta PUTYY en el cual se establece la IP y el puerto de comunicación que es el 22 vía telnet. Para consultar si el protocolo está habilitado en los dispositivos, el comando de verificación es “show SNMP” este se muestra en el Anexo 10.

Para habilitar el protocolo SNMP, es necesario configurar la cadena community con su respectivo comando para la recopilación de la información, en donde RO corresponde a read only y public al nombre de la comunidad a ser gestionada. Su configuración es la siguiente:

```
# enable
# config terminal
switch(config) #SNMP-server community public RO
# exit
# write memory
```

La configuración propuesta funciona tanto como para routers, switches y APs.

Para la configuración del SNMP en los APs es necesario habilitar el agente global en el wireless controller desde su interfaz gráfica.

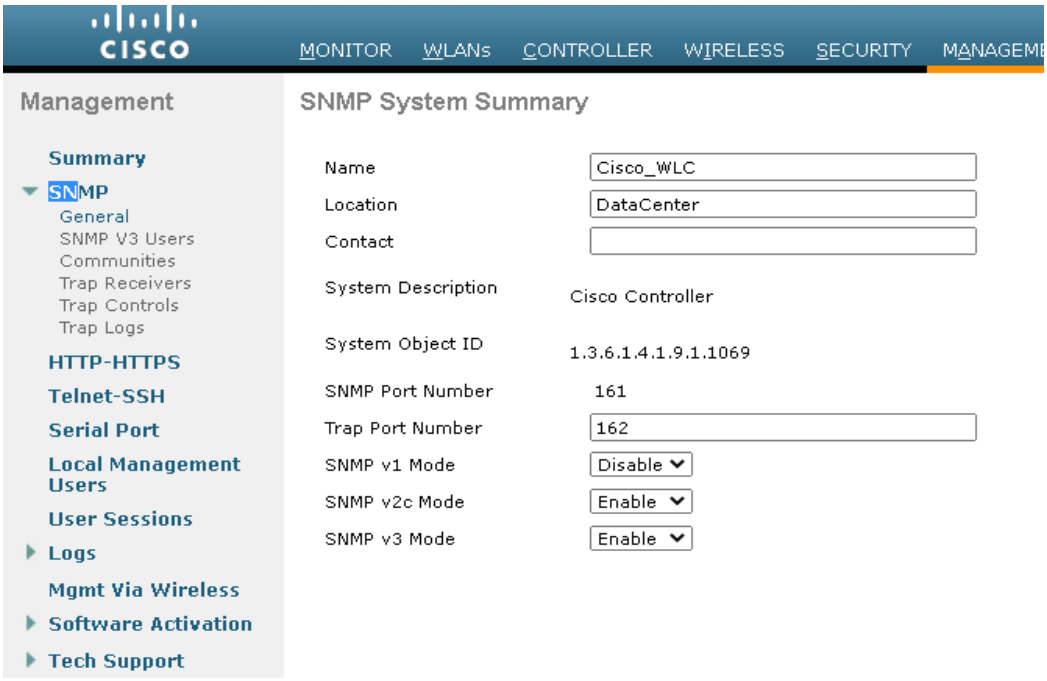


Figura 9. Configuración SNMP Wireless Controller

- **Servidores**

Para la monitorización de los servidores es necesario la instalación de un agente SNMP para que este pueda recopilar información, esta se enviara a la estación gestora en donde se determinara sobre el estado en el que se encuentre el equipo vinculado con la herramienta permitiendo mitigar los problemas que afecten con el rendimiento de los equipos de la red de datos.

En cuanto la habilitación del agente SNMP en los servidores se procede a seguir los siguientes pasos.

- Descargar repositorio de zabbix en su versión 5.0 y actualizar.
- Configurar zabbix agent.
- Iniciar y habilitar zabbix-agent.
- Habilitar puerto 10050/tcp del firewall.
- Reinicio de firewall y del agente zabbix.

Esta instalación se detalla en el "Anexo 13".

- **Firewall cisco asa 5520**

Como primer punto es necesario la habilitación del protocolo SNMP, puesto que por defecto viene deshabilitado, también es necesario definir la interfaz y la ip de la estación gestora definiendo a la comunidad a la que pertenece y será monitorizado, su configuración es la siguiente:

```
# enable
# config terminal
ASA(config)#SNMP-server enable
ASA(config)#SNMP-server host inside 10.X.X.X community public
ASA(config)#SNMP-server community public
ASA(config)#exit
#write memory
```

4.1.2. Metodología FCAPS

Para la implementación de la herramienta de sistema de monitoreo de la red de datos de la infraestructura de la UPEC se utilizó la metodología FCAPS definidas por la ISO cumpliendo con cada uno de los procesos que comprende la metodología.

Figura 10. Modelo de Gestión de Red FCAPS

A continuación, se muestra un esquema del funcionamiento de la herramienta de monitoreo implementada, con cada uno de los dispositivos que esta integra.

1. Gestión de fallos

La gestión de fallos consiste en la detección, aislamiento y resolución de los problemas de red, es el proceso que se encarga del descubrimiento y corrección de los problemas si es el caso. Para este caso se utiliza la detección de fallas mediante las alertas incluidas en la documentación que se pueden dar por telegram o email, dentro de esta acción se utiliza disparadores que están activos 24/7 y verifican cada puerto de todos los switches, APs, y servidores que se esté monitorizando.

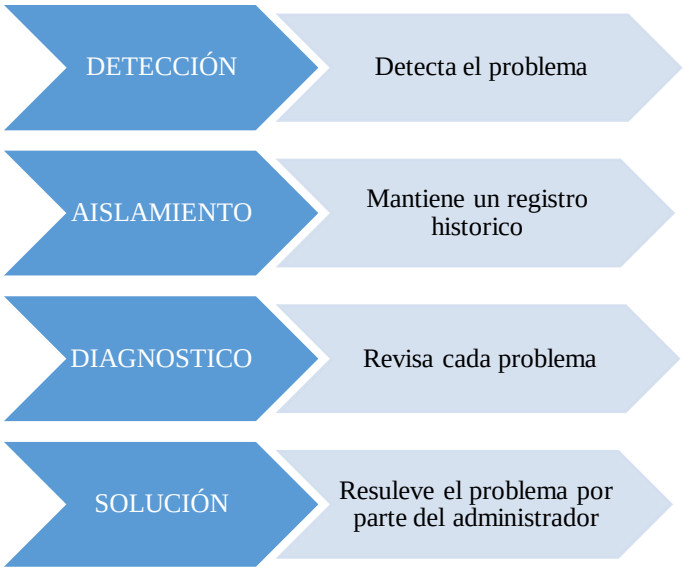


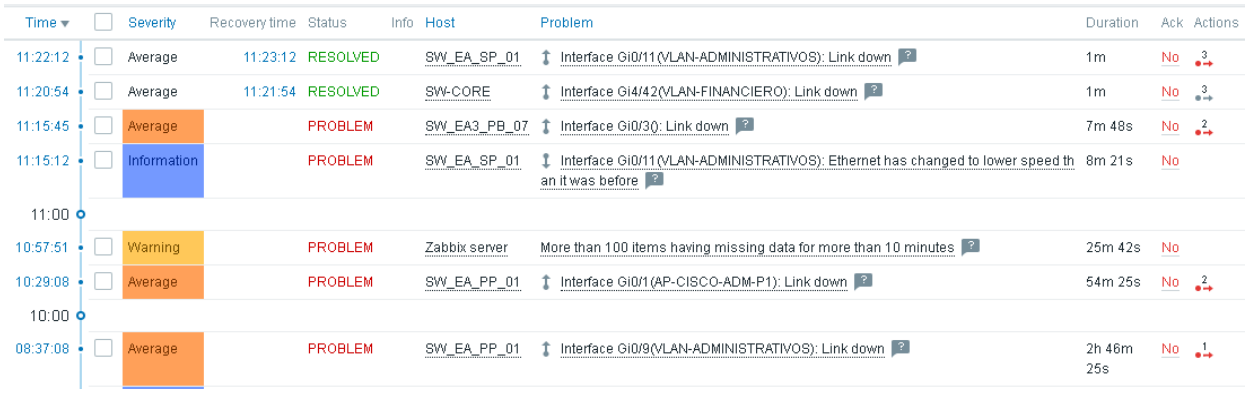
Figura 11. Esquema de Solución de Problemas

En el ejemplo del servidor de reportes se puede ver fácilmente los distintos errores que se han suscitado desde el día que ha sido activado dentro del monitoreo en la herramienta zabbix, además de mostrarse el problema también muestra la severidad de este y brinda una pequeña información detallada del problema en sí.

Time	Severity	Recovery time	Status	Info	Host	Problem	Duration	Ack	Actions
2021-03-15 22:54:10	Warning		PROBLEM		servidor de reportes	PostgreSQL: Failed to get items (no data for 30m)	12h 24m 8s	No	
2021-03-15 22:54:03	Information		PROBLEM		servidor de reportes	MySQL: Failed to fetch info data (or no data for 30m)	12h 24m 15s	No	
2021-03-10 18:14:21	Warning		PROBLEM		servidor de reportes	System time is out of sync (diff with Zabbix server > 60s)	5d 17h 3m	No	
2021-03-10 12:30:46	High		PROBLEM		servidor de reportes	Puerto ssh esta cerrado servidor de reportes HTTP	5d 22h 47m	No	

Figura 12. Reporte de Problemas

En el caso del switch de core se muestran los distintos problemas que van desde la intermitencia del servicio de una vlan a enlaces inactivos de ciertas interfaces, e incluso muestra los distintos problemas de información o error de la misma herramienta, haciendo el trabajo del administrador más fácil en la verificación y corrección de los errores.



Time	Severity	Recovery time	Status	Info	Host	Problem	Duration	Ack	Actions
11:22:12	Average	11:23:12	RESOLVED		SW_EA_SP_01	Interface Gi0/11(VLAN-ADMINISTRATIVOS): Link down	1m	No	3
11:20:54	Average	11:21:54	RESOLVED		SW-CORE	Interface Gi4/42(VLAN-FINANCIERO): Link down	1m	No	3
11:15:45	Average		PROBLEM		SW_EA3_PB_07	Interface Gi0/3(): Link down	7m 48s	No	2
11:15:12	Information		PROBLEM		SW_EA_SP_01	Interface Gi0/11(VLAN-ADMINISTRATIVOS): Ethernet has changed to lower speed than it was before	8m 21s	No	
11:00									
10:57:51	Warning		PROBLEM		Zabbix server	More than 100 items having missing data for more than 10 minutes	25m 42s	No	
10:29:08	Average		PROBLEM		SW_EA_PP_01	Interface Gi0/1(AP-CISCO-ADM-P1): Link down	54m 25s	No	2
10:00									
08:37:08	Average		PROBLEM		SW_EA_PP_01	Interface Gi0/9(VLAN-ADMINISTRATIVOS): Link down	2h 46m 25s	No	1

Figura 13. Problemas del Switch de Core

➢ Alertas vía e-mail y telegram

La herramienta de monitoreo zabbix permite la configuración de alertas vía e-mail y telegram las cuales se enviarán automáticamente cuando ocurre un evento dentro de los dispositivos gestionados. Para él envió de correos se ha configurado desde la frontend de zabbix una cuenta personal de correo electrónico gmail, desde donde se puede tener acceso a todas las alertas que se hayan enviado sean actuales o históricas.

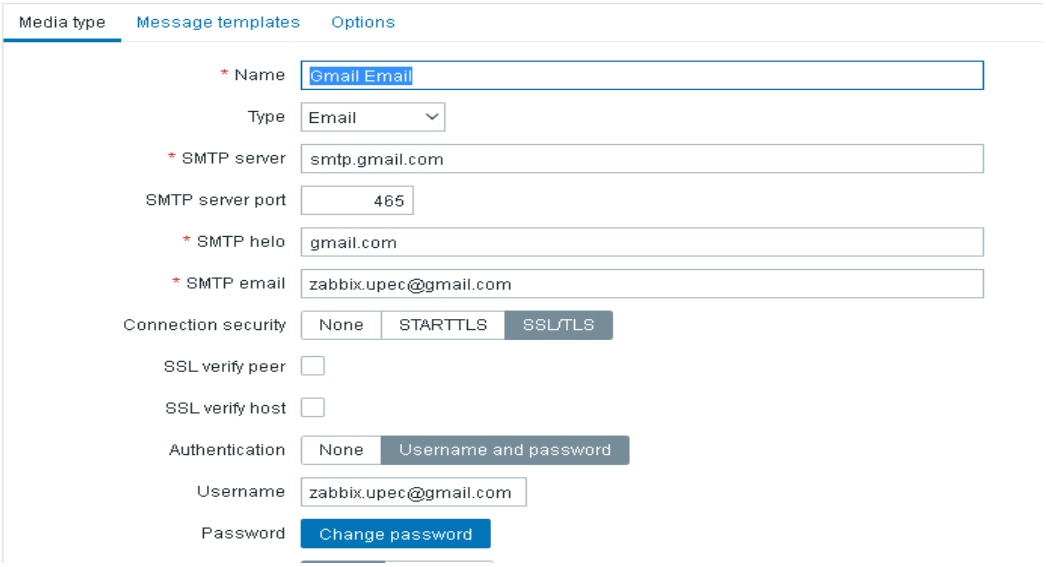


Figura 14. Configuración Alertas Email

Al igual que la configuración para las alertas por e-mail se realiza el mismo procedimiento desde el frontend de zabbix, haciendo uso del api que integra telegram y los tokens que son necesarios para la activación de este tipo de alertas.

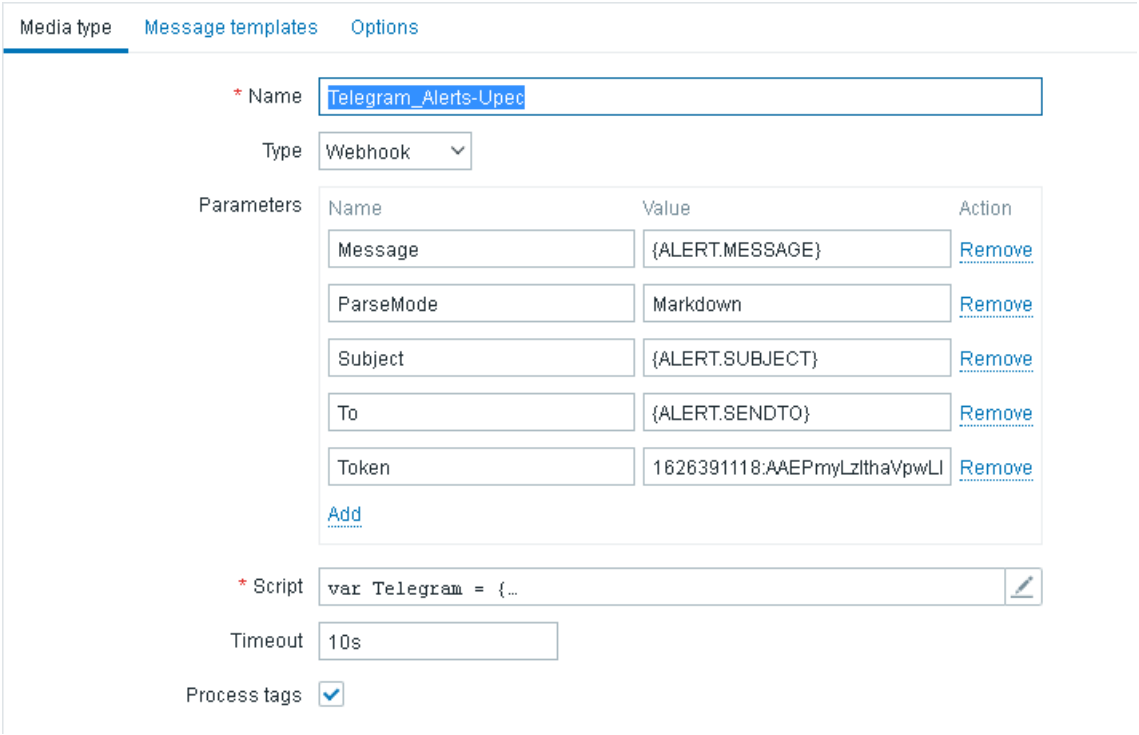


Figura 15. Configuración Alertas Telegram

- **Aislamiento y diagnóstico de fallos**

Esto dependerá de la gravedad del problema, los grados de severidad son representados por distintos colores, estos niveles de severidad, así como las alertas dependiendo a estos niveles son administradas por el administrador de red.

Tabla 16. Grados de Severidad de Problemas en Zabbix

Nº	Severidad	Color	Descripción
0	No clasificado		Dispositivo completamente funcional
1	Información		Dispositivo funcional
2	Advertencia		Alerta
3	Promedio		Problema agravante
4	Alto		Enlaces inactivos
5	Desastre		Dispositivos apagados

- **Solución de falla**

Al conocer la falla que se ha suscitado es mucho más factible realizar una solución breve ya sea desde los controladores que maneja el administrador de red o manualmente en los dispositivos que muestren falencias.

1.1.Gestión de configuraciones

Basada esta gestión en la obtención y almacenamiento de las configuraciones de los distintos sistemas, dispositivos y en sí de la red de datos, realizando el distinto versiona miento de las gestiones en los cambios, incluyendo así también tareas específicas de configuración de hardware y software.

- **Registro de las configuraciones**

Se propone un método el cual consiste en llenar un formulario para cada configuración realizada para cada dispositivo dentro de la red, el cual cuente con la siguiente información:

- **Información general**

  Consta del número de configuración realizada, así como el día y la hora con el formato que se tenga previsto para todo el personal.

- **Información del dispositivo configurado**

  Se identificará el nombre del dispositivo otorgado dentro de la infraestructura lógica de la red, así como su nombre de venta, código de identificación, tipo de dispositivo, su ubicación de acuerdo con lo establecido en las políticas de seguridad y su tipo de conexión a ser posible.

- **Responsable de la configuración**

  Se registrará el nombre de la persona responsable de dicha configuración, así como su cargo y dependencia.

- **Justificación de configuración**

  Se justificará el motivo o razón de la configuración para tener evidencia en escrito.

- **Configuración**

  Se tomará en cuenta cada paso a seguir para la configuración asignada y breve descripción de esta.

- **Observación**

  En caso de tener alguna observación sea esta buena o mala, se tomará en cuenta.

- **Inventario**

La herramienta incorpora un apartado de inventario en donde es posible consultar caractersticas tecnicas sobre cada uno de los equipos gestionados, siempre y cuando este se haya configurado de manera manual, de esta forma el administrador de la red puede obtener la informcacion necesario acerca de cada uno de los dispositivos de manera inmediata como se muestra en la figura 16.

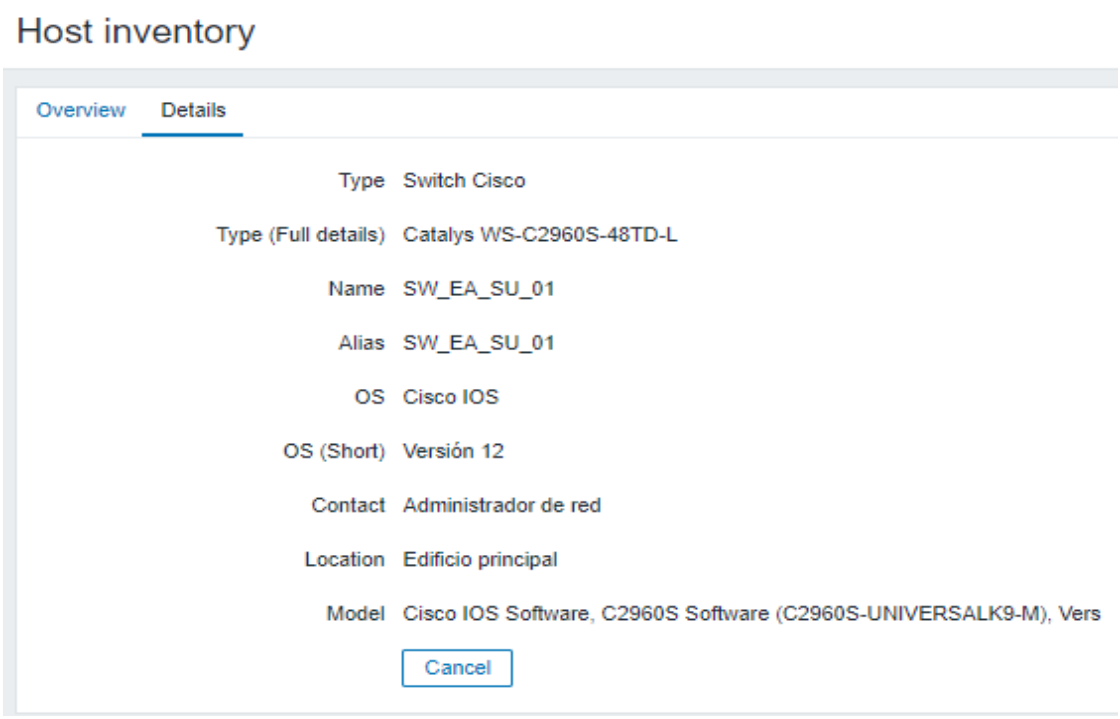


Figura 16. Inventario

1.2.Gestión de contabilidad

Este proceso recopila información sobre la asignación y distribución de recursos de la red. Permitiendo ayudar a planificar los mantenimientos de los recursos de la infraestructura de la red de la institución.

1.2.1. CPU

El uso de la cpu es parte fundamental para monitorizar y esto se lo puede representar mediante graficas dinámicas que incorpora zabbix en tiempo real. En la figura 17 se muestra la representación del uso del cpu del servidor zabbix. Se puede apreciar que el consumo de la cpu es bajo por lo que no existe ningún problema y no se genera ninguna alerta.

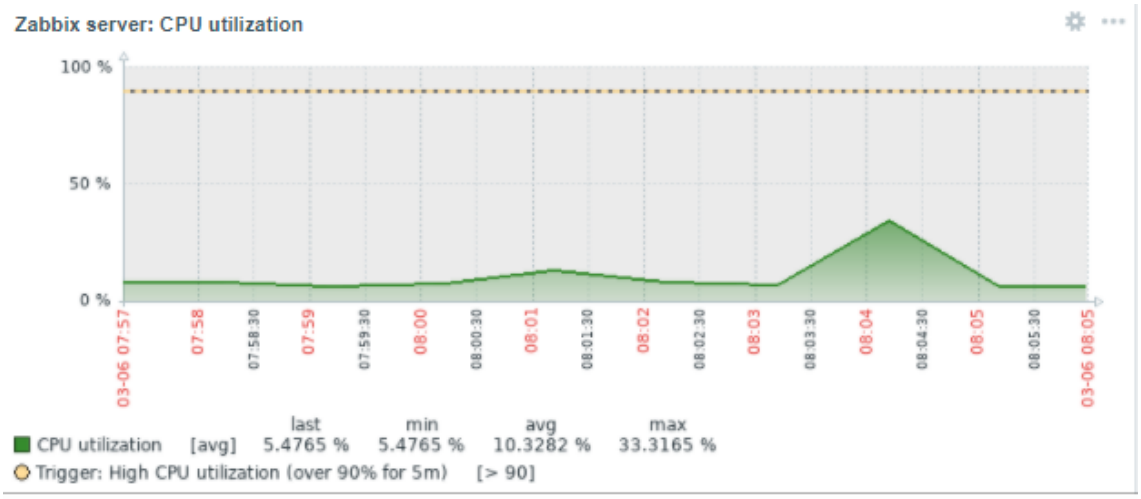


Figura 17. Uso de CPU

1.2.2. Memoria

El uso de memoria dentro de un servidor es parte fundamental para el rendimiento debido a que en este se gestiona toda la carga de los procesos que ocurren dentro del servidor, para ello zabbix visualiza de forma gráfica este recurso de memoria, detallando la memoria en uso y la que se encuentra disponible. La parte marcada de color azul nos indica la memoria utilizada y la línea verde muestra la cantidad total de memoria esta se encuentra representada por GB.

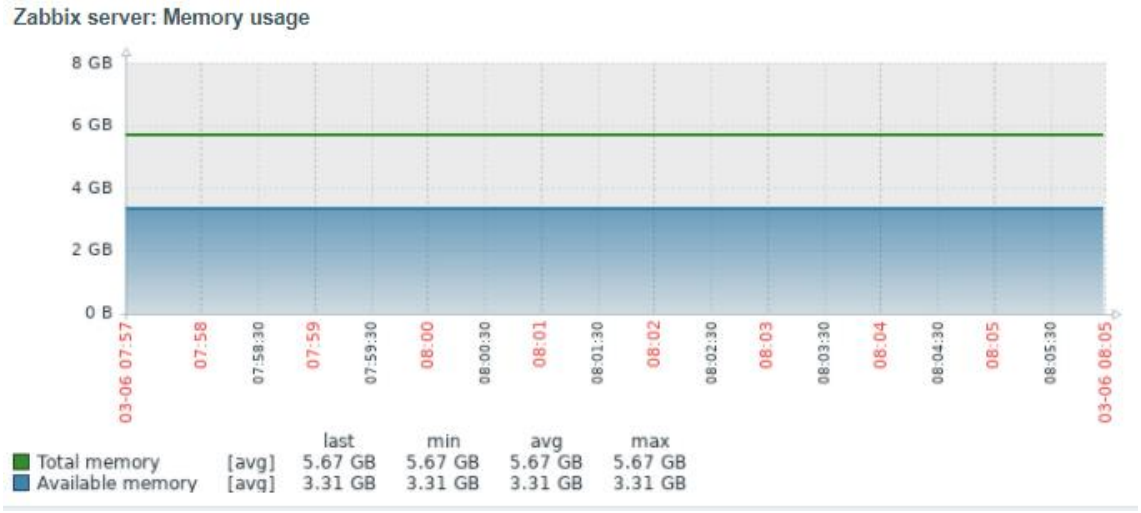


Figura 18. Uso de Memoria RAM

1.2.3. Espacio en disco

Se puede observar el espacio asignado y disponible en el servidor zabbix en la figura 19, el cual se representa por GB, también se puede apreciar una representación porcentual del estado del disco de memoria.

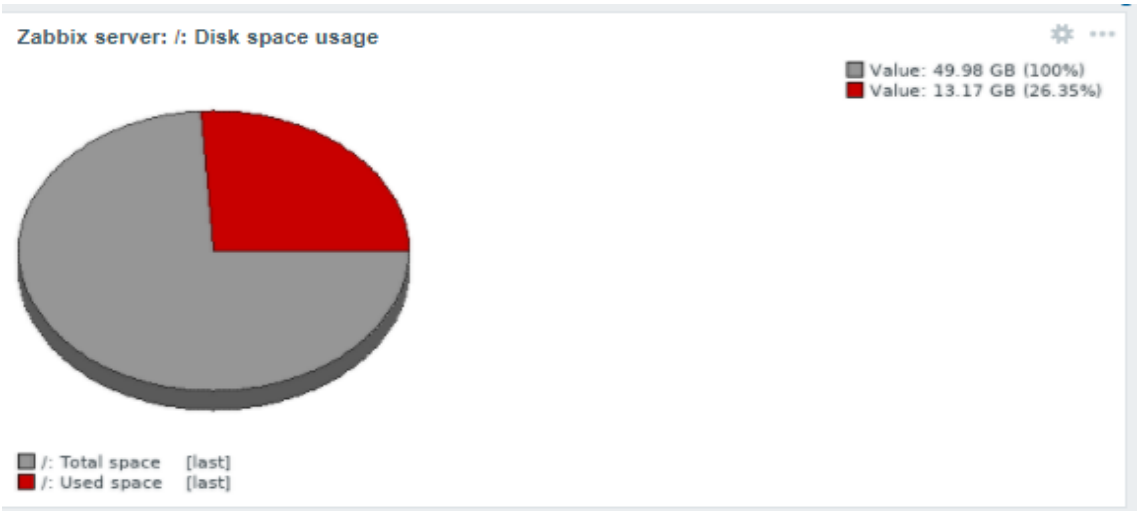


Figura 19. Espacio Total en Disco

1.2.4. Espacio en partición /boot

Se puede apreciar en la figura 20 que en el servidor zabbix, cuenta con una partición /boot, en la cual detalla el espacio total y el espacio usado representado en MB. Este espacio es de importancia a la hora de realizar actualizaciones del kernel en caso de estar lleno no se podría actualizar y se generaría una alerta de criticidad.

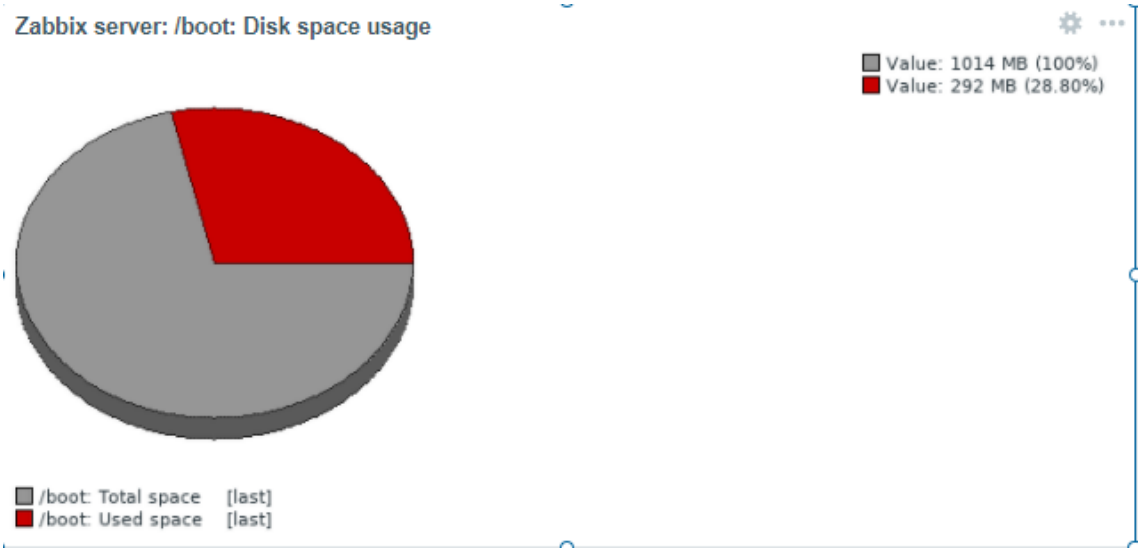


Figura 20. Espacio en Partición Boot

1.2.5. Espacio en partición /home

Otra información que se puede recopilar es el estado del directorio /home, se puede apreciar en la figura 21 el espacio total y el usado representado por un porcentaje, en este caso se muestra que el espacio en este directorio esta libre por lo que no se generaría alertas de problemas de almacenamiento.

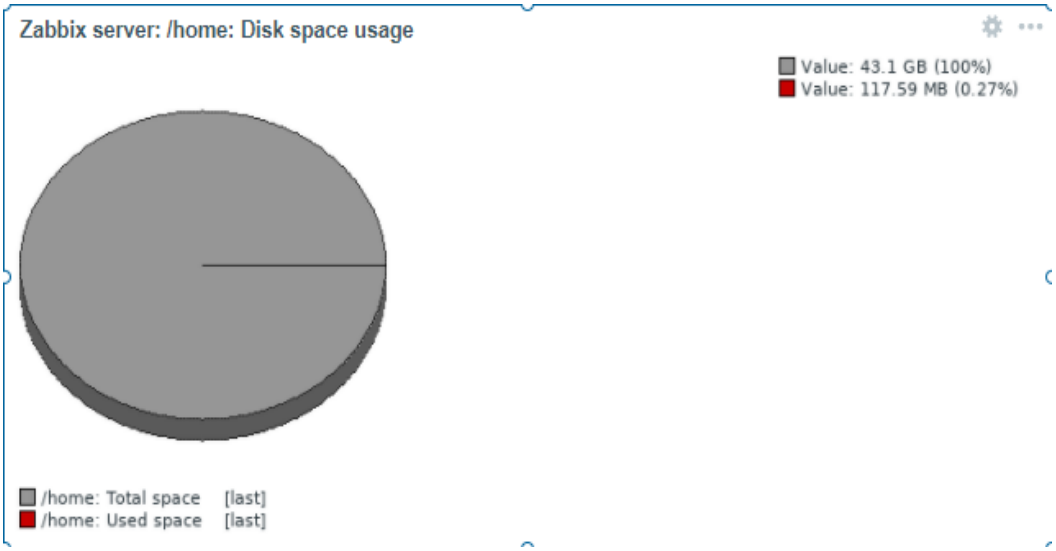


Figura 21. Espacio en Partición /Home

1.2.6. Lectura/escritura de disco

Mediante el template de linux es posible conocer el estado de velocidad de lectura y escritura del disco como se puede apreciar en la figura 22, en color verde se representa el estado de lectura, por lo que se puede decir que el uso de disco es bastante normal permitiendo tener un buen rendimiento del mismo, en color azul se representa la información del estado de escritura del disco, como también podemos visualizar cual es el promedio de escritura del mismo por lo que podemos decir que está en estado normal, aunque existen picos de escritura del disco.

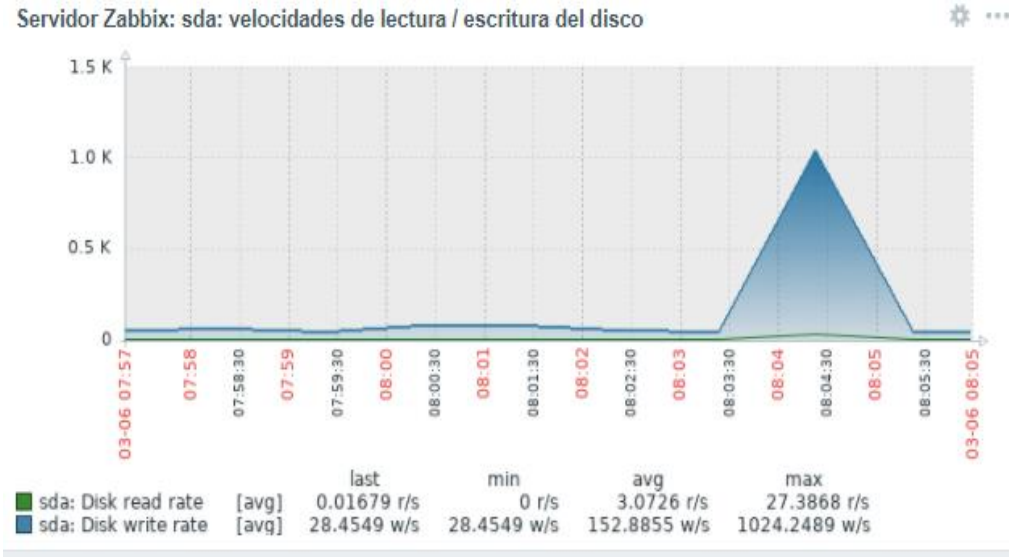


Figura 22. Velocidad de Lectura y Escritura de Disco

1.3.Gestión de prestaciones

Este proceso consiste en monitorizar sobre el estado de salud de la red permitiendo asegurar la disponibilidad de los servicios que provee la institución adelantándonos a la solución de futuros problemas que está presente.

1.3.1. Interfaces de red

Uno de los apartados que integra las plantillas de SNMP es el descubrimiento de interfaces disponibles en la red, en este se muestra el estado y el tráfico que se genera en tiempo real. En el grafico se puede apreciar tanto el tráfico entrante como el saliente de una interfaz de red, en este caso el switch de core en el cual se puede apreciar una interfaz de conexión entre edificios.

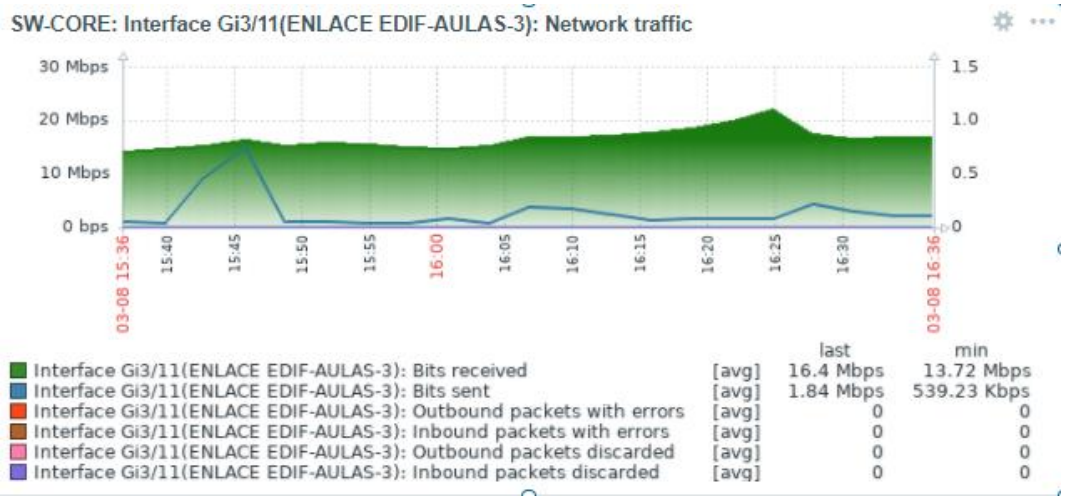


Figura 23. Trafico de Red en la Interfaz GI3/11 del SW-CORE

De igual forma se monitorea el tráfico que se generan en servidores tal es el caso del servidor zabbix, es recomendable conocer el estado del tráfico del servidor debido que permite ver qué cantidad de tráfico se añade a la red cuando este está en funcionamiento. Se puede apreciar en el grafico la cantidad de tráfico que se recibe y se envía por parte de los dispositivos gestionados por la herramienta.

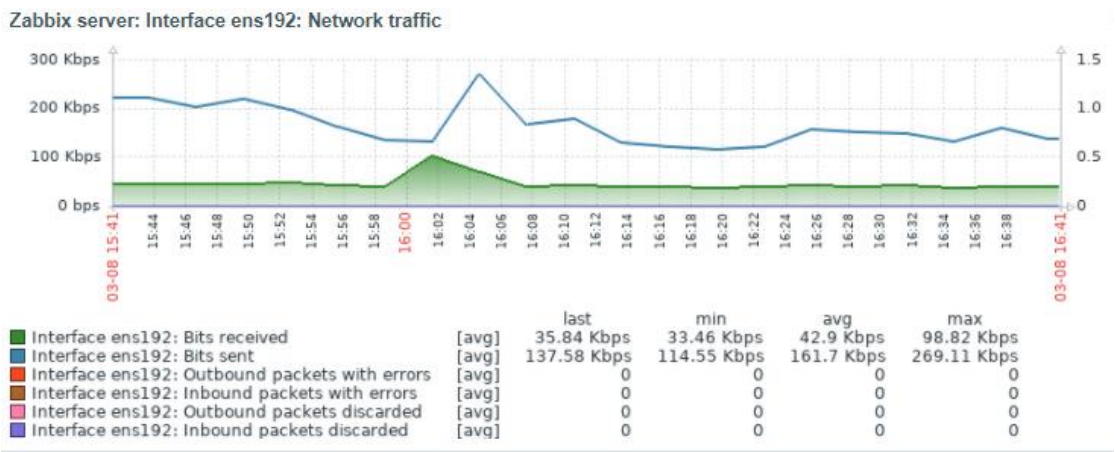


Figura 24. Trafico de Red del Server Zabbix

Del mismo modo se muestra el tráfico que se genera en las interfaces del firewall cisco asa 5520.

- Interfaz externo del tráfico del firewall.

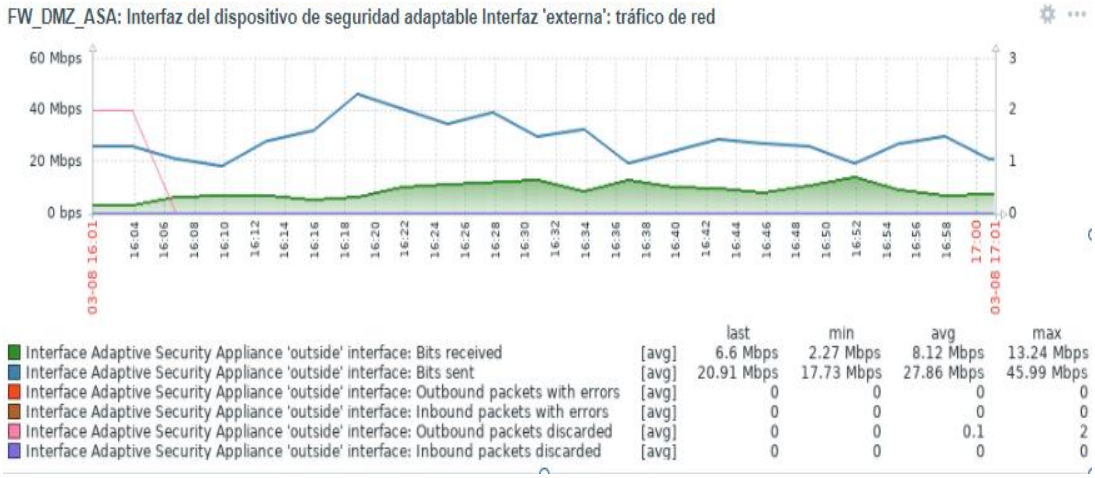


Figura 25. Tráfico de Red Interfaz Externa del Firewall

- Interfaz interna del tráfico del firewall.

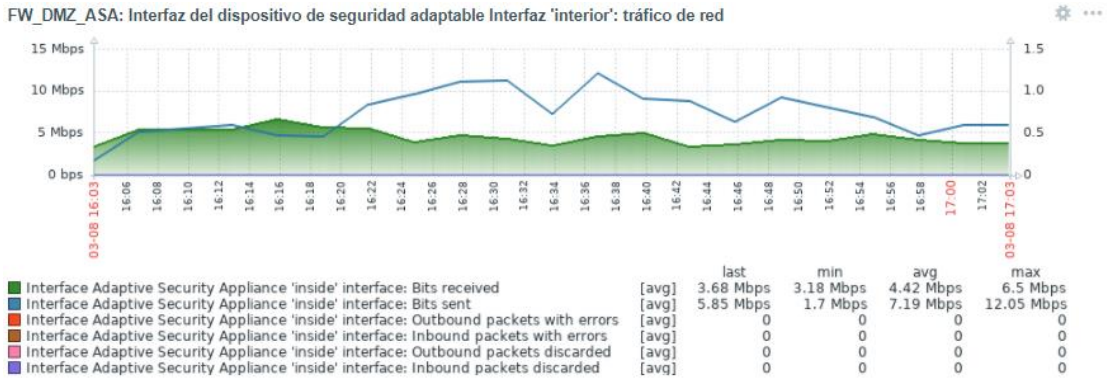


Figura 26. Trafico de Red Interfaz Interna del Firewall

- Interfaz DMZ.

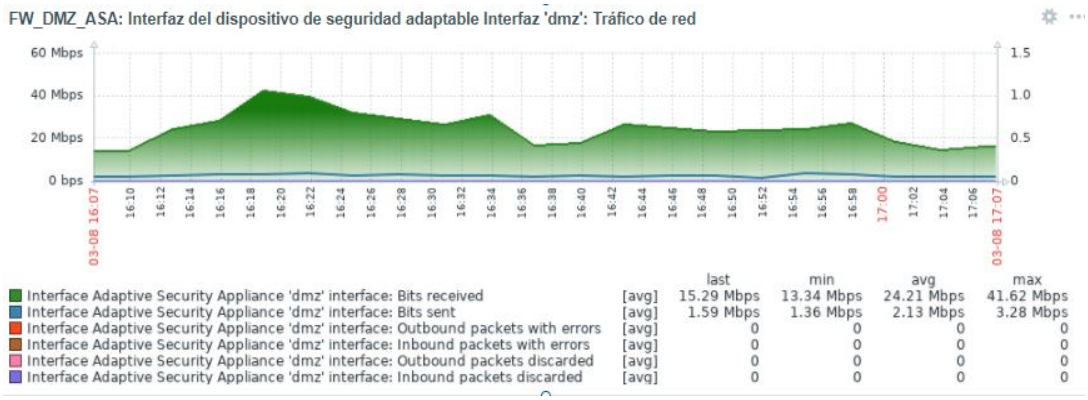


Figura 27. Tráfico de Red Interfaz DMZ del Firewall

1.3.2. Disponibilidad

La herramienta incorpora la generación de reportes de cada equipo de manera general, mostrando el estado de disponibilidad que presenta cada uno de estos equipos representados por un por porcentaje.

Host	Name	Problems	Ok	Graph
SW_EA_PB_01	Interface Gi0/9(VLAN-ADMINISTRATIVOS): High bandwidth usage (> 90%)		100.0000%	Show
SW_EA_PB_01	Interface Gi0/9(VLAN-ADMINISTRATIVOS): High error rate (> 2 for 5m)		100.0000%	Show
SW_EA_PB_01	Interface Gi0/9(VLAN-ADMINISTRATIVOS): Link down		100.0000%	Show
SW_EA_PB_01	Interface Gi0/10(VLAN-ADMINISTRATIVOS): Ethernet has changed to lower speed than it was before		100.0000%	Show
SW_EA_PB_01	Interface Gi0/10(VLAN-ADMINISTRATIVOS): High bandwidth usage (> 90%)		100.0000%	Show
SW_EA_PB_01	Interface Gi0/10(VLAN-ADMINISTRATIVOS): High error rate (> 2 for 5m)		100.0000%	Show
SW_EA_PB_01	Interface Gi0/10(VLAN-ADMINISTRATIVOS): Link down	100.0000%		Show
SW_EA_PB_01	Interface Gi0/11(VLAN-ADMINISTRATIVOS): Ethernet has changed to lower speed than it was before		100.0000%	Show
SW_EA_PB_01	Interface Gi0/11(VLAN-ADMINISTRATIVOS): High bandwidth usage (> 90%)		100.0000%	Show
SW_EA_PB_01	Interface Gi0/11(VLAN-ADMINISTRATIVOS): High error rate (> 2 for 5m)		100.0000%	Show
SW_EA_PB_01	Interface Gi0/11(VLAN-ADMINISTRATIVOS): In half-duplex mode		100.0000%	Show
SW_EA_PB_01	Interface Gi0/11(VLAN-ADMINISTRATIVOS): Link down		100.0000%	Show
SW_EA_PB_01	Interface Gi0/12(PROYECTO VINCULACION): Ethernet has changed to lower speed than it was before		100.0000%	Show
SW_EA_PB_01	Interface Gi0/12(PROYECTO VINCULACION): High bandwidth usage (> 90%)		100.0000%	Show
SW_EA_PB_01	Interface Gi0/12(PROYECTO VINCULACION): High error rate (> 2 for 5m)		100.0000%	Show

Figura 28. Disponibilidad de Equipos

1.3.3. Web escenario

Zabbix incorpora un apartado de monitoreo de escenarios web, en el cual no es necesario instalar un agente o activación del protocolo SNMP, en este ejemplo se monitoriza el repositorio de la UPEC, en el grafico podemos apreciar que ítems generales se puede monitorear de este web escenario. Los ítems más importancia en este caso son los de la velocidad de descarga y el tiempo de respuesta. Estos valores se muestran en tiempo real.

- **other** - (5 Items)				
Download speed for scenario "http://repositorio.upec.edu.ec/".	2021-03-09 20:37:22	340.66 KBps	-44.08 KBps	Graph
Download speed for step "repositorio" of scenario "http://repositorio.upec.edu.ec/".	2021-03-09 20:37:22	340.66 KBps	-44.08 KBps	Graph
Failed step of scenario "http://repositorio.upec.edu.ec/".	2021-03-09 20:37:22	0		Graph
Response code for step "repositorio" of scenario "http://repositorio.upec.edu.ec/".	2021-03-09 20:37:22	200		Graph
Response time for step "repositorio" of scenario "http://repositorio.upec.edu.ec/".	2021-03-09 20:37:22	79.16ms	+9.07ms	Graph

Figura 29. Web Escenario

1.3.3.1.Velocidad de descarga

Mediante este ítem se puede saber la velocidad de descarga de una página web, puesto que es de suma importancia debido a que incide en el rendimiento de esta por ello es necesario mantener un margen de descarga adecuada para que no sature el servicio que la pagina provee, en este caso se puede apreciar que la velocidad de descarga es óptima en este intervalo de tiempo de 40 minutos y se mantiene en el margen promedio por tanto no influyen en el rendimiento.

