HERRAMIENTA DE MONITOREO EN LAS REDES LAN, WLAN Y TELEFONÍA IP PARA LA EMPRESA REDELECTRON-D&S S.A.S.

Universidad del Cauca

CRISTIAN DAVID ESPAÑA GILÓN

Trabajo de Grado
Modalidad Práctica Profesional

Director:
VÍCTOR HUGO MOSQUERA LEYTON
Ph.D. CIENCIAS DE LA ELECTRÓNICA

Asesor:
ING. GIOVANNY ANDRÉS SANDOVAL VELASCO

UNIVERSIDAD DEL CAUCA
Facultad de Ingeniería en Electrónica y Telecomunicaciones
Programa de Ingeniería en Electrónica y Telecomunicaciones
Popayán, Cauca
2023

HERRAMIENTA DE MONITOREO EN LAS REDES LAN, WLAN Y TELEFONÍA IP PARA LA EMPRESA REDELECTRON-D&S S.A.S.

CRISTIAN DAVID ESPAÑA GILÓN

Documento final de Trabajo de Grado presentado a la Facultad de Ingeniería en Electrónica y Telecomunicaciones de la Universidad del Cauca para optar por el título de Ingeniero en Electrónica y Telecomunicaciones

Director:
Ph.D. VÍCTOR HUGO MOSQUERA LEYTON

Asesor:
ING. GIOVANNY ANDRÉS SANDOVAL VELASCO

UNIVERSIDAD DEL CAUCA
Facultad de Ingeniería en Electrónica y Telecomunicaciones
Programa de Ingeniería en Electrónica y Telecomunicaciones
Popayán, Cauca
2023

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

Dedico este trabajo a todas las personas que hicieron parte
de este logro, primero a Dios, por haberme concedido
la capacidad, la fortaleza y el conocimiento para avanzar en este camino;
A mis padres, hermanos, amigos y profesores, pero especialmente
A mi esposa e hijo, quienes me han impulsado a
obtener este logro tan importante en vida profesional.

Cristian David España Gilon

AGRADECIMIENTOS

El autor expresa su agradecimiento al PhD. Victor Hugo Mosquera Leyton, director del trabajo de grado, por su valiosa orientación, y al Ing. Giovanny Andrés Sandoval Velasco, por el valioso acompañamiento a lo largo del trabajo.

A la empresa REDELECTRON-D&S S.A.S. y al Departamento de Telecomunicaciones de la Facultad de Ingenieria en Electrónica y Telecomunicaciones de la Universidad del Cauca, por los aportes y contribuciones en el desarrollo de este trabajo de grado.

También se expresa un agradecimiento muy especial a los compañeros de estudio por su acompañamiento y valioso apoyo durante el proceso de desarrollo del proyecto, quienes participaron paralelamente con su conocimiento y desarrollos similares.

LISTA DE ACRÓNIMOS

LAN	Redes de Área Local, *Local Area Network.*
WLAN	Redes de Área Local Inalámbrica, *Wireless Local Area Network.*
VoIP	Telefonía sobre Internet, *Voice over Internet Protocol.*
VLAN	Redes Virtuales de Area Local, *Virtual Local Area Network*)
UCC	Comunicaciones y Colaboraciones Unificadas,*Unified Communications and Collaboration*
SDN	Redes definidas por software, *Software Defined Networks*
PSTN	Red telefónica pública conmutada, *Public Switched Telephone Network*
SNMP	Protocolo de Adminitración Sencilla de Red, *Simple Network Management Protocol.*
MDF	Centro de distribución principal,*Main Distribution Frame.*
API	Interfaz de programación de aplicaciones, *Application Programming Interfaces.*
NOC	Centro de operaciones de red, *Network Operation Center.*

INTRODUCCIÓN

La necesidad de comunicación en la humanidad ha permitido una evolución en las tecnologías de la información y las comunicaciones, que se ha visto con mayor crecimiento en los últimos años, como lo evidencia el último reporte del portal DATAREPORTAL, donde se dice que el número de usuarios de internet llegó hasta 5.160 millones de personas en el mundo, lo cual significa alrededor del 65 % de la población mundial [1]. Además, con el aumento del uso de las redes sociales, que tiene un poco más de 4.700 millones de usuarios activos [2], genera un aumento en la necesidad de contar con redes de comunicación de alto rendimiento, pues la cantidad de datos que viajan a través de ellas, debido a este fenómeno, es cada vez más grande, lo cual hace crecer la necesidad de mejores servicios.