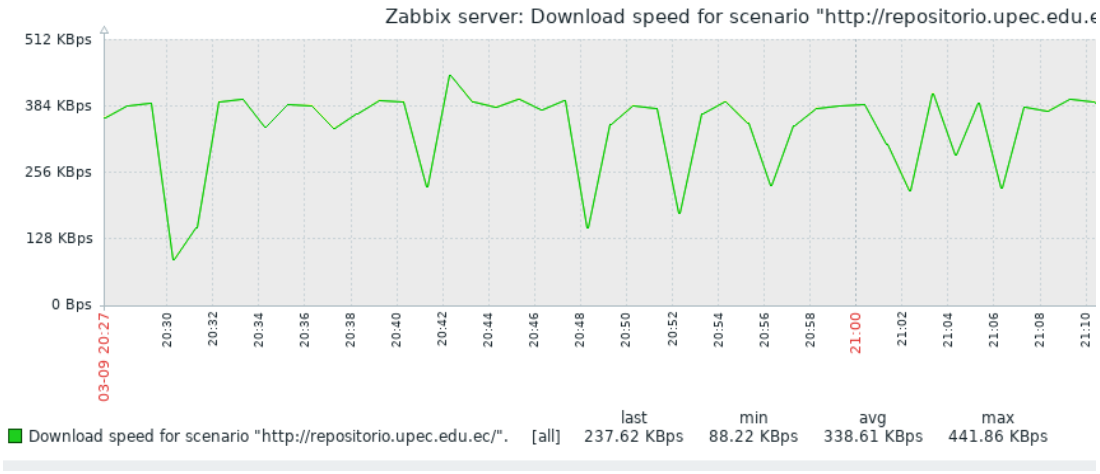


Figura 30. Velocidad de Descarga

1.3.3.2.Tiempo de respuesta

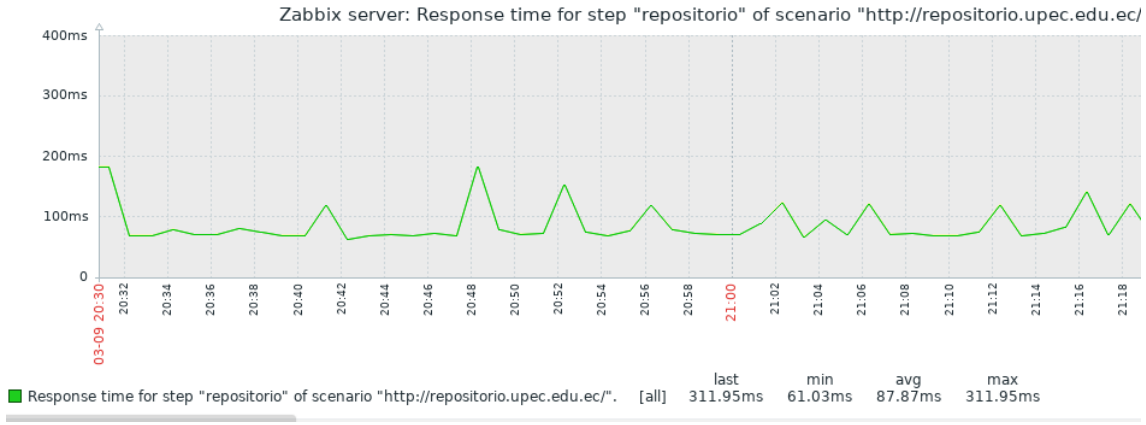


Figura 31. Tiempo de Respuesta

1.3.4. Límites de rendimiento

- **Limitaciones del rendimiento**

En cuanto a las limitaciones del rendimiento de un equipo, se establecen de acuerdo con el tipo de dispositivo.

- **Switch**

El uso de la CPU que este por debajo del 70% de su capacidad se considera que es aceptable. Puesto que puede seguir operando, en cuanto supera el límite de 70% se considera que es un problema debido a que el tiempo de envió de paquetes se va degradando y por ende un bajo rendimiento.

En cuanto a la cpu del switch tiene dos funciones distintas, la primera es la de ejecutar todos los procesos de IOS para desempeñar la función como conmutador y la segunda es la encargada de recibir y enviar los paquetes hacia el hardware de conmutación. "En algunas implementaciones de red, una CPU ocupada es normal. En general, cuanto más grande sea la red de Capa 2 o Capa 3, mayor será la demanda de la CPU para procesar el tráfico relacionado con la red". (Cisco, 2016).

Estos son ejemplos de procesos que tienen el potencial de causar una alta carga de la CPU:

- Árbol de expansión.
- Actualización de la tabla de enrutamiento IP.
- Comandos de cisco IOS.

Por otra parte, el uso de memoria es recomendable de que no supere el 70% de capacidad debido a que puede generar problemas de rendimiento. Definidos estos puntos de criticidad se genera las notificaciones de advertencia en el sistema de monitoreo.

1.4.Gestión de seguridad

Este proceso comprende sobre los accesos a los dispositivos gestionados y el sistema de monitoreo, por ello es necesario determinar su gestión de seguridad para evitar que los datos estén comprometidos.

Para la seguridad del sistema de monitoreo es necesario el cambio de contraseña que viene por defecto, para que no pueda acceder cualquier persona ajena del departamento de TIC's, para realizar este proceso es necesario acceder a el frontend de zabbix con su respectiva ip e ingresar a el apartado de usuarios y se podrá visualizar el usuario admin el cual tendrá un control total sobre los equipos gestionados en la red, para ello es posible realizar el cambio de la contraseña que por defecto del sistema es "Zabbix".

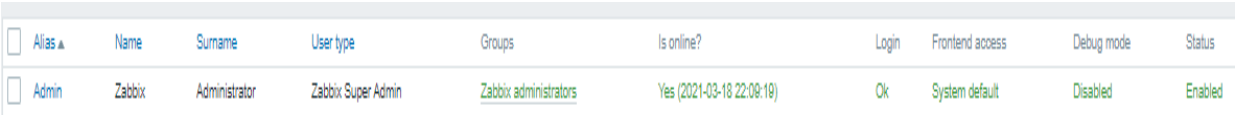


Figura 32. Vista del Usuario Administrador

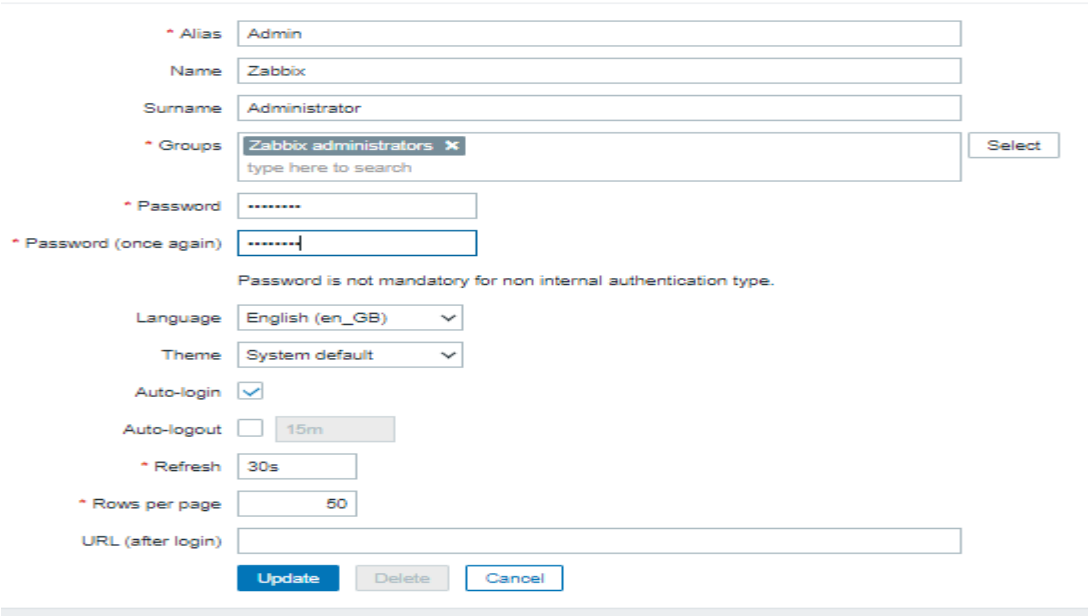


Figura 33. Vista del Cambio de Contraseña del Administrador

- **Funcionamiento del modelo de gestión**

Para la implementación del modelo de gestión se comprende 3 aspectos fundamentales que intervienen en la monitorización de la infraestructura de red de la institución, tales son el gestor, los agentes y el protocolo de gestión. Para ello se realiza un mapeo del funcionamiento de cada uno de los edificios pertenecientes a la institución, el funcionamiento del mapeo se replica en todos los edificios ayudando a tener una mejor visión sobre los problemas que se suscitan dentro de la red de datos de la UPEC, mismos que se pueden ver en el "Anexo 23".

4.2. DISCUSIÓN

- **Validación Interna**

En la investigación se estableció cinco objetivos, uno general y cuatro específicos como se detalla en el capítulo 1, se utilizó la metodología de enfoque mixta debido a que existe una variable cuantitativa y cualitativa, con respecto a la población se definió que es finita de 3301 estudiantes de acuerdo al departamento de dirección académica de la UPEC en el año 2020, al conocer que el número de encuestados es alto se opta por el cálculo de la muestra que como resultado es de 71 encuestados, además se ha enfocado en el método analítico y lógico deductivo permitiendo el método analítico identificar el funcionamiento de la infraestructura física y lógica de la institución determinando problemas que inciden en el rendimiento de la red de datos lo cual conlleva a una insatisfacción por parte de la comunidad universitaria, por otra parte, el método lógico deductivo permitió la identificación e implementación de una herramienta de monitoreo que se ajuste a los requerimientos del departamento de TIC's de la institución permitiendo mitigar problemas como cuellos de botella y lentitud en el ingreso de los servicios, mejorando la intermitencia de la red de datos. Las técnicas implementadas en la recopilación de la información tenemos la entrevista y encuesta; con la encuesta se evidencia que existen problemas frecuentes con los servicios de la red de datos de la institución lo que conlleva a implementar una herramienta especializada en el monitoreo de la red, y la entrevista nos ayuda a determinar las funcionalidades necesarias que debe tener el sistema, como también los equipos que deben ser priorizados a la hora de monitorización. Además, sobre la composición de la red de datos, su topología y el funcionamiento de cada equipo dentro de la institución.

La presente investigación tuvo como finalidad implementar un sistema de monitoreo basado en el protocolo SNMP, utilizando herramientas de Software Libre para la comunidad universitaria, permitiendo mantener la calidad del servicio funcional, dando como resultado una alta disponibilidad de los servicios de la red de datos, después de un análisis de diferentes herramientas de software libre planteadas para la solución se opta por el uso de ZABBIX, debido a su variedad de características como: alertas, representación estadística, registro de eventos, registro de rendimiento de equipos, autodescubrimiento de red entre otros además de que es más reconocida por sus funcionalidades entre los administradores de red, los cuales permiten gestionar mejor los recursos que posee la infraestructura de la institución.

Con la ayuda de la fundamentación bibliográfica y la investigación de campo, formando parte de esta el experimento se determina las herramientas de monitoreo de software libre las cuales tiene gran factibilidad debido a su bajo costo de implementación y buen funcionamiento dentro de una infraestructura de red.

La implementación de la herramienta zabbix se la realiza luego de haber cumplido con los requerimientos del departamento de TIC's de la universidad, esta estará trabajando durante los siete días de la semana y 24 horas al día, permitiendo así que los datos obtenidos sean fácilmente catalogados y analizados, brindando la posibilidad al administrador de mantener siempre en alta disponibilidad todos los servicios que ofrece la universidad. En cuanto al manejo de la herramienta de monitoreo se elaboró una propuesta de políticas de uso enfocadas en la metodología FCAPS, permitiendo así su correcto uso.

- **Validación Externa**

En cuanto a la investigación realizada se determina que se puede replicar en cualquier entidad o institución, debido a que se hace uso de herramientas de software libre y estas no generan ningún costo, logrando resultados que ofrecen mayores ventajas en el servicio de la red, tanto así que este proyecto aporta resultados beneficiosos los cuales pueden conducir futuras investigaciones que busquen solventar problemas similares en distintas instituciones que así lo ameriten.

Con relación a los antecedentes se destaca que el uso de herramientas de software libre con sus respectivos complementos especializados en monitoreo, en instituciones públicas es indispensable para mejorar el rendimiento de la red de datos, debido a que manejan gran cantidad de información y alto número de equipos de comunicación debiendo ser monitoreados constantemente evitando intermitencias, lentitud, baja disponibilidad de servicio y saturaciones en la institución, por otra parte el uso de estos sistemas de monitoreo se puede aplicar en pequeñas, medianas y grandes entidades ya que cuentan con soporte técnico gratuito al ser herramientas sin costo, además estas herramientas son de alta confiabilidad ya que no tiene conflictos con el funcionamiento de la infraestructura lógica y física de la red de datos permitiendo una mejor operatividad en los equipos de comunicación.

Para la implementación del sistema de monitoreo en la UPEC se empleó herramientas de software libre, basado en el protocolo SNMP, similar a el proyecto de la Universidad Técnica del Norte ubicada en la ciudad de Ibarra, cuyo proyecto se enfoca en mejorar la continuidad de operación de la red mediante mecanismo de monitoreo basados en software libre en el edificio central, debido a que se encuentran los equipos de capa core y estos necesitas ser priorizados ante desperfecto de la red, por otra parte el sistema de monitoreo de la UPEC se implementó en toda la universidad priorizando equipos de capa core, acceso y distribución, de modo que el administrador de la red será capaz de encontrar soluciones a tiempo garantizando operatividad de la red. Estas investigaciones tienen en común el uso de herramientas de software libre, en cuanto a los problemas de las dos investigaciones se destaca que no se realizaban registros de las configuraciones de los equipos de interconexión, ni reportes acerca del rendimiento y la usabilidad de la red por ende la necesidad de un sistema de monitoreo.

Por otra parte, en la Universidad Cooperativa de Colombia de la ciudad de Bogotá emplean una herramienta denominada CACTI cuyo objetivo es monitorear los dispositivos y servicios de red, teniendo en cuenta que esta no dispone de funcionalidades que ofrecen otras herramientas de software libre como ejemplo el autodescubrimiento de la red, de forma similar en la UPEC se emplea herramientas de monitoreo de software libre cuya herramienta es ZABBIX la cual permite a diferencia de la primera el autodescubrimiento de la red, aprobando que esta herramienta sea más escalable e idónea a la hora del manejo de redes complejas de modo que permita gestionar gran cantidad de datos simultáneos.

Finalmente se acepta la hipótesis correlacional establecida en el proceso de investigación mismo que se detalla en la Tabla 18.

Tabla 17. Aceptación de la Hipótesis

Hipótesis	**Estado**	**Razones**
El Sistema de monitoreo influye positivamente en la intermitencia y mejora el rendimiento de la red de datos que utilizan los usuarios en la Universidad Politécnica Estatal del Carchi.	Aceptada.	Con la implementación del sistema de monitoreo podrán mejorar los tiempos de respuestas a la solución de un problema que suscite dentro de la red de datos de la institución. Mediante la herramienta se podrá visualizar en graficas dinámicas sobre el estado de cada uno de los equipos que integre la red de datos de la institución. La herramienta de monitoreo contribuye a una mejor operatividad y disponibilidad de los servicios que provee la institución.

V. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- La herramienta de monitoreo permite optimizar los tiempos de respuesta frente a una caída de un servicio o una falla de este, ya que esta cuenta rápidamente con la información necesaria y precisa para reportar la falla dentro de los equipos correspondientes. Tomando en cuenta lo mencionado, se concluye en que el sistema de monitoreo es una herramienta necesaria para brindar un buen servicio a los usuarios a la vez que se contrarrestan los problemas que se generan en la red.
- Debido a que las instituciones públicas deben usar software no privativo, el análisis costo-beneficio al implementarse herramientas de libre distribución se evidencia con la factibilidad del proyecto, destacándose así también las diversas actualizaciones gratuitas de la herramienta implementada, sin interferencia en la infraestructura adicional.
- Las redes de instituciones educativas públicas y privadas al ser complejas por la gran cantidad de datos que manejan deben estar preparadas para soportar la afluencia de usuarios priorizando equipos de capa core y distribución, puesto que estos permiten el buen funcionamiento de la red de datos. De esta manera, se infiere que al usar un sistema de monitoreo se tenga la opción de encontrar debilidades y puntos de inflexión en los cuales trabajar para aportar mayores beneficios al funcionamiento de la red.
- El monitoreo y control en la red de datos de la Universidad Politécnica Estatal del Carchi es fundamental, ya que permite al administrador de la red supervisar el rendimiento de esta, detectándose con prontitud los problemas que se presentan y puedan ser resueltos a tiempo.
- Al haber analizado la infraestructura física y lógica es uno de los primeros pasos a seguir para la toma de acciones apropiadas para lograr la protección de la información, siendo de utilidad el monitoreo de la red ya que permite detectar, analizar, registrar y además, tener información fiable y verídica ante cualquier inconveniente que tenga la red.

5.2. RECOMENDACIONES

- Mantener el funcionamiento de la herramienta de monitoreo, mejorando sus funcionalidades mediante nuevos plugins y templates, dando como resultado una mejor capacidad de monitoreo, que permita al administrador de red tomar acciones necesarias para la buena operatividad de la red.
- Realizar semanalmente mantenimiento preventivo de la infraestructura de red y sus servidores, para que aporten un mejor funcionamiento en el servicio de conectividad, atendiendo los fallos que lleguen a presentarse con mayor eficiencia, evitando la baja disponibilidad del servicio de red.
- Se recomienda al personal de mantenimiento de la red de datos capacitarse sobre el uso de nuevos componentes y funcionalidades que permiten potencializar la herramienta implementada, permitiendo aprovechar el máximo la infraestructura de comunicación.
- Es recomendable analizar la aplicación de las políticas y manual de uso del sistema de monitoreo planteado inicialmente, con la finalidad de hacer cambios pertinentes que permitan mantener actualizado el sistema y aumente un mejor desempeño en sus funciones.
- Es recomendable realizar revisiones paulatinamente a los dispositivos que pertenezcan a la infraestructura de red de la institución, con el fin de establecer límites en los controles que no sobrepasen la capacidad de estos equipos y evitar la aglomeración de fallos en el sistema.

.

VI. REFERENCIAS BIBLIOGRÁFICAS

Álvarez, F.J., y Arteaga, M.M. (2010, noviembre-diciembre). Software libre: áreas de desarrollo, beneficios y usos. *CIES*. Recuperado de http://www.escolme.edu.co/revista/index.php/cies/article/viewFile/25/24

Ariganello, E. (2020). *Protocolo CDP*. Recuperado de https://aprenderedes.com/2020/01/protocolo-cdp/

Báez, J. (2017). *Diseño e Implementación de un Modelo de Gestión de red para la red de Área Local del Edificio Central de la Universidad Técnica del Norte en base al modelo de gestión OSI con el protocolo SNMP (*Tesis de pregrado). Universidad Técnica del Norte. Ibarra. Ecuador

Becerra, E. (2016). *Implementación de Monitoreo de red utilizando los protocolos ICMP y SNMP* (Tesis de pregrado). Universidad Estatal Península de Santa Elena, La Libertad, Ecuador.

Benicio, P. (2015). *Monitoreo y administración de redes usando Zabbix. Trabajo presentado al Curso de Análisis y Desarrollo de Sistemas del Instituto Federal como requisito para obtener el título de Tecnólogo en Análisis y Desarrollo de Sistemas* (Tesis de pregrado). Instituto Federal de Educación, Ciencia y Tecnología de São Paulo - Campus Capivari, São Paulo, Brasil.

Cadena, J., Dulce, E., y Jiménez, R. (2016). La importancia del monitoreo en redes de datos. *Boletí-n Informativo CEI*. Recuperado de http://editorial.umariana.edu.co/revistas/index.php/BoletinInformativoCEI/article/view/1086

CCNA. (2018). Funcionamiento SNMP. Recuperado de https://www.itesa.edu.mx/netacad/networks/course/module8/8.2.1.2/8.2.1.2.html

Cauas, D. (2015). *Definición de las variables, enfoque y tipo de investigación*. Recuperado de https://docplayer.es/13058388-Definicion-de-las-variables-enfoque-y-tipo-de-investigacion.html

Decreto Ejecutivo 1014 (2008). Utilización de Software Libre. Quito, Pichincha, Ecuador: Registro Oficial.

Digital Guide Ionos (2019). *Know How. Conoce los tipos de redes más importantes*. España. IONOS España S.L.U. Recuperado de https://www.ionos.es/digitalguide/servidores/know-how/los-tipos-de-redes-mas-conocidos/

Fruhlinger, J. (2018) *Network World. ¿Qué es la seguridad de la red?* España. The IDG Network. Recuperado de https://www.networkworld.es/seguridad/que-es-la-seguridad-de-la-red

García, F. (30 de junio de 2020). En Ecuador ha aumentado la demanda de internet y el consumo de contenido debido a el aislamiento. *El Universo*. Recuperado de https://www.eluniverso.com/larevista/2020/06/29/nota/7888932/ecuador-ha-aumentado-demanda-internet-consumo-contenido-debido

García, J., y Roa, C. (2020). *Diseño de una herramienta de monitoreo y control de servidores utilizando como eje principal Cacti aplicado a una Pyme Mediana* (Monografía de Grado). Universidad Cooperativa de Colombia, Bogotá DC, Colombia.

García, T., y Moreira, A. (2016). *Evaluación de protocolos de seguridad de las App de redes sociales en dispositivos móviles Android* (Tesis de Pregrado). Escuela Superior Politécnica Agropecuaria de Manabí Manuel Feliz López, Manabí, Ecuador.

Gonzales, D., y Carrasco, C. (2015). *Sistema de monitoreo y Análisis de tráfico en la red* (Tesis de pregrado). Universidad Autónoma de Ciudad Juárez, Ciudad Juárez, México.

Guerrero, M. A. (2016). La investigación cualitativa. *INNOVA Research Journal,1(*2), 1-9.doi: 10.33890/innova.v1.n2.2016.7

Juncosa, M. (2019). *Aprende de Redes. El modelo TCP/IP capa a capa* https://aprendederedes.com/redes/introduccion/modelo-tcp-ip/

Malagón, Ch. (2009). *NetFlow y su aplicación en seguridad.* Recuperado de https://www.rediris.es/difusion/publicaciones/boletin/87/enfoque1.pdf

ManageEngine. (2020). Conceptos básicos del protocolo SNMP. Recuperado de https://www.manageengine.com/es/network-monitoring/what-is-SNMP.html

Martínez, I (2015). *CCDA 15: Protocolos de gestión de red.* Recuperado de https://www.imd.guru/redes/cisco/certificaciones/ccda/ccda-15-protocolos_de_gestion_de_red.html

Méndez, A. (2016). *SYSLOG PROTOCOLO Y SERVICIOS*. Recuperado de https://docplayer.es/3708475-Syslog-protocolo-y-servicios.html

Motadata. (2019). *Conceptos básicos de la supervisión de la red*. New york EU: Mindarray Systems Pvt. Ltd. Recuperado de https://www.motadata.com/es/what-is-network-monitoring/

Naranjo, J. (2016). *Estudio comparativo de factibilidad del uso de herramientas de Control de Dispositivos y Servicios de Red de Datos mediante el Protocolo SNMP y Software Libre* (Tesis de pregrado). Universidad de Guayaquil, Guayaquil, Ecuador.

Narváez, S. (2015). *Estudio de QoS basado en el estándar IEEE 802.11 y alternativas de seguridad para las redes locales inalámbricas aplicado en la Wlan de la Universidad Politécnica Estatal del Carchi* (Tesis de Maestría). Pontificia Universidad Católica del Ecuador, Quito, Ecuador.

Nistal, T. (2018). *Investigación-acción participativa y mapas sociales*. Recuperado de http://comprenderparticipando.com/wp-content/uploads/2016/04/Tomas-Alberich-Nistal-Investigacion-accion-participatival.pdf

Ochoa, A. (2017). *Implementación de una red de datos con servidor de dominio para la red de salud Pacífico Norte – Chimbote; 2017*(Tesis de pregrado). Universidad Católica los Ángeles de Chimbote, Chimbote, Perú.

Ortega, A. (2018). *Enfoques de Investigación*. Recuperado de https://www.researchgate.net/profile/Alfredo_Otero-

Ortega/publication/326905435_ENFOQUES_DE_INVESTIGACION/links/5b6b7f9992851ca650526dfd/ENFOQUES-DE-INVESTIGACION.pdf

Porro, A. (2018). *The Standard CIO Información 360 Estrategia*. Miami. Estados Unidos. The Digital leaders. Recuperado de http://thestandardcio.com/2018/08/28/por-que-es-importante-el-monitoreo-de-redes-en-una-organizacion/

Ríos, D., y La Red Martínez, D. (2018). Nuevo modelo de decisión para gestión de tráfico en redes. *RedUNCI – UNNE*. Recuperado de http://sedici.unlp.edu.ar/bitstream/handle/10915/67131/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y

Rodríguez, E. (2017). *Análisis de tráfico y gestión del rendimiento en las redes de datos* (Tesis de pregrado). Universidad Estatal del Sur de Manabí, Manabí, Ecuador.

Sánchez, D. (2017). *Implementación de un Sistema de Monitoreo y protección de datos en la red de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial* (Tesis de pregrado). Universidad Técnica de Ambato, Ambato, Ecuador.

Soret, A. (2017). *Red Seguridad. Intercambio de información a través de Internet de forma segura.* España. Borrmart S.A. Recuperado de https://www.redseguridad.com/especialidades-tic/intercambio-de-informacion-a-traves-de-internet-de-forma-segura_20170109.html

Terán, R. (2017). *Implementación de un Sistema de Gestión de red de datos para la toma de decisiones de la Empresa CLICKNET S.A*(Tesis de posgrado). Pontificia Universidad Católica del Ecuador Sede Ambato, Ambato, Ecuador.

Trujillo, L. (2019). *Sistema de Gestión de red para internet de las cosas* (Tesis de posgrado). Pontificia Universidad Javeriana, Bogotá, Colombia.

Wittmann, M. (2017). SNMP. Un pilar en TI: lo que debe saber sobre sus versiones y FCAPS. Núremberg, Alemania. Recuperado de https://blog.paessler.com/SNMP-a-pillar-in-it-everything-you-need-to-know-part-1

Zeng, W., y Wang, Y. (2009). Diseño e Implementación de Sistema de Monitoreo de Servidores Basado en SNMP. *Conferencia conjunta internacional sobre inteligencia artificial*, pp. 680-682, doi: 10.1109/JCAI.2009.3

VII. ANEXOS

Anexo 1. Actas de Predefensa

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI
FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES
CARRERA DE INGENIERIA EN INFORMATICA

ACTA

DE LA SUSTENTACIÓN DE PREDEFENSA DEL INFORME DE INVESTIGACIÓN DE:

NOMBRE: Casanova Imbaquingo Edi Santiago **CÉDULA DE IDENTIDAD:** 0401587050
NIVEL/PARALELO: **PERIODO ACADÉMICO:** NOV 2020-MAR 2021

TEMA DE INVESTIGACIÓN: "Implementación del sistema de monitoreo mejora del rendimiento de la red de datos en la Universidad Politécnica Estatal del Carchi"

Tribunal designado por la dirección de esta Carrera, conformado por:

PRESIDENTE: MSC. Naranjo Cedeño Jeffery Alex
LECTOR: MSC. Hidalgo Guijarro Jairo Vladimir
ASESOR: MSC. Del Hierro Mosquera Milton Gabriel

De acuerdo al artículo 21: Una vez entregados los requisitos para la realización de la pre-defensa el Director de Carrera integrará el Tribunal de Pre-defensa del informe de investigación, fijando lugar, fecha y hora para la realización de este acto:

EDIFICIO DE AULAS: 0 **AULA:** 0
FECHA: miércoles, 14 de abril de 2021
HORA: 17H30
Obteniendo las siguientes notas:

1) Sustentación de la predefensa:	6,05
2) Trabajo escrito	2,37
Nota final de PRE DEFENSA	**8,42**

Por lo tanto: **APRUEBA CON OBSERVACIONES** ; debiendo acatar el siguiente artículo:

Art. 24.- De los estudiantes que aprueban el Plan de Investigación con observaciones. - El estudiante tendrá el plazo de 10 días laborables para proceder a corregir su informe de investigación de conformidad a las observaciones y recomendaciones realizadas por los miembros Tribunal de sustentación de la pre-defensa.

Para constancia del presente, firman en la ciudad de Tulcán el miércoles, 14 de abril de 2021

JEFFERY ALEX NARANJO CEDEÑO — Firmado digitalmente por JEFFERY ALEX NARANJO CEDEÑO Fecha: 2021.04.20 22:34:08 -05'00'

MSC. Naranjo Cedeño Jeffery Alex
PRESIDENTE

MILTON GABRIEL DEL HIERRO MOSQUERA — Firmado digitalmente por MILTON GABRIEL DEL HIERRO MOSQUERA Fecha: 2021.04.14 19:08:01 -05'00'

MSC. Del Hierro Mosquera Milton Gabriel
TUTOR

Firmado electrónicamente por: JAIRO VLADIMIR HIDALGO GUIJARRO

MSC. Hidalgo Guijarro Jairo Vladimir
LECTOR

Adj.: Observaciones y recomendaciones

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI
FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES
CARRERA DE INGENIERIA EN INFORMATICA

ACTA

DE LA SUSTENTACIÓN DE PREDEFENSA DEL INFORME DE INVESTIGACIÓN DE:

NOMBRE: Chulde Molina Anderson Xavier **CÉDULA DE IDENTIDAD:** 0401995154
NIVEL/PARALELO: [redacted] **PERIODO ACADÉMICO:** NOV 2020-MAR 2021

TEMA DE INVESTIGACIÓN: "Implementación del sistema de monitoreo mejora del rendimiento de la red de datos en la Universidad Politécnica Estatal del Carchi"

Tribunal designado por la dirección de esta Carrera, conformado por:

PRESIDENTE: MSC. Naranjo Cedeño Jeffery Alex
LECTOR: MSC. Hidalgo Guijarro Jairo Vladimir
ASESOR: MSC. Del Hierro Mosquera Milton Gabriel

De acuerdo al artículo 21: Una vez entregados los requisitos para la realización de la pre-defensa el Director de Carrera integrará el Tribunal de Pre-defensa del informe de investigación, fijando lugar, fecha y hora para la realización de este acto:

EDIFICIO DE AULAS: 0 **AULA:** 0
FECHA: miércoles, 14 de abril de 2021
HORA: 17H30

Obteniendo las siguientes notas:

1) Sustentación de la predefensa:	6,05
2) Trabajo escrito	2,37
Nota final de PRE DEFENSA	**8,42**

Por lo tanto: **APRUEBA CON OBSERVACIONES** ; debiendo acatar el siguiente artículo:

Art. 24.- De los estudiantes que aprueban el Plan de Investigación con observaciones. - El estudiante tendrá el plazo de 10 días laborables para proceder a corregir su informe de investigación de conformidad a las observaciones y recomendaciones realizadas por los miembros Tribunal de sustentación de la pre-defensa.

Para constancia del presente, firman en la ciudad de Tulcán el miércoles, 14 de abril de 2021

JEFFERY ALEX NARANJO CEDEÑO
Firmado digitalmente por JEFFERY ALEX NARANJO CEDEÑO
Fecha: 2021.04.20 22:36:07 -05'00'

MSC. Naranjo Cedeño Jeffery Alex
PRESIDENTE

MILTON GABRIEL DEL HIERRO MOSQUERA
Firmado digitalmente por MILTON GABRIEL DEL HIERRO MOSQUERA
Fecha: 2021.04.14 19:07:39 -05'00'

MSC. Del Hierro Mosquera Milton Gabriel
TUTOR

Firmado electrónicamente por: JAIRO VLADIMIR HIDALGO GUIJARRO

MSC. Hidalgo Guijarro Jairo Vladimir
LECTOR

Adj.: Observaciones y recomendaciones

Anexo 2. Validación del Abstract

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI
FOREIGN AND NATIVE LANGUAGE CENTER

ABSTRACT- EVALUATION SHEET

NAME: Casanova Imbaquingo Edi Santiago y Chulde Molina Anderson Xavier
DATE: 5 de mayo de 2021

TOPIC: "Implementación del sistema de monitoreo y mejora del rendimiento de la red de datos en la Universidad Politécnica Estatal del Carchi"
MARKS AWARDED **QUANTITATIVE AND QUALITATIVE**

VOCABULARY AND WORD USE	**Use new learnt vocabulary and precise words related to the topic**	**Use a little new vocabulary and some appropriate words related to the topic**	**Use basic vocabulary and simplistic words related to the topic**	**Limited vocabulary and inadequate words related to the topic**
	EXCELLENT: 2 ■	**GOOD: 1,5** ☐	**AVERAGE: 1** ☐	**LIMITED: 0,5** ☐
WRITING COHESION	**Clear and logical progression of ideas and supporting paragraphs.**	**Adequate progression of ideas and supporting paragraphs.**	**Some progression of ideas and supporting paragraphs.**	**Inadequate ideas and supporting paragraphs.**
	EXCELLENT: 2 ■	**GOOD: 1,5** ☐	**AVERAGE: 1** ☐	**LIMITED: 0,5** ☐
ARGUMENT	**The message has been communicated very well and identify the type of text**	**The message has been communicated appropriately and identify the type of text**	**Some of the message has been communicated and the type of text is little confusing**	**The message hasn't been communicated and the type of text is inadequate**
	EXCELLENT: 2 ■	**GOOD: 1,5** ☐	**AVERAGE: 1** ☐	**LIMITED: 0,5** ☐
CREATIVITY	**Outstanding flow of ideas and events**	**Good flow of ideas and events**	**Average flow of ideas and events**	**Poor flow of ideas and events**
	EXCELLENT: 2 ☐	**GOOD: 1,5** ■	**AVERAGE: 1** ☐	**LIMITED: 0,5** ☐
SCIENTIFIC SUSTAINABILITY	**Reasonable, specific and supportable opinion or thesis statement**	**Minor errors when supporting the thesis statement**	**Some errors when supporting the thesis statement**	**Lots of errors when supporting the thesis statement**
	EXCELLENT: 2 ☐	**GOOD: 1,5** ■	**AVERAGE: 1** ☐	**LIMITED: 0,5** ☐
TOTAL/AVERAGE	**9 - 10: EXCELLENT** **7 - 8,9: GOOD** **5 - 6,9: AVERAGE** **0 - 4,9: LIMITED**	**TOTAL 9**		

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI
FOREIGN AND NATIVE LANGUAGE CENTER

Informe sobre el Abstract de Artículo Científico o Investigación.

Autor: Casanova Imbaquingo Edi Santiago y Chulde Molina Anderson Xavier

Fecha de recepción del abstract: 5 de mayo de 2021
Fecha de entrega del informe: 5 de mayo de 2021

El presente informe validará la traducción del idioma español al inglés si alcanza un porcentaje de: 9 – 10 Excelente.

Si la traducción no está dentro de los parámetros de 9 – 10, el autor deberá realizar las observaciones presentadas en el ABSTRACT, para su posterior presentación y aprobación.

Observaciones:
Después de realizar la revisión del presente abstract, éste presenta una apropiada traducción sobre el tema planteado en el idioma Inglés. Según los rubrics de evaluación de la traducción en Inglés, ésta alcanza un valor de 9, por lo cual se validad dicho trabajo.

Atentamente

Firmado electrónicamente por:
EDISON BOANERGES
PENAFIEL ARCOS

Ing. Edison Peñafiel Arcos MSc
Coordinador del CIDEN

Anexo 3. Encuesta

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES

CARRERA DE INGENIERÍA EN INFORMÁTICA

La presente encuesta se elaboró con el objetivo de determinar el nivel de satisfacción de los usuarios de la red de datos de la Universidad Politécnica Estatal del Carchi, formando parte de la investigación denominada "Implementación de un sistema de monitoreo y mejora de la red de datos de la UPEC", desde ya anticipamos nuestro agradecimiento.

Indicaciones

La encuesta dispone de 12 preguntas las cuales deberá marcar con una X según su criterio.

Fecha: ……. …

.

1) ¿Con que frecuencia hace usted uso de la red de datos inalámbrica (Wifi) de la institución?
   - ☐ Diariamente
   - ☐ Semanalmente
   - ☐ Mensualmente
   - ☐ Nunca
2) ¿Con que frecuencia tuvo usted problemas de conexión con la red de datos inalámbrica (Wifi) en la institución?
   - ☐ Una vez por día
   - ☐ Más de una vez por día
   - ☐ Una vez por semana
   - ☐ Más de una vez por semana
3) De acuerdo con su experiencia ¿En qué lugar del campus universitario ha tenido una mejor conectividad a la red inalámbrica (Wifi) de la institución?
   - ☐ En el Aula
   - ☐ Biblioteca Luciano Coral
   - ☐ Edificio Central
   - ☐ Áreas verdes
   - ☐ Coliseo Universitario 5 de abril

4) ¿Qué servicios de red de la institución accede con más frecuencia para el desarrollo de actividades académicas?

- ☐ Aulas Virtuales
- ☐ Correo electrónico
- ☐ Página Web
- ☐ Carga y Descarga de Archivos

5) ¿Ha experimentado usted problemas con las plataformas (Aulas virtuales, Portafolio académico, Correo electrónico, Pagina Web) institucional?

- ☐ Siempre
- ☐ Regularmente
- ☐ Ocasionalmente
- ☐ Nunca

6) ¿Cuáles han sido los problemas más comunes al utilizar las plataformas (Aulas virtuales, Portafolio académico, Correo electrónico, Pagina Web) de la institución?

- ☐ Restricción de ingreso
- ☐ Demora del servicio
- ☐ Indisponibilidad del servicio
- ☐ Ninguno

7) ¿Conoce usted cuales son las Políticas de uso de servicios de red que se encuentran vigentes en la institución?

- ☐ Si
- ☐ No

8) ¿Cree usted que el cumplimiento de las políticas de uso de servicios de red en la institución debe cumplirse para asegurar la calidad de los servicios de red y mantengan sus datos seguros?

- ☐ Siempre
- ☐ A veces
- ☐ Nunca

9) ¿Cree usted necesario que el departamento de TIC’s monitoree el uso de los servicios de red para hacer cumplir las políticas y así mantener la calidad de los servicios?

- ☐ Siempre
- ☐ Solo cuando existan problemas
- ☐ Nunca

10) ¿Indique el nivel de funcionalidad de la Pagina Web de la institución?

- [ ] Muy bueno
- [ ] Bueno
- [ ] Regular
- [ ] Deficiente

11) ¿Indique el nivel de funcionalidad del servicio de correo electrónico de la institución?

- [ ] Muy bueno
- [ ] Bueno
- [ ] Regular
- [ ] Deficiente

12) ¿Indique el nivel de funcionalidad del servicio de Aulas virtuales?

- [ ] Muy bueno
- [ ] Bueno
- [ ] Regular
- [ ] Deficiente

Anexo 4. Entrevista

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI
FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES
CARRERA DE INGENIERÍA EN INFORMÁTICA

Entrevista:

La presente entrevista se la elaboro con el objetivo de conocer la situación actual de la infraestructura física y lógica de la red de datos, recopilando información y determinando la calidad de los servicios que brinda el departamento de TIC's de la UPEC.

1. **¿Se establece algún procedimiento para mitigar una falla en la red, al conocerse de alguna?**

   Básicamente los procedimientos son resolver de manera inmediata las fallas al momento de ser detectadas, ya que pueden existir diferentes fallas no existe un procedimiento preestablecido.

2. **¿Mantienen evidencia sobre los diferentes eventos de fallos en la red y de las configuraciones respectivas sobre los equipos y cuál es su proceso para hacerlo?**

   No se guarda evidencia de los diferentes eventos de fallos, pero de las configuraciones de los equipos si se tiene un respaldo, esto se lo realiza 1 vez al mes de los equipos principales.

3. **¿Qué herramientas utilizan para la detección de fallos en la red?**

   Al momento no poseemos ningún Hardware ni Software que nos permita detectar los fallos en la red institucional.

4. **¿Qué tiempo lleva detectar una falla en la red?**

   Los fallos en la red son comunicados por aquellas personas que lo detectan, por ejemplo, si no existe conectividad de un teléfono IP, el usuario es quien inmediatamente lo comunica al área de Redes y Telecomunicaciones.

5. **¿Cuál es el proceso para la solución del problema en caso de ser detectado?**

   El proceso es muy simple, aunque no poseemos un esquema que nos indique el procedimiento para cada uno de los eventos de fallas, solo se detecta la falla analizar la solución y aplicarla. Existen eventos de fallas que son muy comunes dentro de la red los cuales su solución ya es conocida y reparar esta falla no lleva mucho tiempo.

6. **¿Se generan periódicamente registros acerca del rendimiento de los dispositivos de red?**

   No se han generado registros del rendimiento de ninguno de los equipos activos de la red institucional.

7. **¿Cómo calificaría la disponibilidad de los servicios que provee la red de datos de la UPEC?**

   Dentro de una escala del 1 al 10, lo calificaría con un 8 ya que, debido a la obsolescencia de algunos de los equipos, hay períodos cortos en los que los equipos no responden y es necesario su reinicio.

8. **¿Cuál es el proceso de gestión de acceso a los dispositivos de red de la Universidad?**

   Para la gestión de acceso a los dispositivos, se lo hace vía remota y solamente el administrador de redes y telecomunicaciones conoce y hace uso de las direcciones IP, usuarios y claves para acceder y realizar las configuraciones necesarias en los equipos.

9. **¿Cuántos son los equipos con los cuales cuenta la red actual de la Universidad?**

   Dentro de la red institucional, contamos con más de 200 equipos activos de red, entre los que tenemos, Switch de Core, Firewall, Servidores, Switch de acceso, Access Point, entre otros.

10. **¿Se ha levantado la topología actual de la infraestructura física de la UPEC?**

    Dentro de nuestros esquemas tenemos diseñado una topología física de la red, aunque no se encuentra actualizada por los cambios constantes que se producen. Además, y de igual forma, la topología física se la tiene documentada.

11. **¿La universidad cuenta con una herramienta de sistema de monitoreo?**

    La universidad no cuenta con herramientas de monitores de la red.

12. **¿Qué equipos tienen mayor necesidad de ser monitoreados?**

    Los equipos activos de red, es decir: Switch de Core, firewall, switch de acceso, servidores, Access points.

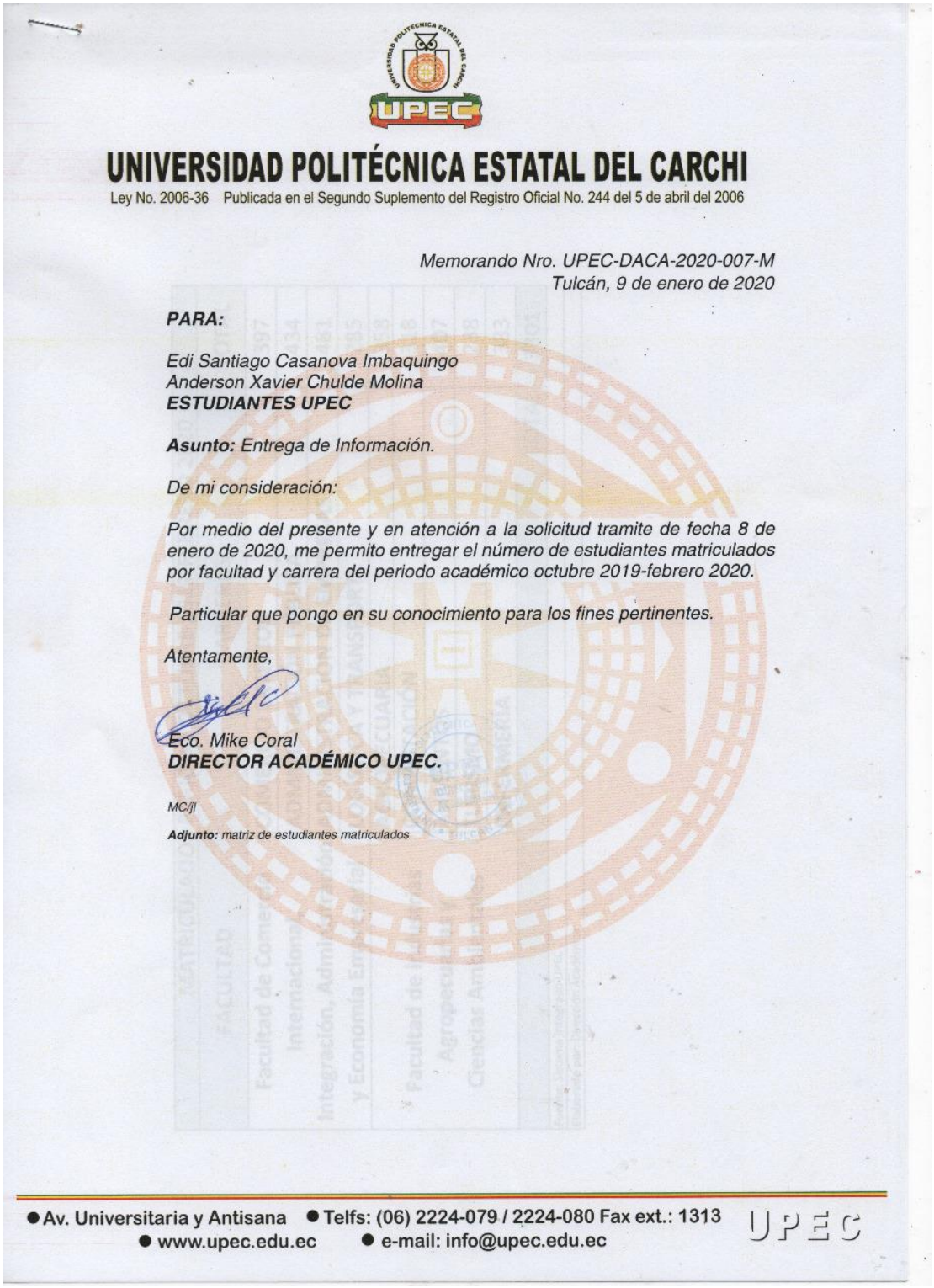
13. **¿Equipos o programa de monitoreo que conoce o maneja usted?**

    Bueno existen algunos, PRTG, Nagios, NTOP, entre otros que son free y licenciados. Y manejo Zabbix, para el monitoreo del enlace principal de internet el cual nos provee CEDIA.

14. **¿Basado en su experiencia cuales serían los requerimientos mínimos para implementar un sistema de monitoreo**

Debido a que somos una institución pública y nos basamos en recursos estatales, nuestro principal requerimiento es que sea un software de plataforma libre, así no incurrir en gastos de licenciamiento. Que nos permita ver a cada uno de nuestros usuarios por IP, que nos indique las características físicas que son ocupadas por cada uno de nuestros equipos activos de red y que se pueda generar reportes para su análisis de datos.

Anexo 5. Certificado del número de estudiantes matriculados en el periodo 2020



UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Ley No. 2006-36 Publicada en el Segundo Suplemento del Registro Oficial No. 244 del 5 de abril del 2006

Memorando Nro. UPEC-DACA-2020-007-M
Tulcán, 9 de enero de 2020

PARA:

Edi Santiago Casanova Imbaquingo
Anderson Xavier Chulde Molina
ESTUDIANTES UPEC

Asunto: *Entrega de Información.*

De mi consideración:

Por medio del presente y en atención a la solicitud tramite de fecha 8 de enero de 2020, me permito entregar el número de estudiantes matriculados por facultad y carrera del periodo académico octubre 2019-febrero 2020.

Particular que pongo en su conocimiento para los fines pertinentes.

Atentamente,

Eco. Mike Coral
DIRECTOR ACADÉMICO UPEC.

MC/jl

Adjunto: *matriz de estudiantes matriculados*

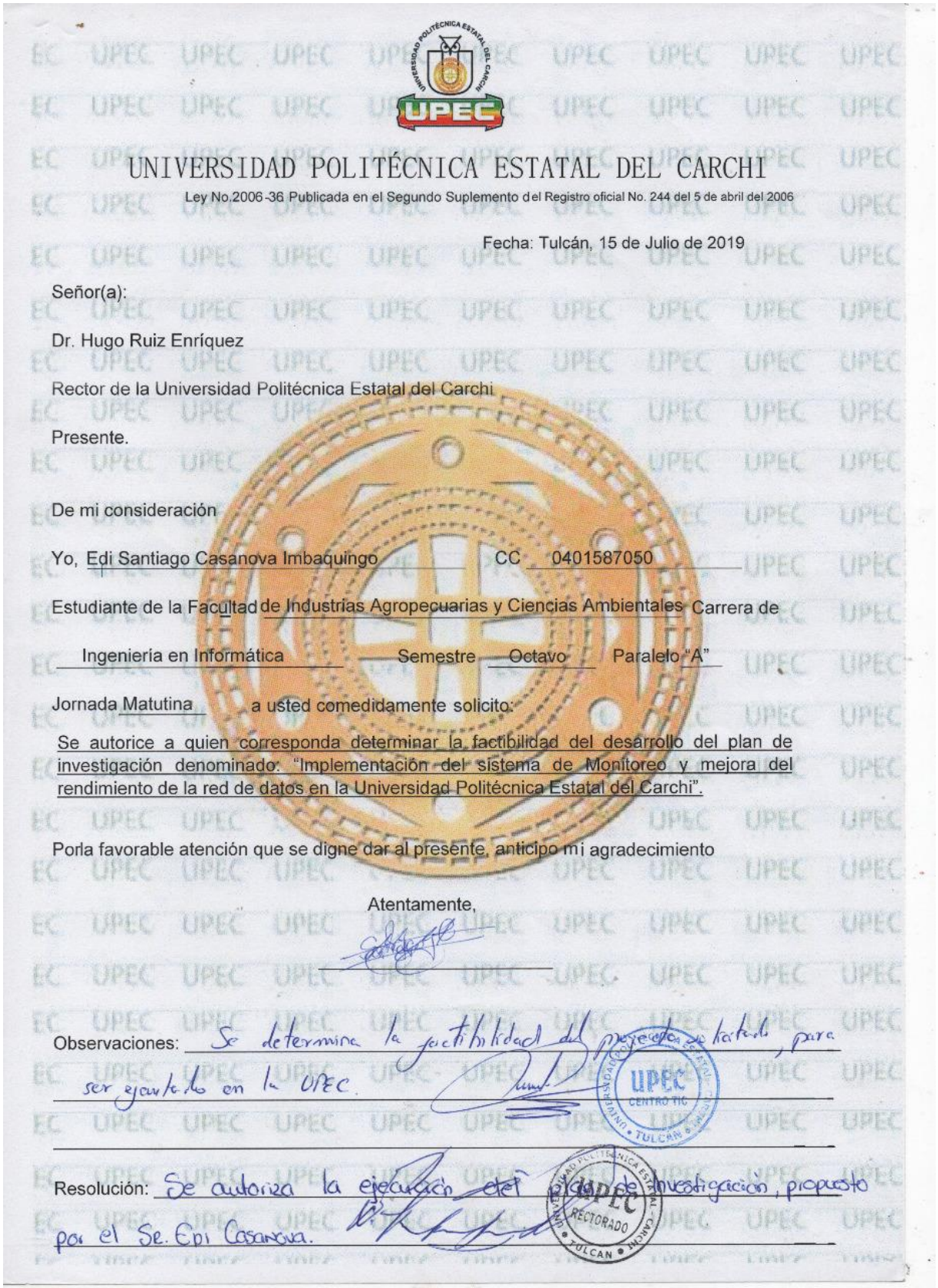
● Av. Universitaria y Antisana ● Telfs: (06) 2224-079 / 2224-080 Fax ext.: 1313
● www.upec.edu.ec ● e-mail: info@upec.edu.ec
UPEC

Anexo 6. Número de estudiantes matriculados en el periodo octubre 2019- febrero 2020

MATRICULADOS PERIODO OCTUBRE 2019-FEBRERO 2020		
FACULTAD	CARRERAS	TOTAL
Facultad de Comercio Internacional, Integración, Administración y Economía Empresarial	COMERCIO EXTERIOR	397
	ADMINISTRACIÓN PÚBLICA	434
	ADMINISTRACION DE EMPRESAS	481
	LOGÍSTICA Y TRANSPORTE	285
Facultad de Industrias Agropecuarias y Ciencias Ambientales	AGROPECUARIA	358
	COMPUTACIÓN	318
	ALIMENTOS	407
	TURISMO	238
	ENFERMERÍA	383
	TOTAL	3301

Fuente: Sistema Integrado UPEC
Elaborado por: Dirección Académica

Anexo 7. Solicitud de autorización 1



UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Ley No.2006-36 Publicada en el Segundo Suplemento del Registro oficial No. 244 del 5 de abril del 2006

Fecha: Tulcán, 15 de Julio de 2019

Señor(a):

Dr. Hugo Ruiz Enríquez

Rector de la Universidad Politécnica Estatal del Carchi

Presente.

De mi consideración

Yo, Edi Santiago Casanova Imbaquingo CC 0401587050

Estudiante de la Facultad de Industrias Agropecuarias y Ciencias Ambientales Carrera de Ingeniería en Informática Semestre Octavo Paralelo "A"

Jornada Matutina a usted comedidamente solicito:

Se autorice a quien corresponda determinar la factibilidad del desarrollo del plan de investigación denominado: "Implementación del sistema de Monitoreo y mejora del rendimiento de la red de datos en la Universidad Politécnica Estatal del Carchi".

Porla favorable atención que se digne dar al presente, anticipo mi agradecimiento

Atentamente,

Observaciones: Se determina la factibilidad del proyecto de tesis, para ser ejecutado en la UPEC

Resolución: Se autoriza la ejecución del plan de investigación, propuesto por el Se. Edi Casanova.

Anexo 8. Solicitud de autorización 2

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Ley No.2006-38 Publicada en el Segundo Suplemento del Registro oficial No. 244 del 5 de abril del 2006

Fecha: Tulcán, 15 de Julio de 2019

Señor(a):

Dr. Hugo Ruiz Enriquez

Rector de la Universidad Politécnica Estatal del Carchi

Presente.

De mi consideración

Yo, Anderson Xavier Chulde Molina CC 0401995154

Estudiante de la Facultad de Industrias Agropecuarias y Ciencias Ambientales Carrera de Ingeniería en Informática Semestre Octavo Paralelo "A"

Jornada Matutina a usted comedidamente solicito:

Se autorice a quien corresponda determinar la factibilidad del desarrollo del plan de investigación denominado: "Implementación del sistema de Monitoreo y mejora del rendimiento de la red de datos en la Universidad Politécnica Estatal del Carchi".

Por la favorable atención que se digne dar al presente, anticipo mi agradecimiento

Atentamente,

Observaciones: Se determina la factibilidad del proyecto solicitado, para ser ejecutado en la UPEC

Resolución: Se autoriza la ejecución del Plan de Investigación propuesto por el Sr. Postulante Chulde

Anexo 9. Requerimientos de la herramienta de gestión de la red de datos

Para le recopilación de la información se aplicó la técnica de la entrevista dirigida a el Ing. Javier Torres administrador de la red de datos de la institución, quien tiene responsabilidad de la conectividad y operatividad de la red de datos interna de la institución, fue quien nos aportó con toda la información técnica sobre cómo se encuentra estructurada la infraestructura física y lógica de la red, como también los requerimientos de los equipos y servicios que se necesita priorizar durante la implementación de la herramienta.

Además, la aplicación de la entrevista se determinó sobre las funcionalidades más importantes a tomar en cuenta para la implementación de la herramienta de monitoreo.

- Monitorización remota
- Alertas y notificación
- Graficas
- Seguridad
- Disponibilidad
- Reportes
- Escalabilidad
- Rendimiento
- Salud de la red
- Cambios de configuración
- Autodescubrimiento de la red

Monitorización remota: la herramienta está diseñada específicamente para la monitorización y registro del estado de varios servicios de la red, siendo estos servidores y hardware, además se integra las redes wifi-desplegadas guardando todo un inventario histórico de los problemas o configuraciones.

Alertas y notificaciones: la herramienta de monitoreo estará en capacidad de alertar en caso de encontrar una anomalía dentro de la red y esta se notificará de manera inmediata mediante aplicaciones de mensajería en este caso mediante correo electrónico y telegram a el encargado de la red de datos con el objetivo de alertar el problema para su solución inmediata.

Graficas: Esta característica permitirá que la información de la red se visualice en graficas dinámicas para una mejor interpretación de lo que ocurre dentro de la red de datos de la institución, este apartado es indispensable a la hora de monitorizar una infraestructura de red dado a que nos muestra en tiempo real la actividad o el estado de los equipos que se encuentran siendo monitorizados.

Seguridad: Es uno de los puntos más importantes a tomar en cuenta en el uso de la herramienta de gestión de la red, debido a que se manejan datos relevantes sobre equipos e infraestructura de la red de la institución por ende esta debe ser confidencial para este apartado es necesario la creación de grupos para clasificar quienes puedan acceder a los datos que recopila el sistema en este caso la persona encargada en la gestión de los usuarios y grupos es el administrador de la red, quien tendrá el control total del sistema.

Disponibilidad: El sistema de gestión de red garantiza su funcionamiento las 24 horas por los 7 días de la semana, monitoreando toda la infraestructura de la red buscando alertar sobre problemas que se presenten en el transcurso de los 7 días.

Reportes: el sistema está en capacidad de generar reportes diarios, semanales, mensuales y anuales según sea el requerimiento del departamento de TIC's acerca de los dispositivos monitorizados.

Escalabilidad: el sistema deberá estar en capacidad de añadir más dispositivos sin afectar el desempeño de este.

Rendimiento: Uso del ancho de banda, como también la utilización de la CPU y memoria de los equipos principales de la infraestructura de la red.

Salud de la red: Estado de los equipos de interconexión en estado crítico/advertencia.

Cambios de configuración: cambios de estado de configuración internos de los equipos e interfaces de red.

Autodescubrimiento de la red: el sistema está en capacidad de descubrir nuevos elementos de red y agregarlos automáticamente al sistema de gestión guardando en un registro toda la configuración que este posea al momento del autodescubrimiento, o en alguna actualización.

Además, se requiere monitorizar de las siguientes características principales de los equipos.

- ✓ **CPU:** Carga de la CPU, para prevenir el mal funcionamiento del equipo y medir los estados de carga de este.
- ✓ **Uso de memoria:** para un análisis preventivo y correctivo de este.
- ✓ **Estado de disco duro:** nivel de tasa de lectura y escritura del disco, determinando picos de funcionamiento.
- ✓ **Ancho de banda:** determinar el segmento de red que tiene un consumo inadecuado del ancho de banda.
- ✓ **Cortes de red:** determinar sobre la estabilidad de la red.
- ✓ **Estado de enlaces:** estado de los equipos, si estos están activos o caídos.

Anexo 10. Instalación de CentOS 7

Inicio de instalación, opción install CentOS 7.

Figura 34. Instalación de CentOS 7

El primer paso es la selección de idioma y la distribución del teclado del equipo, una vez seleccionado estos parámetros damos click en continuar.

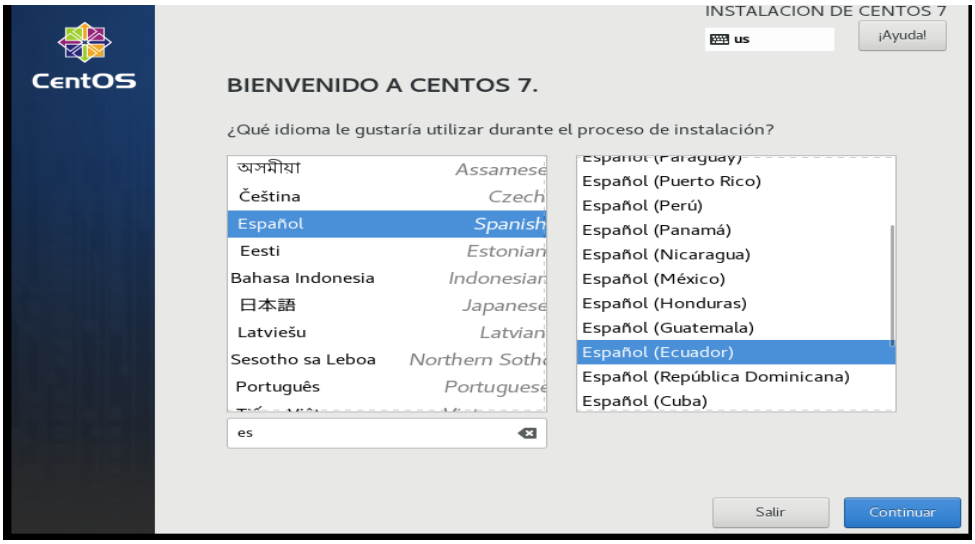


Figura 35. Selección de Idioma de CentOS7

En el resumen de instalación, seleccionar el software de instalación.

Figura 36. Resumen de Instalación

En este caso seleccionamos escritorio GNOM y habilitar complementos necesarios para el uso del servidor. hacer click en botón listo.

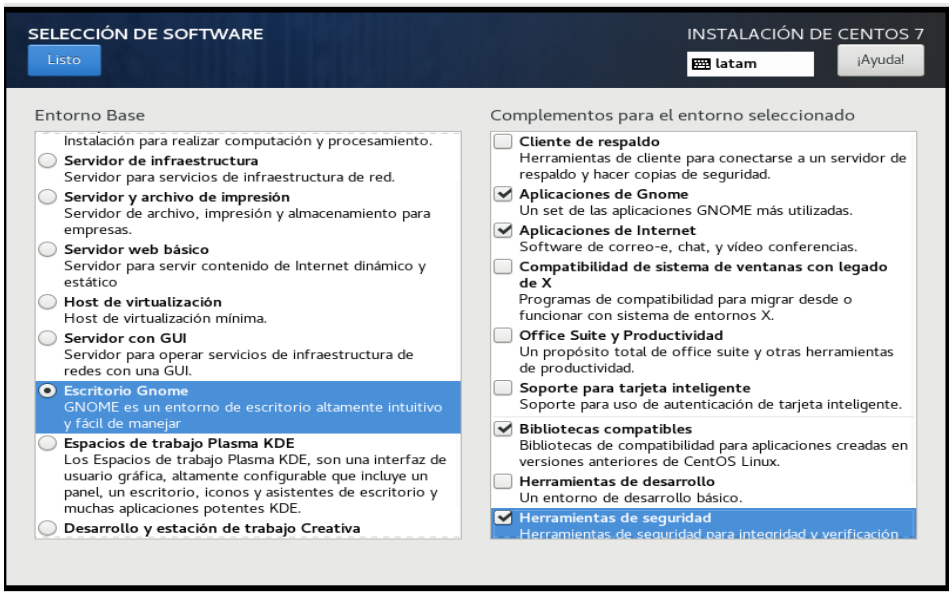


Figura 37. Selección del Software

Se selecciona donde se instalará CentOS7.

Figura 38. Destino de Instalación

En el apartado general del resumen de instalación, seleccionamos red y nombre de equipo, habilitamos la tarjeta de red. hacer click en listo.

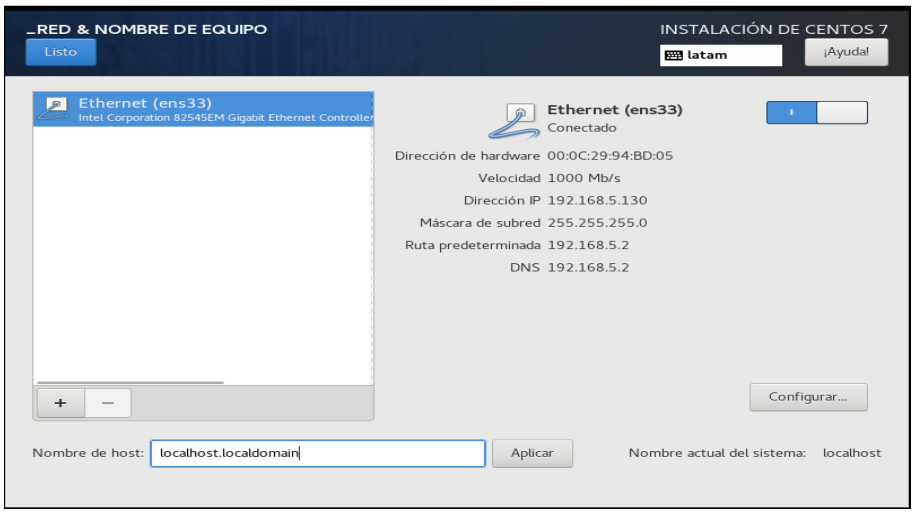


Figura 39. Tarjeta de Red

Una vez finalizado el proceso de configuración se procede a iniciar la instalación, en este proceso no pedirá la creación de una contraseña para el usuario root, administrador del sistema, como también la creación de un usuario.

Figura 40. Proceso de Instalación

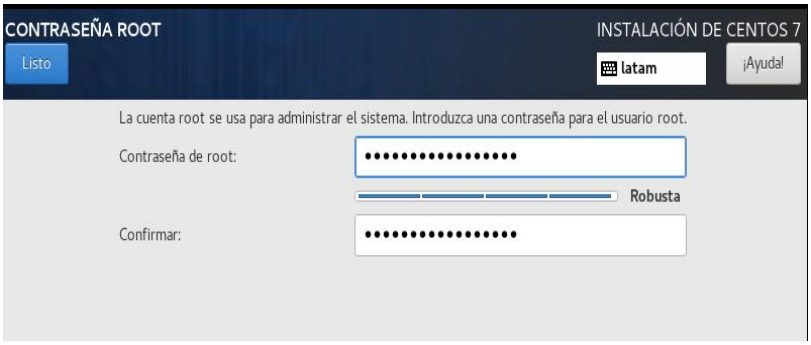


Figura 41. Contraseña a Usuario Root

Una vez creado la contraseña de root, finalizaremos con las configuraciones y continuara con la instalación hasta que finalice.

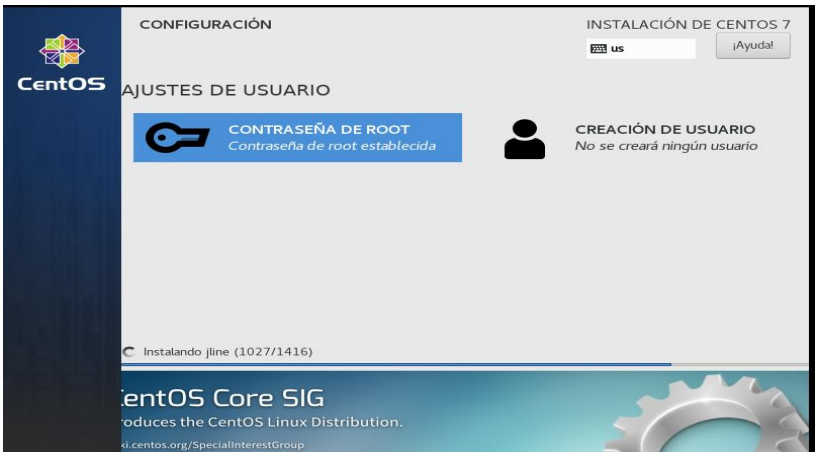


Figura 42. Instalación de CentosOS7

Anexo 11. Instalación de Zabbix

Mediante herramienta putty, accedemos al servidor de manera remota por SSH.

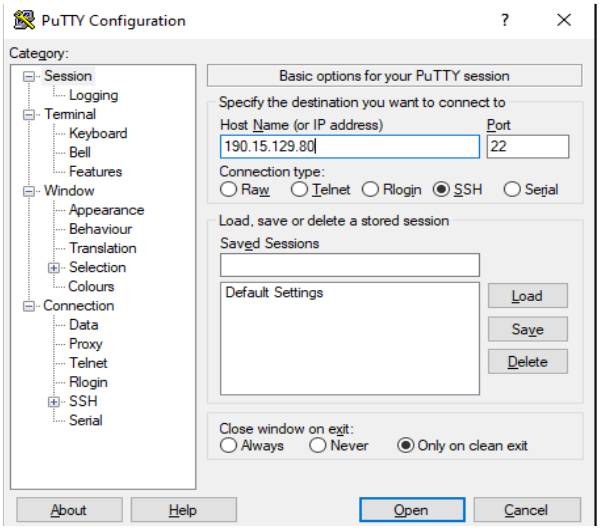


Figura 43. Acceso al Servidor Mediante Putty

Conexión al servidor.

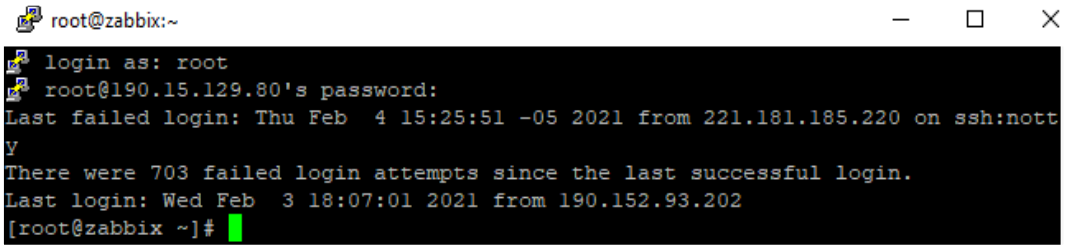


Figura 44. Conexión al Servidor Zabbix

Antes de la instalación de zabbix, es necesario instalar paquetes del repositorio EPEL y actualizar el sistema.

```
# rpm -Uvh https://repo.Zabbix.com/Zabbix/5.0/rhel/7/x86_64/Zabbix-release-5.0-1.el7.noarch.rpm
# yum install epel-release -y
# yum update -y
```

Descargar repositorio zabbix 5.0 para CentOS 7 y limpiamos paquetes innecesarios.

```
# yum clean all
```

Instalación de zabbix server y agente.

```
# yum install Zabbix-server-mysql -y
# yum install Zabbix-agent -y
```

Instalación de paquetes reléase.

```
#yum install Centos-release-scl -y
```

Habilitar repositorio de frontend de zabbix, enabled = 1 y guardamos los cambios.

```
# nano /etc/yum.repos.d/Zabbix.repo
[Zabbix-frontend]
enabled=1
```

Instalar paquetes frontend, apache y mysql.

```
# yum install Zabbix-web-mysql-scl Zabbix-apache-conf-scl -y
```

Instalar mariadb server, habilitarlo e iniciar.

```
# yum -y install mariadb-server
# systemctl start mariadb
# systemctl enable mariadb
```

Crear la base de datos y usuario zabbix.

En este apartado creamos la base de datos zabbix y el usuario llamado “Zabbixupec” con su respectiva contraseña. El usuario será usado por el servidor zabbix y el web frontend.

- Conectar al servicio de consola mysql.

```
# mysql -u root -p
```

- El primer paso será crear la base de datos en este caso “Zabbixupecdb”.

```
mysql> # create database Zabbixupecdb character set utf8 collate
utf8_bin;
```

- Creación de usuario “Zabbixupec_user” con su respectiva contraseña.

```
mysql>#  create  user  Zabbixupec_user@localhost  identified  by  '
ZabUpec_2021 ';
```

- Para finalizar damos privilegios a el usuario para la base de datos.

```
mysql>  #  grant  all  privileges  on  Zabbixupecdb.*  to
Zabbixupec_user@localhost;
mysql> # flush privileges;
mysql> # exit;
```

Configuración de acceso a la base de datos.

```
# nano /etc/Zabbix/Zabbix_server.conf
DBname:Zabbixupecdb
DBuser:Zabbixupec_user
DBpassword:xxxxx
```

Configuración zona horaria php.

- Configuración de php para zabbix en CentOS 7, mediante el ingreso del archivo.

```
# nano /etc/opt/rh/rh-php72/php-fpm.d/Zabbix.conf
php_value[max_execution_time]= 300
php_value[memory_limit]=128M
php_value[post_max_size]= 16M
php_value[upload_max_filesize]= 8M
php_value[max_input_time]= 300
php_value[date.timezone]= America/Guayaquil
```

Activación de servicios zabbix, agentes y servicio httpd.

```
# systemctl restart Zabbix-server Zabbix-agent httpd rh-php72-php-fpm
# systemctl enable Zabbix-server Zabbix-agent httpd rh-php72-php-fpm
```

Deshabilitar selinux para el servidor zabbix.

```
# nano /etc/selinux/config
SELINUX=disabled
```

Habilitar puertos de conexión de los servicios.

```
# firewall-cmd --permanent --add-port=10050/tcp
# firewall-cmd --permanent --add-port=10051/tcp
```

```
# firewall-cmd --permanent --add-port=80/tcp
# firewall-cmd -reload
# firewall-cmd -permanent -add-service=http
# systemctl restart firewalld
```

Para finalizar la instalación se procede a acceder a el zabbix frontend, comprobamos acceso del front end de zabbix, click en “next step”.

Figura 45. Configuración en el Frontend de Zabbix

Comprobar los requisitos previos para la configuración.

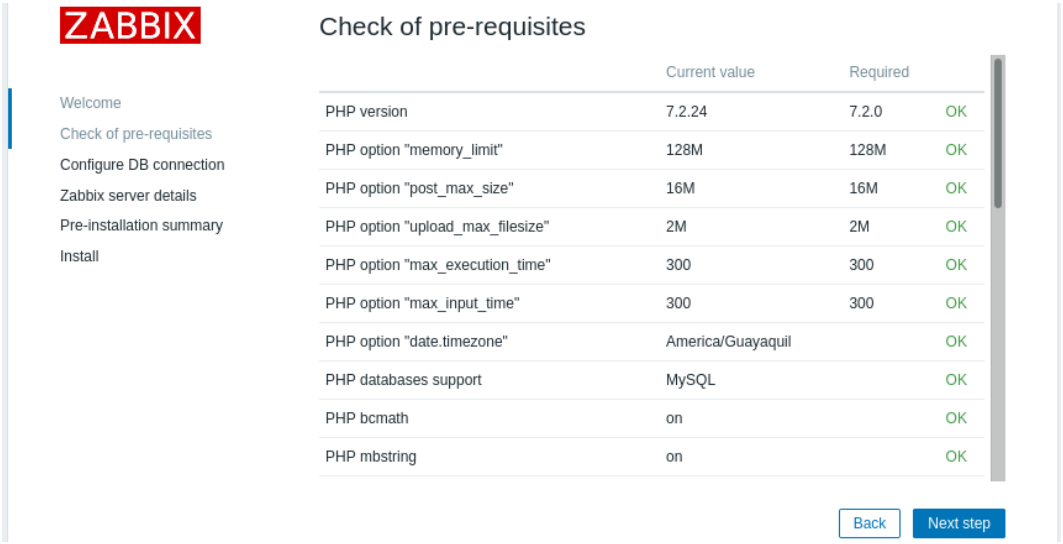


Figura 46. Requisitos de Inicio de Zabbix

Configuración de la base de datos, para la conexión.

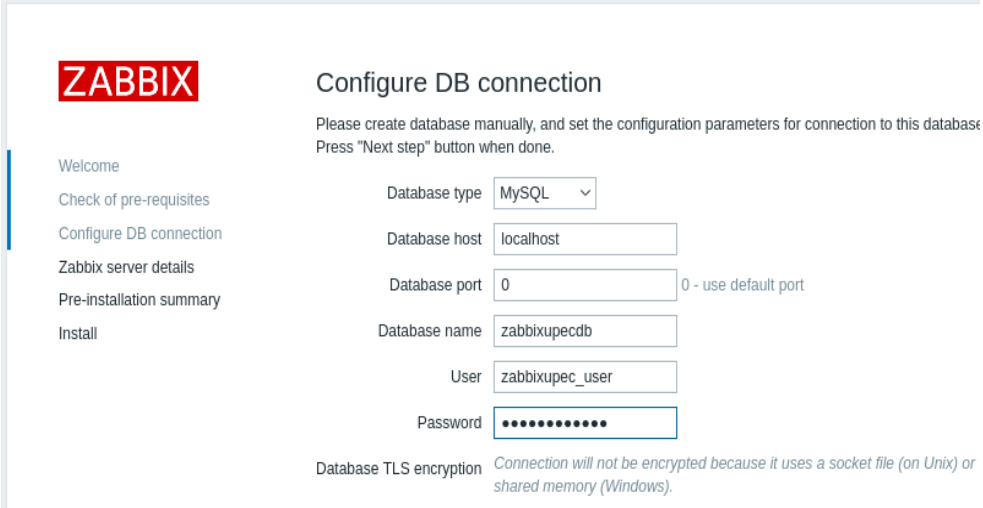


Figura 47. Conexión BD

Detalles del servidor zabbix.

Figura 48. Detalle de Servidor Zabbix

Resumen de la preinstalación, se puede apreciar en la imagen un resumen de instalación del frontend de zabbix.

Figura 49. Resumen de Configuración

Estado de la instalación del frontend.

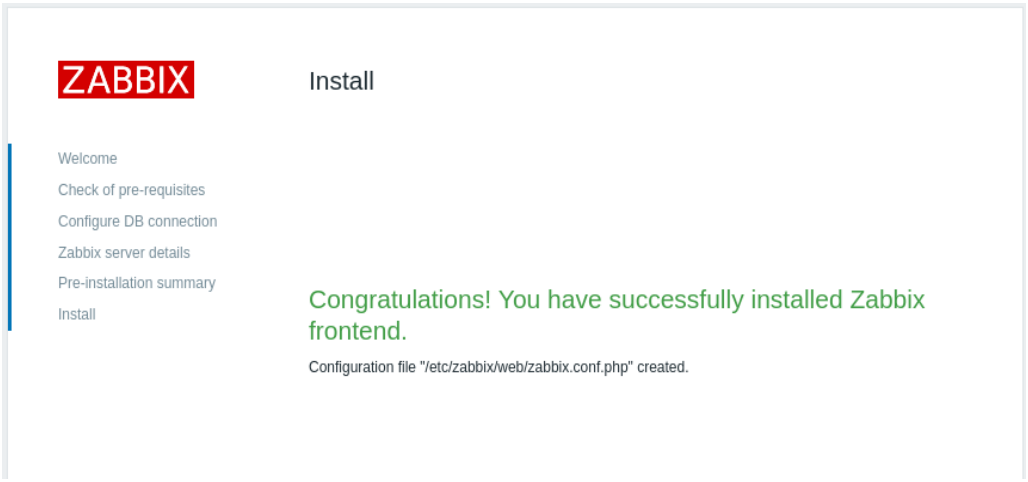


Figura 50. Estado de Instalación

Inicio de sesión de zabbix

Usuario y contraseña por defecto del sistema: username: admin, password: Zabbix, por lo que es recomendable cambiarla en el instante.

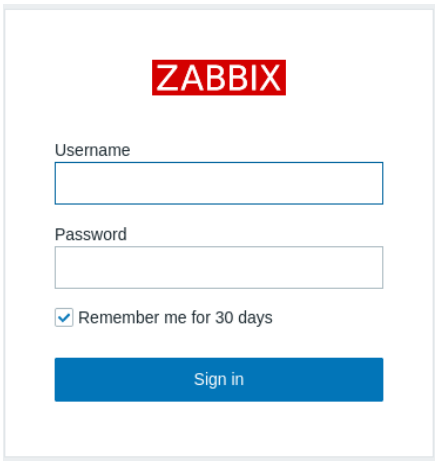


Figura 51. Inicio de Sesión de Zabbix

Panel general del servidor zabbix.

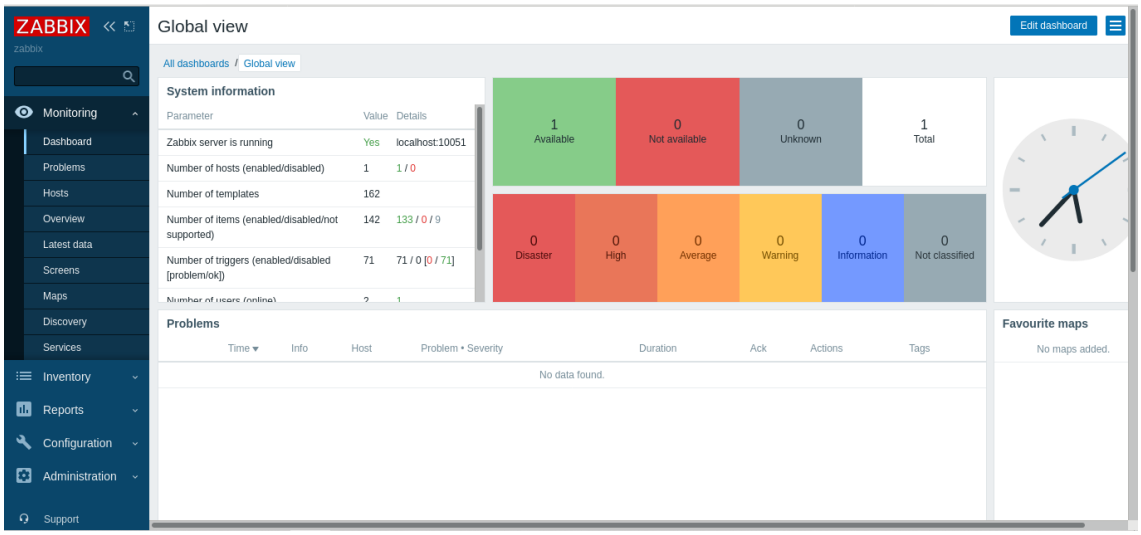


Figura 52. Frontend de Zabbix

Anexo 12. Habilitar SNMP en Switches

Ingreso a equipos vía SSH.

-Acceso con credenciales de equipos switches.

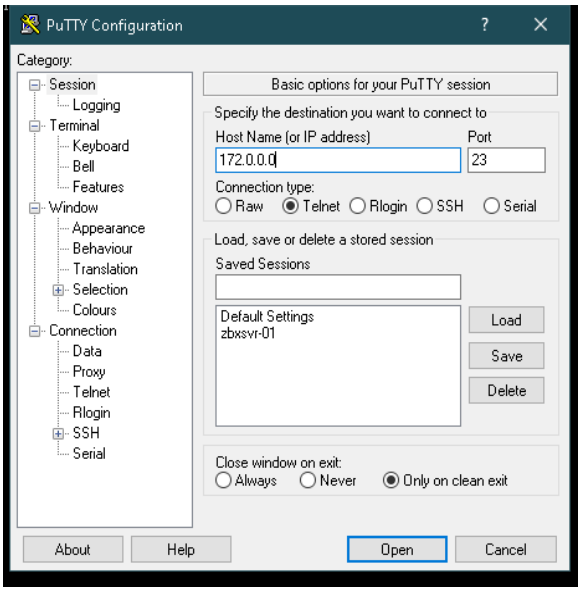


Figura 53. Acceso SSH a un Switch

Configuración y habilitación de protocolo SNMP en los equipos.

```
# enable
# conf terminal
switch(config)# SNMP-server community public RO
switch(config)# SNMP-server community private RW
# exit
# write memory
```

Verificamos que el agente SNMP este activo.

```
# show SNMP
```

```
[OK]
MBL#show snmp
Chassis: FOC1622Y3DG
20542 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    758621 Number of requested variables
    0 Number of altered variables
    19063 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
    0 Input queue packet drops (Maximum queue size 1000)
20542 SNMP packets output
    67 Too big errors (Maximum packet size 1500)
    0 No such name errors
    0 Bad values errors
    0 General errors
    20542 Response PDUs
    0 Trap PDUs
SNMP global trap: disabled

SNMP logging: disabled
SNMP agent enabled
```

Figura 54. Verificación de SNMP

Anexo 13. Agregar host al servidor zabbix

Iniciada sesión en zabbix frontend, iremos a “Configuration” / “Hosts”.

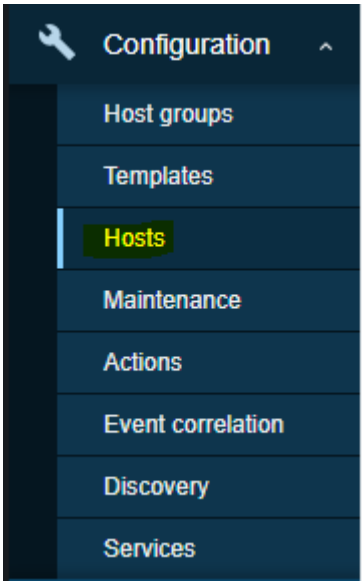


Figura 55. Menú de Configuración

Para agregar un nuevo host, pulsaremos en el botón “Create host” y desplegara un formulario.

- **Host name:** Ingrese un nombre del host a monitorizar.
- **Host name visible:** Repite el nombre del host, opcional.
- **Group:** Ingrese el dispositivo a un grupo que pertenezca.
- **Interfaces:** Agregar la ip del nombre del host.

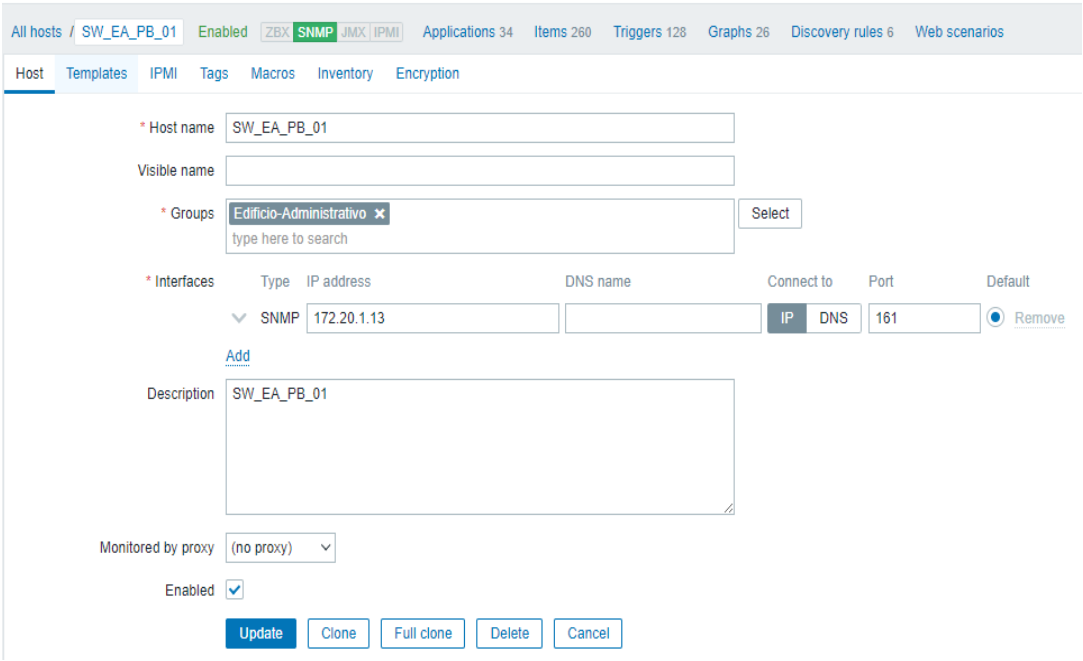


Figura 56. Configuración SNMP de un Host

Insertar templates.

- Linked new template: colección de ítems, triggers y gráficos diseñados para dispositivos de interconexión.

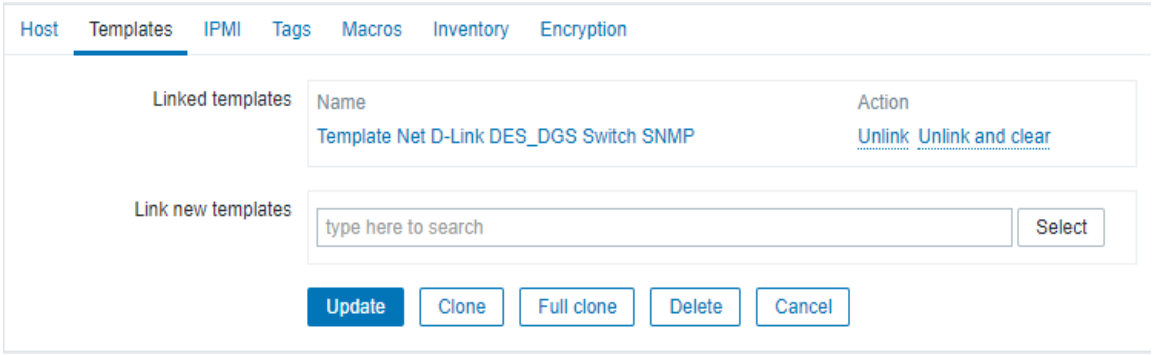


Figura 57. Vista de un Template

Para finalizar con el registro de un host se procede a insertar la macro, la cual tendrá un identificador sobre la comunidad a la que pertenezca, actualizamos cambios.

- **Macro:** Variable de identificación del dispositivo.
- **Value:** Comunidad a la que pertenece el equipo.

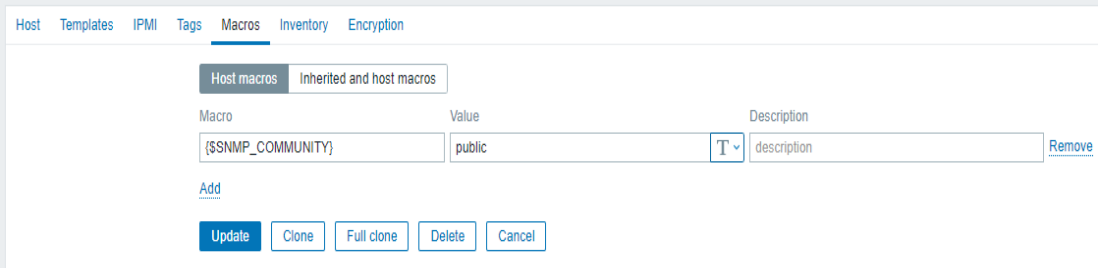


Figura 58. Configuración de la comunidad de un host

Visualización del dispositivo.

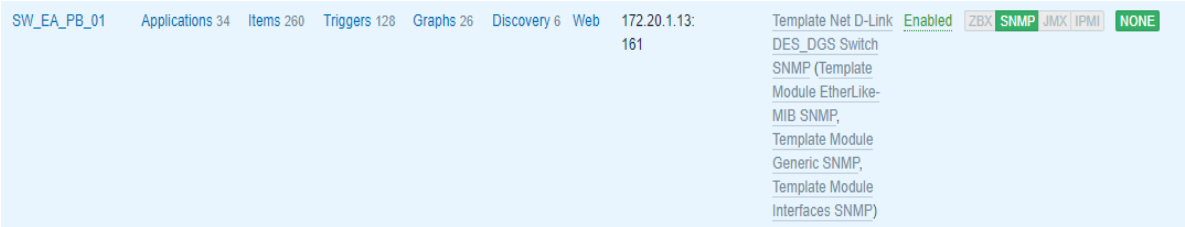


Figura 59. Vista de un Host

Anexo 14. Instalación de Grafana

Para integrar grafana en nuestro servidor zabbix, como primer punto es necesario crear una nueva base de datos.

- Conectamos a la base de datos del servidor.

```
#mysql -u root p
MariaDB [(none)]> #create database grafana;
```

Después asignamos privilegios a un usuario con una contraseña.

```
MariaDB [(none)]> #grant all privileges on grafana.* to grafana@localhost identified by "Grafana_2021";
```

Actualizamos privilegios y salimos.

```
MariaDB [(none)]>#flush privileges;
MariaDB [(none)]># exit;
```

Una vez instalado nuestra base de datos se precede a instalar el paquete de grafana, para su instalación.

```
# yum install https://dl.grafana.com/oss/release/grafana-7.4.3-1.x86_64.rpm
```

Creamos una copia del archivo grafana.ini.

```
#cp /etc/grafana/grafana.ini{,..org}
```

Apuntamos la configuración de la base de datos, editamos el archivo grafana.ini.

```
#nano grafana.ini
type= mysql
host=127.0.0.1:3306
name=grafana
user=grafana
```

Guardamos cambios y habilitamos el servicio.

```
#systemctl enable grafana-server
#systemctl daemon-reload
```

```
#systemctl start grafana-server
```

Para finalizar procedemos a dar permisos en firewall para que el servicio de grafana pueda conectarse mediante el puerto 3000.

```
#firewall-cmd -permanent -add-port =3000/tcp
#firewall-cmd -reload
```

Una vez instalado y con los permisos en el firewall procedemos a el navegador a acceder a grafana mediante el puerto 3000.

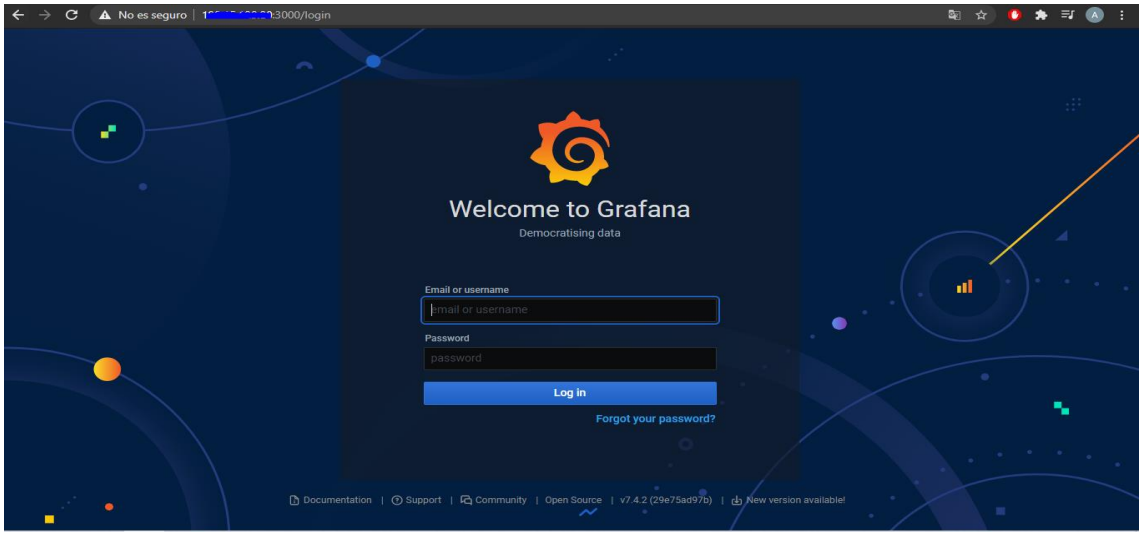


Figura 60. Frontend de Grafana

Usuario por defecto admin y contraseña admin, por lo cual grafana te solicita cambiarla.

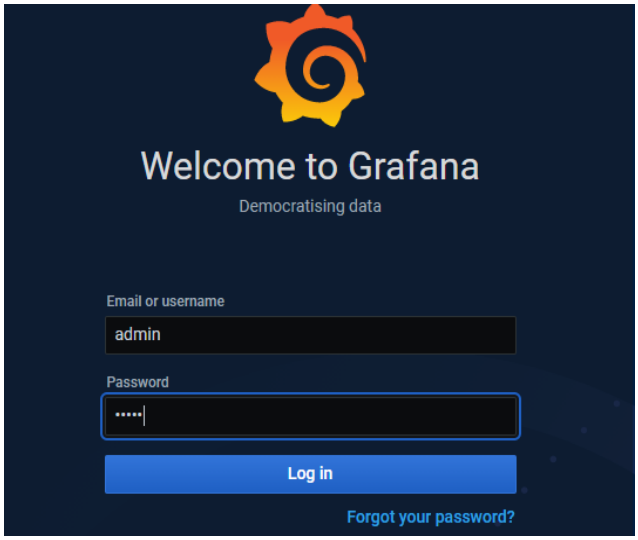


Figura 61. Inicio de Sesión de Grafana

Panel principal de grafana.

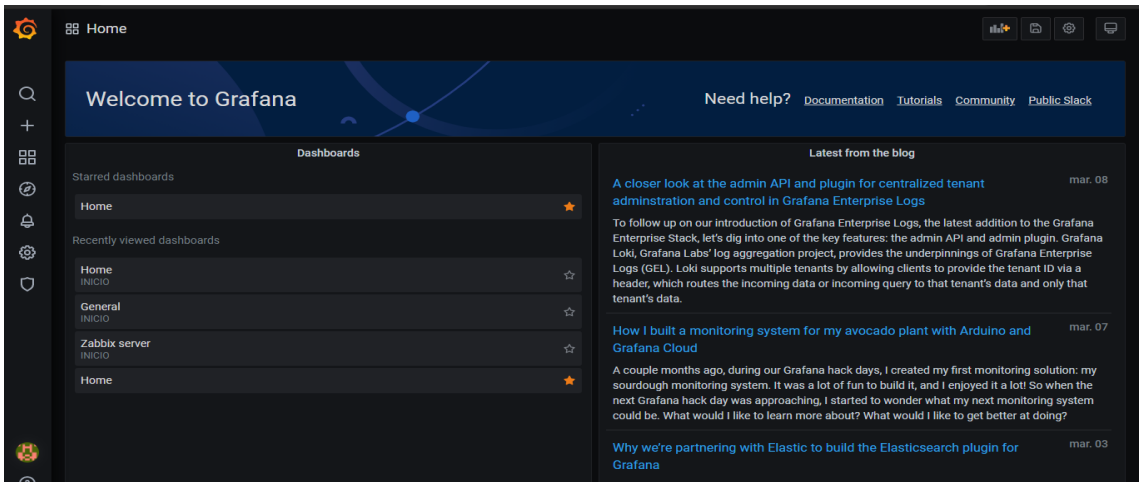


Figura 62. Vista General de Grafana

Instalación de un plugin de zabbix en grafana desde la terminal, este se encuentra en la documentación oficial de grafana.

```
#grafana-cli plugins install alexanderzobnin-Zabbix-app
```

Después restablecemos los servicios de grafana.

```
#systemctl restart grafana-server
```

Para integrar zabbix con grafana es necesario habilitar el plugin instalado, para la habilitación accedemos desde el frontend a el apartado de configuraciones de grafana en plugins.