Por otra parte, con el aumento de datos que viajan a través de internet, se incrementa también el número de ataques contras las redes que los transportan, pues existen personas que quieren obtener estos datos para ejercer un control sobre las personas o entidades. Colombia se ha convertido el segundo país de América Latina con más ciberataques [3], lo cual implica una necesidad en las organizaciones y usuarios finales, de proteger sus datos. Uno de los factores de riesgo se encuentra en las posibles vulnerabilidades que puedan presentarse en las redes de comunicación que transportan los datos, y para ello, es importante que se logre contar con sistemas de ciberseguridad más seguros, con todo lo que implica el despliegue de dichos sistemas.

Uno de los factores importantes, es poder tener un control sobre los equipos que se usan para brindar conectividad, en este sentido, las herramientas de monitoreo, donde se pueden observar los estados de los dispositivos, toma mayor importancia, pues la optimización de las redes y su seguridad vienen dadas por su buen estado. Gracias a estos sistemas se han logrado mitigar los posibles errores que puedan surgir en las redes, mitigando al mismo tiempo los niveles de vulnerabilidad físicos. Por ello, es necesario para las organizaciones que se pueda tener el control de los sistemas que transportan los datos de todo tipo de complejidades.

Debido a ello, en el presente trabajo se dará a conocer la implementación de una herramienta de gestión para las redes de comunicación soportadas por la empresa REDELECTRON-D&S S.A.S. donde se busca ofrecer a sus clientes un mejor servicio, donde se pueda tener mejores rendimientos de dichas redes y lograr mitigar las posibles fallas que de ellas puedan surgir. A continuación, se describirá el contenido de trabajo, que se distribuye en cuatro capítulos de acuerdo a las etapas de diseño y desarrollo establecidas para llevar a buen término la implementación.

Capítulo 1: Generalidades.

En este capítulo se realizará un acercamiento a las necesidades del proyecto, identificando los objetivos del mismo, para finalmente realizar una explicación detallada de los procesos que realiza la empresa REDELECTRON-D&S S.A.S. en los diferentes sectores productivos donde opera, dando mayor énfasis a los productos y servicios en las tecnologías de información y comunicaciones.

Capítulo 2: Diseño y análisis de las herramientas de monitoreo para las redes administradas por la empresa REDELECTRON-D&S S.A.S.

En este capítulo se hará un análisis a profundidad de la infraestructura de las redes administradas por la empresa, ya que existe la necesidad de tener un monitoreo remoto constante de estas redes implementadas; adicionalmente, se realizará el análisis de las herramientas de monitoreo *Open Source* de redes de telecomunicaciones más importantes en la actualidad.

Capítulo 3: Implementación de la herramienta de monitoreo.

En este capítulo se realizará la elección del sistema idóneo que logre cumplir con las necesidades de la empresa para el monitoreo de las redes administradas. Durante este proceso se realizará la integración con la herramienta de asignación de tareas con la que cuenta la empresa.

Capítulo 4: Pruebas y resultados.

En este capítulo se presentarán las pruebas de implementación realizadas, se analizarán los resultados obtenidos para verificar el comportamiento de la herramienta de monitoreo, así como para definir si existe la necesidad de realizar correcciones.

Capítulo 5: Conclusiones, recomendaciones y trabajos futuros.

En este capítulo se darán conclusiones sobre el proyecto y sobre la implementación del mismo, resaltando los resultados obtenidos. Luego se darán una serie de recomendaciones con el fin de buscar el buen funcionamiento de la herramienta. Finalmente, se propondrán los trabajos futuros que podrán surgir a partir de este proyecto de desarrollo.

Palabras clave:

Tecnologías de la información y la comunicación, Arquitectura de gestión de red en internet, protocolo de administración sencilla de red (SNMP), base de información de administración (MIB), estructura de administración de información (SMI).