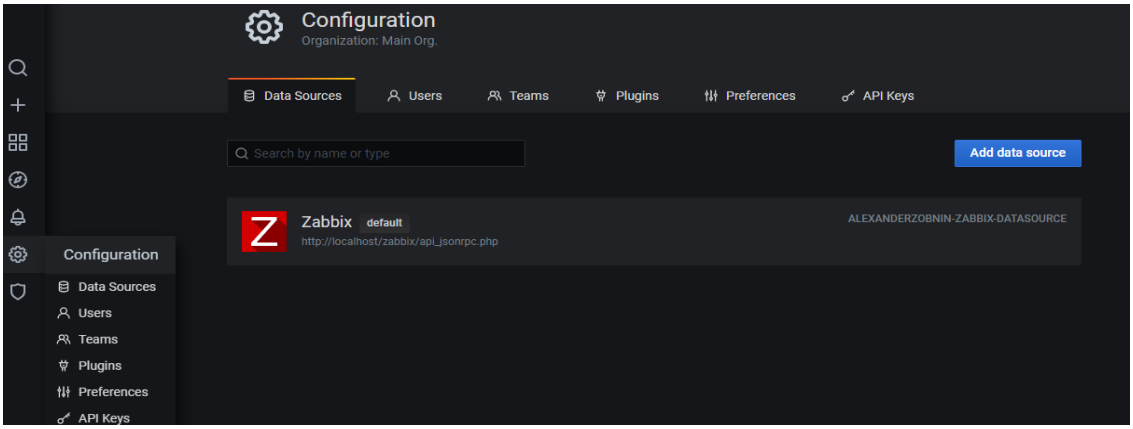


Figura 63. Configuración de Plugins

Habilitamos el plugin.

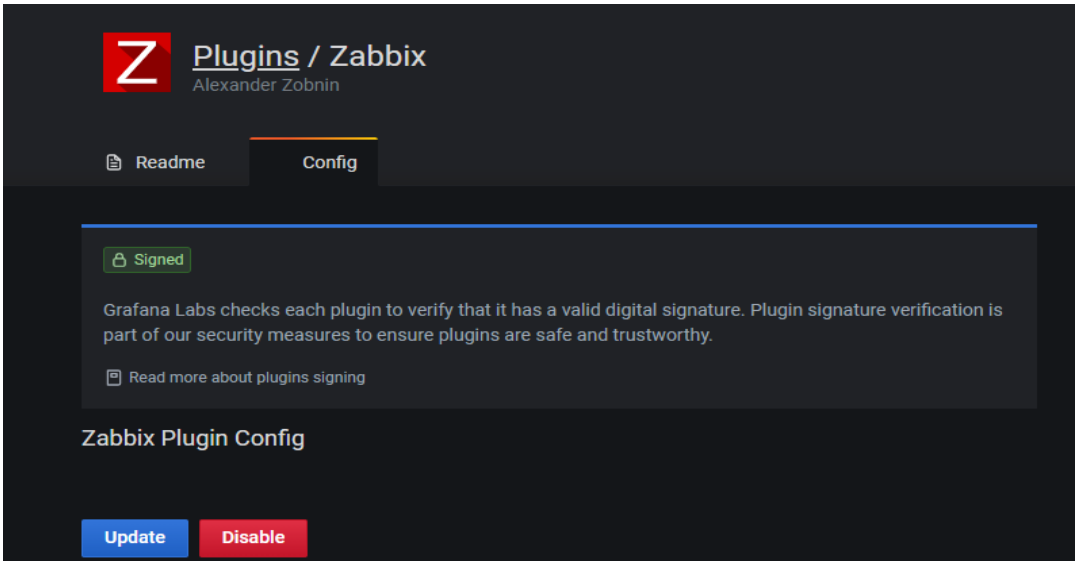


Figura 64. Habilitación de Plugins

Una vez habilitado el plugin de zabbix en grafana, procedemos a acceder a la data sources y agregar la conexión de zabbix con grafana.

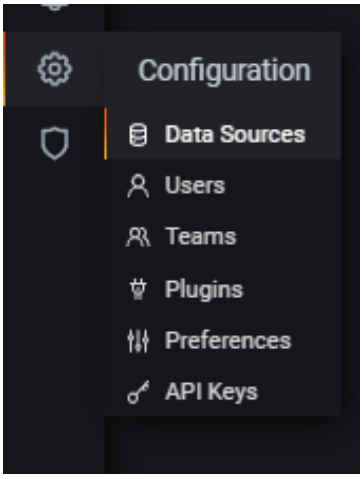


Figura 65. Data Source de Grafana

Configuración de conexión a zabbix.

- **Name:** Nombre por defecto.
- **URL**: Dirección del servidor zabbix.
- **Acces:** El medio por el cual se va a acceder.

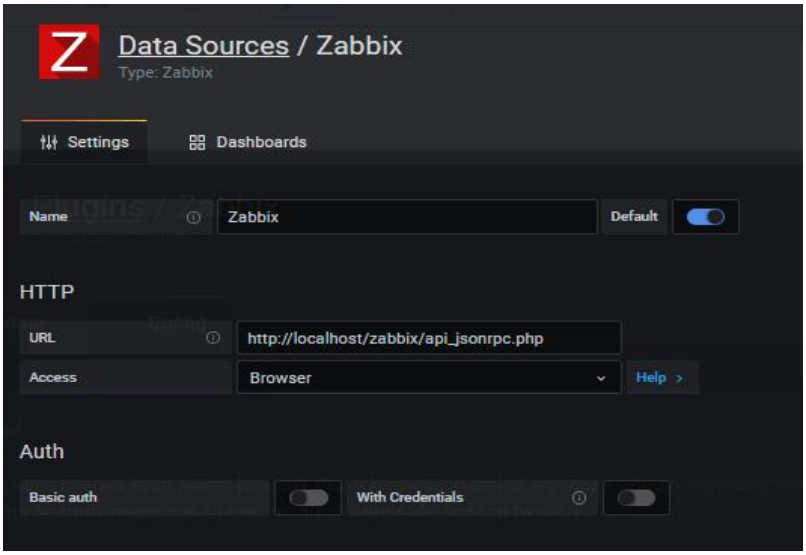


Figura 66. Conexión de Zabbix con Grafana

Credenciales de acceso a zabbix y guardamos la configuración.

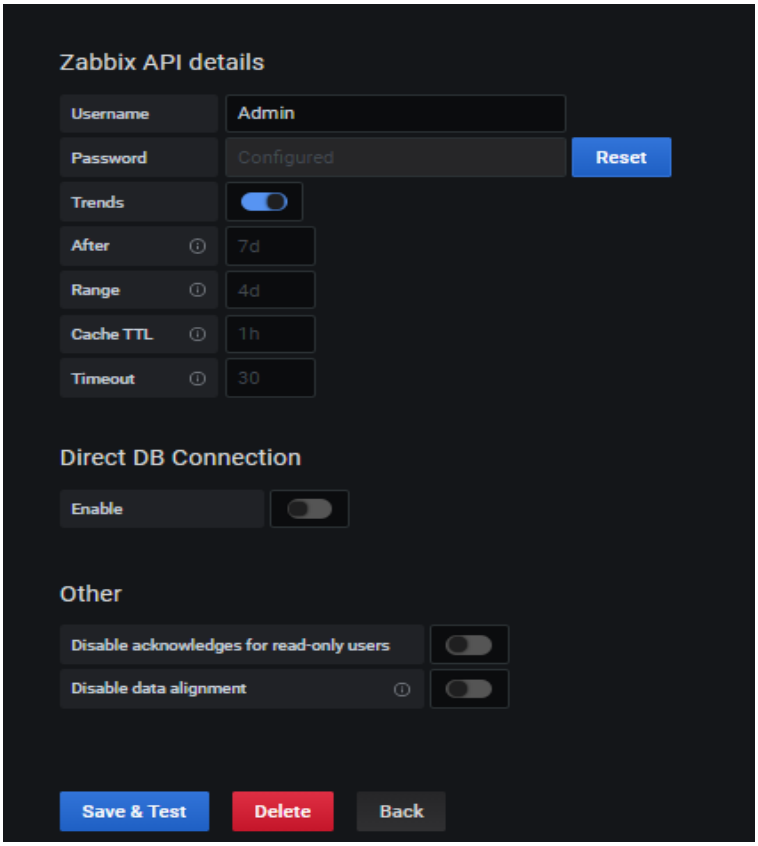


Figura 67. Credenciales de Zabbix de Acceso a Grafana

Importamos dashboards y finalizamos la configuración de grafana

Figura 68. Templates de Grafana

Se puede visualizar un dashboard preconfigurado de la información de los equipos registrados en el servidor zabbix, además de los problemas que presentan de cada dependencia de la institución, estas plantillas pueden ser personalizadas, dependiendo de las necesidades del departamento de TIC's.

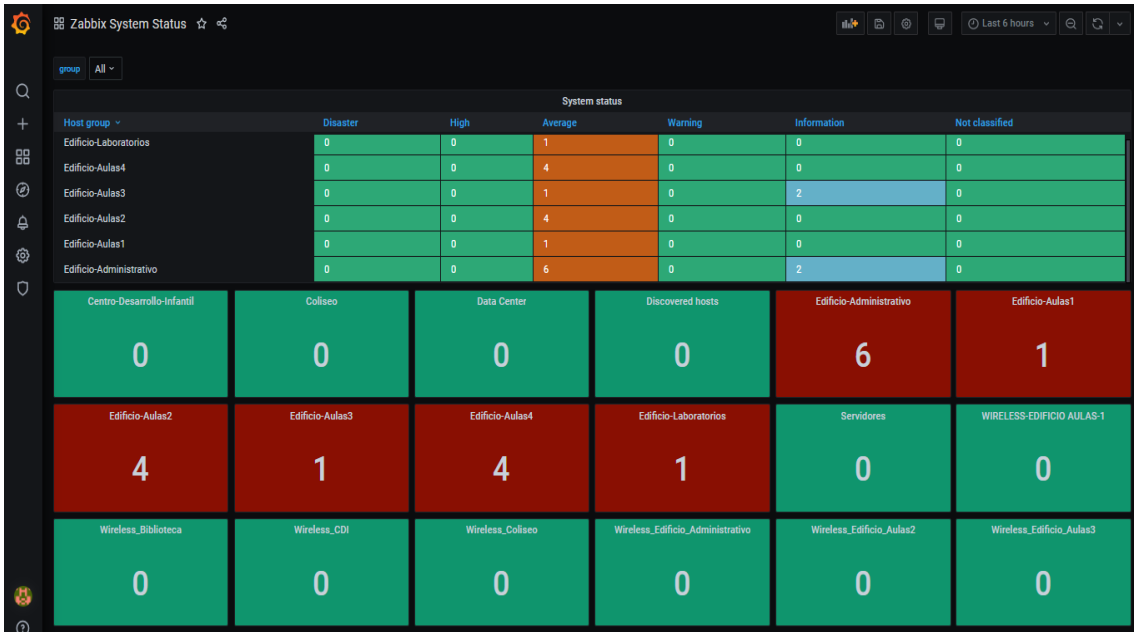


Figura 69. Vista general de un Template

Anexo 15. Instalar agente Zabbix en servidor Debian

Selección de instalación de zabbix-agent del repositorio de página oficial de zabbix.

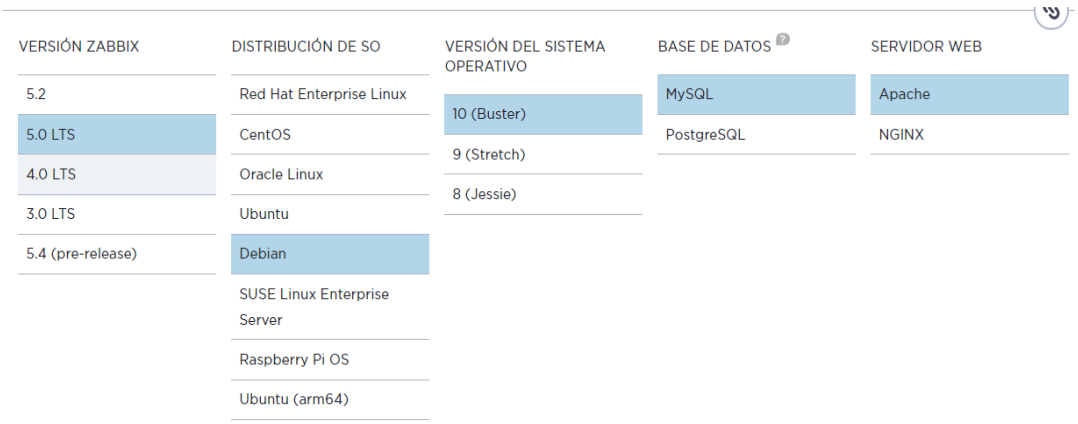


Figura 70. Instalación del Agente en Debian

Descargar repositorio de zabbix en su versión 5.0 para debian e instalar zabbix-agent.

```
#wgethttps://repo.Zabbix.com/Zabbix/5.0/debian/pool/main/z/Zabbix-release/Zabbix-release_5.0-1+buster_all.deb
# dpkg -i Zabbix-release_5.0-1+buster_all.deb
# apt update
# apt install Zabbix-agent
```

Configurar zabbix-agent.

```
# nano /etc/Zabbix/Zabbix_agentd.conf
Server=172.20.x.x
Listenport=10050
ServerActive=172.20.x.x
```

Iniciar y habilitar el zabbix-agent en el servidor.

```
# systemctl start Zabbix-agent
# systemctl enable Zabbix-agent
```

Habilitar puerto 10050/tcp en el firewall y reiniciamos el agente.

```
# sudo ufw allow 10050/tcp
# systemctl restart Zabbix-agent
```

Anexo 16. Instalar agente zabbix en servidor Oracle Linux

Selección de instalación de zabbix-agent del repositorio de página oficial de zabbix.

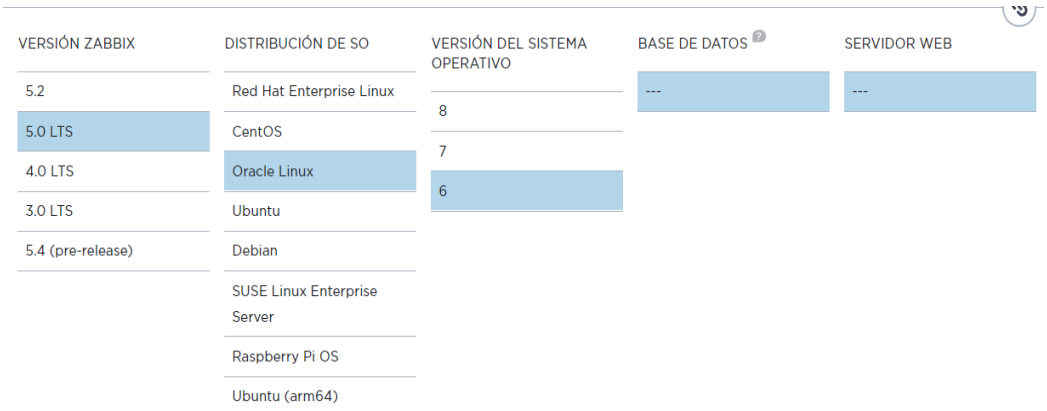


Figura 71. Instalación del Agente en Oracle Linux

Descargar repositorio de zabbix en su versión 5.0 para oracle e instalar el agente zabbix.

```
# rpm -Uvh https://repo.Zabbix.com/Zabbix/5.0/rhel/6/x86_64/Zabbix-release-5.0-1.el6.noarch.rpm
# yum clean all
# yum install Zabbix-agent
```

Configurar zabbix agent.

```
# nano /etc/Zabbix/Zabbix_agentd.conf
Server:172.20.x.x
Listenport:10050
ServerActive: 172.20.x.x
```

Iniciar y habilitar zabbix agent en el servidor.

```
# service Zabbix-agent start
# chkconfig --level 35 Zabbix-agent on
```

Habilitar puerto 10050/tcp en iptables y reiniciar el agente.

```
# iptables -A INPUT -i eth0 -p tcp --dport 10050 -m state --state NEW, ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -o eth0 -p tcp --sport 10050 -m state --state ESTABLISHED -j ACCEPT
# service Zabbix-agent restart
```

Anexo 17. Configuración de Correo Electronico.

Para el funcionamiento de las notificaciones es necesario instalar paquetes necesarios en el servidor zabbix para la entrega de correos.

```
# yum install ssmtp mailx
```

Editamos archivo de configuración del email.

```
# nano /etc/ssmtp/ssmtp.conf
## Editamos ##
root=Zabbixupec@gmail.com
mailhub=smtp.gmail.com:465
hostname= Zabbix
FromlineOverride=Yes
useTLS=Yes
## Insertar líneas de autentificación ##
AuthUser= Zabbixupec@gmail.com
AuthPass= xxxxxxxxx
```

Media type

Para configurar el tipo de notificación, procedemos a dirigirnos a el apartado de Administration/media types.

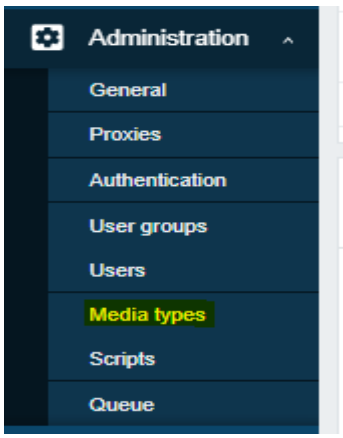


Figura 72. Administración Media Types

En el apartado de media types, se procede a crea uno nuevo, en la parte superior derecha hacemos click en create media type, en este se desplegará un formulario, los parámetros seleccionados con una marca roja son obligatorios y los demás los podemos dejar por defecto. Los siguientes parámetros para la configuración de correo electrónico son:

- **Name:** Nombre del medio a agregar.
- **Type:** El tipo de envió de notificaciones.
- **SMTP server:** Servidor de correo electrónico configurado.
- **SMTP server port:** Puerto de comunicación para los mensajes salientes.
- **SMTP helo:** Nombre de dominio.
- **SMTP email:** Dirección de envío de notificaciones de zabbix.
- **Authentication:** Nivel de autentificación.
- **Username:** Dirección de correo electrónico para autentificación.
- **Password:** Contraseña de correo electrónico para autentificación.

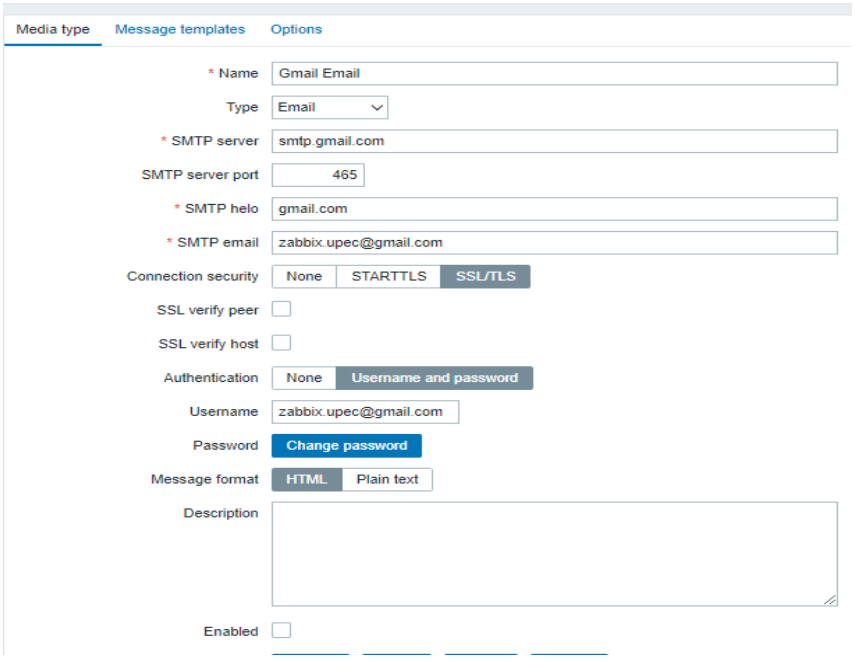


Figura 73. Creación de un Media Type

Una vez agregado el media type, procedemos ir a agregar el medio de notificación al usuario en el apartado Administration/Users. Posteriormente en el usuario accedemos a el apartado de media.

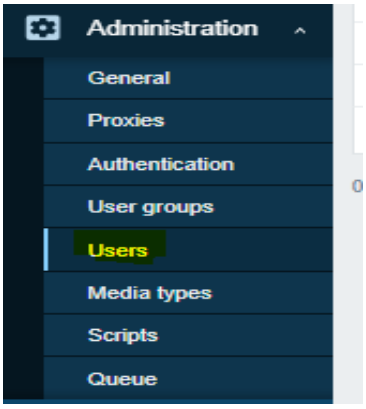


Figura 74. Usuarios

En el usuario administrador, en el apartado "Media" agregamos un nuevo tipo de notificación. A continuación, se describe los parámetros a tomar en cuenta:

- **Type:** Tipo de envío de notificación.
- **Send to**: Destinatario de la notificación de zabbix.
- **When active:** Periodo de activación de las notificaciones.
- **Use if severity:** Envío del grado de severidad del problema.

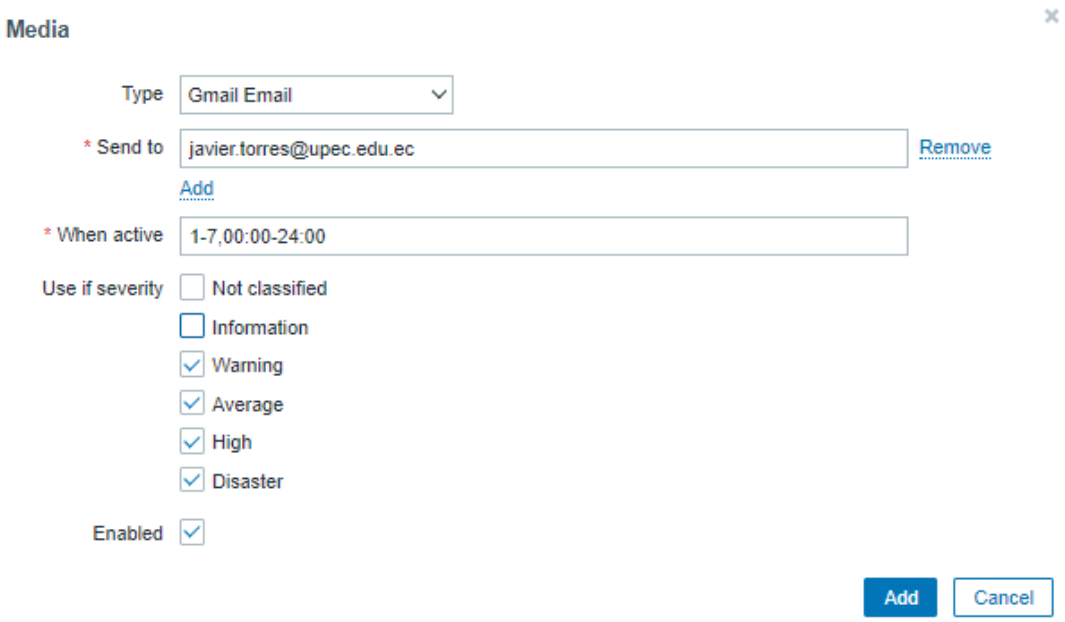


Figura 75. Asignación de un Media Type

Una vez agregado el tipo de notificación al usuario, se podrá apreciar los mediatypes que están asignados a ese usuario y se mostrará así:

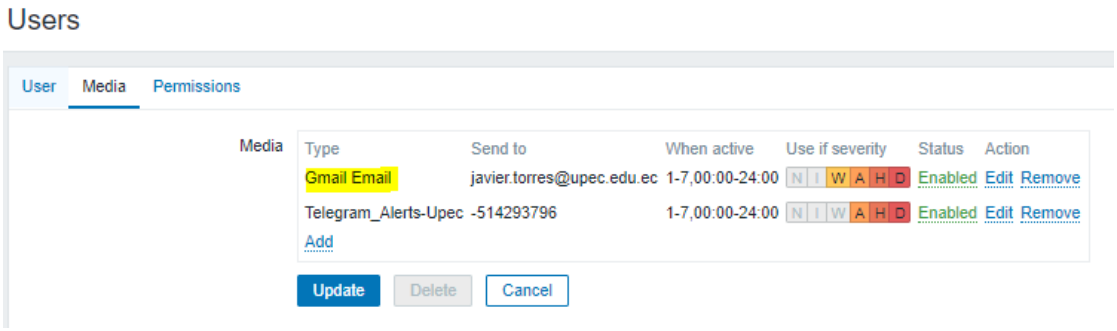


Figura 76. Media Types Configurados

Anexo 18. Resultados de la Encuesta

1 ¿Con que frecuencia hace usted uso de la red de datos inalámbrica (WiFi) de la institución?

Tabla 18. Resultados de la Pregunta 1

Opciones	Cantidad	Resultado
Diariamente	62	87,3%
Semanalmente	6	8,5%
mensualmente	2	2,8%
Nunca	1	1,4%
Total	**71**	**100%**

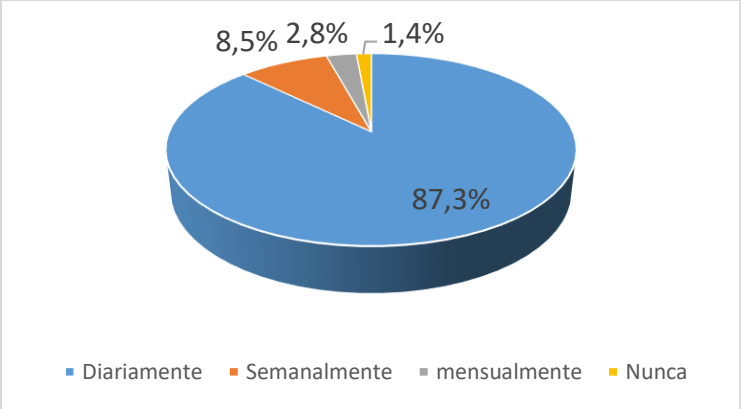


Figura 77. Resultados de la Pregunta 1

En la Tabla 19, se observa que un 87.3 % de los encuestados manifestaron que hacen uso frecuente de la red de datos inalámbrica wifi de la institución, mientras que un 1.4% menciona que no hace uso de la red wifi.

Por tanto, el uso de la red de datos wifi de la institución es de uso frecuente por lo que debe ser priorizada ante problemas que se susciten en la red.

2 ¿Con que frecuencia tiene usted problemas de conexión con la red de datos inalámbrica (WIFI) en la institución?

Tabla 19. Resultados de la Pregunta 2

Opciones	Cantidad	Resultado
Una vez por día	15	21,1%
Mas de una vez por día	38	53,5%
Una vez por semana	11	15,5%
Mas de una vez por semana	7	9,9%
Total	71	100%

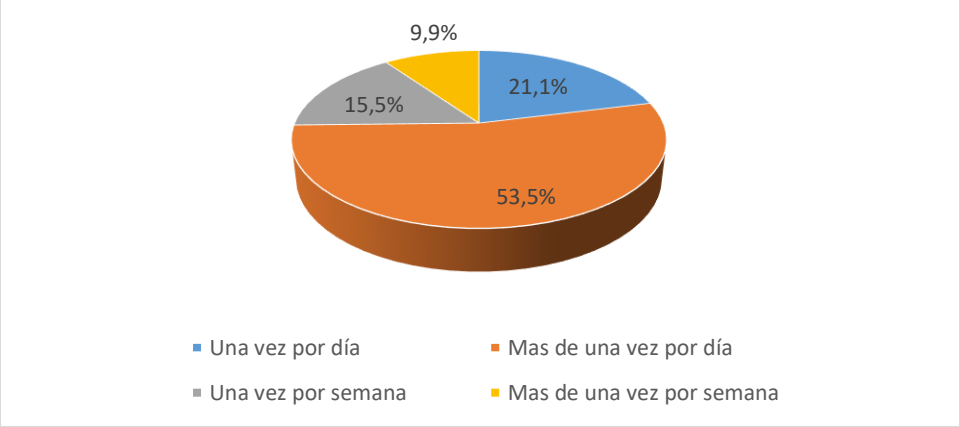


Figura 78. Resultados de la Pregunta 2

En la Tabla 20, la mayor parte de los encuestados un 53.5% manifiesta que los problemas son recurrentes y estos iban de más de una vez por día en lo que corresponde a la conexión de la red de datos inalámbrica (WIFI), y en un porcentaje de 21.1 % responden que sus problemas con la conexión se dan una vez por día, con esto se puede decir que la conexión es deficiente e intermitente la cual no satisface a los usuarios.

3 De acuerdo con su experiencia ¿En qué lugares del campus universitario tiene una mejor conectividad a la red inalámbrica (WIFI) de la institución?

Tabla 20. Resultados de la Pregunta 3

Opciones	**Cantidad**	**Resultado**
En el Aula	17	23.9%
Biblioteca Luciano Coral	33	46.5%
Edificio Central	42	59.2%
Áreas Verdes	2	2.8%
Coliseo Universitario 5 de abril	3	4.2%

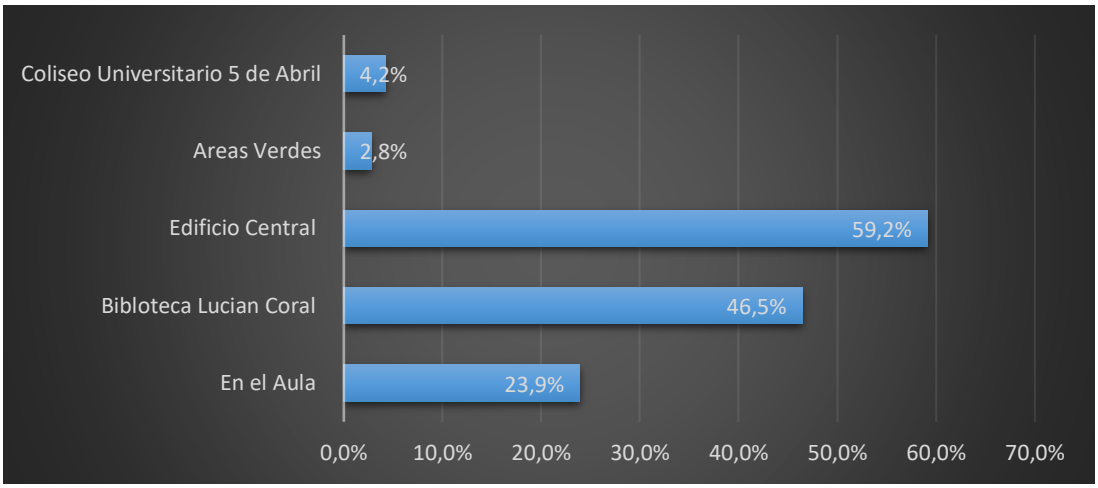


Figura 79. Resultados de la Pregunta 3

En la Tabla 21, el porcentaje de 59.2% han mencionado que la mejor conectividad a la red de datos se da en el edificio central, esto se debería a la poca afluencia de estudiantes y a que la mayoría de personal administrativo hace uso de la red por conexión cableada, en un 46.5% mencionan como segunda opción de mejor conectividad a la biblioteca Luciano coral, debiéndose a que es un lugar de estudio colectivo y en baja cantidad de 23.9% la conectividad es en el aula por lo cual se diría que al momento de las horas de clase no se tiene buena conectividad por lo cual se dificulta el aprendizaje o investigación.

4 ¿Qué servicios de red de la institución accede con más frecuencia para el desarrollo de actividades académicas?

Tabla 21. Resultados de la Pregunta 4

Opciones	**Cantidad**	**Resultado**
Aulas Virtuales	62	87,3%
Correo Electrónico	17	23.9%
Página Web	21	29.6%
Carga y Descarga de Archivos	32	45.1%

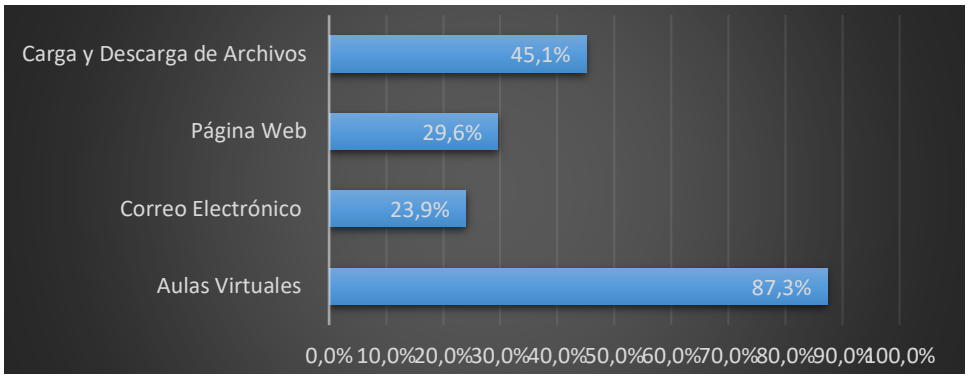


Figura 80. Resultados de la Pregunta 4

En la Tabla 22, debido a que es una pregunta que puede ser contestada con más de un literal se interpreta de la siguiente manera, en un 87.3% de los encuestados hacen uso a diario de las aulas virtuales para sus actividades académicas y como se debería identificar en el proceso se incluye la carga y descarga de archivos el cual tiene un porcentaje de 45.1%, esto concuerda con el uso y manejo de las aulas virtuales con la subida de deberes o trabajos.

5 ¿Ha experimentado usted problemas con las plataformas (Aulas virtuales, Portafolio académico, Correo electrónico, Pagina Web) institucional?

Tabla 22. Resultados de la Pregunta 5

Opciones	**Cantidad**	**Resultado**
Siempre	6	8.5%
Regularmente	32	45.1%
Ocasionalmente	31	43.7%
Nunca	2	2.8%
Total	**71**	**100%**

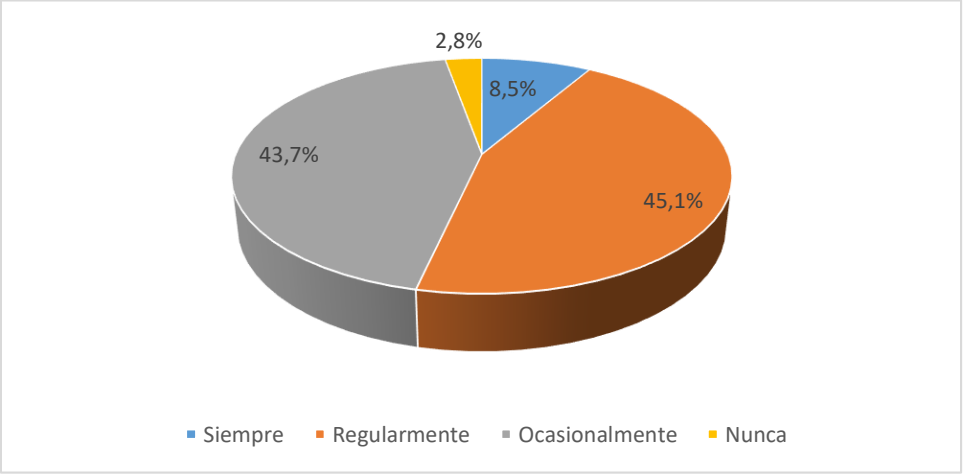


Figura 81. Resultados de la Pregunta 5

En la Tabla 23, Se puede observar que un 45.1 % del total presenta regularmente problemas con plataformas (Aulas Virtuales, Portafolio Académico, correo electrónico, página web) de la institución, seguido de un 43.7% de los encuestados afirmando que ocasionalmente han sufrido de problemas con las plataformas virtuales. Por lo que se puede apreciar existe un porcentaje alto de usuarios que presentan problemas con plataformas virtuales de la institución, evidenciando que los problemas de las plataformas virtuales son recurrentes.

6 ¿Cuáles han sido los problemas más comunes al utilizar las plataformas (Aulas virtuales, Portafolio académico, Correo electrónico, Pagina Web) de la institución?

Tabla 23. Resultados de la Pregunta 6

Opciones	**Cantidad**	**Resultado**
Restricciones Ingreso	13	18.3%
Demora del Servicio	53	74.6%
Indisponibilidad del Servicio	28	39.4%
Ninguno	2	2.8%

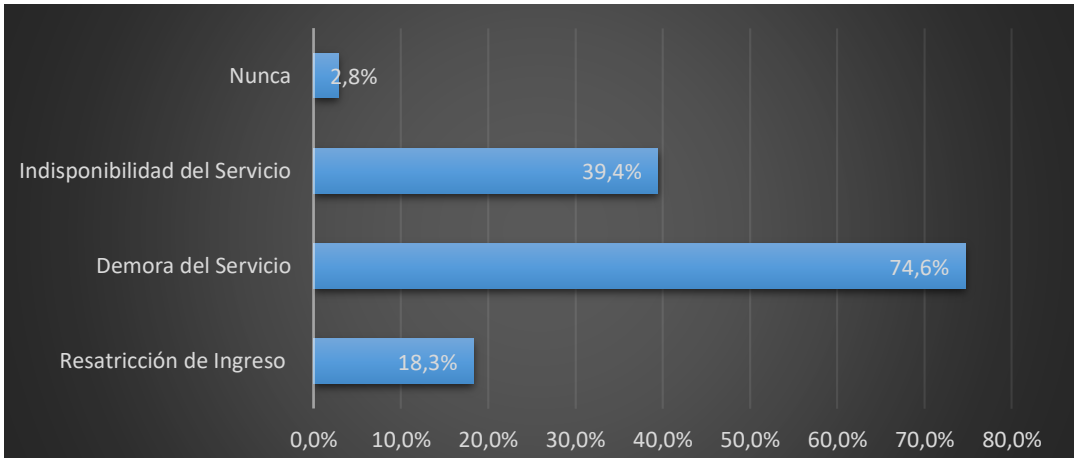


Figura 82. Resultados de la Pregunta 6

En la Tabla 24, siendo esta una pregunta que puede ser contestada con más de un literal, muestra que los encuestados han tenido varios problemas con las plataformas que ofrece la UPEC siendo así que en un 74.6% el problema más frecuente es la demora en el servicio y por otro lado está la indisponibilidad del servicio constatándose en un 39.4%

de problemas al ingresar a los diferentes servicios que no ofrecen, determinándose que por la demora de servicios muchas veces no se puede aprovechar todo el potencial que las plataformas brindan.

7 ¿Conoce usted cuales son las Políticas de uso de servicios de red que se encuentran vigentes en la institución?

Tabla 24. Resultados de la Pregunta 7

Opciones	Cantidad	Resultado
Si	50	70.4%
No	21	29.6%
Total	**71**	**100%**

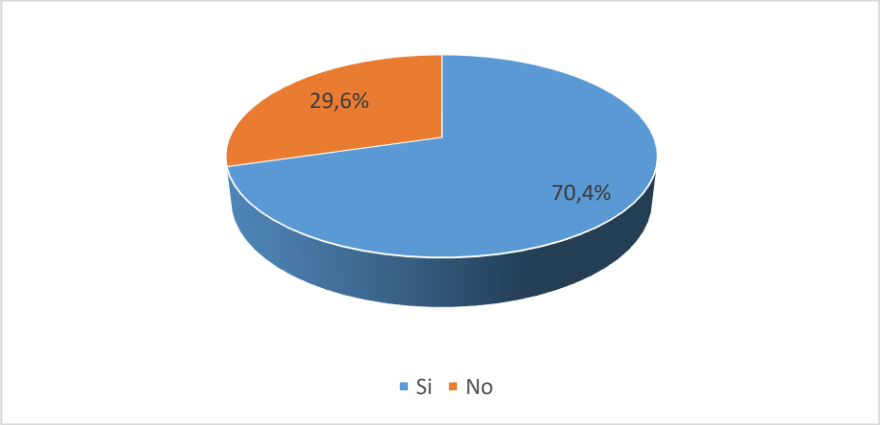


Figura 83. Resultados de la Pregunta 7

En la Tabla 25, Se observa que un 70.4% de los encuestados no conocen acerca de las políticas de uso de la red de datos de la institución, mientras que un 29.6% si las conocen.

Por lo que es necesario socializar las políticas de uso de la red de datos a la comunidad universitaria indicando sobre el uso adecuado del consumo del ancho de banda permitiendo garantizar la disponibilidad de la red de datos.

8 ¿Cree usted que el cumplimiento de las políticas de uso de servicios de red en la institución debe cumplirse para asegurar la calidad de los servicios de red y mantengan sus datos seguros?

Tabla 25. Resultados de la Pregunta 8

Opciones	Cantidad	Resultados
Siempre	59	83.1%
A veces	11	15.5%
Nunca	1	1.4%
Total	**71**	**100%**

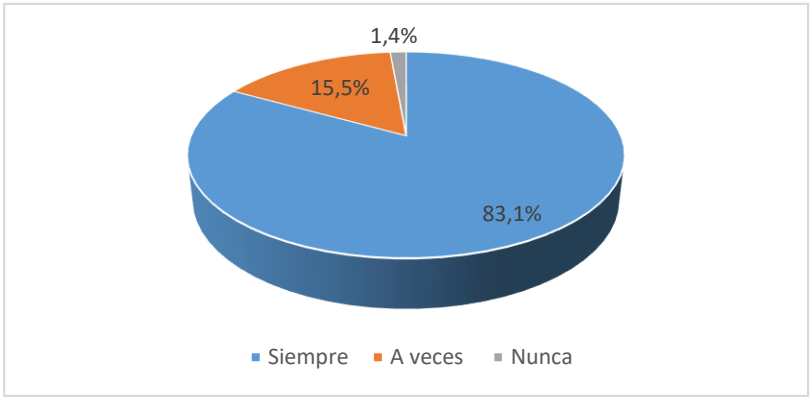


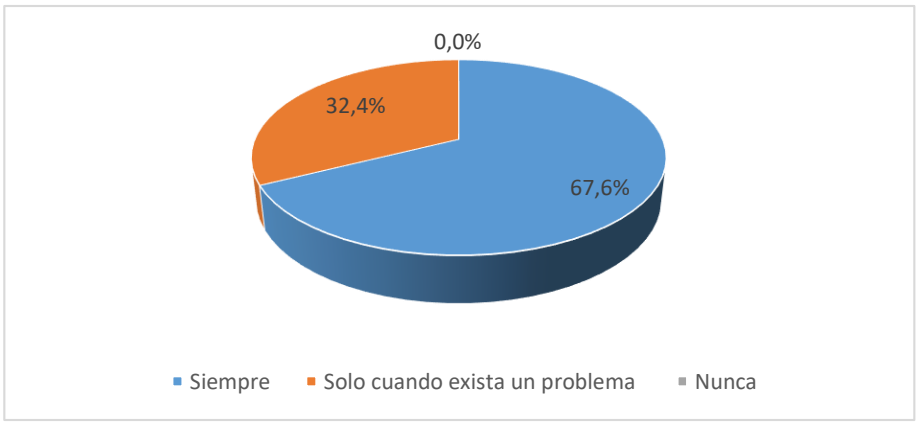
Figura 84. Resultados de la Pregunta 8

En la Tabla 26, Se pude observar que un 83.1% de los encuestados creen que es necesarios aplicar el cumplimiento de las políticas de uso de la red de datos de la institución y este repercuta en la calidad del servicio, mientras que un 15.5% manifiesta que al aplicar políticas de uso de la red de datos no provocaría una mejora en la calidad del servicio.

9 ¿Cree usted necesario que el departamento de TIC's monitoree el uso de los servicios de red para hacer cumplir las políticas y así mantener la calidad de los servicios?

Tabla 26. Resultados de la Pregunta 9

Opciones	Cantidad	Resultado



Siempre	48	67.6%
Solo cuando existan problemas	23	32.4%
Nunca	0	0%
Total	**71**	**100%**

Figura 85. Resultados de la Pregunta 9

En la Tabla 27, Se puede observar que un 67.6% de los encuestados indican que es necesario que el departamento de TIC's monitoree la red de datos aplicando el uso de las políticas de acceso a la red de datos de la institución para mantener una red operativa de calidad, mientras que un 32.4% manifiesta que se monitoreo siempre y cuando existan problemas que degraden el servicio de la red de datos de la institución. Por tanto, es necesario una herramienta especializada en la monitorización de la red que permita gestionar de mejor manera los recursos de la red de datos de la institución, garantizando siempre los servicios que esta provea.

10 ¿Indique el nivel de funcionalidad de la Pagina Web de la institución?

Tabla 27. Resultados de la Pregunta 10

Opciones	**Cantidad**	**Resultado**
Muy Bueno	1	1.4%
Bueno	48	67.6%
Regular	20	28.2%
Deficiente	2	2.8%
Total	**71**	**100%**

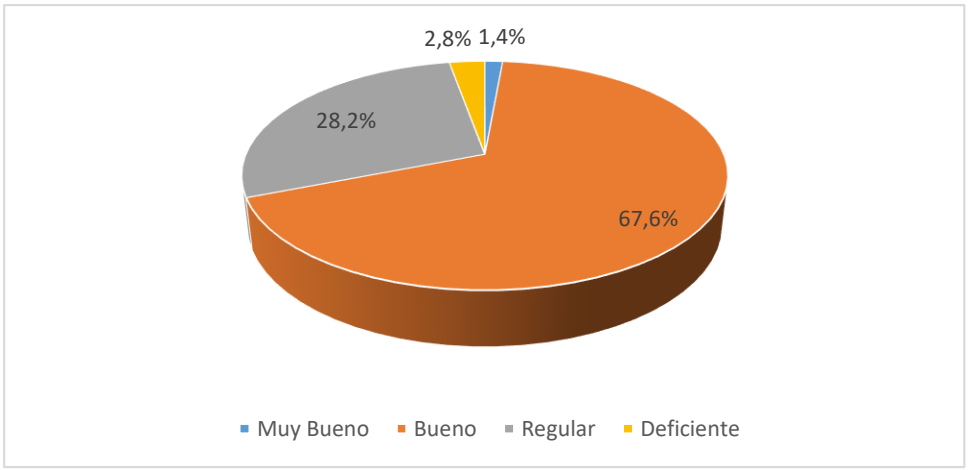


Figura 86. Resultados de la Pregunta 10

En la Tabla 28, Se observa que un 67.6% de los encuestados indican que el nivel de funcionalidad de la página web institucional es buena, seguido de un 28.2 % el cual mencionan que el nivel de funcionalidad es regular. Dejando un 1.4% del total de que el nivel de funcionalidad es muy bueno.

11 ¿Indique el nivel de funcionalidad del servicio de correo electrónico de la institución?

Tabla 28. Resultados de la Pregunta 11

Opciones	Cantidad	Resultado
Muy Bueno	9	12.7%
Bueno	44	62%
Regular	18	25.4%
Deficiente	0	0%
Total	**71**	**100%**

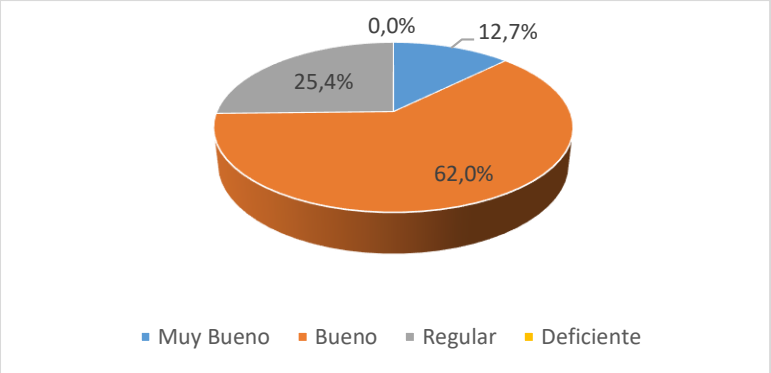


Figura 87. Resultados de la Pregunta 11

En la Tabla 29, se constata que del número de encuestados los cuales hacen uso del correo electrónico institucional el 62% lo evalúa como bueno manifestando así que es de uso consecutivo y forma parte de sus recursos, en un 25.4% de encuestados lo evalúan como regular corroborando que muy pocas veces lo utilizan y en un 12.7% los estudiantes lo catalogan como muy bueno confirmando que forma parte de su diario aprendizaje.

12 ¿Indique el nivel de funcionalidad del servicio de Aulas virtuales?

Tabla 29. Resultados de la Pregunta 12

Opciones	Cantidad	Resultado
Muy Bueno	4	5.6%
Bueno	47	66.2%

Regular	18	25.4%
Deficiente	2	2.8%
Total	**71**	**100%**

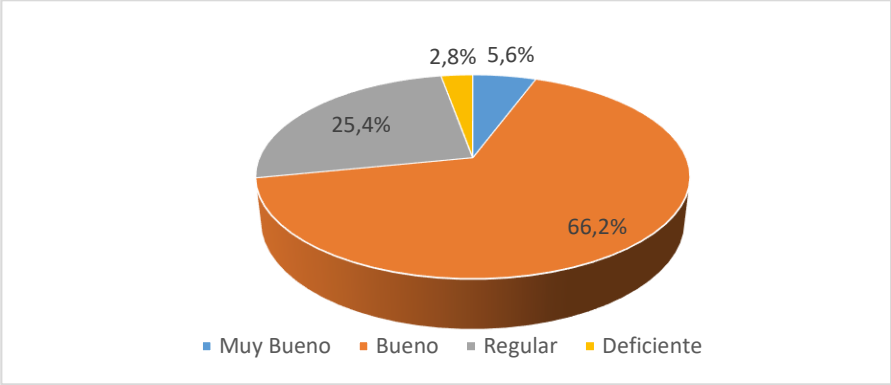


Figura 88. Resultados de la Pregunta 12

En la Tabla 30, se puede constatar que del número de encuestados un 66.2% de ellos afirman que la funcionalidad del aula virtual es buena corroborando que hacen uso diario de ella, un 25.4% de los encuestados contrastan que el aula virtual es regular y que no cumple con todas las expectativas, y un bajo porcentaje del 5.6% dicen que es muy buena y cumple con todas las expectativas dándose así que la funcionalidad no está al máximo de lo esperado.

Anexo 19. Switching

Ubicación	Por planta	Cantidad	Tipo	IP	Switch
Edificio Administrativo	Subsuelo	1	WS-C2960S-48TD-L	172.xx.1.11	SW_EA_SU_01
	Planta Baja	2	WS-C2960G-48TC-L	172.xx.1.12	SW_EA_SU_02
				172.xx.1.13	SW_EA_PB_01
	Primer Piso	2	WS-C2960G-24TC-L	172.xx.1.14	SW_EA_PP_01
	Segundo Piso			172.xx.1.15	SW_EA_SP_01
Edificio de Aulas 1	Planta Baja	2	WS-C2960G-48TC-L	172.xx.1.20	SW_EA1_PB_01
				172.xx.1.21	SW_EA1_PB_02
	Primer Piso	2	WS-C2960G-24TC-L	172.xx.1.22	SW_EA1_PP_01
	Segundo Piso			172.xx.1.23	SW_EA1_SP_01
Edificio de Aulas 2	Planta Baja	1	WS-C3560E-12SD	172.xx.1.30	SW_EA2_PB_01
		2	WS-C2960S-48TS-L	172.xx.1.31	SW_EA2_PB_02
				172.xx.1.32	SW_EA2_PB_03
		1	WS-C2960G-48TC-L	172.xx.1.33	SW_EA2_PB_04
		1	WS-C2960S-48TS-L	172.xx.1.34	SW_EA2_PB_05
	Primer Piso	1	WS-C2960S-48TD-L	172.xx.1.35	SW_EA2_PP_01
	Segundo Piso	1	WS-C2960G-48TC-L	172.xx.1.36	SW_EA2_SP_01
		1	WS-C2960X-24TS-LL	172.xx.1.37	SW_EA2_SP_02
COLISEO	Sector Administrativo	1	WS-C2960G-24TC-L	172.xx.1.41	SW_COL_01
LABORATORIOS	Planta Baja	1	WS-C2960X-24TS-LL	172.xx.1.51	SW_EL_PB_01
Edificio de Aulas 4	Planta Baja	8	WS-C2960X-24TS-LL	172.xx.1.52	SW_EA4_PB_01
				172.xx.1.53	SW_EA4_PB_02
				172.xx.1.54	SW_EA4_PB_03
				172.xx.1.55	SW_EA4_PB_04
				172.xx.1.56	SW_EA4_PB_05
				172.xx.1.57	SW_EA4_PB_06
				172.xx.1.58	SW_EA4_PB_07
				172.xx.1.59	SW_EA4_PB_08
	Primer Piso	1	WS-C2960X-24TS-L	172.xx.1.60	SW_EA4_PP_01

				172.xx.1.62	SW_EA4_PP_02
				172.xx.1.63	SW_EA4_PP_03
		5	WS-C2960X-24TS-LL	172.xx.1.64	SW_EA4_SP_01
	Segundo Piso			172.xx.1.65	SW_EA4_SP_02
				172.xx.1.66	SW_EA4_SP_03
Centro de Desarrollo Infantil	CDI	1	WS-C2960S-24TS-S	172.xx.1.61	SW_CDI_01
				172.xx.1.70	SW_EA3_PB_01
		4	WS-C2960S-24TS-LL	172.xx.1.71	SW_EA3_PB_02
				172.xx.1.72	SW_EA3_PB_03
	Planta Baja			172.xx.1.73	SW_EA3_PB_04
		1		172.xx.1.74	SW_EA3_PB_05
				172.xx.1.75	SW_EA3_PB_06
		3	WS-C2960S-24TS-LL	172.xx.1.76	SW_EA3_PB_07
Edificio de Aulas 3				172.xx.1.77	SW_EA3_PB_08
		1	WS-C2960S-24TS-L	172.xx.1.78	SW_EA3_PP_01
	Primer Piso			172.xx.1.79	SW_EA3_PP_02
				172.xx.1.80	SW_EA3_PP_03
		5	WS-C2960S-24TS-LL	172.xx.1.81	SW_EA3_SP_01
	Segundo Piso			172.xx.1.82	SW_EA3_SP_02
				172.xx.1.83	SW_EA3_SP_03

Anexo 20. Ap

UBICACIÓN	POR PLANTA	CANTIDAD	TIPO	IP	Access Point
Edificio Aulas 1	Planta baja	5	AIR-CAP2702E-A-K9	17x.xx.2.11	EA1-PB-AP01
			AIR-CAP2702E-A-K9	17x.xx.2.12	EA1-PB-AP02
			AIR-CAP2702E-A-K9	17x.xx.2.13	EA1-PB-AP03
			AIR-CAP2702E-A-K9	17x.xx.2.14	EA1-PB-AP04
			AIR-CAP2702E-A-K9	17x.xx.2.15	EA1-PB-AP05
	Primer piso	5	AIR-CAP2702E-A-K9	17x.xx.2.16	EA1-PA1-AP01
			AIR-CAP2702E-A-K9	17x.xx.2.17	EA1-PA1-AP02
			AIR-CAP2702E-A-K9	17x.xx.2.18	EA1-PA1-AP03
			AIR-CAP2702E-A-K9	17x.xx.2.19	EA1-PA1-AP04
			AIR-CAP2702E-A-K9	17x.xx.2.20	EA1-PA1-AP05
	Segundo piso	5	AIR-CAP2702E-A-K9	17x.xx.2.21	EA1-PA2-AP01
			AIR-CAP2702E-A-K9	17x.xx.2.22	EA1-PA2-AP02
			AIR-CAP2702E-A-K9	17x.xx.2.23	EA1-PA2-AP03
			AIR-CAP2702E-A-K9	17x.xx.2.24	EA1-PA2-AP04
			AIR-CAP2702E-A-K9	17x.xx.2.25	EA1-PA2-AP05
Edificio Aulas 2	Planta baja	5	AIR-LAP1262N-A-K9	17x.xx.2.31	EA2-PB-AP01
			AIR-LAP1262N-A-K9	17x.xx.2.32	EA2-PB-AP02
			AIR-LAP1262N-A-K9	17x.xx.2.33	EA2-PB-AP03

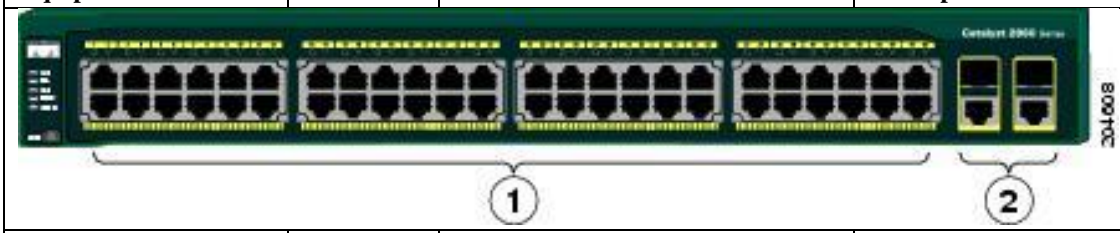
			AIR-LAP1262N-A-K9	17x.xx.2.34	EA2-PB-AP04
			AIR-LAP1262N-A-K9	17x.xx.2.35	EA2-PB-AP05
			AIR-LAP1262N-A-K9	17x.xx.2.36	EA2-PA1-AP01
			AIR-LAP1262N-A-K9	17x.xx.2.37	EA2-PA1-AP02
	Primer piso	5	AIR-LAP1262N-A-K9	17x.xx.2.38	EA2-PA1-AP03
			AIR-LAP1262N-A-K9	17x.xx.2.39	EA2-PA1-AP04
			AIR-LAP1262N-A-K9	17x.xx.2.40	EA2-PA1-AP05
			AIR-LAP1262N-A-K9	17x.xx.2.41	EA2-PA2-AP01
			AIR-LAP1262N-A-K9	17x.xx.2.42	EA2-PA2-AP02
	Segundo piso	5	AIR-LAP1262N-A-K9	17x.xx.2.43	EA2-PA2-AP03
			AIR-LAP1262N-A-K9	17x.xx.2.44	EA2-PA2-AP04
			AIR-LAP1262N-A-K9	17x.xx.2.45	EA2-PA2-AP05
			AIR-CAP2702E-A-K9	17x.xx.2.51	EA3-PB-AP01
			AIR-CAP2702E-A-K9	17x.xx.2.52	EA3-PB-AP02
	Planta baja	5	AIR-CAP2702E-A-K9	17x.xx.2.53	EA3-PB-AP03
Edificio Aulas 3			AIR-CAP2702E-A-K9	17x.xx.2.54	EA3-PB-AP04
			AIR-CAP2702E-A-K9	17x.xx.2.55	EA3-PB-AP05
			AIR-CAP2702E-A-K9	17x.xx.2.56	EA3-PA1-AP01
	Primer piso	5	AIR-CAP2702E-A-K9	17x.xx.2.57	EA3-PA1-AP02

			AIR-CAP2702E-A-K9	17x.xx.2.58	EA3-PA1-AP03
			AIR-CAP2702E-A-K9	17x.xx.2.59	EA3-PA1-AP04
			AIR-CAP2702E-A-K9	17x.xx.2.60	EA3-PA1-AP05
			AIR-CAP2702E-A-K9	17x.xx.2.61	EA3-PA2-AP01
			AIR-CAP2702E-A-K9	17x.xx.2.62	EA3-PA2-AP02
	Segundo piso	5	AIR-CAP2702E-A-K9	17x.xx.2.63	EA3-PA2-AP03
			AIR-CAP2702E-A-K9	17x.xx.2.64	EA3-PA2-AP04
			AIR-CAP2702E-A-K9	17x.xx.2.65	EA3-PA2-AP05
			AIR-CAP2702E-A-K9	17x.xx.2.71	EA4-PB-AP01
			AIR-CAP2702E-A-K9	17x.xx.2.72	EA4-PB-AP02
	Planta baja	5	AIR-CAP2702E-A-K9	17x.xx.2.73	EA4-PB-AP03
			AIR-CAP2702E-A-K9	17x.xx.2.74	EA4-PB-AP04
			AIR-CAP2702E-A-K9	17x.xx.2.75	EA4-PB-AP05
Edificio Aulas 4			AIR-CAP2702E-A-K9	17x.xx.2.76	EA4-PA1-AP01
			AIR-CAP2702E-A-K9	17x.xx.2.77	EA4-PA1-AP02
	Primer piso	5	AIR-CAP2702E-A-K9	17x.xx.2.78	EA4-PA1-AP03
			AIR-CAP2702E-A-K9	17x.xx.2.79	EA4-PA1-AP04
			AIR-CAP2702E-A-K9	17x.xx.2.80	EA4-PA1-AP05
	Segundo piso	5	AIR-CAP2702E-A-K9	17x.xx.2.81	EA4-PA2-AP01

			AIR-CAP2702E-A-K9	17x.xx.2.82	EA4-PA2-AP02
			AIR-CAP2702E-A-K9	17x.xx.2.83	EA4-PA2-AP03
			AIR-CAP2702E-A-K9	17x.xx.2.84	EA4-PA2-AP04
			AIR-CAP2702E-A-K9	17x.xx.2.85	EA4-PA2-AP05
	Planta baja	2	AIR-CAP2702E-H-K9	17x.xx.2.91	EL-PB-AP01
			AIR-CAP2702E-H-K9	17x.xx.2.92	EL-PB-AP02
Edificio Laboratorios	Primer piso	2	AIR-CAP2702E-H-K9	17x.xx.2.93	EL-PA1-AP01
			AIR-CAP2702E-H-K9	17x.xx.2.94	EL-PA1-AP02
	Segundo piso	2	AIR-CAP2702E-H-K9	17x.xx.2.95	EL-PA2-AP01
			AIR-CAP2702E-H-K9	17x.xx.2.96	EL-PA2-AP02
	Subsuelo	1	AIR-CAP2702E-A-K9	17x.xx.2.101	EA-SS-AP01
	Planta baja	3	AIR-CAP1602I-A-K9	17x.xx.2.102	EA-PB-AP01
			AIR-AP1041N-A-K9	17x.xx.2.103	EA-PB-AP02
			AIR-AP1041N-A-K9	17x.xx.2.104	EA-PB-AP03
	Primer piso	3		17x.xx.2.105	EA-PA1-AP01
				17x.xx.2.106	EA-PA1-AP02
				17x.xx.2.107	EA-PA1-AP03
Edificio Administrativo	Segundo piso	3	AIR-CAP2702E-E-K9	17x.xx.2.108	EA-PA2-AP01
			AIR-CAP2702E-E-K9	17x.xx.2.109	EA-PA2-AP02
			AIR-CAP2702E-E-K9	17x.xx.2.110	EA-PA2-AP03
	Tercer piso	2	AIR-LAP1131AG-A-K9	17x.xx.2.111	EA-PA3-AP01
				17x.xx.2.112	EA-PA3-AP02
Biblioteca	Planta baja	2	AIR-CAP2702E-A-K9	17x.xx.2.121	B-PB-AP01

	Primer piso	2	AIR-CAP2702E-A-K9	17x.xx.2.122	B-PB-AP02
			AIR-CAP2702E-A-K9	17x.xx.2.123	B-PA-AP01
			AIR-CAP2702E-A-K9	17x.xx.2.124	B-PA-AP02
Coliseo	Planta baja	5	AIR-LAP1041N-A-K9	17x.xx.2.131	C-CD-AP01
			AIR-LAP1041N-A-K9	17x.xx.2.132	C-CD-AP02
			AIR-LAP1141N-A-K9	17x.xx.2.133	C-CD-AP03
			AIR-CAP1602I-A-K9	17x.xx.2.134	C-CD-AP04
			AIR-CAP2702E-H-K9	17x.xx.2.135	C-PA-AP01
CDI	Planta baja	1	AIR-LAP1262N-A-K9	17x.xx.2.141	CDI-AP01

Anexo 21. Características técnicas switches

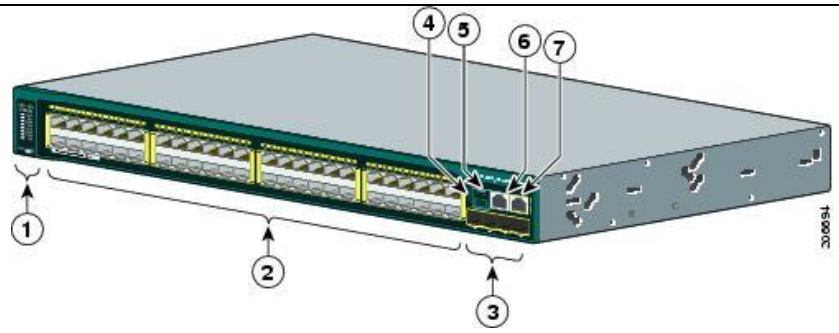
Equipo	Cantidad	Característica	Descripción
			
• Switch Cisco Catalys WS-C2960G-48TC-L	6	48 Ethernet 10/100 puertos	El Catalyst 2960 ofrece seguridad integrada, incluyendo el control de admisión de red (NAC), la calidad de servicio avanzada (QoS), y la resistencia para entregar servicios inteligentes para el borde de la red.
		2 enlaces ascendentes de doble propósito (cada puerto de enlace, doble propósito)	
		1 puerto activo)	
		1 puerto 10/100/1000 Ethernet y un puerto Gigabit Ethernet basado en SFP 1	
		1 RU de configuración fija Imagen de base LAN	

Equipo	Características	Descripción
		
Cisco Catalys 4506-E Switch de CORE	Contenido: FACTORY DIRECT ONLY - Catalyst 4500 E-Series Bundles - 4506-E Chassis, two WS-X4648-RJ45V+E, Sup7L-E, LAN Base	Series Switches permitir a las redes sin fronteras, proporcionando un alto rendimiento, móviles y experiencias de usuario seguras a través de inversiones de capa 2-4 de

	Fabricante ID pieza: WS-C4506E-S7L+96V+	conmutación. Permiten seguridad, movilidad, rendimiento de aplicaciones, video y ahorro de energía en una infraestructura que admite resiliencia, virtualización y automatización. Brindan rendimiento, escalabilidad y servicios sin fronteras con un costo total de propiedad (TCO) reducido y una protección superior de la inversión.
	SKU: DHWSC4506ES7LP96V UPC: 882658479410	
	Fabricante: Cisco	
	Categoría: Networking	

Equipo	**Cantidad**	**Característica**	**Descripción**
			
Switch Cisco Catalys WS-C2960G-24TC-L	5	• 2x1GE uplink. • 8, 24, y 48 puertos de configuraciones Fast Ethernet • Advanced QoS, limitante de la velocidad, listas de control de acceso (ACL), la gestión de IPv6 y servicios de multidifusión. • PoE completo con un máximo de 15,4 W por puerto para un máximo de 48 puertos.	Fácil de usar y de actualizar, estos switches de acceso de configuración Fast Ethernet fijos ofrecen capa superior de 2 capacidades de defensa de amenazas y Capa 3 enrutamiento estático básico con 16 rutas.

Equipo	**Cantidad**	**Características**	**Descripción**

			
Switch Cisco Catalys 2960 WS-C2960S-48TS-L	3	• Mode button and switch LEDs • 10/100/1000 ports • SFP+module-slots • USB Type A port • USB mini-Type B (console) port • 48 Ethernet 10/100/1000 puertos • RJ-45 console port • Ethernet management port • FlexStack Cisco Opcional apilamiento apoyo • 2 puertos SFP 1 Gigabit Ethernet de uplink ports • Imagen de base LAN	Implementación de la conectividad por cable rentable en entornos tradicionales de escritorio del área de trabajo La implementación de calidad de servicio (QoS) para proporcionar un tratamiento prioritario de las aplicaciones empresariales de voz y crítica Hacer cumplir las políticas de seguridad básicas para limitar el acceso a la red y mitigar las amenazas Reducir el costo total de propiedad a través de simplificar las operaciones y la automatización

Equipo	**Cantidad**	**Características**	**Descripción**

			
Switch Cisco Catalys 2960 WS-C2960X-24TS-LL	27	Puertos básicos de conmutación RJ-45:24 Capacidad de conmutación:100 Gbit/s Tipo de interruptor: Gestionado Velocidad de reloj:600 MHz Memoria interna:512 MB Voltaje:CA 120/230 V Frecuencia requerida:50/60 Hz 24 puertos Gigabit 10/100/1000 - 02 puertos Gigabit para fibra SFP	Conmutadores Gigabit Ethernet apilables que proporcionan acceso de clase empresarial para aplicaciones de campus y sucursales de configuración fija. Diseñado para la simplicidad operacional al coste total de propiedad más bajo, que permiten, operaciones de negocios seguras y eficientes energéticamente escalables.

Equipo	**Cantidad**	**Características**	**Descripción**
			
Switch Cisco Catalys 2960 WS-C2960X-24TS-L	2	Switch Administrable Cisco Catalyst 2960X-24PS-L 512 MB RAM 128 MB Memoria flash Cisco LAN Base IOS Software 24 puertos Gigabit 10/100/1000	conmutadores Gigabit Ethernet apilables, proporcionan acceso de clase empresarial para aplicaciones de campus y sucursales de configuración fija. Diseñado para la simplicidad operacional al coste total de propiedad más bajo, que permiten, operaciones de negocios

		04 puertos Gigabit para fibra SFP Rack-mountable	seguras y eficientes energéticamente escalables.

Equipo	**Cantidad**	**Características**	**Descripción**
			
Switch Cisco Catalys 2960 WS-C3560E-12SD		Administrable 24 puertos fast ethernet 1 RU de configuración fija Imagen de base LAN Tipo incluido: Montaje en rack - 1U Capacidad de conmutación: 32 Gbp Rendimiento de reenvío (tamaño de paquete de 64 bytes) : 6.5 Mpp Puertos: 24 x 10/100 + 2 x Gigabit SFP combinado 24 puertos Ethernet 10/100 PoE y 2 enlaces ascendentes de dual-purpose	Función Power over Ethernet que le permite implementar fácilmente nuevas funciones como comunicaciones por voz e inalámbricas sin necesidad de realizar nuevas conexiones. Capacidad de configurar LAN virtuales de forma que los empleados estén conectados a través de funciones de organización, equipos de proyecto o aplicaciones en lugar de por criterios físicos o geográficos.

Anexo 22. Características tecinas Ap

Equipo	Cantidad	Característica	Descripción
Cisco AIR-LAP1262N-A-K9	5	Estándar 802.3af Power over Ethernet	La serie Cisco Aironet 1260 es un componente de la red inalámbrica unificada de Cisco, que puede llegar hasta a 18.000 puntos de acceso con plena capa 3 la movilidad a través de lugares centrales o remoto en el campus de la empresa, en las sucursales, y en sitios remotos
		Temperatura de funcionamiento extendido y componentes resistentes para el despliegue en condiciones ambientales extremas.	
		Hardware de montaje que fácilmente modernizaciones a los actuales 1130 y 1240 Series soportes de montaje para simplificar la migración 802.11n.	
		UL 2043 plenum para las opciones de instalación en el techo por encima o suspensión de falsos techos.	

Equipo	Cantidad	Característica	Descripción
Cisco AIR-CAP2702E-A-K9	5	canal de 80 MHz	Los Access Point Aironet Serie 2700 presentan HD (High Density Experience) la mejor arquitectura de RF de su clase, que brinda cobertura de alto rendimiento para una alta densidad de dispositivos cliente, brindando al usuario final una experiencia inalámbrica sin inconvenientes.
		Proporciona inteligencia de espectro proactiva alta velocidad en canales de 20, 40, 80MHz	
		Temperatura de operación de -20° a 50°C	
		Fuente de alimentación e inyector de alimentación 100 a 240 VCA; 50 a 60 Hz / 44 a 57 VDC	
		Dual Band controller-based 802.11a/g/n/ac Velocidad máxima de datos de 1,3 Gbps	
		Evita problemas de rendimiento por interferencia inalámbrica	

Equipo	Cantidad	Característica	Descripción
Cisco AIR-LAP1041N-A-K9	5	Auto-sensor por dispositivo, alimentación mediante Ethernet (PoE), activable, soporte DFS, soporte Wi-Fi Multimedia (WMM).	Un diseño elegante que se integra en los entornos empresariales. Capacidad de ser alimentado con 802.3af Power over Ethernet estándar. Antenas optimizadas y radios que ofrecen una experiencia de movilidad de gran alcance. Automatizado de auto-sanación que reduce los puntos muertos y mantiene conexiones de cliente. Una garantía limitada de por vida que incluye sustitución avanzada de hardware de 10 días.
		Velocidad de transferencia de datos 300 Mbps	
		Indicadores de estado Error, estado	
		Protocolo de interconexión de datos IEEE 802.11b, IEEE 802.11a, IEEE 802.11g, IEEE 802.11n Banda de frecuencia 2.4 GHz	
		Tecnología de conectividad Inalámbrico	
		Tecnología 2T2R MIMO, Maximum Ratio Combining (MRC)	

Equipo	Cantidad	Característica	Descripción
Cisco AIR-LAP1131AG-A-K9	2	Cisco Aironet 1131 AG ligero de IEEE 802.11 a/b/g,	Cisco Aironet 1131 AG ligero de IEEE 802.11 a/b/g, punto de acceso proporcionar alta capacidad, de alta seguridad, Características de clase empresarial en una discreta, office-class diseño, ofreciendo acceso WLAN con el menor coste total de propiedad
		Proporciona plena compatibilidad para Legacy WLAN 802.11b clientes. /P	
		Cisco Aironet 1131 AG IEEE 802.11 a/b/g ligero aprovecha al máximo	
		Ofreciendo 108 Mbps tasas de transferencia de datos en el 5 y bandas de 2,4 GHz	
		Acceso WLAN con el menor coste total de propiedad. Dos radios de alto rendimiento proporcionan soporte simultáneo para estándares 802.11 g y 802.11 a	
		Punto de acceso proporcionar alta capacidad, de alta seguridad	

		Características de clase empresarial en una discreta, office-class diseño	

Anexo 23. Características técnicas firewall

FIREWALL	
	
Características	Descripción
Puertos	4 Gigabit Ethernet y 1 Fast Ethernet
Rendimiento	Capacidad de cortafuegos: 450 Mbps
Tasa de conexión de Firewall	12000 conexiones por segundo
Capacidad VPN (3DES/AES) de Firewall	225 Mbps
Memoria RAM	2Gb
Tipo de auteticacion	Secure Shell (SSH), RADIUS, TACACS+
Algoritmo de cifrado	DES, Triple DES, AES
Protocolo de Gestion	SNMP 1, SNMP 2, SNMP 3, SNMP 2c

Anexo 24. Distribución de VLAN's

VLANS
Vlan 1: Switching
Vlan 2: Equipos-WLC
Vlan 3: Telefonía IP
Vlan 4: CCTV
Vlan 5: IPs-Públicas
Vlan 6: DMZ
Vlan 7: NAT-Interno
Vlan 8: CTIC
Vlan 10: Autoridades
Vlan 12: Financiero
Vlan 14: Comunicaciones
Vlan 16: Administrativos
Vlan 22: Docentes
Vlan 24: Servidores-Informatica
Vlan 25: Carrera-Informatica
Vlan 26: Labs-PC-Informatica
Vlan 72: Wireless-Eventos
Vlan 80: WIFI-UPEC
Vlan 98: Lab-Ingles
Vlan 100: Lab-Biblioteca
Vlan 101: Lab-Informatica-01
Vlan 102: Lab-Informatica-02
Vlan 103: Lab-Informatica-03
Vlan 104: Lab-Informatica-04
Vlan 105: Lab-Informatica-05
Vlan 106: Lab-Informatica-06
Vlan 107: Lab-Informatica-07
Vlan 108: Lab-Informatica-08
Vlan 109: Lab-Informatica-09
Vlan 110: Lab-Informatica-10
Vlan 111: Lab-Informatica-11
Vlan 112: Lab-Informatica-12
Vlan 113: Lab-Informatica-13

Anexo 25. Políticas de uso del sistema de monitoreo

I. POLÍTICAS DE USO DEL SISTEMA DE MONITOREO

Para la elaboración de las políticas de uso de la herramienta se basó en el modelo de gestión ISO, FCAPS, esta comprende a cada uno de los procesos que integra el modelo, su objetivo principal es de definir las reglas de uso para asegurar el correcto funcionamiento del sistema.

II. PROPÓSITO

El propósito del presente documento permitirá definir las reglas del correcto uso de la herramienta de monitoreo, permitiendo garantizar el funcionamiento adecuado del sistema de gestión de la red de datos de la institución.

III. NIVELES ORGANIZACIONALES

Director: Autoridad superior del departamento de TIC's de la UPEC.
Administrador de red: Persona encargada en administrar los recursos de la red de datos de la UPEC.

IV. ESTRUCTURA DE LAS POLÍTICAS DE GESTIÓN.

1. POLÍTICAS DE GESTIÓN DE CONFIGURACIONES

1.1.Ingreso de dispositivo a la herramienta de monitoreo

1.2.Configuración de dispositivos

1.3.Inventario

2. POLÍTICAS DE GESTIÓN DE FALLOS

2.1.Administración de fallos.

2.2.Informe de fallos.

3. POLÍTICAS DE GESTIÓN DE CONTABILIDAD

3.1.Gestión de recursos

4. POLÍTICAS DE GESTIÓN DE PRESTACIONES

4.1.Rendimiento

5. POLÍTICAS DE GESTIÓN DE SEGURIDAD

5.1. Sistema de monitoreo

5.2.Dispositivos administrados

POLÍTICAS DE GESTIÓN DE CONFIGURACIONES

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI	
	
Proceso	1. Políticas de gestión de configuraciones
Subproceso	1.1.Ingreso de dispositivo a la herramienta de monitoreo
Encargado	Administrador de la red
Art. 1. Los nuevos dispositivos que se agreguen al sistema de monitoreo se deberá habilitar el protocolo SNMP en cada uno de ellos, además de configurar su comunidad de gestión al que pertenezcan para poder ser monitoreados.	

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI	
	
Proceso	1. Políticas de gestión de configuraciones
Subproceso	1.2.Configuración de dispositivos
Encargado	Administrador de la red
Art. 2. El administrador de la red será la única persona encargada de realizar las configuraciones de los dispositivos que pertenezcan a la institución.	

Art. 3. Mantener respaldos de la información de cada uno de los dispositivos en caso de perderse la información. **Art4.** Previamente a la configuración de un dispositivo o equipo de la red, se deberá realizar un respaldo de la configuración funcional del dispositivo.

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI	
	
Proceso	1. Políticas de gestión de configuraciones
Subproceso	1.3.Inventario
Encargado	Administrador de la red
Art. 5. Se deberá tener un inventario de todos los dispositivos o equipos de red, pertenecientes a la red de datos con todas sus características más importantes.	

POLÍTICAS DE GESTIÓN DE FALLOS

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI	
	
Proceso	2. Políticas de gestión de fallos
Subproceso	2.1. Administración de fallos
Encargado	Administrador de la red
Art. 6. Mediante la interfaz gráfica del sistema de monitoreo se verificará periódicamente todos los problemas que ocurran dentro de la infraestructura de red de la institución y proceder con su solución.	

Art. 7. El administrador de la red podrá asignar tareas de reparación y aislamientos de problemas de la red a personas que integren el departamento de TIC's de la institución. **Art.8.** El administrador de la red u otra persona dentro del área del departamento de TIC's serán los únicos encargados de solventar el problema detectado en la infraestructura de la red de la institución, evitando inconvenientes en las funciones que desempeñe los usuarios.

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI	
Proceso	2. Políticas de gestión de fallos
Subproceso	2.2.Documentación de fallos
Encargado	Administrador de la red
Art. 9. Se deberá realizar una documentación periódica de los fallos ocurridos dentro de la red de datos de la institución con su respectiva solución, para que posteriormente cuando se suscite este mismo problema pueda solucionarse de manera inmediata.	

POLÍTICAS DE GESTIÓN DE CONTABILIDAD

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI	
Proceso	3. Políticas de gestión de contabilidad
Subproceso	3.1.Gestión de contabilidad
Encargado	Administrador de la red

Art. 10. Mediante la herramienta se tendrá un registro periódico sobre el consumo de los recursos de servidores tales como: CPU, memoria, disco duro, velocidad de lectura y escritura entre otros. **Art. 11.** El administrador de red podrá tener graficas estadísticas históricas sobre el uso de los recursos de la red de datos.

POLÍTICAS DE GESTIÓN DE PRESTACIONES

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI	
	
Proceso	4. Políticas de gestión de Prestaciones
Subproceso	4.1. Rendimiento
Encargado	Administrador de la red
Art. 12. El administrador establecerá límites de consumo de los recursos de la red de datos y con ello la generación de alertas sobre algún problema. **Art. 13.** El administrador podrá obtener reportes sobre el tráfico y consumo del ancho de banda de cada una de las interfaces de red que este disponga. **Art. 14.** Los umbrales de aceptación de los equipos serán dispuestos de acuerdo con las políticas de gestión de configuraciones y fallos.	

POLÍTICAS DE GESTIÓN DE SEGURIDAD

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI	
	
Proceso	5. Políticas de gestión de Seguridad

Subproceso	5.1. Sistema de monitoreo
Encargado	Administrador de la red

Art. 15. Para la creación de usuarios dentro del sistema únicamente se autoriza al administrador de la red de la institución.

Art. 16. El administrador de la red considerara los privilegios de acceso a la herramienta de monitoreo.

Art. 17. El acceso al sistema estará autorizado únicamente a todos los usuarios creados por el administrador de la red.

Art. 18. Las notificaciones de todos los eventos suscitados dentro de la red se enviarán únicamente al correo electrónico o red social privada del administrador de red.

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Proceso	5. Políticas de gestión de Seguridad
Subproceso	5.2. Equipos administrados
Encargado	Administrador de la red

Art. 19. Las claves de acceso a los dispositivos gestionados por la herramienta únicamente tendrán acceso el personal autorizado por el administrador de la red.

Art. 20. Los equipos monitoreados serán de conocimiento único del administrador de red debido a su seguridad.

Anexo 26. Mapeo de Gestión de red

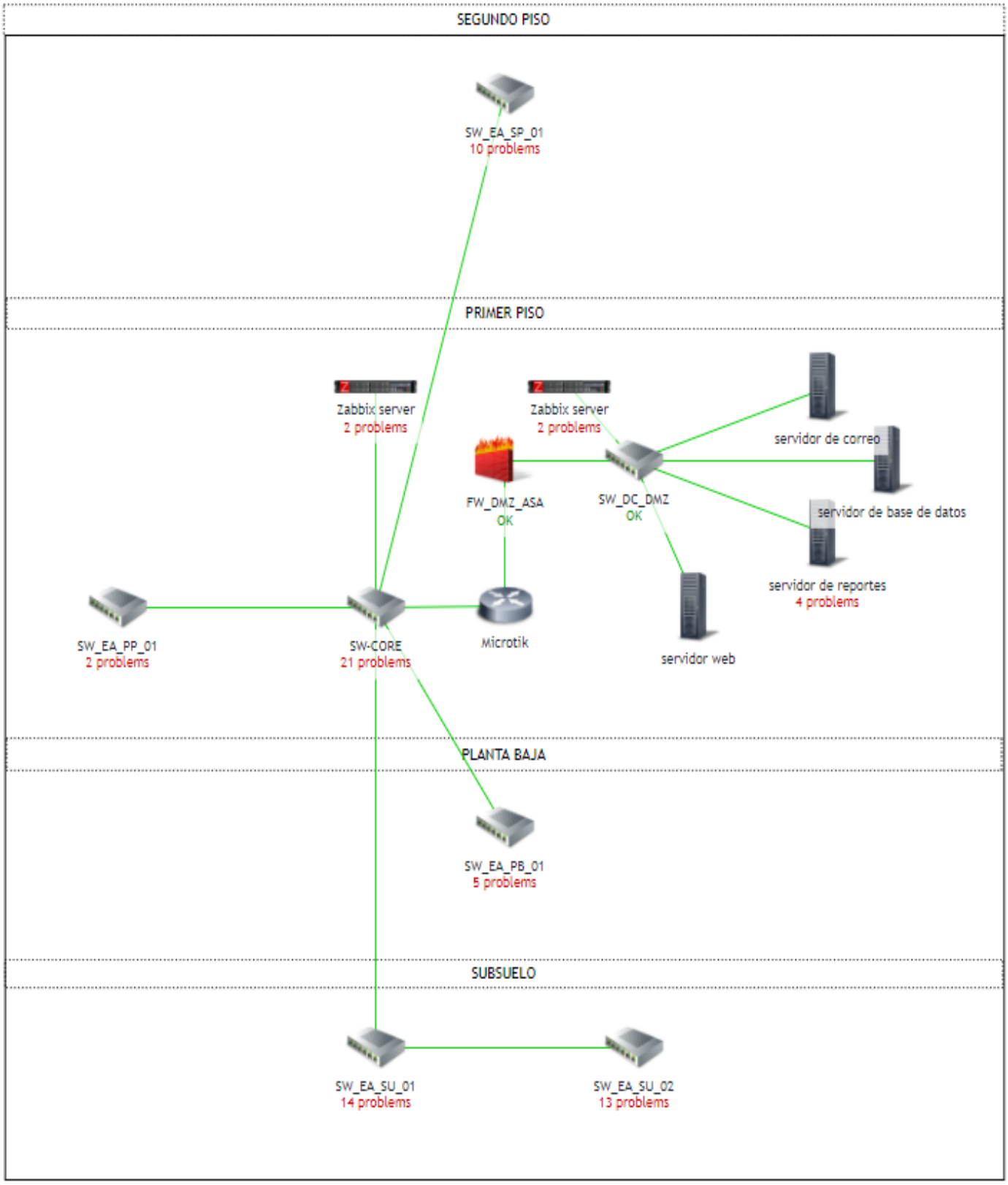


Figura 89. Esquema de Gestión de red del Edificio Administrativo

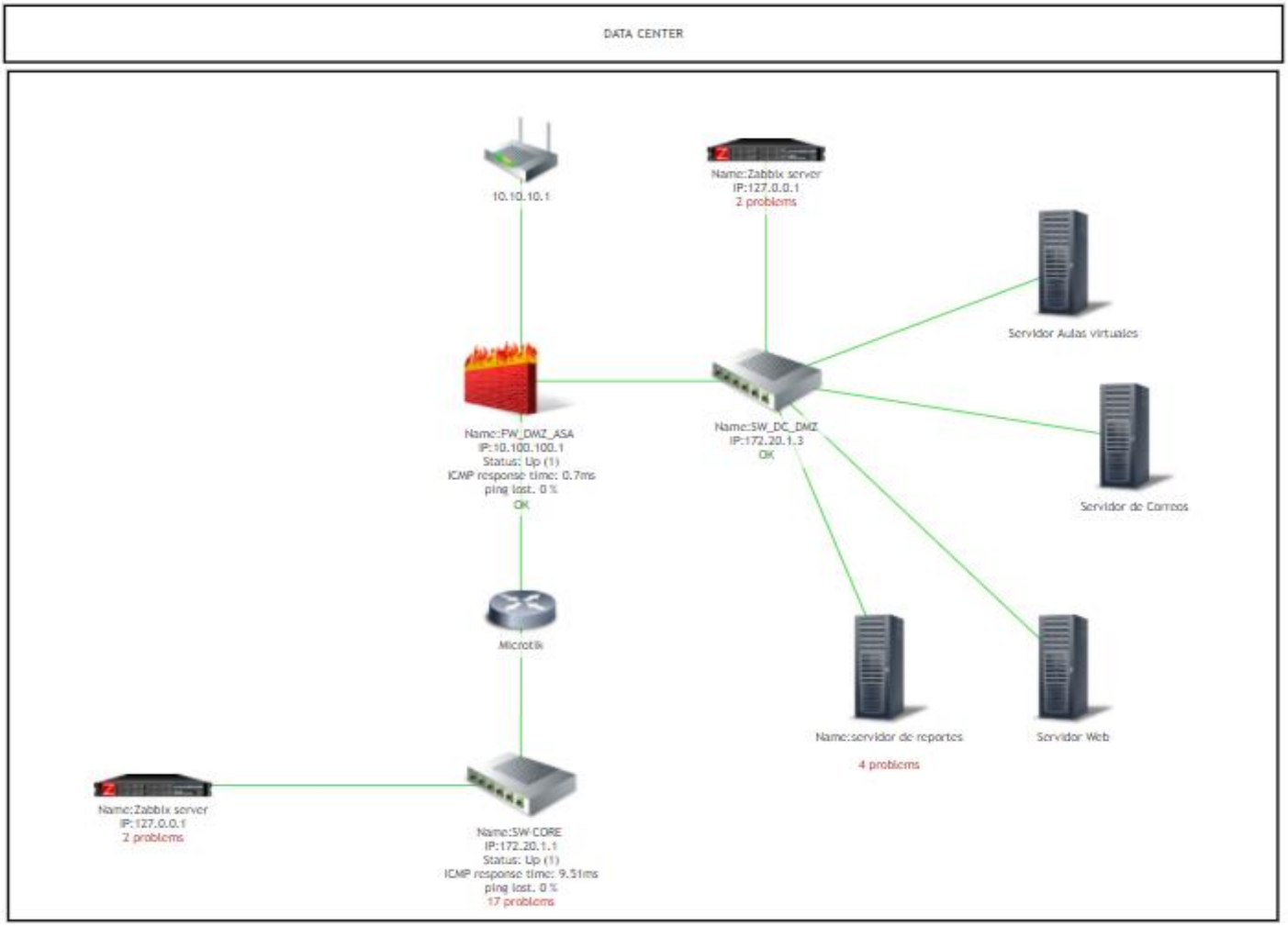


Figura 90. Esquema de Gestión del Data Center

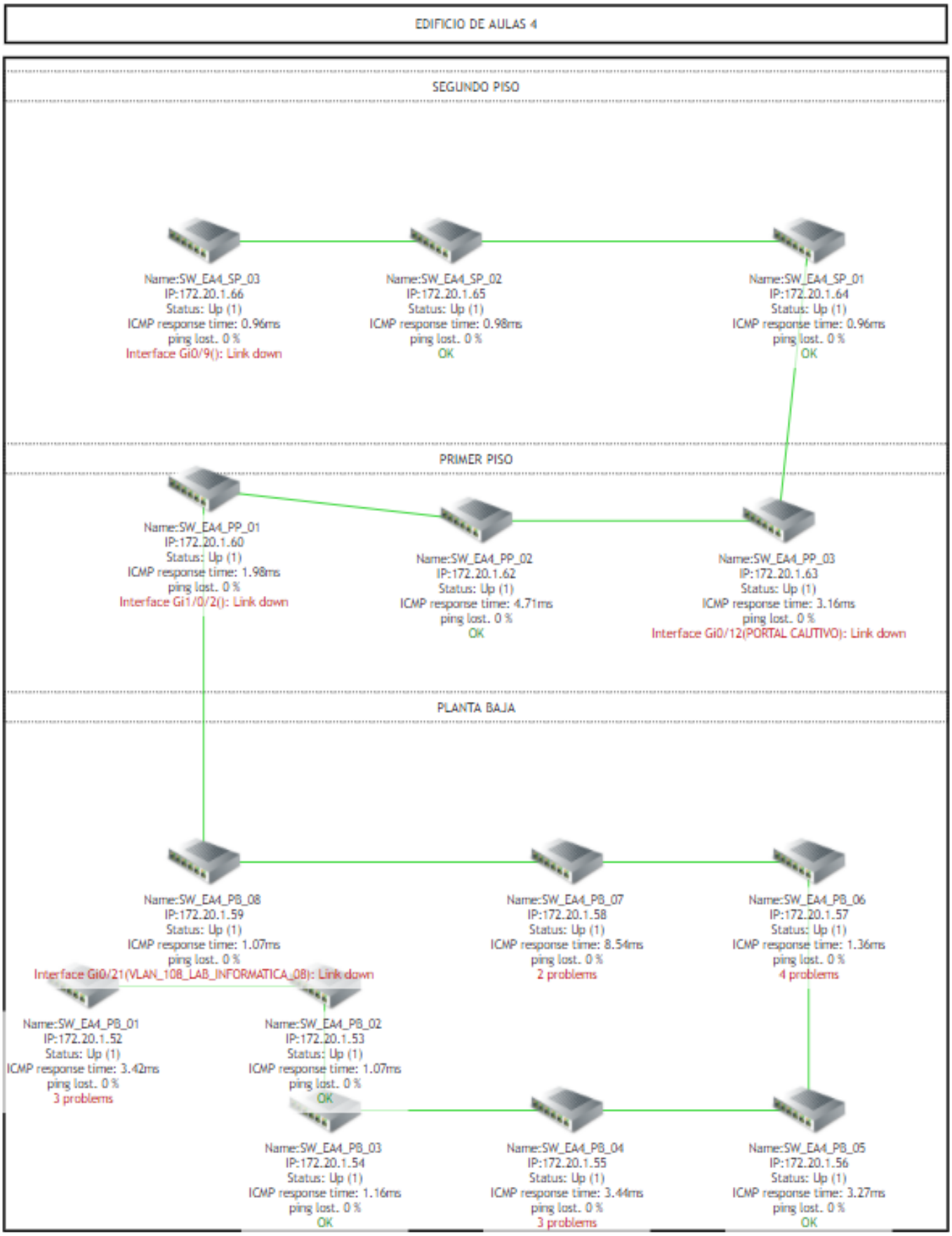


Figura 91. Esquema de Gestión de red de Switches del Edificio Aulas 4

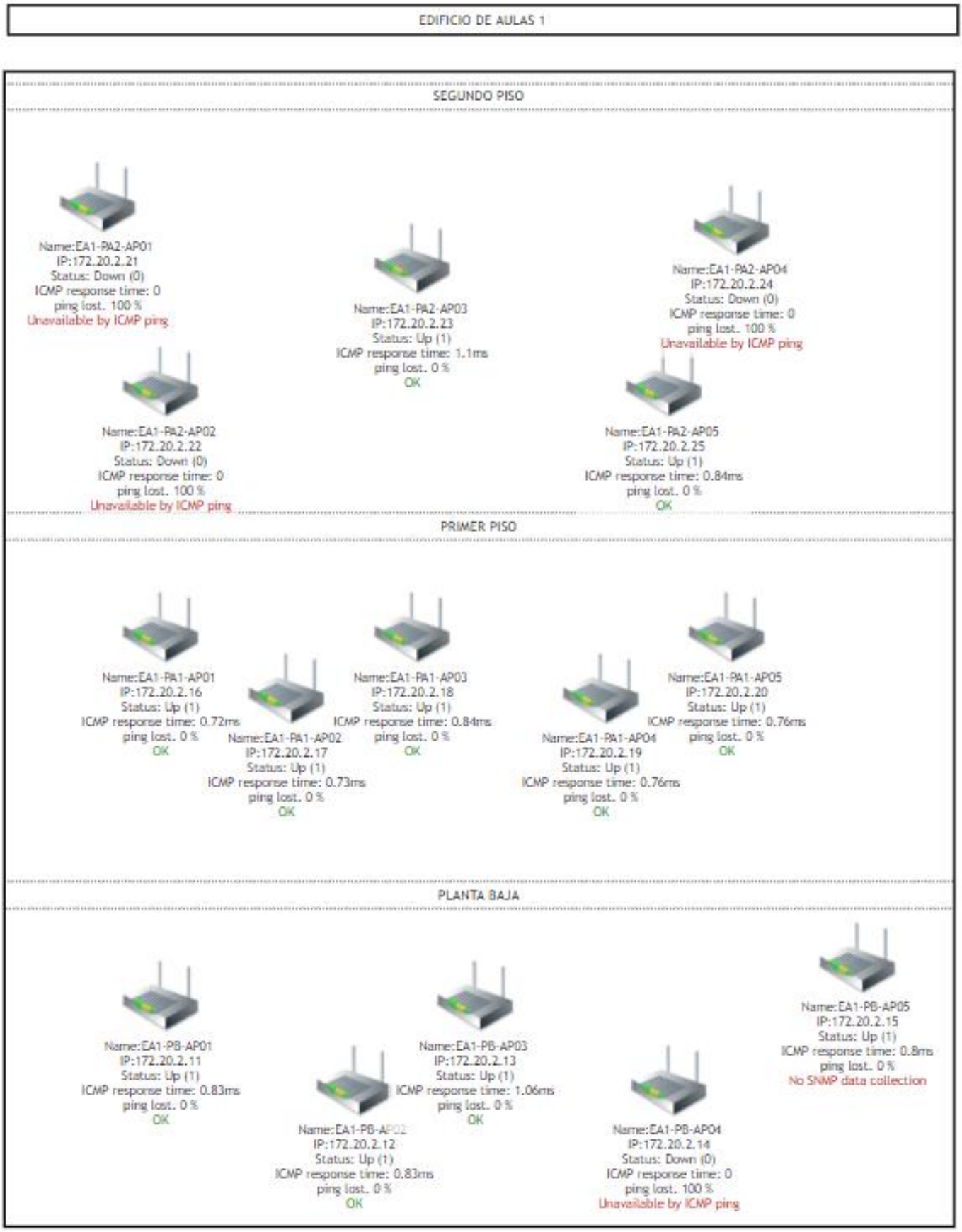


Figura 92. Esquema de Gestión de Red de Ap Edificio Aulas 1

Anexo 27. Acta de fin de proyecto

Educamos para transformar el mundo

ACTA DE FIN DE PROYECTO

La Universidad Politécnica Estatal del Carchi, a través de la unidad de redes y telecomunicaciones, en colaboración con estudiantes de la carrera de ingeniería en informática, buscan integrar proyectos tecnológicos que permitan mejorar la continuidad y operatividad de la red de datos de la institución, por ello se ve la necesidad de implementar un sistema de monitoreo de software libre para mantener un control centralizado de los recursos de la red.

De acuerdo con los requerimientos y características de la red, se determinó que la implementación cuente con los siguientes parámetros.

- Uso de software libre
- Interfaz gráfica
- Monitoreo remoto de equipos
- Alertas y notificaciones
- Gráficas dinámicas
- Seguridad
- Reportes
- Escalabilidad
- Autodescubrimiento

Gracias al apoyo de los estudiantes, se ha podido plasmar el sistema de monitoreo el cual permite:

- Monitorear la infraestructura de red.
- Monitoreo de servidores.
- Monitoreo de aplicaciones y servicios.
- Verificar la disponibilidad de los equipos de la red.
- Visualizar datos estadísticos sobre la CPU, uso de disco, memoria, ancho de banda de la red entre otros.
- Permitir la visualización de grafica de los recursos de cada equipo.
- Alertar de problemas que ocurren en la red de forma inmediata al administrador.
- Generación de reportes históricos de cada uno de los equipos monitorizados

- Ampliación de la red sin inconveniente en la monitorización.
- Creación de grupos y usuarios

Este proyecto se lo desarrollo como requisito de titulación denominado: "Implementación del sistema de monitoreo y mejora del rendimiento de la red de datos de la Universidad Politécnica Estatal del Carchi", realizado por los estudiantes Casanova Imbaquingo Edi Santiago con C.I.0401587050 y Chulde Molina Anderson Xavier con C.I 040199515-4

Para los fines pertinentes, me suscribo.