ABSTRACT

The need for communication in humanity has allowed an evolution in information and communication technologies, which has seen the greatest growth in recent years, as evidenced by the latest report from the DATAREPORTAL portal, where it is said that the number of Internet users reached 5.160 million people in the world, which means about 65 % of the world population [1]. In addition, with the increase in the use of social networks, which has a little more than 4,700 million active users [2], generates an increase in the need for high-performance communication networks, since the amount of data that travels through them, due to this phenomenon, is getting bigger, which makes the need grow for better services.

On the other hand, the increase in data that travels through the Internet also increases the number of attacks against the networks that transport them, since there are people who want to obtain this data to exercise control over people or entities. Colombia has become the second country in Latin America with the most cyberattacks [3], which implies a need for organizations and end users, to protect your data. One of the risk factors is found in the possible vulnerabilities that may arise in the communication networks that transport the data. For this, it is important to have cybersecurity systems that are more insurance, with everything that implies the deployment of said systems.

One of the important factors is to be able to have control over the equipment that is used to provide connectivity, in this sense, monitoring tools, where the states of the devices can be observed, becomes more important, since the optimization of the networks and their security are given by their good condition. Thanks to these systems have been able to mitigate the possible errors that may arise in the networks while mitigating physical vulnerability levels. Therefore, it is necessary for organizations that have control of the systems that transport data of all kinds of complexities.

Due to this, in the present work the implementation of a management tool for communication networks supported by the company REDELECTRON-D&S S.A.S. seeks to offer its customers a better service, where it is possible to have better performance of said networks and to mitigate possible failures that can arise from them. Next, the content of the work will be described, which will be distributed in four chapters according to the design and development stages established to bring the implementation to a successful conclusion.

Chapter 1: Generalities.

In this chapter an approach to the needs of the project will be made, identifying its objectives, to finally make a detailed explanation of the processes carried out by the companyREDELECTRON-D&S S.A.S. in the different productive sectors where it operates, giving greater emphasis to products and services in information and communication technologies.

Chapter 2: Networks infrastructure managed by the company REDELECTRON-D&S S.A.S.

In this chapter, an in-depth analysis of the network infrastructure managed by the company will be made, since there is a need for remote monitoring constant of these implemented networks.

Chapter 3: Implementation of monitoring tool.

In this chapter, the analysis of the most important at present Open Source monitoring tools is carried out, to make the choice of the ideal system that reaches to meet the needs of the company for network monitoring. During this process, the integration will be carried out with the assignment of tasks that the company has.

Chapter 4: Tests and results.

This chapter will present the implementation tests performed, analyze the results obtained to verify the behavior of the monitoring tool, as well as to define if there is a need for corrections.

Chapter 5: Conclusions, recommendations, and future works

This chapter will provide conclusions about the project and its implementation, highlighting the results obtained. Then, a series of recommendations will be given to ensure the proper functioning of the tool. Finally, future work from this development project will be proposed.

Keywords:

Information and communication technologies, network management architecture on the Internet, Simple Network Management Protocol (SNMP), Management Information Base (MIB), and Structure Management Information (SMI).

CAPÍTULO 1

GENERALIDADES.

En este capítulo, se da a conocer la empresa REDELECTRON-D&S S.A.S., donde se realizó la implementación del proyecto, planteando las necesidades que dieron origen al mismo y las cuales han dado las bases para establecer la elección de la herramienta adecuada para el desarrollo del proyecto. Posteriormente, se darán a conocer los objetivos del trabajo y los aportes. Se detalla la metodología para la implementación del proyecto y finalmente, se hará un acercamiento a la historia de la empresa para poder dar a conocer los productos y servicios que ofertan.

1.1. PLANTEAMIENTO DEL PROBLEMA

Desde hace cuatro años la empresa REDELECTRON-D&S S.A.S. ha llevado a cabo diferentes proyectos de implementación de Redes de Área Local, *Local Area Network.* (LAN), Redes de Área Local Inalámbrica, *Wireless Local Area Network.* (WLAN) y Telefonía sobre Internet, *Voice over Internet Protocol.* (VoIP) en la ciudad de Popayán [4]. Estos proyectos han tenido como objetivo principal, brindar una solución integral de conectividad a diferentes entidades privadas, con el fin de entregar, como producto final, redes que cumplan con los mejores estándares de calidad, pero que sean funcionales para los diferentes usuarios que aprovechan estos servicios empresariales.

Los diferentes proyectos se han entregado de manera exitosa, con certificaciones de cada uno de los productos implementados, tanto en el cableado estructurado como en los equipos de red y terminales finales. Este es considerado como uno de los pilares de la empresa, pues es un claro indicador de excelencia. En cumplimiento con la misión, se busca entregar un servicio de calidad y profesionalismo a todos los clientes [5]. Esta excelencia ha permitido que la empresa vaya abriéndose camino dentro del sector de las telecomunicaciones a nivel regional.

Es sabido que por diferentes motivos, los equipos en las redes de telecomunicaciones, que funcionan como soluciones de conectividad, pueden llegar a presentar fallas o problemas que afectan los servicios que se prestan a los usuarios finales [6]. Dichas fallas son reportadas normalmente por el cliente, quien se comunica con la empresa para solicitar soportes ante cualquier inconveniente presentado. Aunque estas fallas no se presentan en la actualidad de manera constante, para el futuro de la empresa podría convertirse en un problema de gestión de personal; debido a que el crecimiento constante de los proyectos que quedan a cargo de la empresa incrementaría el número de solicitudes por parte del cliente. Por este motivo, se hace necesaria una herramienta que permita

tener el control de las diferentes redes que son soportadas por la empresa, con el fin de contar con retroalimentación del estado de los equipos de red, un monitoreo constante y detectar las fallas [7].

Sumado a esto, las fallas que se presentan en los sistemas de telecomunicaciones tienen diferentes niveles de criticidad, esto quiere decir que, en algunas ocasiones, los tiempos de respuesta ante estas fallas deben ser muy cortos, debido al grado de afectación del servicio; ya que podría tenerse una pérdida total que bajaría los niveles de disponibilidad de la red. Sin embargo, este no es el único caso que podría presentarse, existen también los niveles bajos de criticidad, para los cuales el tiempo de respuesta puede ser bajo, pues la falla que se presenta no es grave para el servicio y la visita puede esperar. Normalmente, estas últimas no son perceptibles por el cliente, pero pueden convertirse en afectaciones de mayor criticidad, ya que son alertas tempranas del servicio que si no son mitigadas alcanzan niveles altos de riesgo; estos pueden también evitarse realizando visitas anticipadas de mantenimientos o resolverse rápido una vez establecidas [8].

Por este motivo, se hace necesario que se logre diseñar e implementar una herramienta que permita monitorear los equipos implementados en las redes que se encuentran bajo el soporte de la empresa REDELECTRON-D&S S.A.S., ya que en la actualidad no se cuenta con ella. El diseño de un sistema de monitoreo de las redes que se encuentra bajo la administración de la empresa permitiría realizar una atención oportuna a los fallos de menor criticidad y atender de forma rápida las alertas reportadas con mayor criticidad. Esta implementación daría a la empresa una herramienta que le permitiría entregar un mejor servicio a los clientes y ofrecer a los clientes un valor agregado frente a nuevos proyectos.

1.2. OBJETIVOS

1.2.1. Objetivo general.

- Desarrollar una herramienta de monitoreo, hardware y software, para las redes LAN, WLAN y Telefonía IP, implementadas por la empresa REDELECTRON-D&S S.A.S. que se articule con el programa de control de tareas de mantenimiento y seguimiento de atención de la empresa.

1.2.2. Objetivos específicos.

- Implementar una herramienta de monitoreo de las redes LAN, WLAN y Telefonía IP, que están a cargo de la empresa REDELECTRON-D&S S.A.S.

- Integrar el sistema de control de tareas de mantenimiento y soporte de la empresa REDELECTRON-D&S S.A.S. con la herramienta de monitoreo de redes

implementada.

- Evaluar el funcionamiento de la herramienta implementada sobre las redes LAN, WLAN y Telefonía IP bajo la administración de REDELECTRON-D&S S.A.S.

1.3. APORTES

- El diseño del establecimiento de prioridades y la clasificación de la criticidad de las alarmas para dar respuesta a las fallas del servicio de las redes administradas por la empresa REDELECTRON-D&S S.A.S.

- Integración de la herramienta de monitoreo implementada con el sistema de asignación de tareas y control de atención a los clientes de la empresa REDELECTRON-D&S S.A.S., así como también el establecimiento de los procedimientos a realizar