Ing. Andrés Zabala Villarreal MSc.
DIRECTOR DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Anexo 28. Informe final

Tulcán, 30 de marzo de 2021

No. 001

De:

Edi Santiago Casanova Imbaquingo

Anderson Xavier Chulde Molina

Recibido
30-03-2021
09:36

Para:

Unidad de Redes y Telecomunicaciones

Dirección de TICs de la UPEC

Asunto: Informe final de Implementación del sistema de Monitoreo en la red de datos de la Universidad Politécnica Estatal del Carchi.

De nuestras consideraciones.

INDICE

INFORME FINAL DE PROYECTO

1 Resumen

La importancia del proyecto de investigación se evidencia a la hora de la identificación de problemas que se presentan dentro de la infraestructura de red de la institución, puesto que no existen herramientas especializadas en el monitoreo y control de dispositivos de red en tiempo real, el objetivo principal es implementar un sistema de monitoreo de software libre que permita gestionar los recursos de la red de datos de la institución, permitiendo de manera oportuna agilizar los tiempos de solución ante eventos que degraden el servicio de red.

2 Principales logros del proyecto

Con la implementación del sistema de monitoreo se logró cubrir funcionalidades fundamentales, que permitan solventar problemas que aquejan a la infraestructura de la institución, garantizando disponibilidad sobre los recursos y servicios que ofrece esta. Para ello se determinó las funcionalidades más importantes a tomar en cuenta para la implementación de la herramienta de monitoreo.

- Monitorización remota
- Alertas y notificación
- Graficas
- Seguridad
- Disponibilidad
- Reportes
- Escalabilidad
- Cambios de configuración
- Autodescubrimiento de la red

2.1 Monitorización remota

Permite capturar la información acerca de los equipos monitorizados, así como su CPU, memoria, consumo de ancho de banda y esto en tiempo real a través de la herramienta de monitoreo, manteniendo un registro del estado de equipos o servicios que integren la red.

2.2 Alertas y Notificaciones

La herramienta de monitoreo está en capacidad de alertar en caso de encontrar una anomalía dentro de la red y ésta se notificará de manera inmediata mediante aplicaciones de mensajería en este caso mediante correo electrónico y telegram al administrador de la red de datos con el objetivo de mejorar los tiempos de respuesta ante posibles fallas en el servicio de la red de datos de la institución.

2.3 Graficas

Esta característica permitirá que la información de la red se visualice en graficas dinámicas para una mejor interpretación de lo que ocurre dentro de la red de datos de la institución, este apartado es indispensable a la hora de monitorizar una infraestructura de red dado a que nos muestra en tiempo real la actividad o el estado de los equipos que se encuentran siendo monitorizados.

2.4 Seguridad

Es uno de los puntos más importantes a tomar en cuenta en el uso de la herramienta de gestión de la red, debido a que se manejan datos relevantes sobre equipos e infraestructura de la red de la institución por ende esta debe ser confidencial para este apartado es necesario la creación de grupos para clasificar quienes puedan acceder a los datos que recopila el sistema en este caso la persona encargada en la gestión de los usuarios y grupos es el administrador de la red, quien tendrá el control total del sistema .

2.5 Disponibilidad

El sistema de gestión de red garantiza su funcionamiento las 24 horas por los 7 días de la semana, monitoreando toda la infraestructura de la red buscando alertar sobre problemas que se presenten en el transcurso de los días.

2.6 Reportes

El sistema está en capacidad de generar reportes diarios, semanales, mensuales y anuales según sea el requerimiento del departamento de TIC's acerca de los dispositivos monitorizados.

2.7 Escalabilidad

El sistema está en la capacidad de continuar añadiendo más dispositivos sin afectar el desempeño de la herramienta de monitoreo, manteniendo una alta disponibilidad de los recursos de la red de datos y reduciendo costos de almacenamiento.

2.8 Cambios de configuración

Con la herramienta de monitoreo implementada en la red de datos de la institución, está la posibilidad de verificación de los distintos cambios en cada uno de los dispositivos y la supervisión de estos.

2.9 Autodescubrimiento

El sistema está en capacidad de descubrir nuevos elementos de red y agregarlos automáticamente al sistema de gestión guardando en un registro toda la configuración que este posea al momento del autodescubrimiento, o en alguna actualización.

Por ello se implementó el sistema de monitoreo Zabbix, herramienta que se ajusta a los requerimientos del departamento de TIC's cumpliendo con cada una de las funcionalidades presentadas, permitiendo monitorizar todos los recursos de la infraestructura de red de datos de la institución como son:

- Switch de Core
- Firewall Cisco ASA 5520
- Switches Cisco de acceso en sus diferentes versiones
- Servidores
- APs

3 Implementación

Para la implementación del modelo de gestión de la red de la institución, conformada por la estación gestora, dispositivos gestionando y protocolo de gestión. Se describe como se encuentra implementado el sistema identificando la estación gestora y los dispositivos monitoreados mediante el protocolo SNMP, permitiendo obtener información acerca del estado en el que se encuentra cada uno de los equipos que pertenecen a cada una de las dependencias de la institución.

Una vez definido la herramienta de monitoreo de la infraestructura de la red de datos se define la arquitectura de funcionamiento de dicha herramienta.

3.1 Gestor o estación gestora.

Este es el encargado de recibir toda la información de los equipos monitorizados, comprobando el estado en el que se encuentre el equipo enlazado, mediante alarmas definidas y estas se almacenaran en una base de datos.

Para el levantamiento del sistema de monitoreo de la red de datos de la institución, mediante la documentación oficial de la página de Zabbix se evalúa los requerimientos necesarios para la selección del equipo que mejor se ajuste a los requerimientos de dicha herramienta, por otra parte, se detalla las características del equipo en el cual será implementado.

Características	Descripción
CPU	Intel(R) Xeon(R) Silver 4214R CPU @ 2.40GHz
Arquitectura	64 bits
Memoria	6 GB de memoria RAM
Disco	100GB
Cache	16KiB L1 cache
Video	SVGA II Adapter

3.2 Dispositivos gestionados

Dispositivos gestionados (Agentes) son aquellos que van a ser monitorizados con el fin de recopilar información en tiempo real, permitiendo generar alertas al momento de suscitarse un problema que afecte el rendimiento y caída del servicio que disponga la institución. Para ello es necesario que los dispositivos gestionados tengan habilitado el protocolo SNMP para que puedan ser monitorizados. La herramienta de monitoreo de la red soporta el protocolo en sus versiones SNMPv1, SNMPv2 y SNMPv3. La versión de SNMP a implementarse en cada uno de los dispositivos de interconexión es la SNMPv2 puesto que esta es la más soportada por la mayoría de los dispositivos que integra la institución además por su configuración es más simple, no se tomó en cuenta la versión de SNMPv3 debido a que los mecanismos de seguridad

que esta integra generan más carga para el CPU provocando que el sistema degrade en su rendimiento.

3.2.1 Switch Serie Catalyst

Para el acceso de los dispositivos de interconexión de la institución es necesario utilizar una herramienta remota que permita la habilitación del protocolo SNMP, debido a que por defecto viene deshabilitado en este caso se hace uso de la herramienta PUTYY en el cual se establece la IP y el puerto de comunicación que es el 23 vía TELNET. Para consultar si el protocolo está habilitado en los dispositivos, el comando de verificación es "show snmp"

3.2.2 Servidores

En cuanto la habilitación del Agente SNMP en los servidores se procede a seguir los siguientes pasos.

- Descargar repositorio de zabbix en su versión 5.0 y actualizar.
- Configurar zabbix agent
- Iniciar y habilitar zabbix-agent
- Habilitar puerto 10050/tcp del firewall
- Reinicio de firewall y del agente zabbix

3.2.3 Firewall Cisco ASA 5520

- Como primer punto es necesario la habilitación del protocolo SNMP, puesto que por defecto viene deshabilitado, también es necesario definir la interfaz y la ip de la estación gestora (NMS) definiendo a la comunidad a la que pertenece y será monitorizado

4 Implementación de Políticas de uso del sistema de monitoreo

I. POLÍTICAS DE USO DEL SISTEMA DE MONITOREO

Para la elaboración de las políticas de uso de la herramienta se basó en el modelo de gestión ISO, FCAPS, esta comprende a cada uno de los procesos que integra el modelo, su objetivo principal es de definir las reglas de uso para asegurar el correcto funcionamiento del sistema.

II. PROPÓSITO

El propósito del presente documento permitirá definir las reglas del correcto uso de la herramienta de monitoreo, permitiendo garantizar el funcionamiento adecuado del sistema de gestión de la red de datos de la institución.

III. NIVELES ORGANIZACIONALES

Director: Autoridad superior del departamento de TICs de la UPEC.

Administrador de red: Persona encargada en administrar los recursos de la red de datos de la UPEC.

IV. ESTRUCTURA DE LAS POLÍTICAS DE GESTIÓN.

1. POLÍTICAS DE GESTIÓN DE CONFIGURACIONES

1.1.Ingreso de dispositivo a la herramienta de monitoreo

1.2.Configuración de dispositivos

1.3.Inventario

2. POLÍTICAS DE GESTIÓN DE FALLOS

2.1.Administración de fallos.

2.2.Informe de fallos.

3. POLÍTICAS DE GESTIÓN DE CONTABILIDAD

3.1.Gestión de recursos

4. POLÍTICAS DE GESTIÓN DE PRESTACIONES

4.1.Rendimiento

5. POLÍTICAS DE GESTIÓN DE SEGURIDAD

5.1. Sistema de monitoreo

5.2.Dispositivos administrados

5 Control de acceso a la herramienta Zabbix

5.1 Gestión de seguridad

Este proceso comprende sobre los accesos a los dispositivos gestionados y el sistema de monitoreo, por ello es necesario determinar su gestión de seguridad para evitar que los datos estén comprometidos.

Para la seguridad del sistema de monitoreo es necesario el cambio de contraseña que viene por defecto, para que no pueda acceder cualquier persona ajena del departamento de TIC's, para

realizar este proceso es necesario acceder a el frontend de zabbix con su respectiva ip e ingresar a el apartado de usuarios y se podrá visualizar el usuario Admin el cual tendrá un control total sobre los equipos gestionados en la red, para ello es posible realizar el cambio de la contraseña que por defecto del sistema es "zabbix".

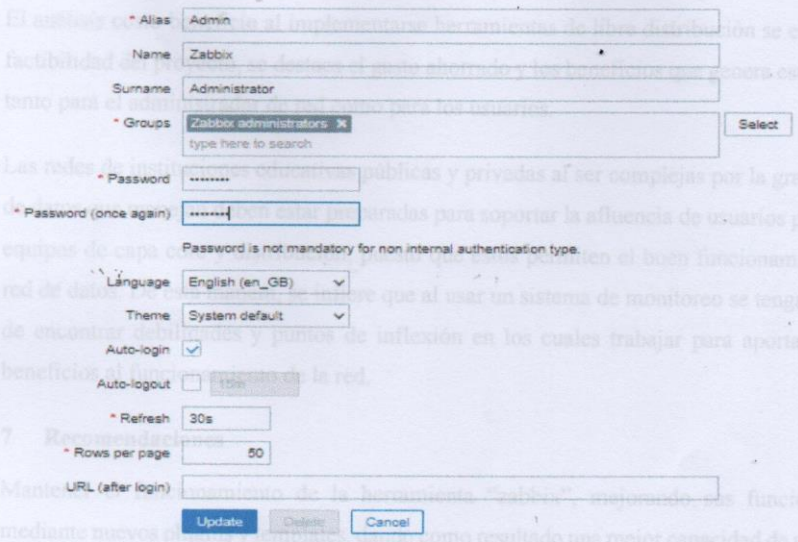


Figura 1. Vista del Cambio de Contraseña del Administrador

6 Conclusiones

El monitoreo y control en la red de datos de la Universidad Politécnica Estatal del Carchi es fundamental, ya que permite al administrador de la red supervisar el rendimiento de esta, detectándose con prontitud los problemas que se presentan y puedan ser resueltos a tiempo.

El análisis costo-beneficio al implementarse herramientas de libre distribución se evidencia la factibilidad del proyecto, se destaca el gasto ahorrado y los beneficios que genera este proyecto tanto para el administrador de red como para los usuarios.

Las redes de instituciones educativas públicas y privadas al ser complejas por la gran cantidad de datos que manejan deben estar preparadas para soportar la afluencia de usuarios priorizando equipos de capa core y distribución, puesto que estos permiten el buen funcionamiento de la red de datos. De esta manera, se infiere que al usar un sistema de monitoreo se tenga la opción de encontrar debilidades y puntos de inflexión en los cuales trabajar para aportar mayores beneficios al funcionamiento de la red.

7 Recomendaciones

Mantener el funcionamiento de la herramienta "zabbix", mejorando sus funcionalidades mediante nuevos plugins y templates, dando como resultado una mejor capacidad de monitoreo, que permita al administrador de red tomar acciones necesarias para la buena operatividad de la red.

Realizar semanalmente mantenimiento preventivo de la infraestructura de red, y sus servidores, para que aporten un mejor funcionamiento en el servicio de conectividad, atendiendo los fallos que lleguen a presentarse con mayor eficacia, evitando la baja disponibilidad del servicio de red.

Es recomendable realizar revisiones paulatinamente a los dispositivos que pertenezcan a la infraestructura de red de la institución, con el fin de establecer límites en los controles que no sobrepasen la capacidad de estos equipos y evitar la aglomeración de fallos en el sistema.

Atentamente,

Sr. Edi Santiago Casanova
C.I.:0401587050

Sr. Anderson Chulde
C.I.:0401995154

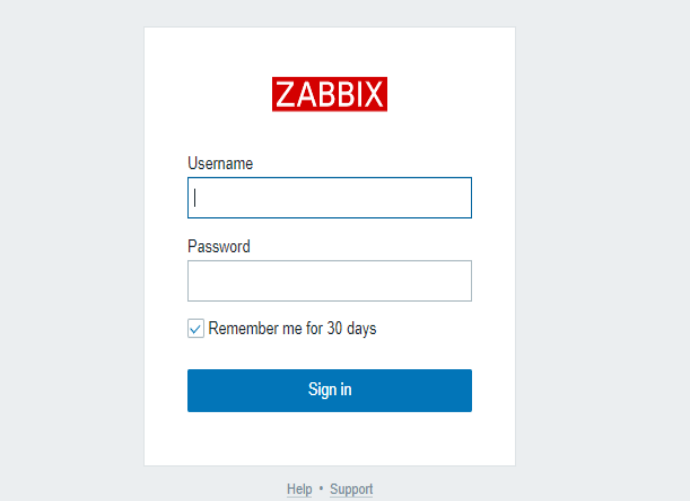
Anexo 29. Manual de gestión del sistema de monitoreo zabbix

Contenido

1. INGRESO A EL SISTEMA

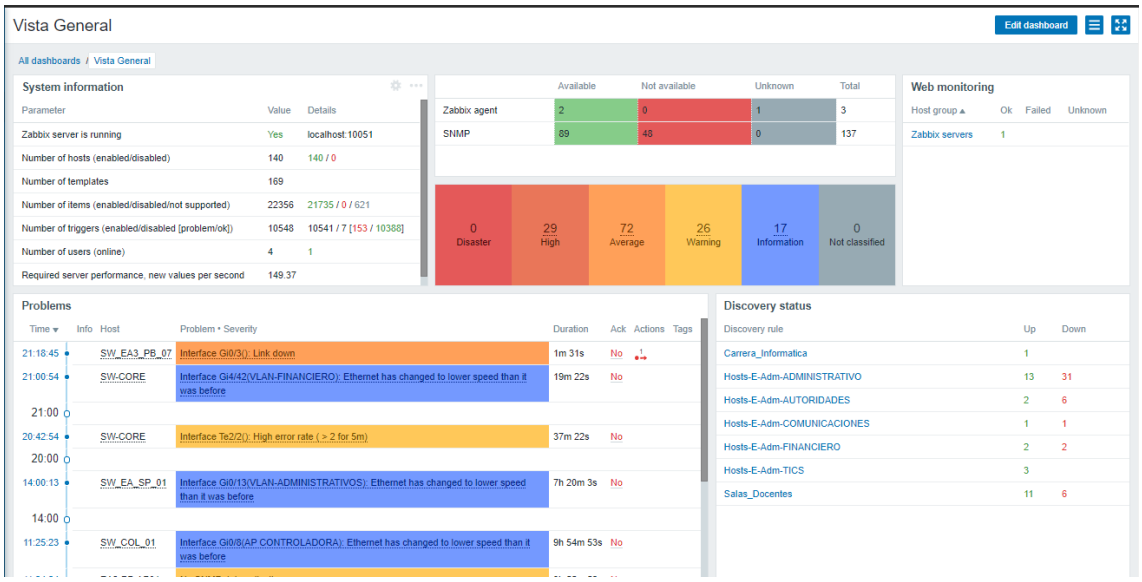
1.1.Sistema de monitoreo

Para el ingreso a la interfaz del sistema de monitoreo de zabbix, se lo puede realizar desde cualquier navegador y en la barra de búsqueda ingresamos la dirección de URL http://190.15.129.80/zabbix/ en la cual nos pedirá las credenciales de acceso al sistema.

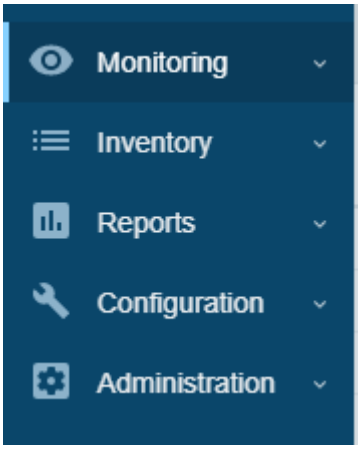


1.2.Interfaz principal

En este apartado tenemos una vista general del sistema de monitoreo zabbix, en el cual se puede apreciar de manera rápida un resumen de los problemas que presentan algunos equipos monitorizados de la infraestructura de red, así como los gráficos de severidad y la distribución de los equipos. Esta herramienta cuenta con 5 menús principales.



Menús principales que integra el servidor zabbix en el frontend



1.2.1. Menú Monitoreo

Muestra la información proporcionada y recolectada por los dispositivos monitoreados y lo presenta a través de gráficos estadísticos, graficas de SLA, pantallas con iconos dinámicos y números exactos de dispositivos, así como sus principales problemas.

- **Tablero:** Esta sección está diseñada para mostrar un resumen general del sistema como los últimos eventos ocurridos.
- **Problemas:** vista de todos los problemas que encuentra el sistema de monitoreo sobre los equipos gestionados.
- **Equipos:** vista de todos los equipos vinculados a el sistema de monitoreo.
- **Visión General:** desde aquí se podrá mostrar un resumen de todos los parámetros monitorizados de cada equipo y el estado en el que se encuentra cada uno de estos parámetros.
- **Últimos datos:** muestra los últimos datos recolectados por el sistema, además estos pueden ser filtrados por grupos y equipos. estos datos pueden mostrase en graficas de cada parámetro monitorizado sobre el estado del equipo vinculado con la herramienta.

- **Pantallas:** se pueden crear a partir de gráficos ya existentes.
- **Mapas:** esta sección podemos mirar, configurar y administrar mapas de red.
- **Descubrimientos:** Estado de las reglas de descubrimiento que se hayan definido para la identificación de nuevos equipos vinculados con el sistema.

1.2.2. Menú de Inventario

Presenta un inventario completo de hardware y software recolectados por zabbix de cada grupo o subgrupo de dispositivos

- **Equipos:** vista sobre las características definidas en el host.

1.2.3. Menú de Reportes

Integra opciones básicas de reportes, información que puede ser tomada desde el mismo administrador web en caso de requerir informes.

- **Información del sistema:** vista del estado del sistema, el número de equipos monitorizados, templates, ítems, triggers, usuarios y el rendimiento del servidor.
- **Informe de disponibilidad:** informe sobre la disponibilidad de cada equipo.
- **Triggers top 100:** vista de los 100 disparados que han registrado más actividad en el sistema.
- **Auditoria:** muestra todos los cambios de configuraciones que se generan en el servidor Zabbix, como también los inicios de sesión.
- **Notificaciones:** muestra los mensajes enviados mediante el medio previamente configurado.

1.2.4. Menú de Configuración

Este menú constituye la parte funcional del sistema el cual permite el registro de los dispositivos, grupos, plantillas, mantenimiento, acciones, modo edición, mapas y descubrimiento de dispositivos a través de la segmentación.

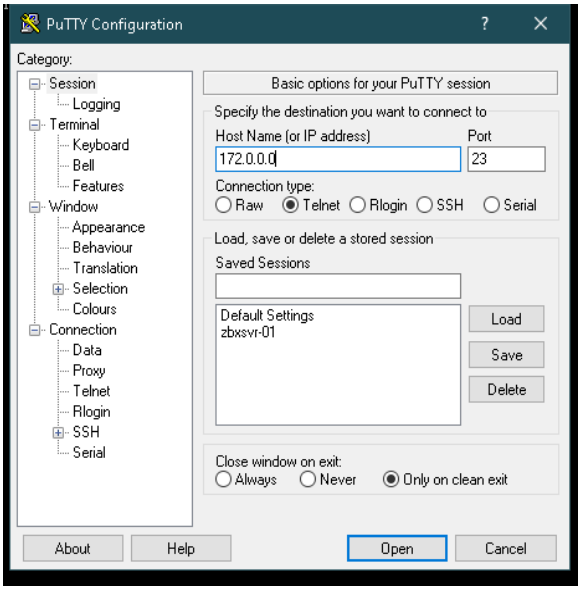
1.2.5 Menú de Administración

Constituye los métodos de autentificación de los usuarios, permite la configuración del frontend, servicios zabbix server y usuarios con sus respectivas alertas de problemas o notificaciones de uso.

2. CONFIGURACIÓN

2.1.Host SNMP

Ingreso a equipos vía SSH.
Acceso con credenciales de equipos switches.

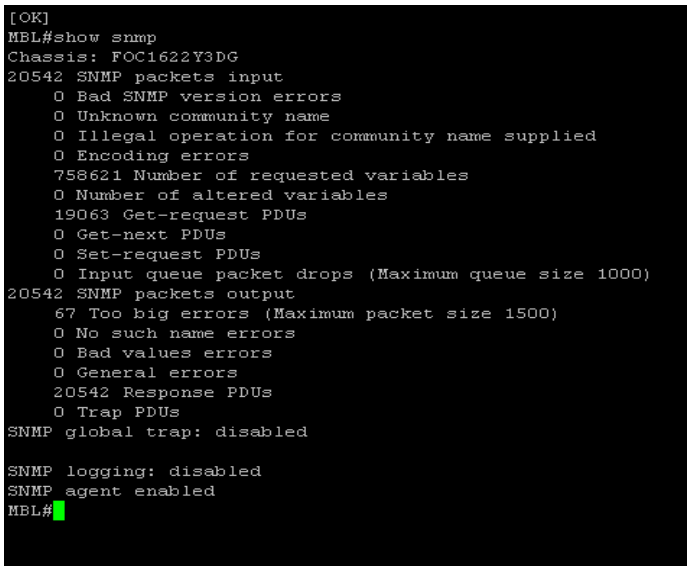


Configuración y habilitación de protocolo SNMP en los equipos.

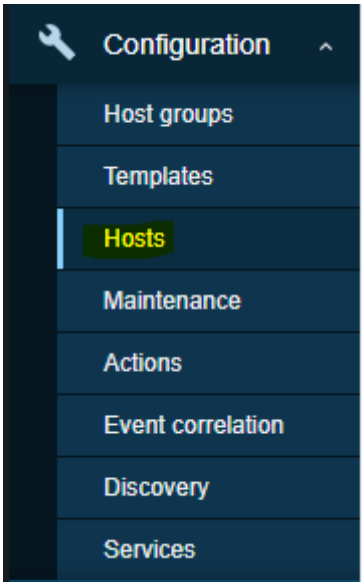
```
# enable
# conf terminal
switch(config)# snmp-server community public RO
switch(config)# snmp-server community private RW
# exit
# write memory
```

Verificamos que el agente SNMP este activo.

```
# show snmp
```

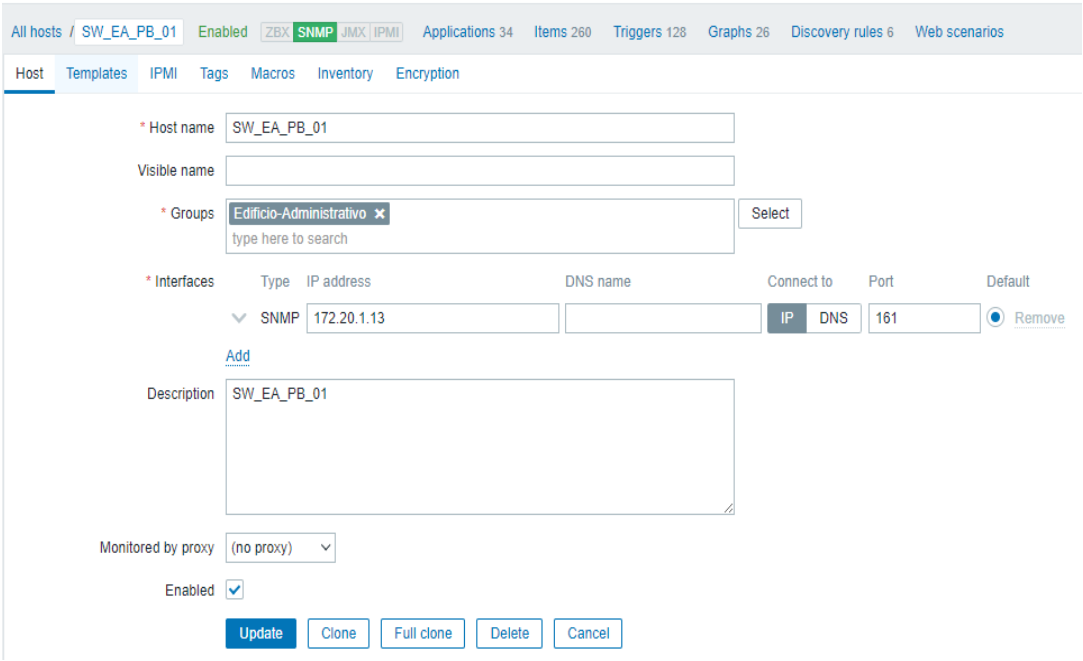


Después, iniciada sesión en Zabbix Front-end, iremos a “Configuration” / “Hosts”.



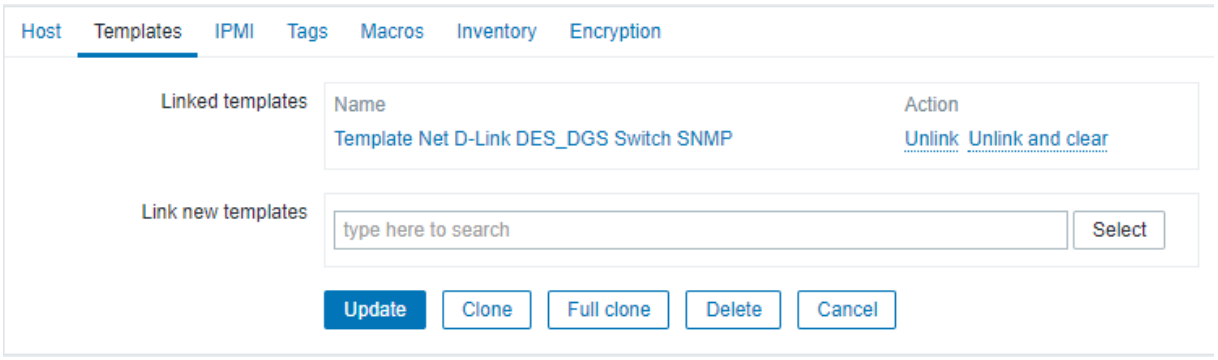
Para agregar un nuevo host, pulsaremos en el botón “Create host” y desplegara un formulario.

- **Host name:** Ingrese un nombre del host a monitorizar.
- **Host name visible:** repite el nombre del host, opcional.
- **Group:** Ingrese el dispositivo a un grupo que pertenezca.
- **Interfaces:** agregar la ip del nombre del host.



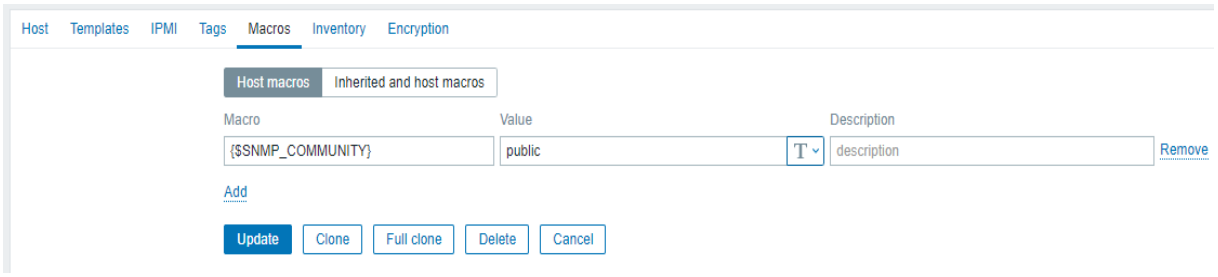
Insertar Templates.

- **Linked new template:** colección de ítems,triggers y gráficos diseñados para dispositivos de interconexión.

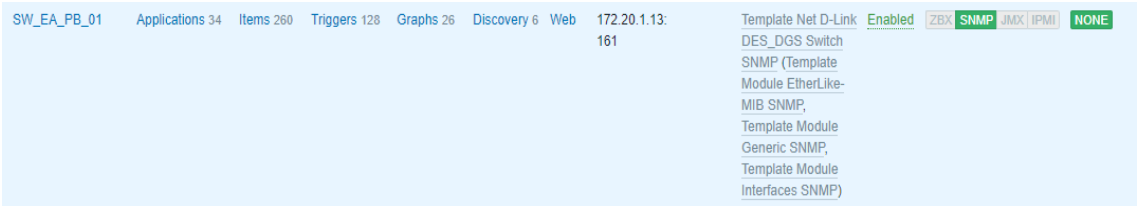


Para finalizar con el registro de un host se procede a insertar la macro, la cual tendrá un identificador sobre la comunidad a la que pertenezca, actualizamos cambios.

- **Macro**: variable de identificación del dispositivo.
- **Value:** comunidad a la que pertenece el equipo.



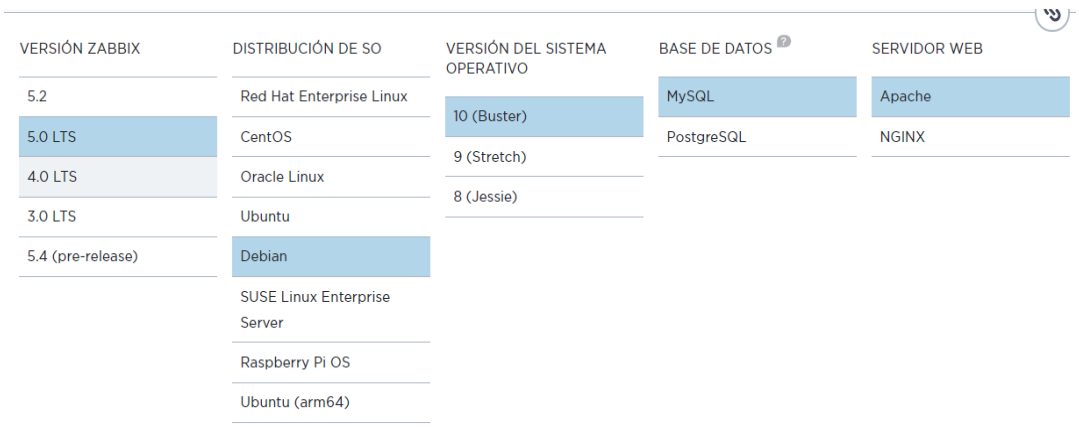
Visualización del dispositivo.



2.2.Host Agent SNMP

2.2.1. Servidor Debian

Selección de instalación de zabbix-agent del repositorio de página oficial de zabbix.



Descargar repositorio de zabbix en su versión 5.0 para Debian e instalar zabbix-agent.

```
# wget https://repo.zabbix.com/zabbix/5.0/debian/pool/main/z/zabbix-release/zabbix-release_5.0-1+buster_all.deb
# dpkg -i zabbix-release_5.0-1+buster_all.deb
# apt update
# apt install Zabbix-agent
```

Configurar Zabbix-agent.

```
# nano /etc/zabbix/zabbix_agentd.conf
Server=172.20.x.x
Listenport=10050
ServerActive=172.20.x.x
```

Iniciar y habilitar el Zabbix-agent en el servidor.

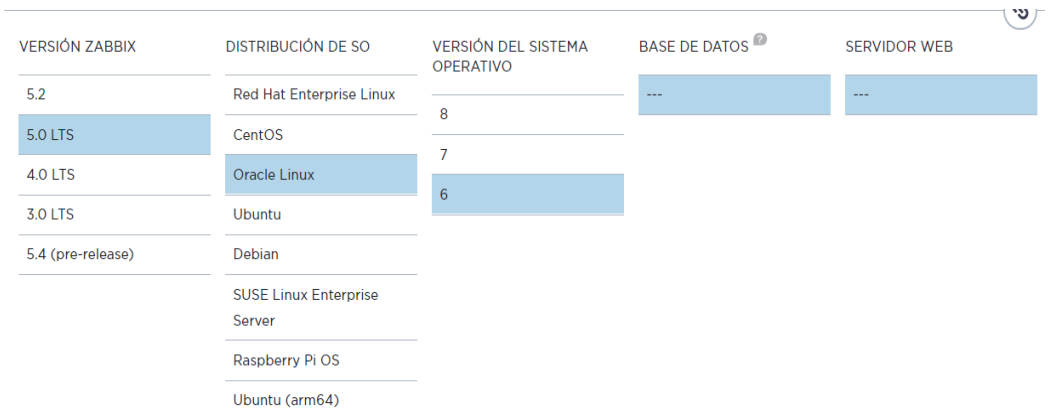
```
# systemctl start zabbix-agent
# systemctl enable zabbix-agent
```

Habilitar puerto 10050/tcp en el firewall y reiniciamos el agente.

```
# sudo ufw allow 10050/tcp
# systemctl restart zabbix-agent
```

2.2.2. Servidor Oracle Linux

Selección de instalación de Zabbix-agent del repositorio de página oficial de zabbix.



Descargar repositorio de zabbix en su versión 5.0 para Oracle e instalar el agente zabbix.

```
# rpm -Uvh https://repo.zabbix.com/zabbix/5.0/rhel/6/x86_64/zabbix-release-5.0-1.el6.noarch.rpm
# yum clean all
# yum install zabbix-agent
```

Configurar Zabbix agent.

```
# nano /etc/zabbix/zabbix_agentd.conf
Server:172.20.x.x
Listenport:10050
ServerActive: 172.20.x.x
```

Iniciar y habilitar Zabbix agent en el servidor.

```
# service zabbix-agent start
# chkconfig --level 35 zabbix-agent on
```

Habilitar puerto 10050/tcp en iptables y reiniciar el agente.

```
# iptables -A INPUT -i eth0 -p tcp --dport 10050 -m state --state NEW, ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -o eth0 -p tcp --sport 10050 -m state --state ESTABLISHED -j ACCEPT
# service zabbix-agent restart
```

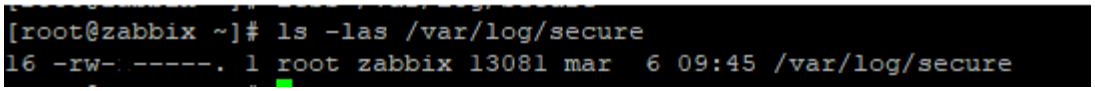
2.3. Log /var/log/secure

Vista de los logs de inicio de sesión en el servidor zabbix.

```
# les /var/log/secure
```

Para la monitorización de los logs en este caso el /var/log/secure log de autentificación del servidor Zabbix, es necesario tener permisos de lectura sobre este directorio, para ello como primer punto se verifica los permisos, por defecto tendremos que asignar estos permisos puesto que estos permisos solo están asignados para root.

```
# ls -las /var/log/secure
```



Asignar permisos de lectura para el usuario y grupo zabbix al directorio /var/log/secure. En este caso nos dirigimos a el directorio etc/logrotate.d el cual contiene toda la configuración de los logs.

```
# cd /etc/logrotate.d
# ll
```

Visualizamos los permisos que tiene la carpeta syslog, el cual contiene 5 archivos de logs para monitorizar, en cuanto a la monitorización tenemos el directorio /var/log/secure por lo que se procede a dar permisos de escritura al grupo zabbix.

```
# nano /syslog
create 0640 root zabbix
```

Permisos de lectura para el grupo zabbix, descrito en lo anterior se describe que “6” =usuario, “4” =grupo y “0” =otros.

rwx	7	Lectura, escritura y ejecución
rw-	6	Lectura, escritura
r-x	5	Lectura y ejecución
r--	4	Lectura
-wx	3	Escritura y ejecución
-w-	2	Escritura
--x	1	Ejecución
---	0	Sin permisos

permisos	pertenece
rwx------	usuario
---r-x---	grupo
------r-x	otros

Verificamos el grupo zabbix.

```
# getent group zabbix
zabbix:x:1000: zabbix
```

Para que se generen los cambios con los nuevos permisos, es necesario ejecutar la siguiente instrucción.

```
# logrotate --force syslog
```

Verificamos que los permisos estén hechos para el directorio /secure.

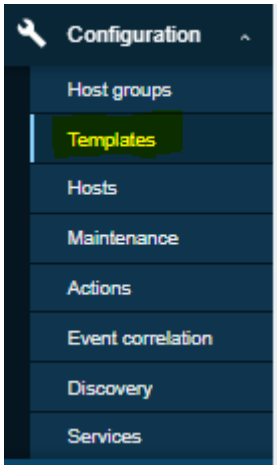
```
# cd /var/log
# ll
```

root@zabbix:/var/log

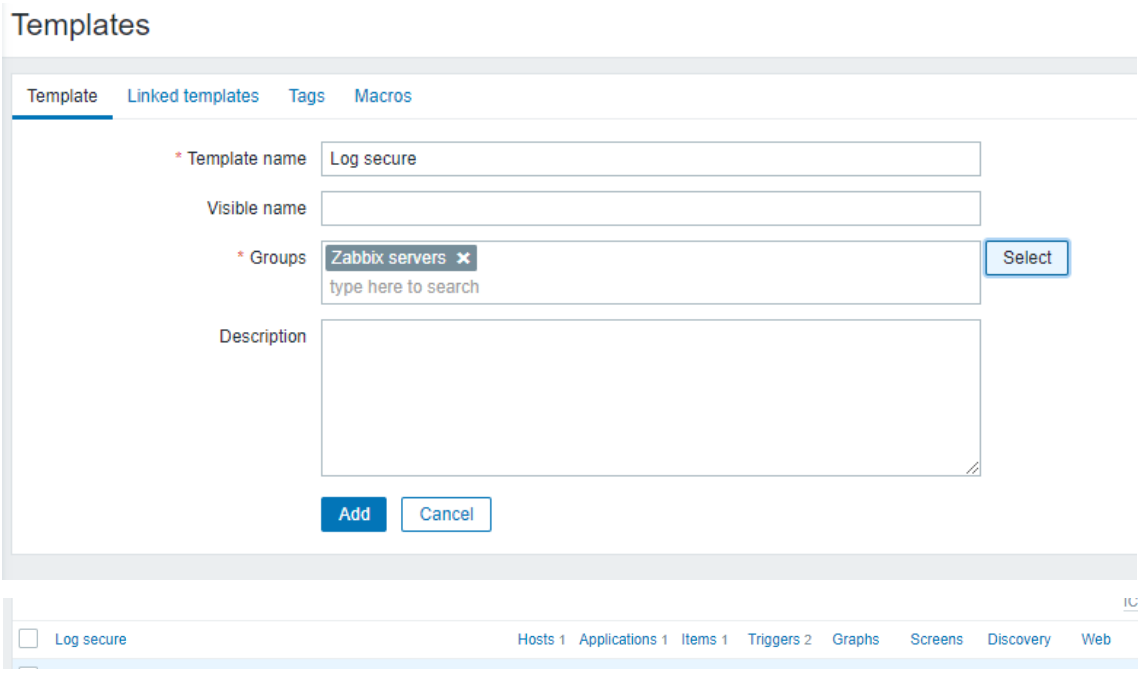
```
drwx------. 3 root    root          18 nov 16 11:30 libvirt
-rw-r-----. 1 root    zabbix         0 mar  6 10:04 maillog
-rw-------. 1 root    root         780 feb  4 17:10 maillog-20210207
-rw-------. 1 root    root        1920 feb 14 00:09 maillog-20210214
-rw-------. 1 root    root         768 feb 19 22:44 maillog-20210221
-rw-------. 1 root    root         576 feb 23 12:01 maillog-20210228
drwxr-x---. 2 mysql   mysql         25 feb  4 16:03 mariadb
-rw-r-----. 1 root    zabbix      8620 mar  6 10:07 messages
-rw-------. 1 root    root      902986 feb  7 03:39 messages-20210207
-rw-------. 1 root    root    29811993 feb 14 03:21 messages-20210214
-rw-------. 1 root    root    14515981 feb 21 03:28 messages-20210221
-rw-------. 1 root    root    15430511 feb 28 03:11 messages-20210228
drwxr-xr-x. 2 ntp     ntp           6 jun 23  2020 ntpstats
drwxr-xr-x. 3 root    root          18 feb  3 11:01 pluto
drwx------. 2 root    root          6 feb 27  2020 ppp
drwxr-xr-x. 2 root    root          6 ago  8  2019 qemu-ga
drwxr-xr-x. 2 root    root          6 feb  3 11:06 rhsm
drwxr-xr-x. 2 root    root       4096 mar  2 23:53 sa
drwx------. 3 root    root         17 dic 15 11:41 samba
-rw-r-----. 1 root    zabbix      2244 mar  6 10:07 secure
```

Una vez aplicado los permisos procedemos a configurar un nuevo template desde el frontend de zabbix.

Templates / create Template.

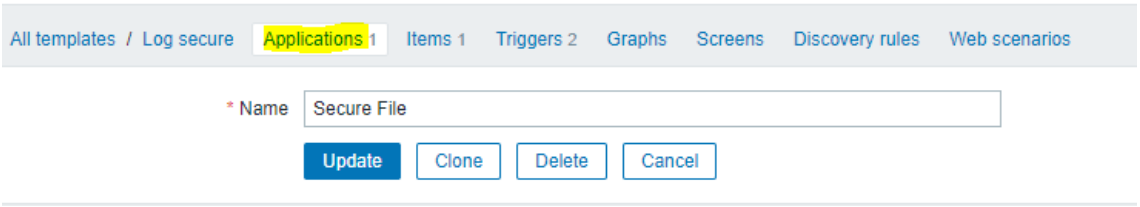


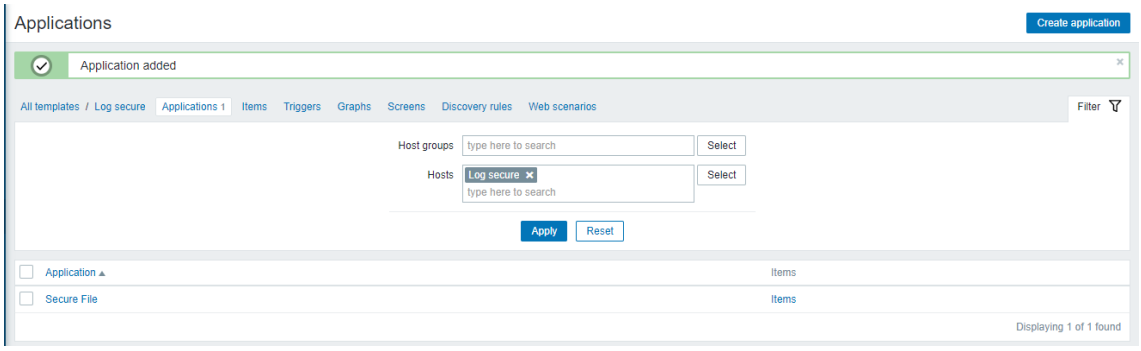
- **Template name**: nombre general de la plantilla.
- **Group:** Grupo al que pertenecerá la plantilla.
- **Descripcion**: una breve descripción del funcionamiento de la platilla.



Una vez creado el Template procedemos a crear una aplicación, esta será lo que se va a monitorear.

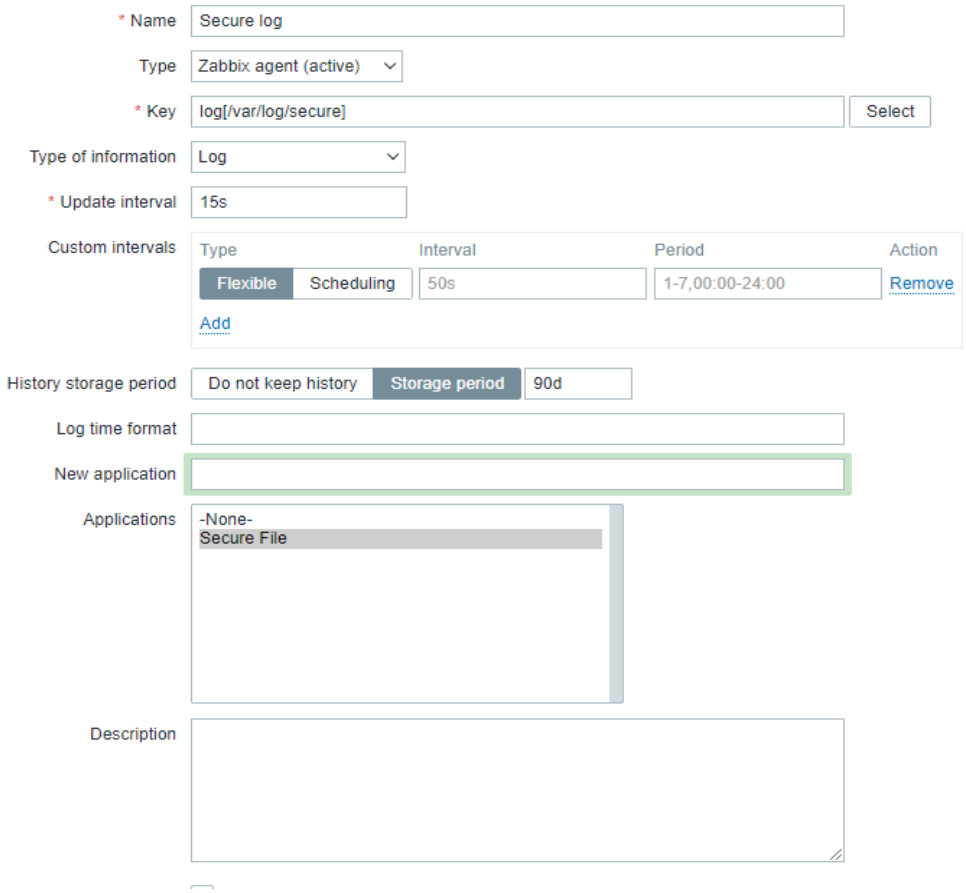
- Create aplication





Ya creada la aplicación, se procede a crear un Item y definir el tipo de monitoreo a realizar, en este caso será tipo de agente activo, el cual tendrá la capacidad de analizar el log de manera asíncrona. Definimos una key especificando que directorio se va a monitorear.

- **Name:** nombre del item
- **Type:** el tipo de monitoreo.
- **Key:** ruta del directorio a monitorizar.
- **Type of information:** formato de la información que devuelve.
- **Update Interval:** tiempo de actualización del log.

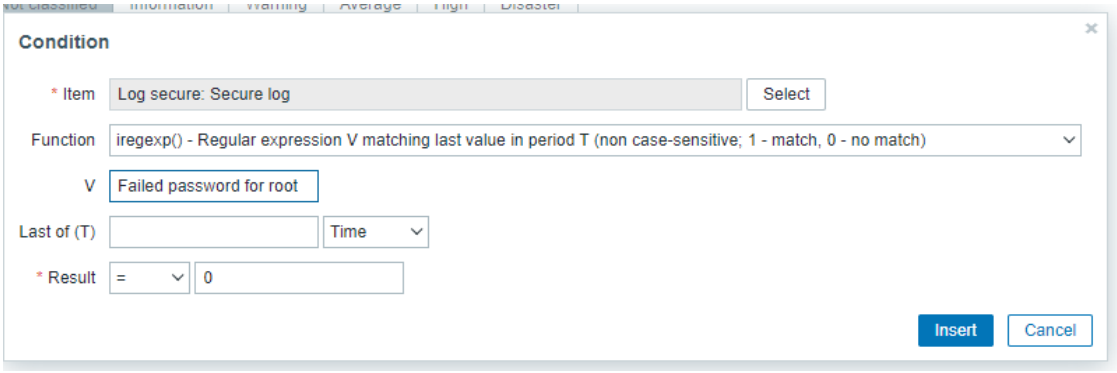


Agregamos el item.

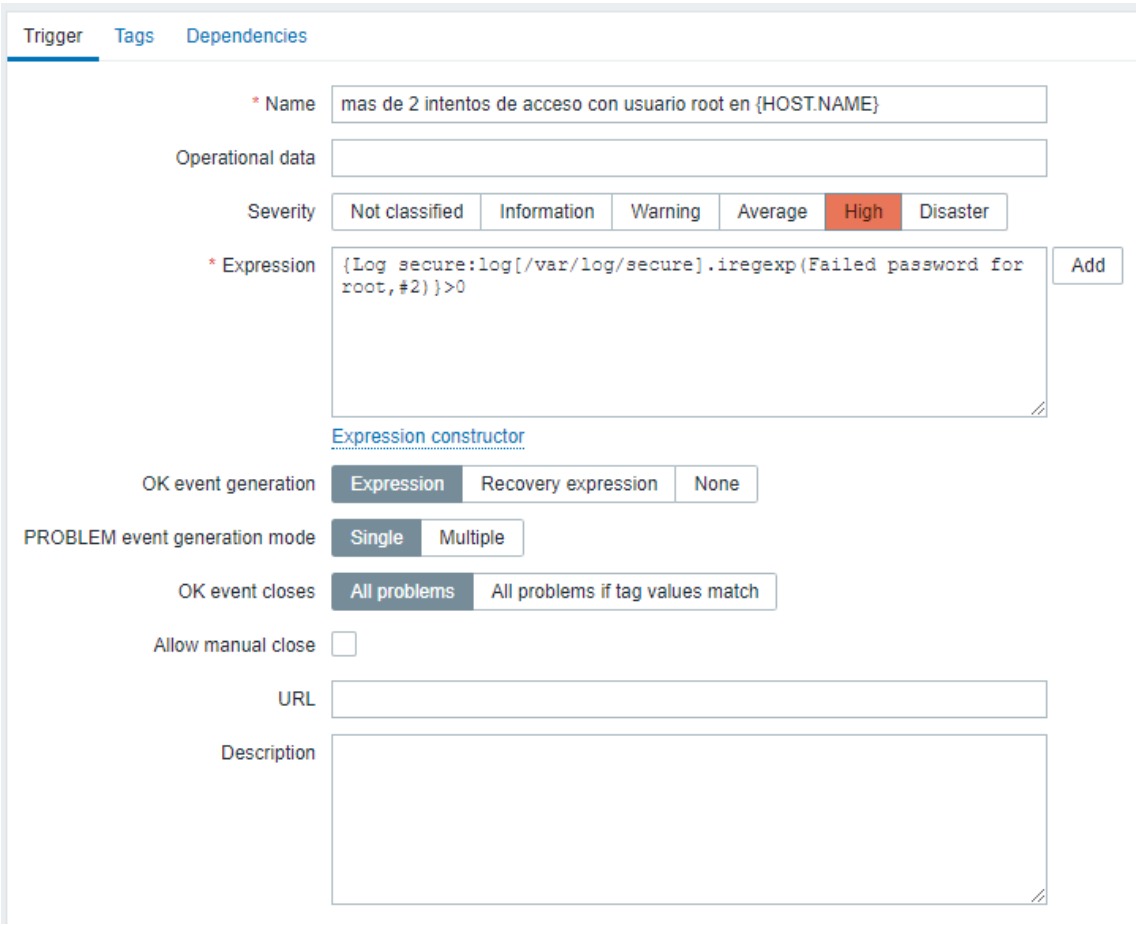
Name ▲	Triggers	Key	Interval	History	Trends	Type	Applications	Status
Secure log		log[/var/log/secure]	3s	90d		Zabbix agent (active)	Secure File	Enabled

Para la ejecución de alertas sobre el log creado es necesario la creación de un Trigger informando sobre si ocurre un evento, en este caso si un usuario intenta iniciar sesión por más de dos veces en el servidor zabbix.

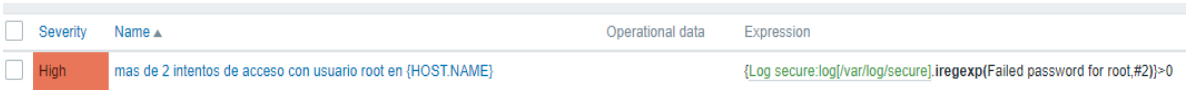
- **Severity:** Nivel de criticidad del problema.
- **Expression:** expresión que se ejecuta cuando ocurre este evento.



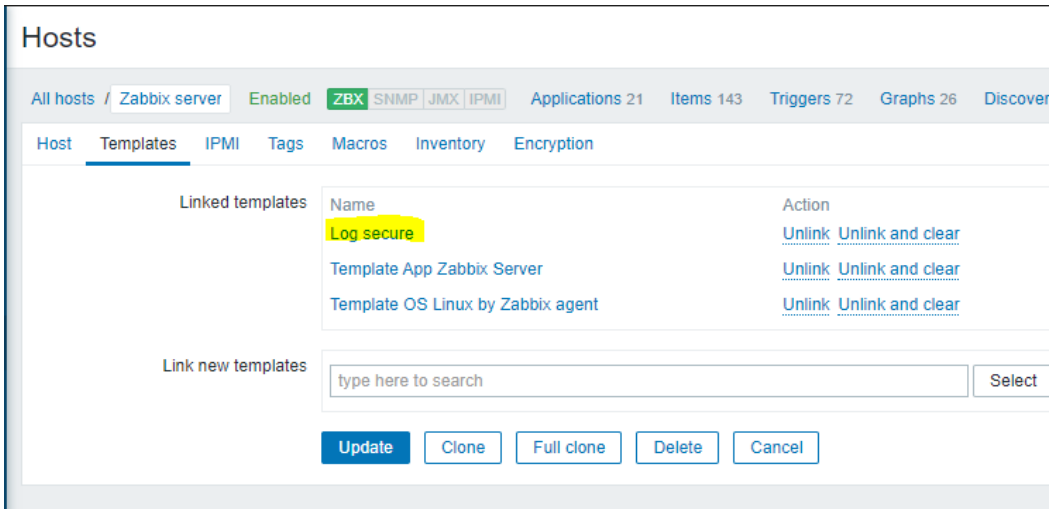
Configuración final.



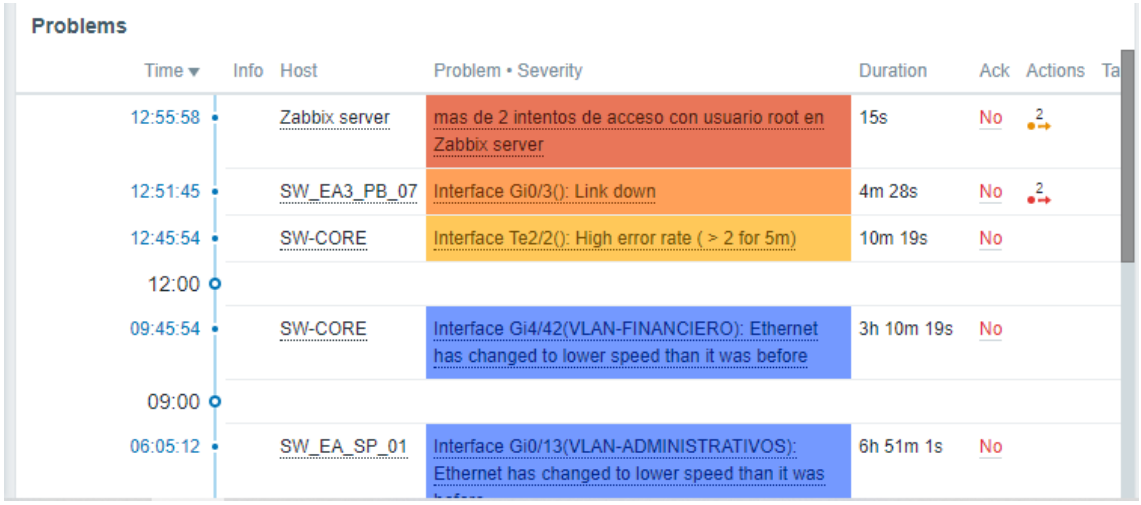
- Agregamos el trigger



Una vez creado el trigger procedemos a asignar el Template creado, para verificar el funcionamiento de este sobre el servidor zabbix.



Vista de la ejecución del trigger.

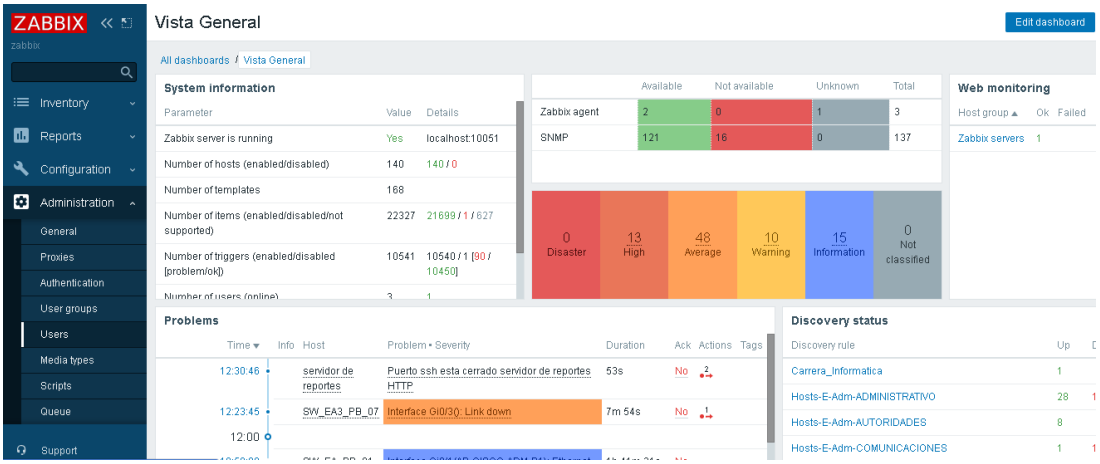


Además, zabbix incorpora un historial de estos logs.

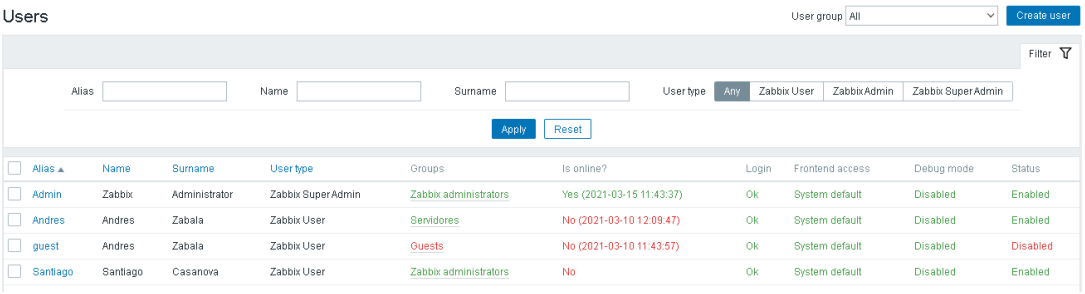
2.4.Usuarios.

Desde la vista general de la herramienta zabbix se nos permite la creación de distintos usuarios, cada uno con un rol especifico o administrador.

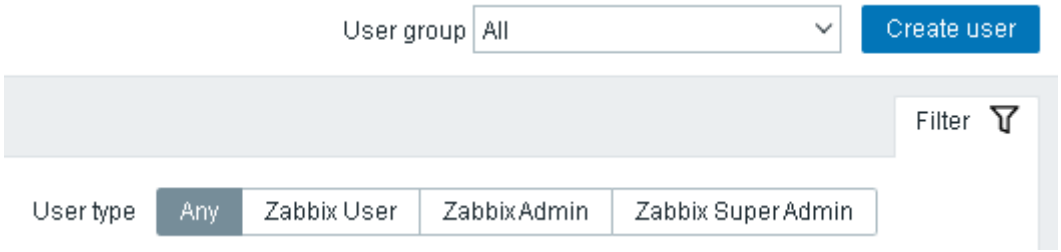
Ingresamos al panel principal en el desplegable “Administration” y la opción “Users”.



La opción “Users” nos permitirá observar un panel donde se precisa los usuarios habilitados y la creación de estos.



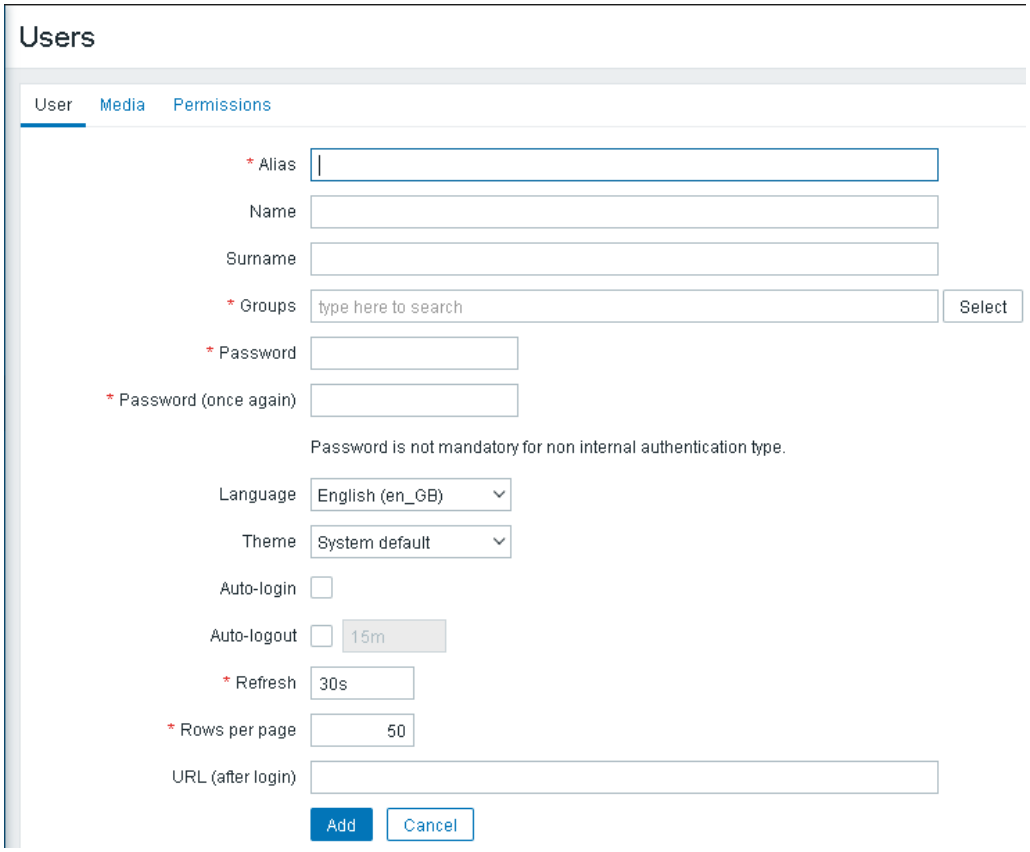
En el lado derecho tenemos la opción de “Create User” permitiendo la ampliación de una nueva ventana.



En la nueva ventana nos permite llenar un formulario el cual se empleara para obtener las credenciales necesarias para un nuevo ingreso.

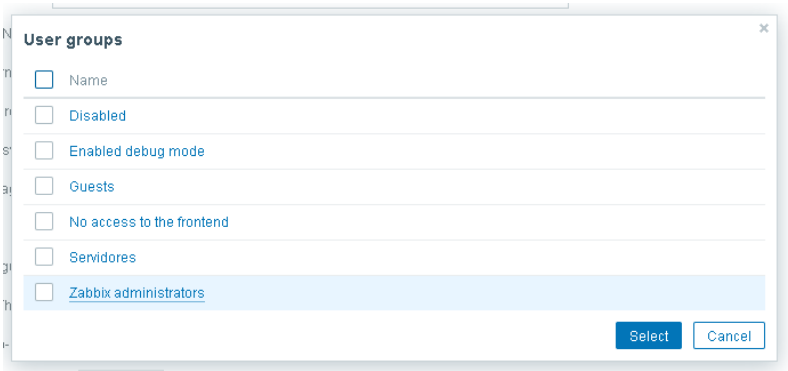
Subventana de User, ingreso de datos en el formulario.

- **Alias**: Nombre de usuario para el ingreso.
- **Name:** Nombre del usuario para reconocimiento por el administrador.
- **Surname:** Apellido del usuario.

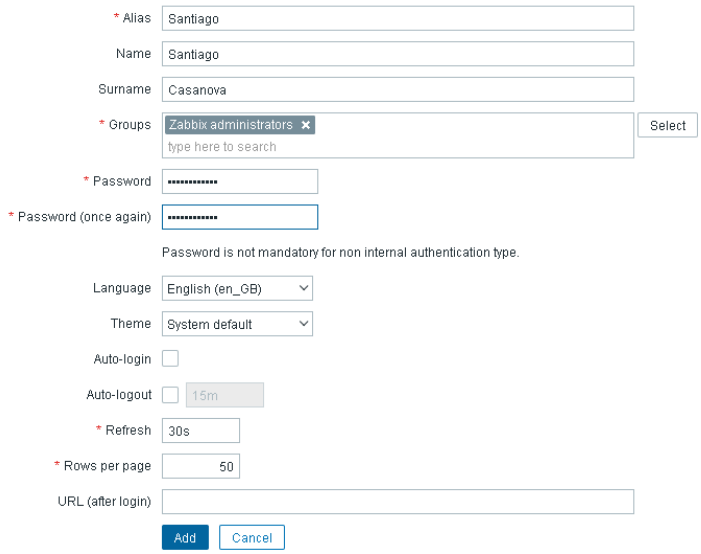


Asignación al grupo de usuarios al que se le permitirá el ingreso.

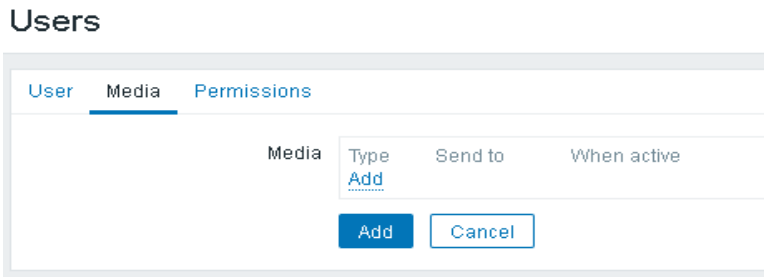
- **Groups:** Asignacion del administrador para el usuario.
- **Password:** Contraseña para el ingreso.



Formulario completo en todos los campos obligatorios y grupo de usuarios al que se tiene acceso.

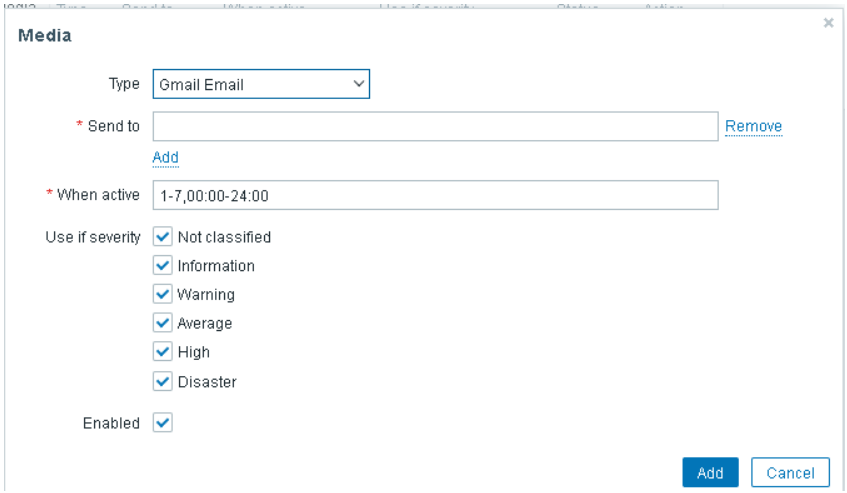


Ingreso a la subventana “Media”.

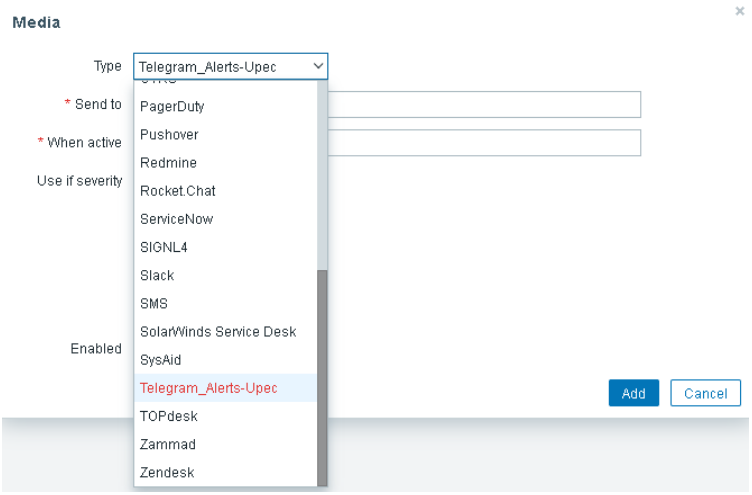


Creación de la “Media” en este caso:

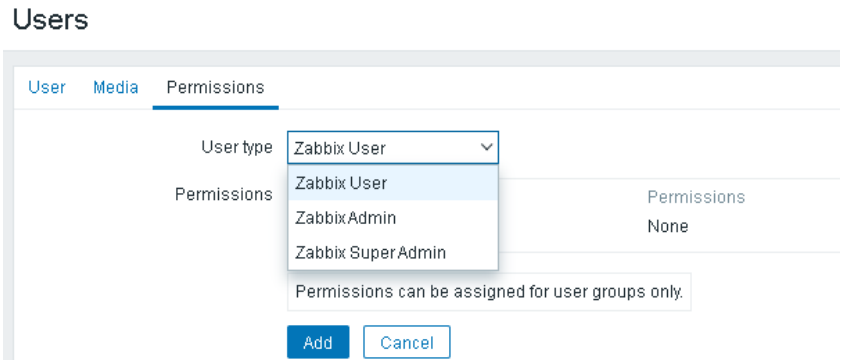
- Envió de alertas mediante de correo electrónico “Gmail”.



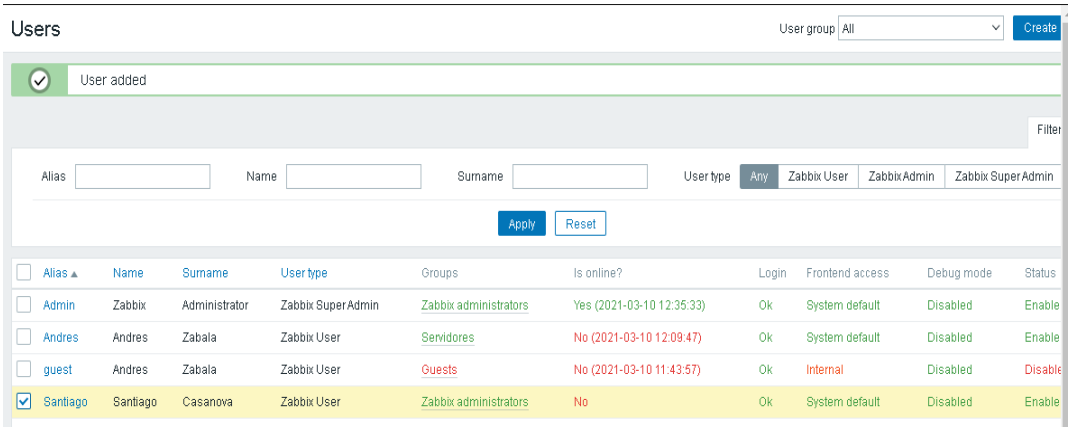
- Envió de alertas mediante de la red social Telegram.



Ingreso a la ventana “Permissions”, aquí se le otorgara los respectivos permisos dependiendo el tipo de usuario.



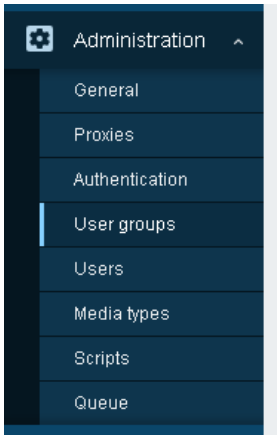
Verificación de la creación del usuario final, así como sus accesos y restricciones.



2.5.Grupos.

Desde la vista general de la herramienta Zabbix se nos permite la creación de distintos grupos de usuarios.

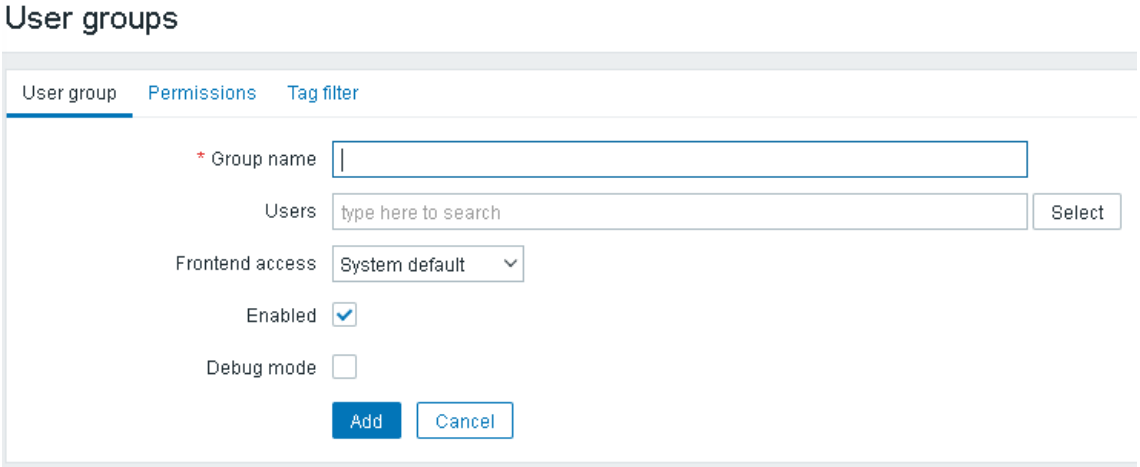
- Ingresamos al panel principal en el desplegable “Administration” y la opción “Users groups”.



En el panel de la ventana de “User Groups” se presenta un formulario el cual está compuesto por:

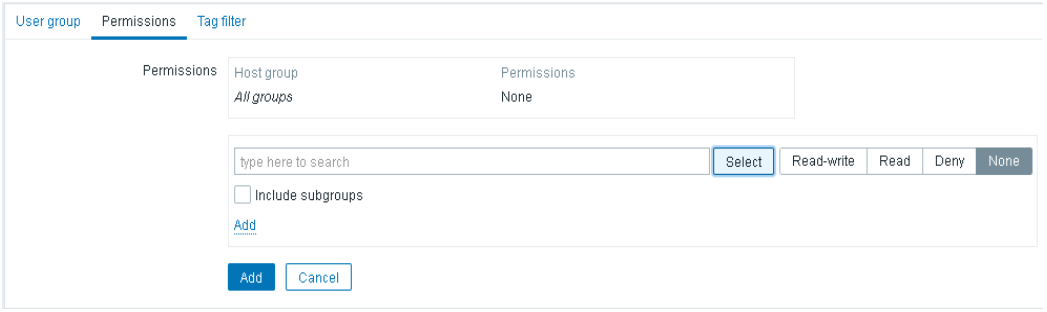
En la subventana “User group” se presenta un formulario con las siguientes características.

- **Group name:** el nombre del grupo que le asignara el administrador.
- **Users:** se podrá añadir los usuarios que se deseen.

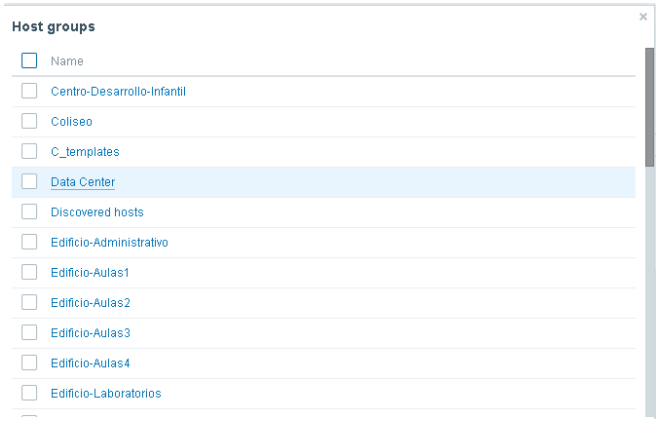


- Agregar usuario.

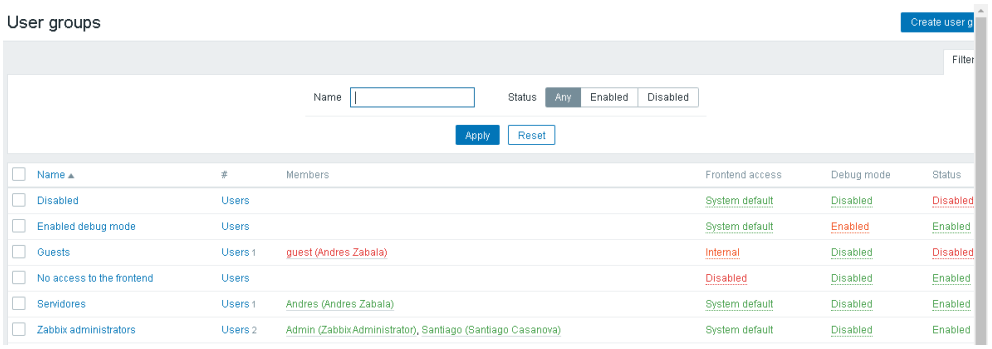
- En la subventana “Permissions” podemos añadir los grupos que el administrador crea conveniente, además se añade las reglas de “Lectura y Escritura”.



- Selección del grupo de dispositivos los cuales monitoreara dicho usuario creado.



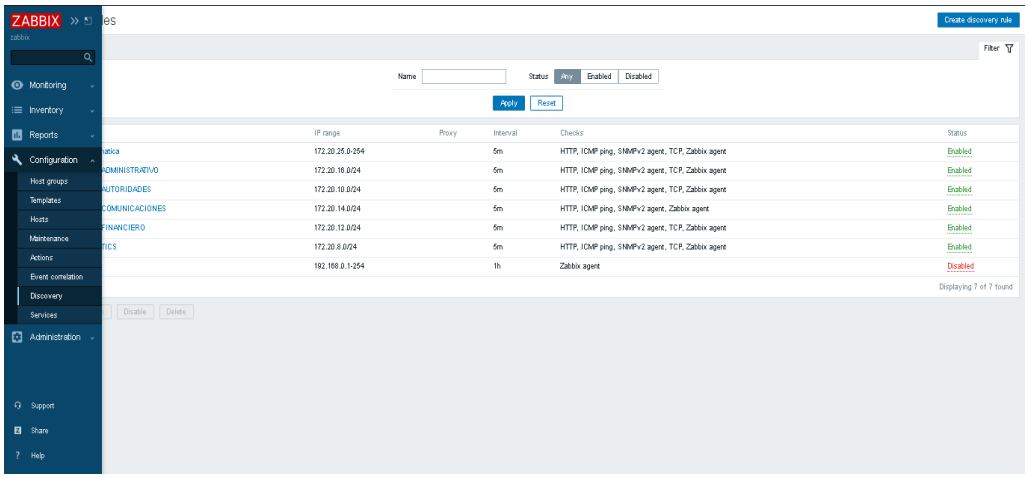
Al haber finalizado el proceso se mostrará los respectivos grupos de usuarios con los usuarios creados con anterioridad, y estos ya tendrán los permisos de acceder sea a parte de la información o toda la información.



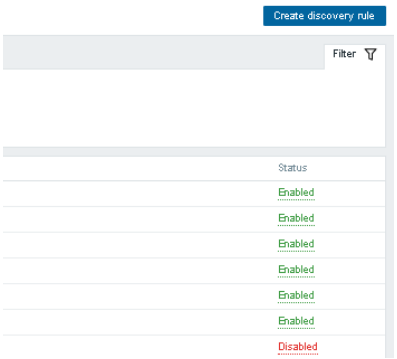
2.6.Autodescubrimiento

En la creación de una acción el administrador de la red puede configurar y mantener las reglas de correlación de los elementos.

Seleccionamos en la parte del panel izquierdo “configuration” y escogemos la opción “Discovery” dirigiéndonos a un panel completo de la creación de reglas de descubrimiento.

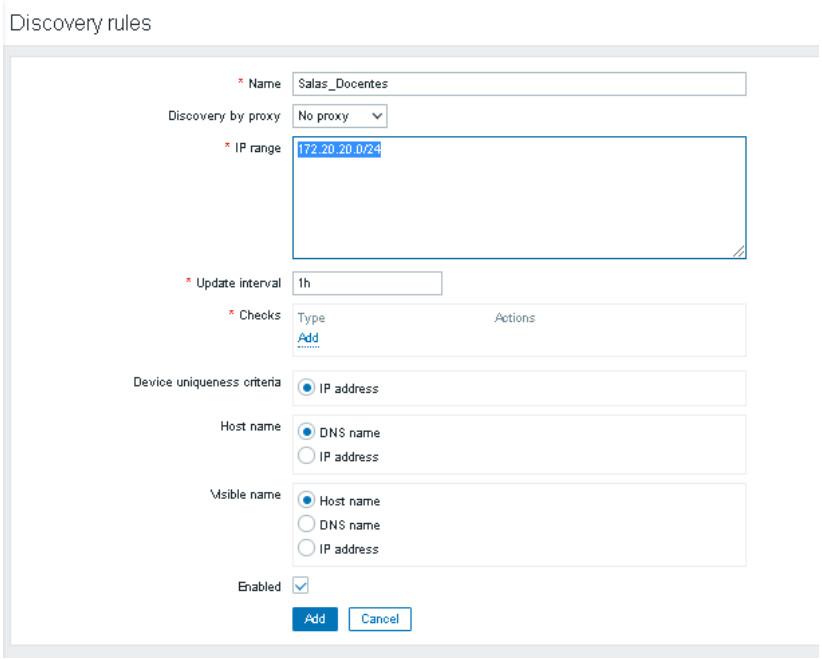


Ya en el panel nos muestra al lado derecho un botón color azul “Create Discovery rule” hacemos clic en este.

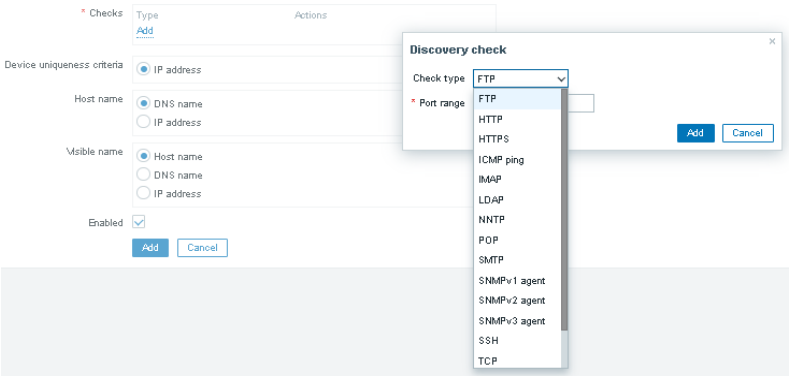


Ya en el panel de “Create Discovery rule” continuamos llenando la información requerida.

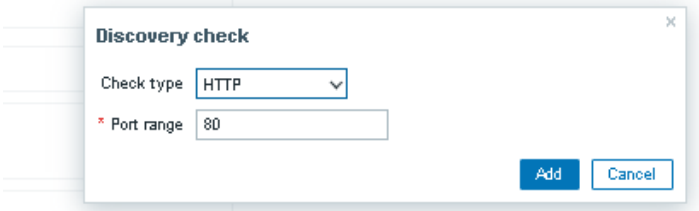
- **Name:** podemos poner el nombre con el cual se identificará esa regla.
- **IP range:** rango de ip a ser monitorizada con su respectiva mascara de subred.
- **Update interval:** el intervalo de la actualización de la regla.



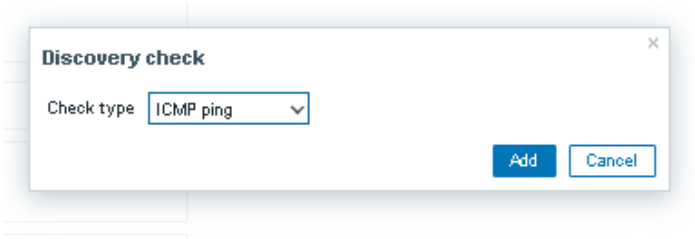
En las opciones de chequeo del descubrimiento nos permitirá distintas opciones y ya que en el caso de Wireless escogeremos las siguientes:



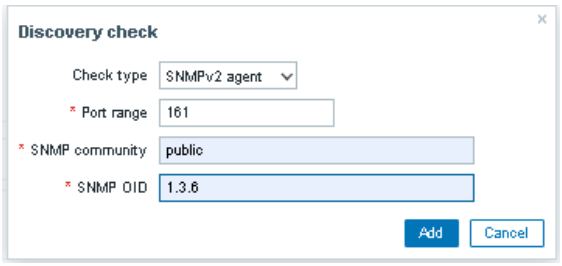
- Check Type: HTTP.
- Port Range: 80.



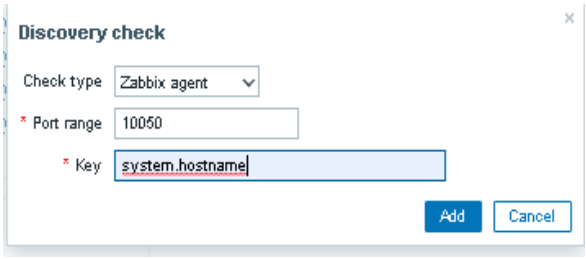
- Check Type: ICMP ping.



- Check Type : SNMPv2 agent.
- Port range: 161.
- SNMP community: public.
- SNMP OID: 1.3.6.



- Check Type: Zabbix agent.
- Port range: 10050.
- Key: system.hosname.



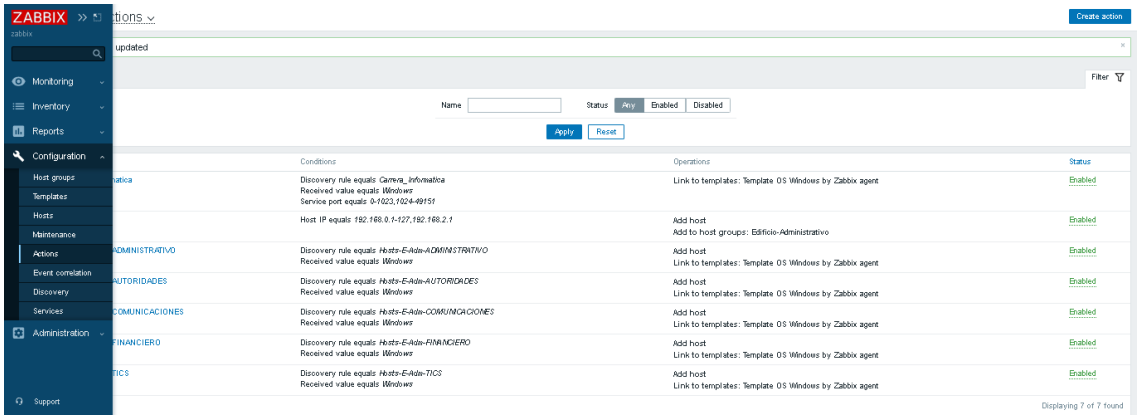
Al terminar de configurar los tipos de chequeo de autodescubrimiento añadimos la regla, la cual nos permitirá conocer la siguiente información

- Nombre identificador.
- Rango de IPs monitoreadas.
- Intervalo de tiempo en actualizar.
- Tipos de chequeo para monitorear.
- Estado de la regla (habilitado/inhabilitado).

2.6.1.Acciones

Esta funcionalidad de auto descubrimiento, en realidad es una acción que se ejecuta cuando un cliente arranca, en el momento informa al server de que está vivo y le pasa información como el nombre, la ip y entre otros datos el HostMetadata que es lo que utilizaremos para configurar la acción de autodescubrimiento.

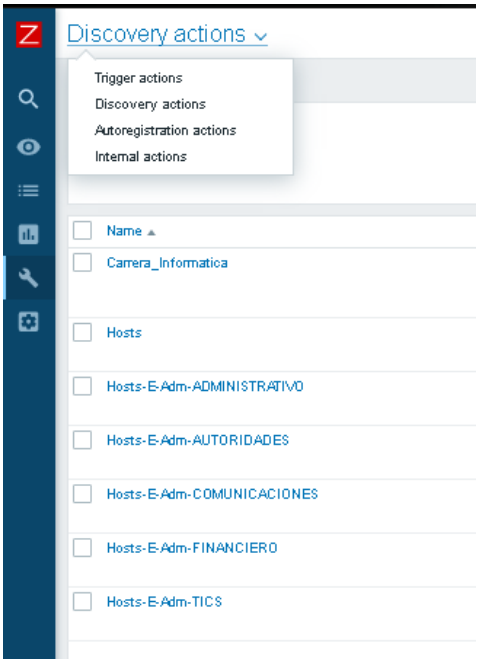
Seleccionamos “configuration” y escogemos la opcion “Actions”, donde nos dirigira a una ventana donde se mostraran las acciones ya realizadas o en ejecucion.



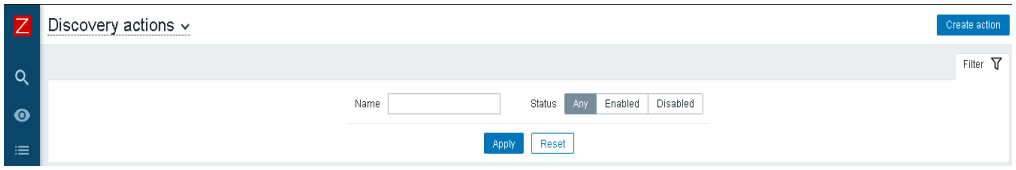
Al ingresar en la ventana de “actions” nos mostrara la opcion de:

- Trigger actions.
- Discovery actions.
- Autoregistration actions.
- Internal actions.

Al mostrar las diferentes opciones, escogemos “Discovery actions” la cual nos permitira realizar una regla de descubimiento.



Al escoger la opcion “Discovery actions” nos mostrara la ventana siguiente donde pincharemos la opcion “create action”.

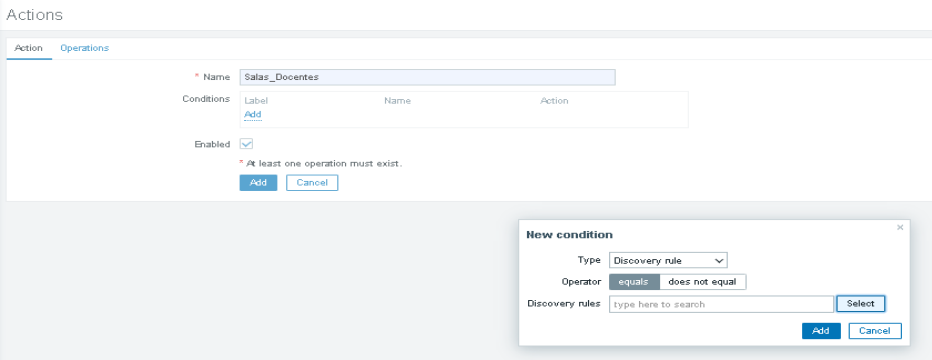


Al crear la accion nos mostrara la ventana de formulario donde colocaremos los datos:

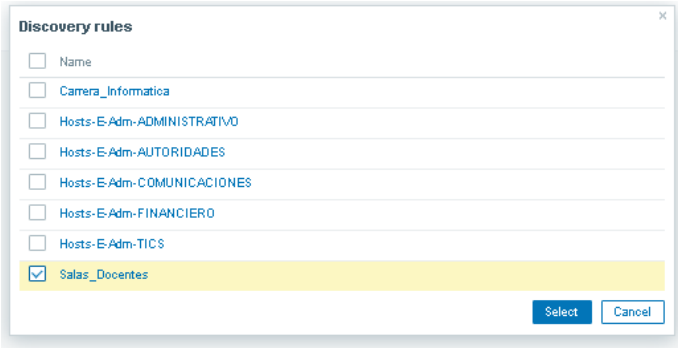
- Nombre de la accion.
- Condicion de la accion.

En la nueva condicion colocamos lo siguiente:

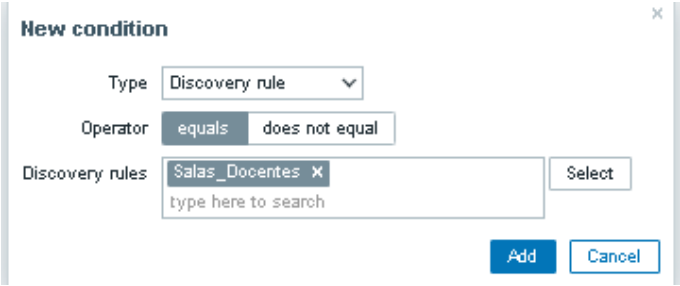
- **Type: Discovery rule,** donde se colocara el nombre de la regla creada anteriormente para tener concordancia.
- **Operator:** equals.



En la selección, elegimos el nombre de la accion creada.

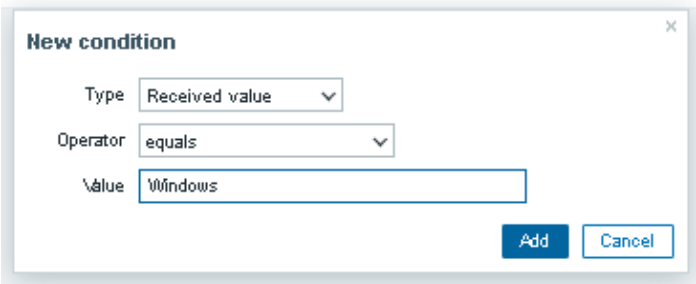


Nueva condicion.



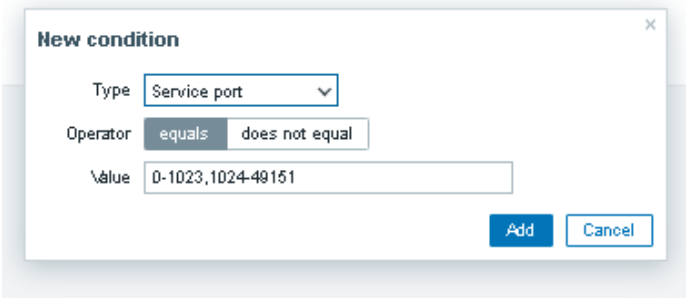
Una nueva condicion al conseguir los datos de la accion creada seria la evaluacion del sistema operativo con el cual estaria trabajando el dispositivo que se estaria monitoreando.

- **Type:** Received value.
- **Operator:** equals.
- **Value:** windows.

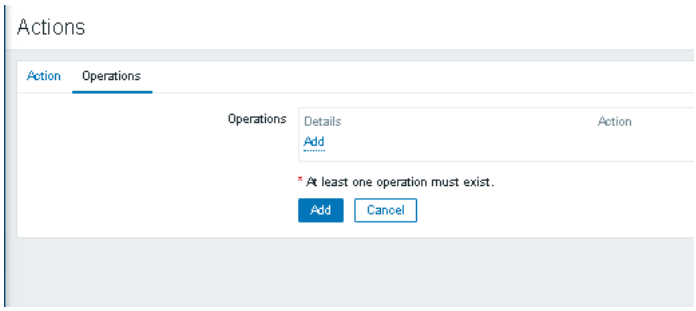


La condicion en este caso sera permitir monitorear todos los puertos disponibles en un rango que se crea conveniente o especifico.

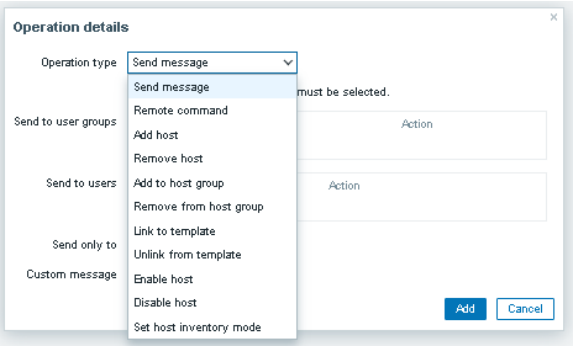
- **Type:** Service port.
- **Operator:** equals.
- **Value:** 0-49151.



Cambiaremos a la nueva subventana donde nos mostrara “operations” y se nos permitira añadir operaciones.

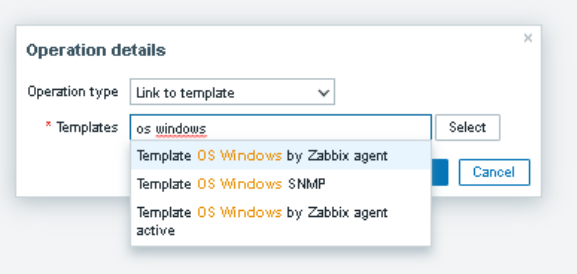


Nos permitira distintas opciones entre ellas y las que mas neceasariamente son para este tipo de accion es:

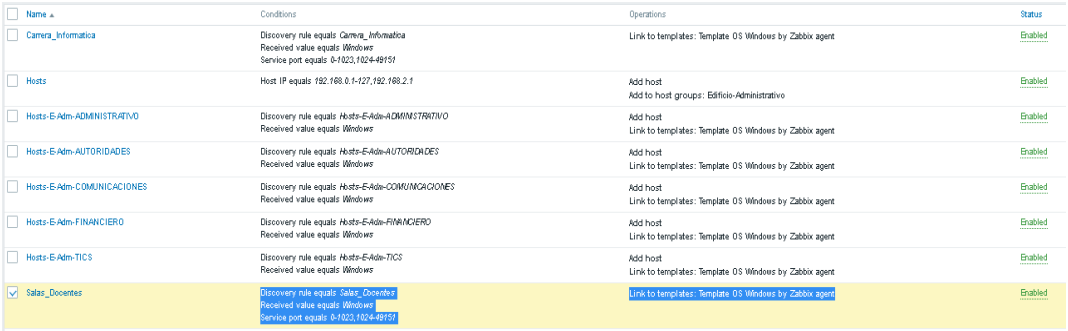


Escogeremos la opcion de:

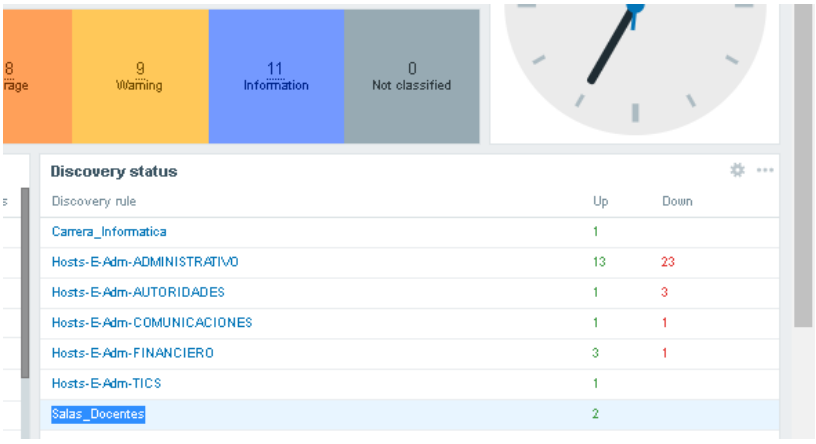
Link to template: En este caso nos permite la opcion de escoger el template que mejor se ajuste a las opciones de busqueda, conociendo las diferentes macreos que trabajan en dico template.



Al haber creado la accion se nos mostrara las condiciones y operaciones que se la ha impuesto anteriormente.



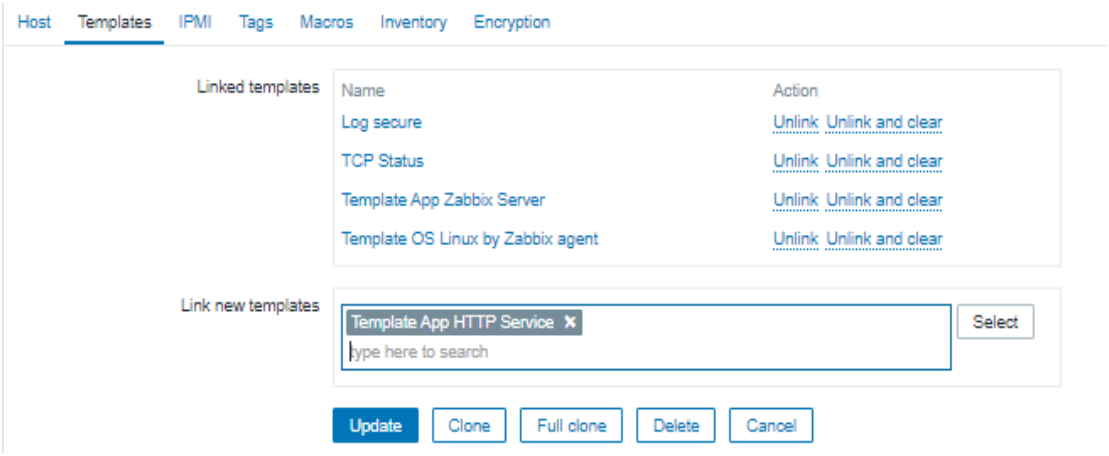
Ya en la vista general en el apartado de lado derecho se puede observar la distintas acciones creadas y los hosts que han sido añadidos por autodescubrimiento al haber creado las reglas y acciones.



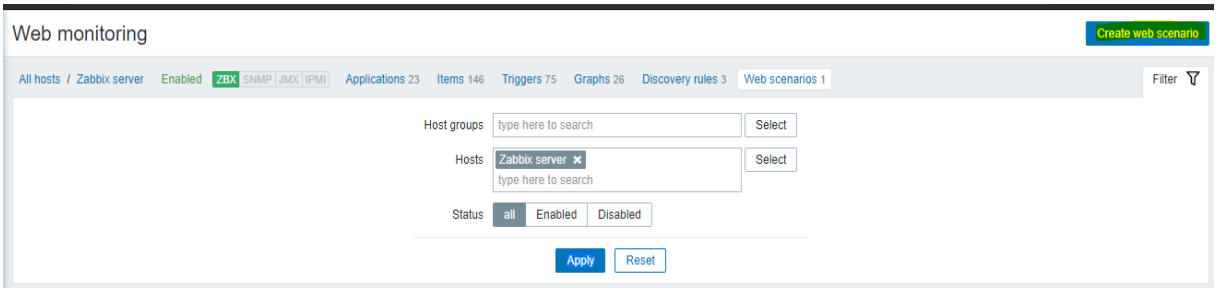
2.7. Web escenarios

Los web escenarios permiten monitorear un sitio web sin necesidad de instalar un agente o activar el protocolo SNMP.

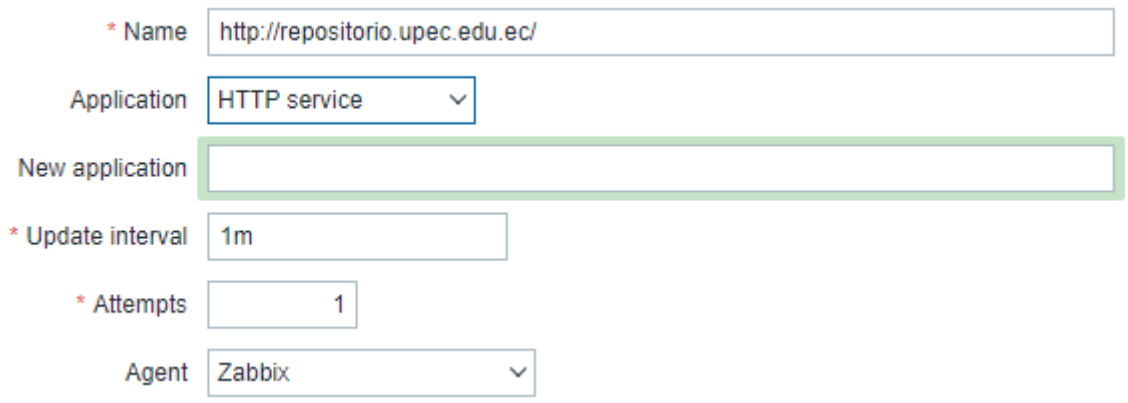
Para añadir un web escenario se debe crear un nuevo host o usar uno ya existente en el cual se monitorizará el servicio, en este caso se usará el servidor zabbix en el cual se deberá integrar la plantilla de monitoreo HTTP.



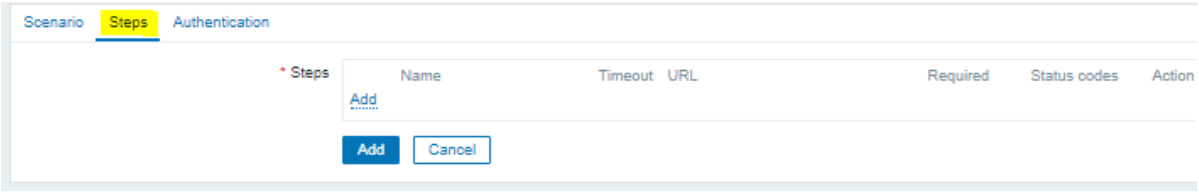
Una vez añadido la plantilla procedemos a la creación del web escenario.



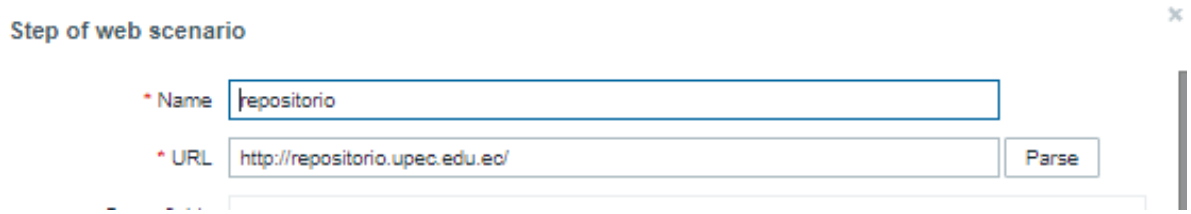
Agregamos el enlace de nuestro web escenario con la aplicación HTTP y los demás campos los dejamos en blanco por defecto.



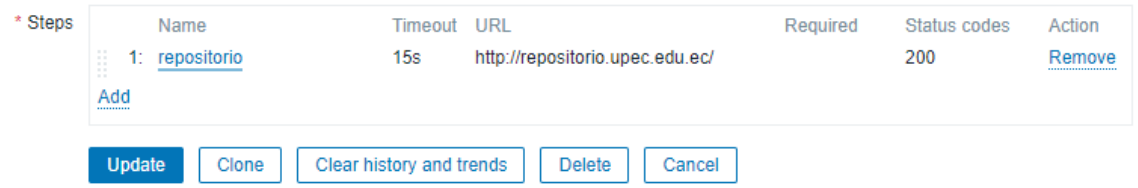
Se procede a el apartado de Steps.



Agregamos el nombre y la url a monitorizar, consecuentemente agregamos un valor de 200 en requiered status code y guardamos los cambios.



Una vez guardados los cambios se visualizará el web escenario.



En el apartado de lates data del servidor zabbix se podrá visualizar todos los datos recogidos del sitio web.

HTTP service (7 Items)			
Download speed for scenario "http://repositorio.upec.edu.ec/".	2021-03-29 23:08:06	373.02 KBps	-2.84 KBps
Download speed for step "repositorio" of scenario "http://repositorio.upec.edu.ec/".	2021-03-29 23:08:06	373.02 KBps	-2.84 KBps
Failed step of scenario "http://repositorio.upec.edu.ec/".	2021-03-29 23:08:06	0	
HTTP service is running	2021-03-29 23:08:25	Up (1)	
Last error message of scenario "http://repositorio.upec.edu.ec/".			
Response code for step "repositorio" of scenario "http://repositorio.upec.edu.ec/".	2021-03-29 23:08:06	200	
Response time for step "repositorio" of scenario "http://repositorio.upec.edu.ec/".	2021-03-29 23:08:06	72.29ms	+0.55ms

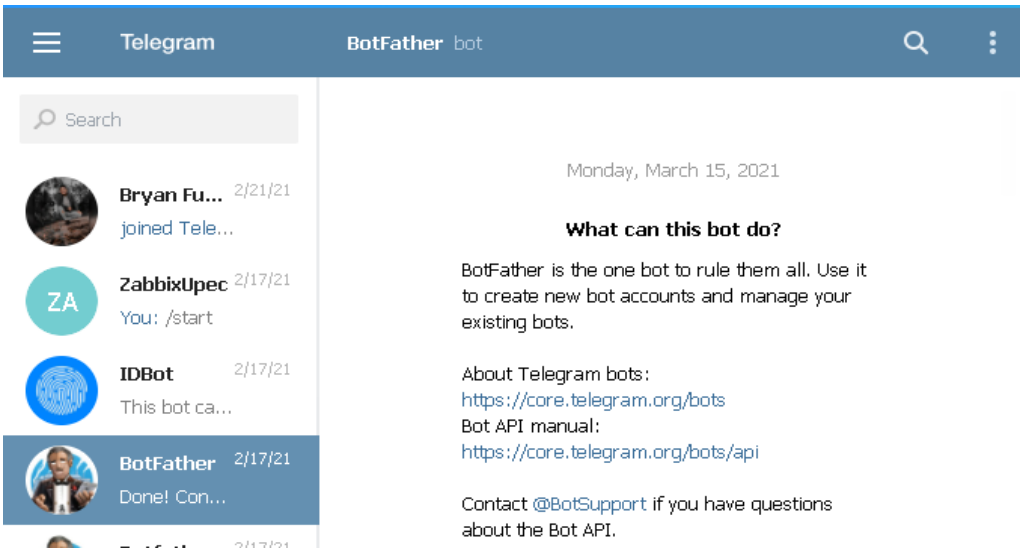
3. MEDIOS DE NOTIFICACIÓN

3.1.Telegram

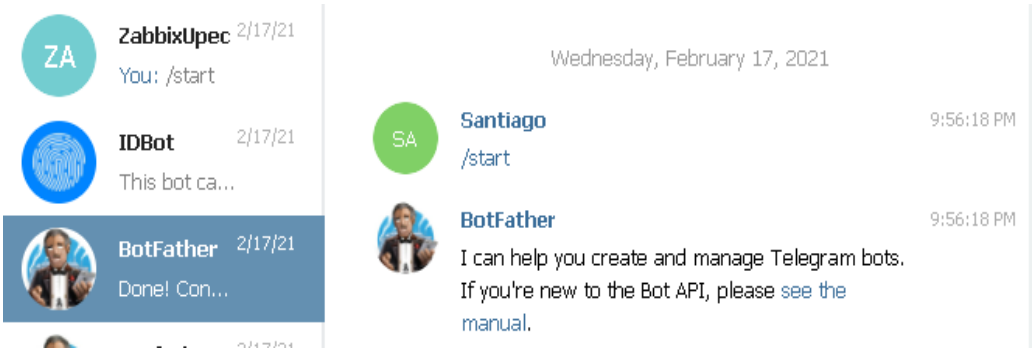
Los pasos serán los siguientes:

Creamos y configuramos el bot en telegram.

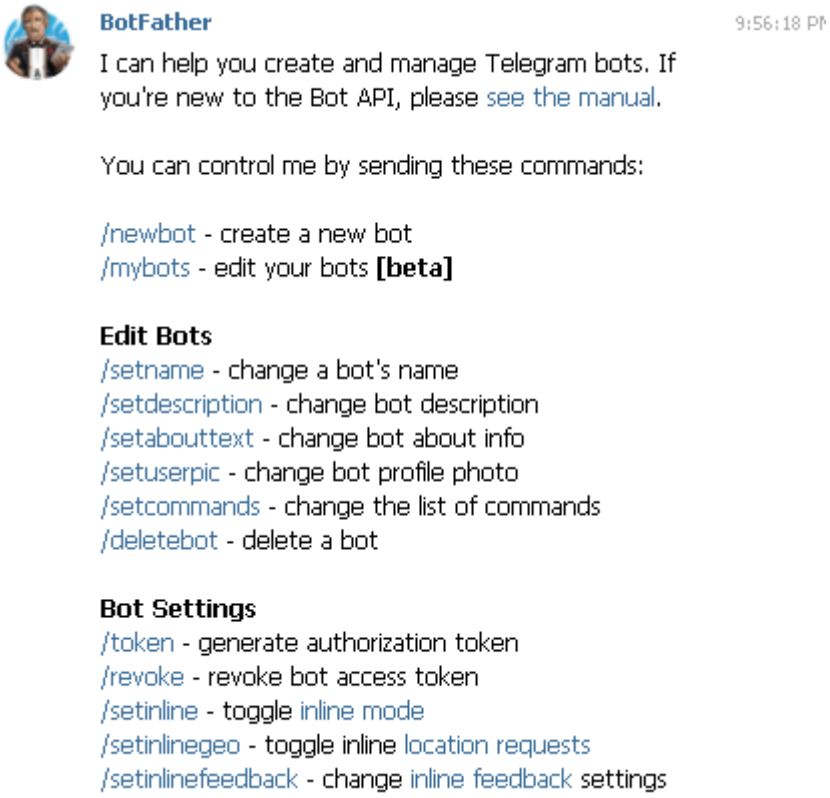
Ingresamos a él bot de telegram sea desde el móvil o telegram web.



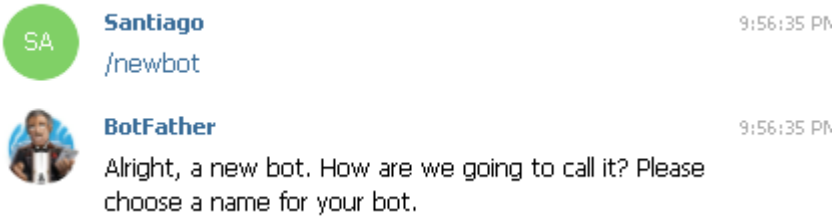
Añadimos el comando /start para la confirmación de inicio dentro del bot.



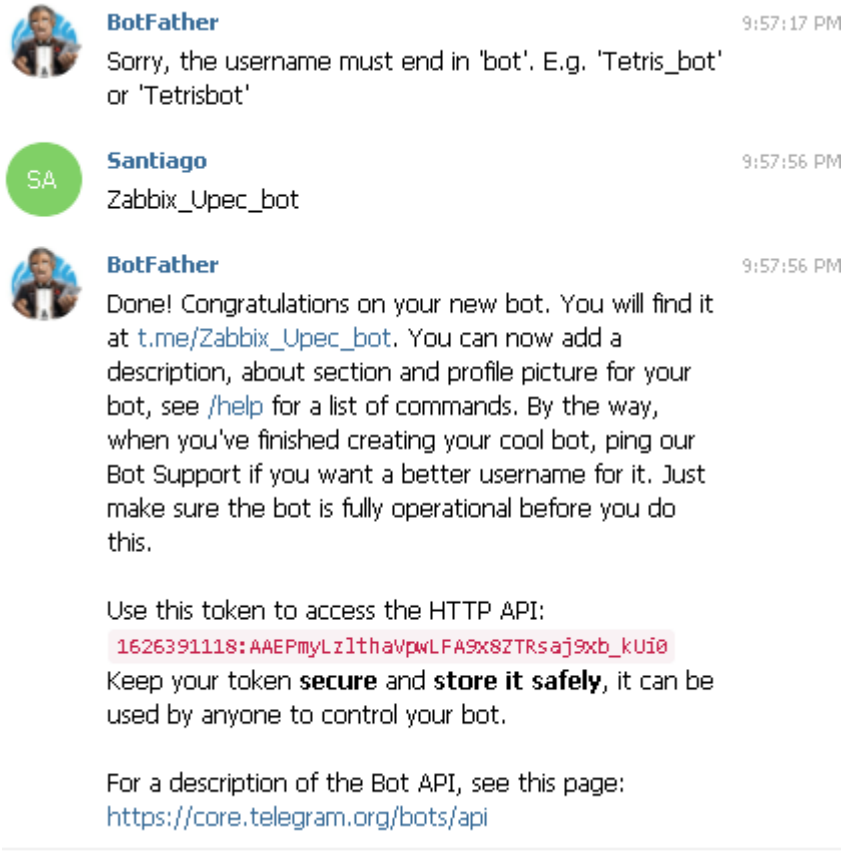
Escoger la opción indicada dentro de las posibilidades que este comando muestra.



Elección de opción más idónea para el caso.

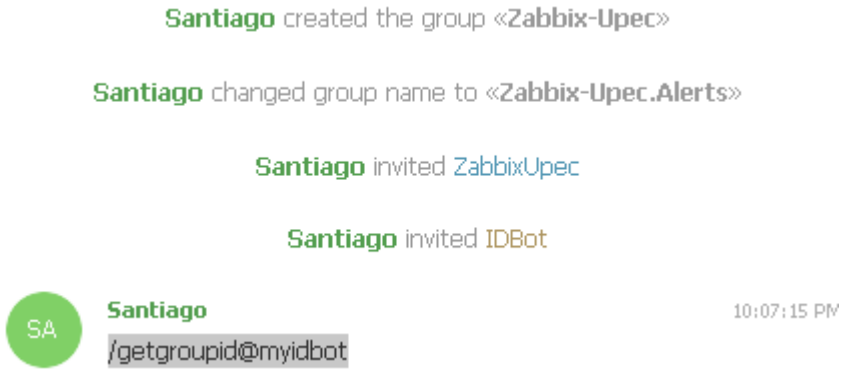


Creación de nuevo bot para uso de las alertas internas de Zabbix. Siguiendo el ejemplo que se muestra se crea el nuevo bot el cual adicional a este nos entrega una API para un acceso determinado.



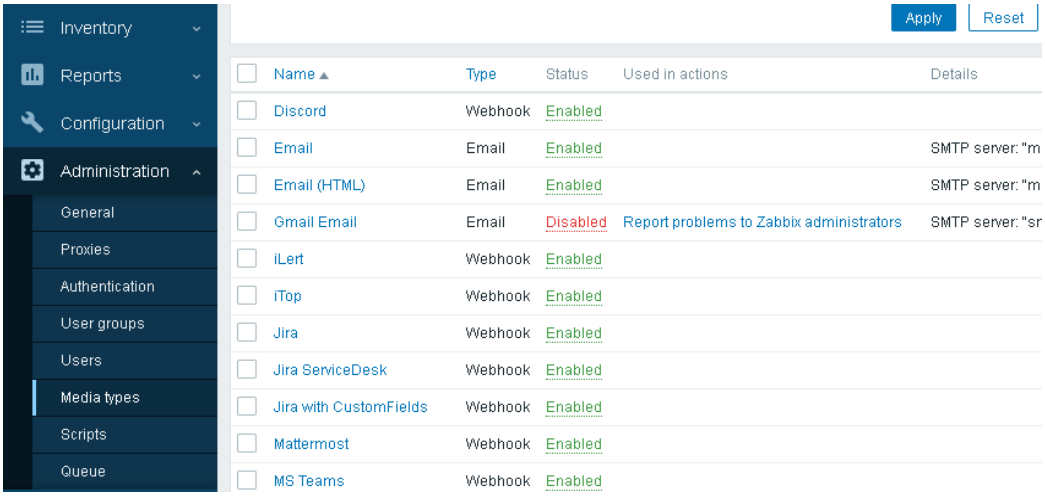
Adicionalmente, se crea un grupo donde los usuarios que recibirán las alertas a diario y cumpliendo las 24 horas del día 365 días al año.

Obtendremos el ID del grupo mediante el siguiente comando **/getgroupid@myidbot.**

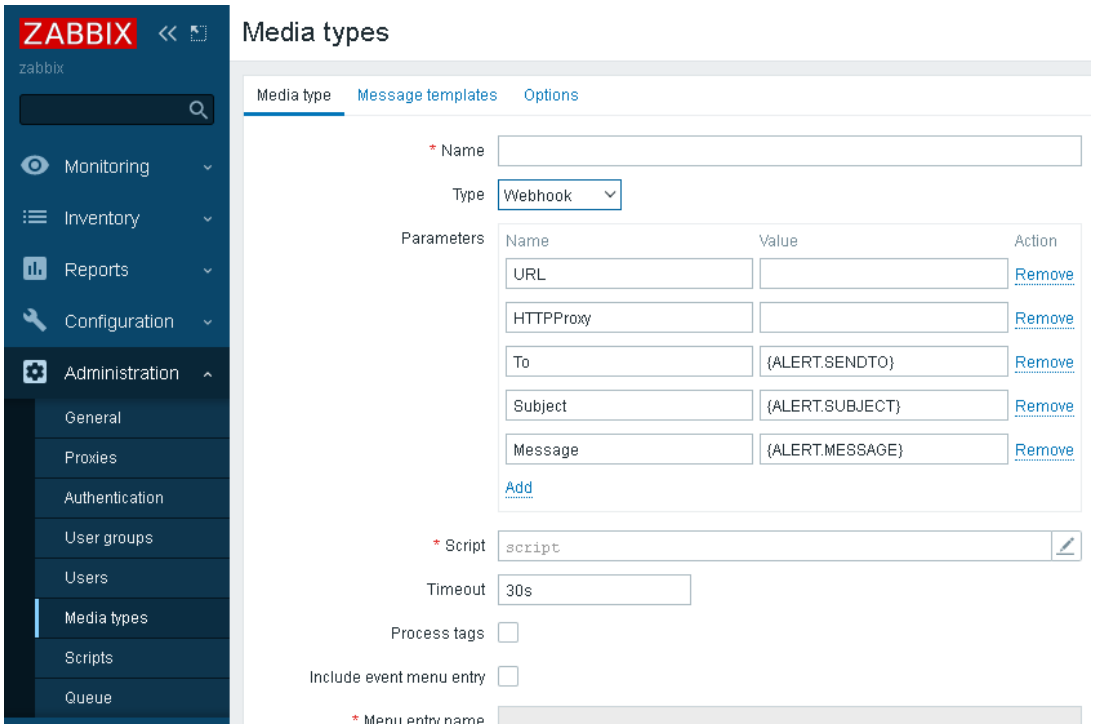


Configuramos la Media de telegram en el zabbix frontend

Ingresamos a la opción “Adinistration” seguido de “Media types”, donde se nos mostrara distintas opciones de configuración de alertas



En caso de no tener preconfigurada la opción que se desea, se procede a la creación de una nueva “Media types”



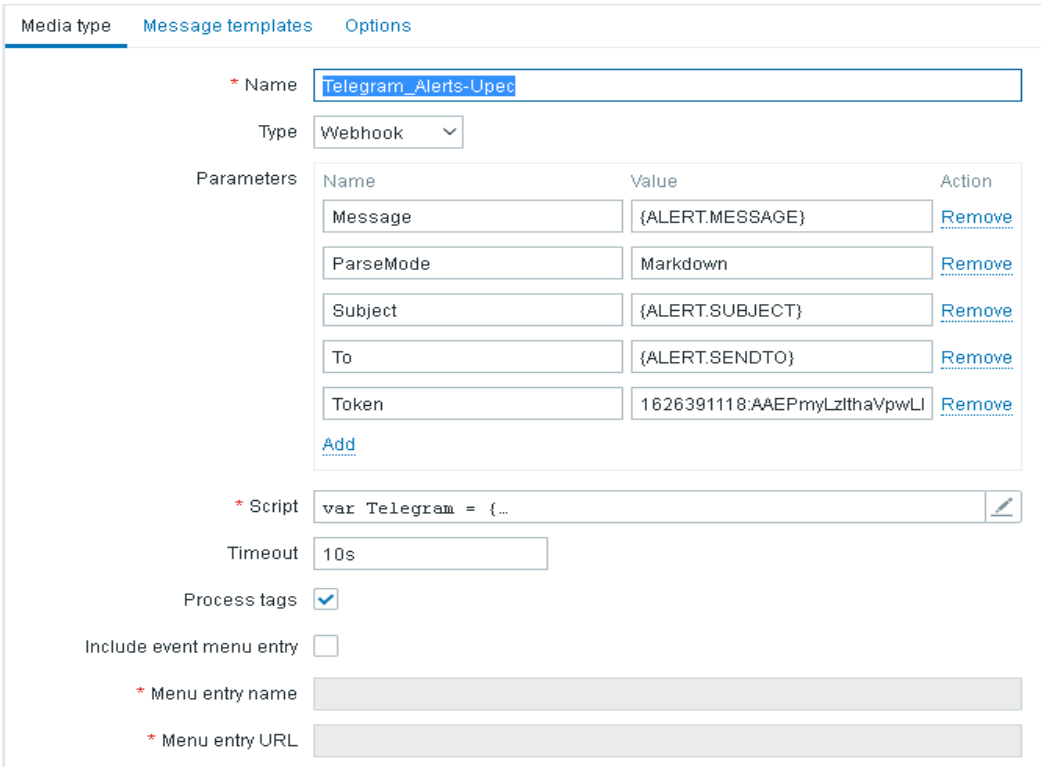
En el formulario que se muestra por “Media Type” se procede a llenar de la siguiente manera.

- **Name:** Nombre asignado por el administrador.
- **Type:** WEBHOOK.

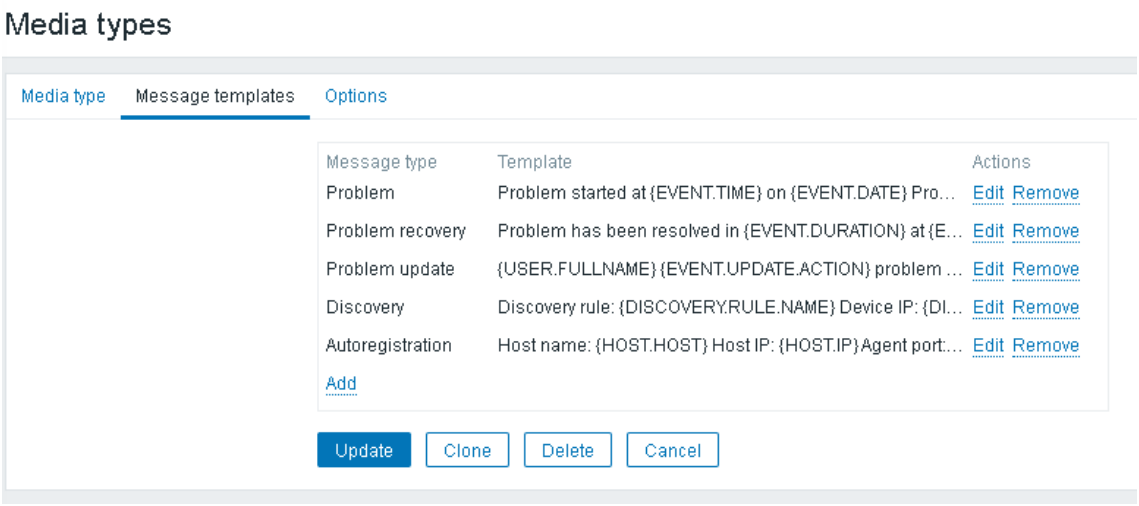
Parámetros

- **Message**: {ALERT.MESSAGE}
- **ParseMode**: Markdown
- **Subject**: {ALERT.SUBJECT}

- **To**: {ALERT.SENDTO}
- **Token**: Administrado por el bot de telegram.

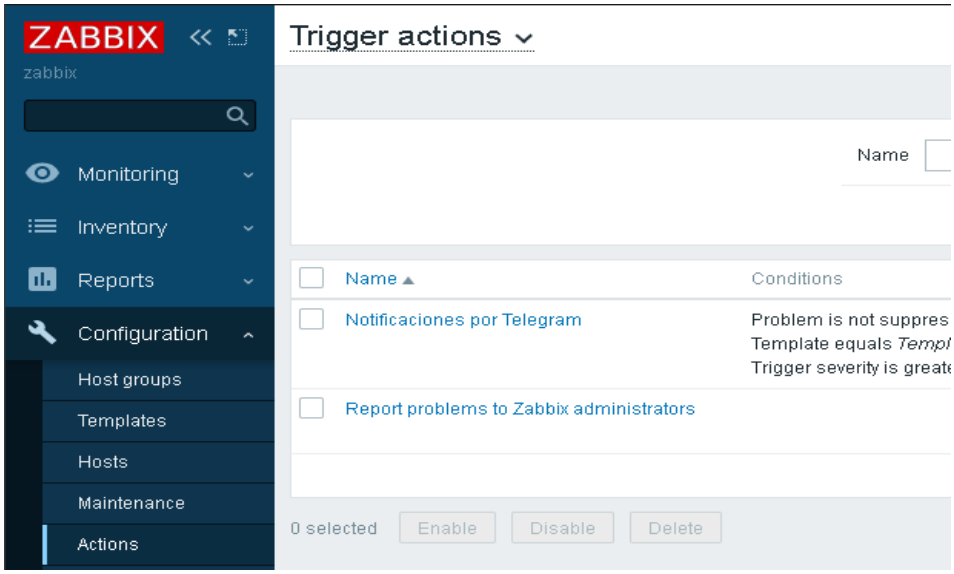


En la opción “Message templates” podremos añadir las distintas fases del problema en sí y las respectivas configuraciones que podemos añadirle para que la alerta sea verificable y verídica.



Creamos una acción de tipo Trigger.

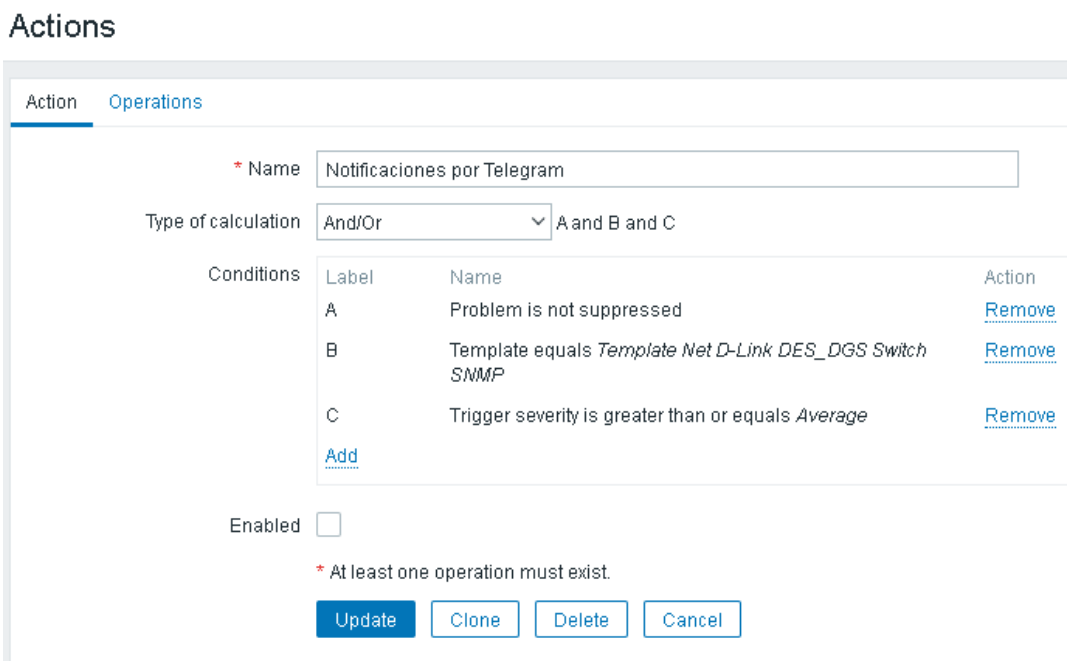
Ingresando al panel principal escogemos la opción de “Configuration” seguido “Actions” y el tipo de acciones que se utilizará será de un disparador o “Trigger”.



Creamos una nueva acción y nos permitirá hacer uso de diferentes variables.

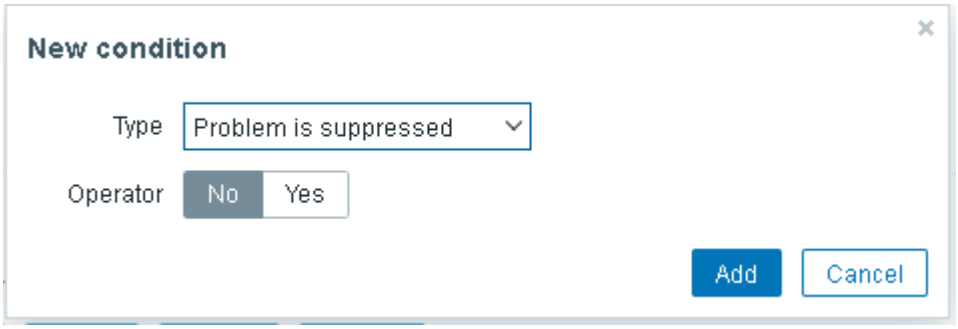
En la creación de la nueva acción se nos permitirá hacer ingreso a las variables y un formulario.

- **Name**: Nombre asignado por el administrador.
- **Type of calculation:** And/or para que escoja cualquier opción.

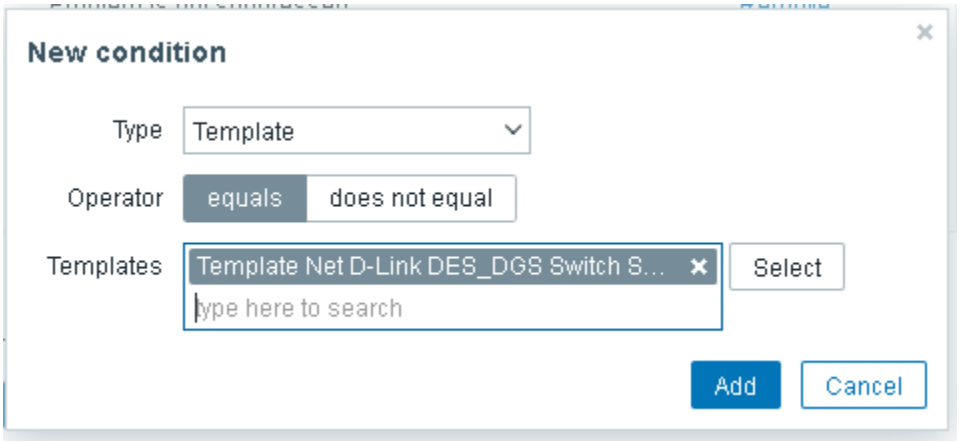


Creación de condiciones.

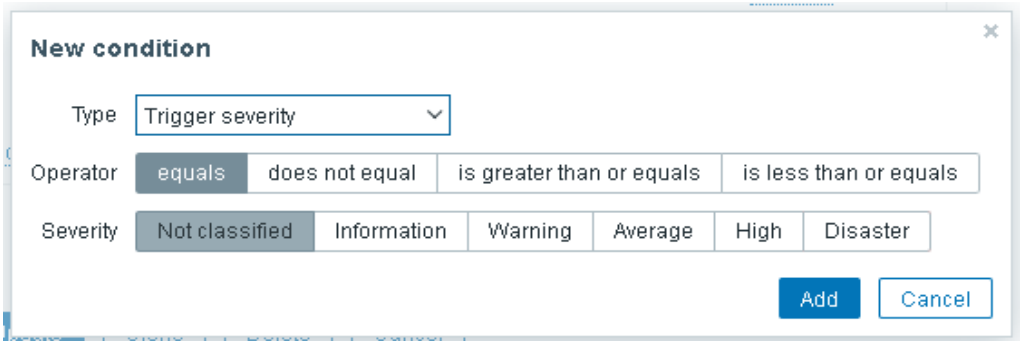
- **Type:** Problem is surppressed.
- **Operator**: NO.



- **Type:** Template.
- **Templates:** Se escoge de acuerdo con el administrador.

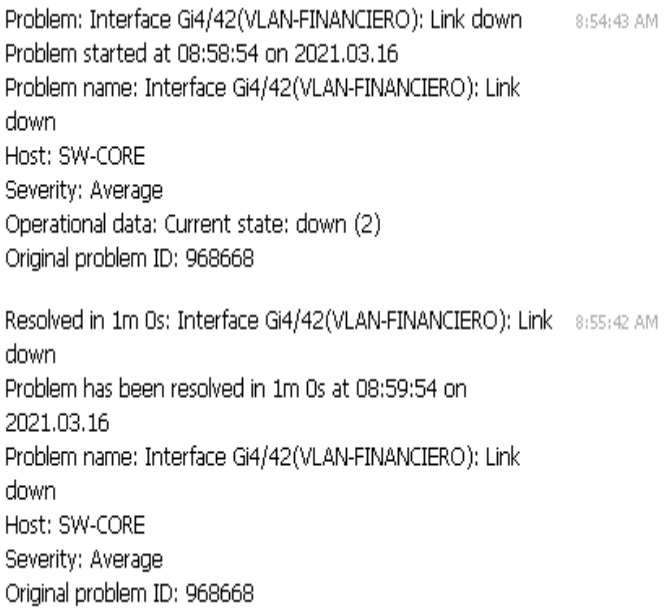


- **Type:** Ttrigger severity.
- **Operator:** equals.
- **Severity:** Depende del tipo de notificación, que el administrador considere necesarias.



Generamos un evento para ver como envía el mensaje vía telegram.

La generación de alertas se realiza automático apenas se habilite el trigger.



3.2.Email

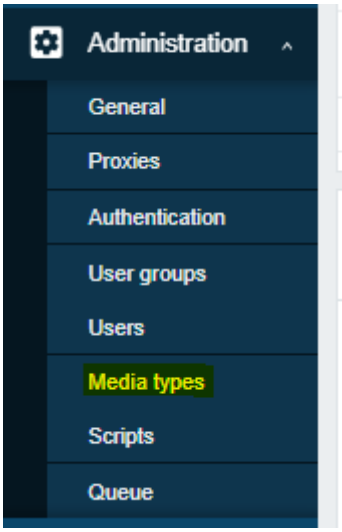
Para el funcionamiento de las notificaciones es necesario instalar paquetes necesarios en el servidor Zabbix para la entrega de correos.

```
# yum install ssmtp mailx
```

Editamos archivo de configuración del email.

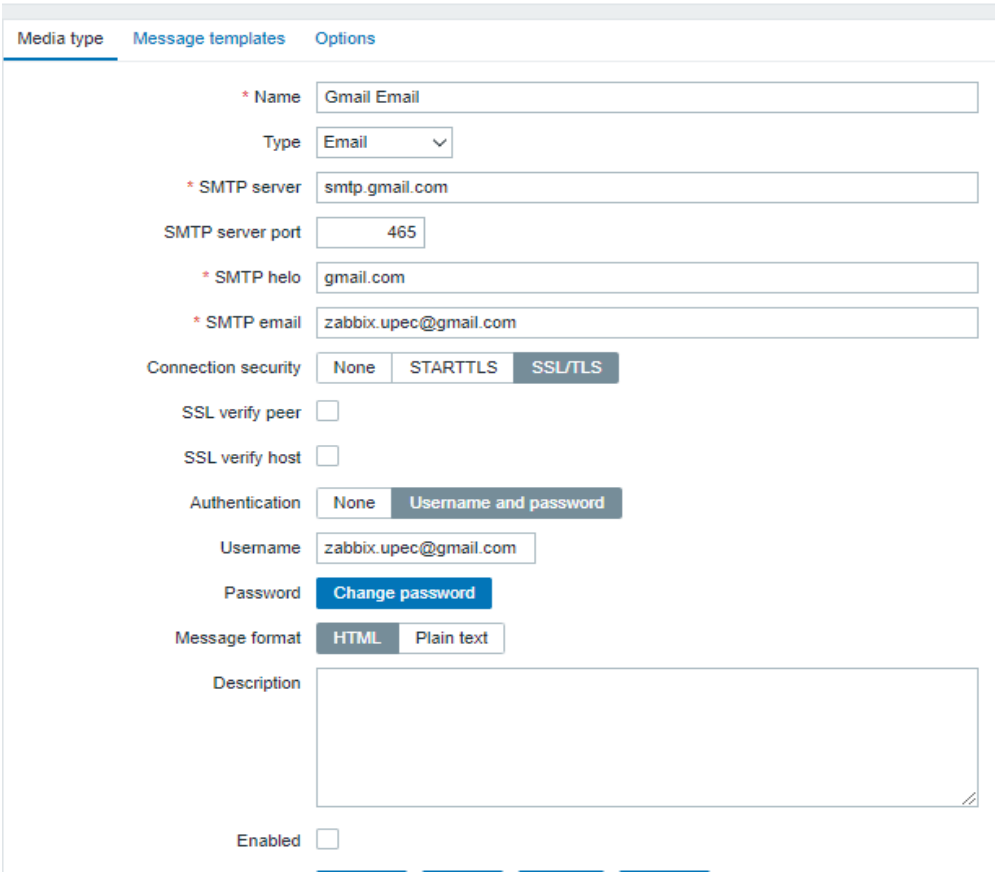
```
# nano /etc/ssmtp/ssmtp.conf
## Editamos ##
root=zabbixupec@gmail.com
mailhub=smtp.gmail.com:465
hostname= Zabbix
FromlineOverride=Yes
useTLS=Yes
## Insertar líneas de autentificación ##
AuthUser= zabbixupec@gmail.com
AuthPass= xxxxxxxxx
```

Para configurar el medio de notificación en el frontend de zabbix, procedemos a dirigirnos a el apartado de Administrador/media types.

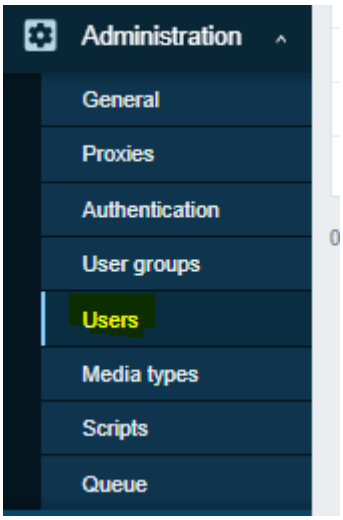


En el apartado de media types, se procede a crea uno nuevo, en la parte superior derecha hacemos click en create media type, en este se desplegará un formulario, los parámetros seleccionados con una marca roja son obligatorios y los demás los podemos dejar por defecto. Los siguientes parámetros para la configuración de correo electrónico son:

- **Name:** nombre del medio a agregar.
- **Type:** el tipo de envió de notificaciones.
- **SMTP server:** servidor de correo electrónico configurado.
- **SMTP server port**: puerto de comunicación para los mensajes salientes.
- **SMTP helo:** nombre de dominio.
- **SMTP email:** dirección de envío de notificaciones de zabbix.
- **Authentication:** Nivel de autentificación.
- **Username:** dirección de correo electrónico para autentificación.
- **Password:** Contraseña de correo electrónico para autentificación.



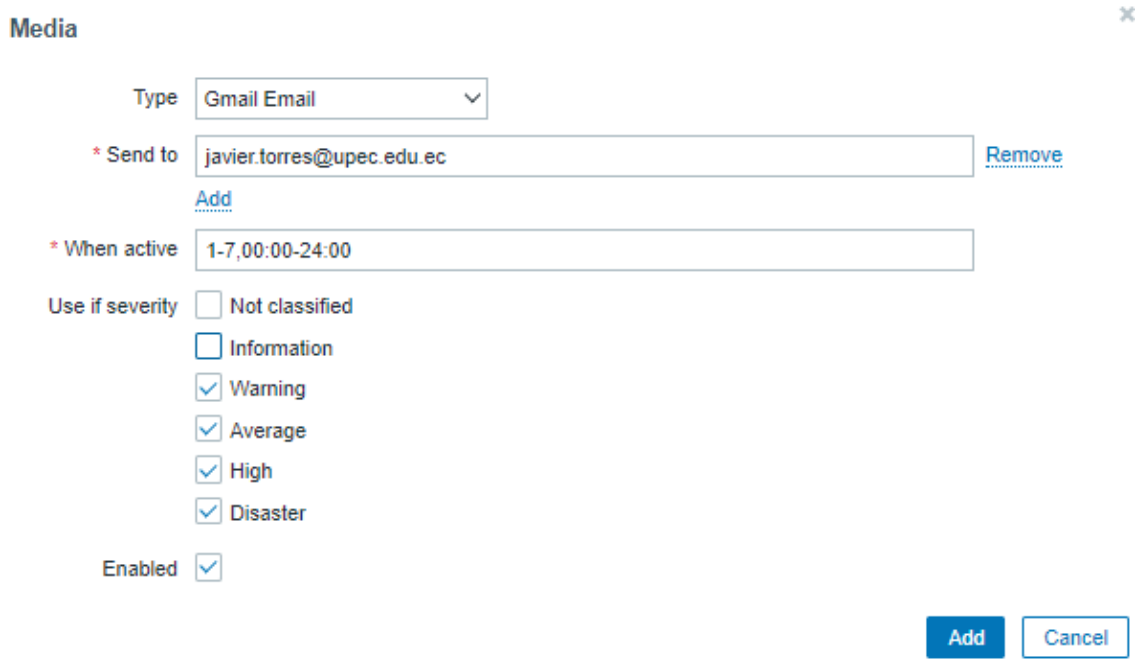
Una vez agregado el media type, procedemos ir a agregar el medio de notificación al usuario en el apartado Administrador/User.



En el usuario administrador, agregamos una nueva media type. A continuación, se describe los parámetros a tomar en cuenta:

- **Type:** Tipo de envío de notificación.
- **Send to:** destinatario de la notificación de Zabbix.

- **When active:** periodo de activación de las notificaciones.
- **Use if severity:** envío del grado de severidad del problema.



Una vez agregado el tipo de notificación al usuario, se podrá apreciar los mediatypes que están asignados a ese usuario y se mostrará así: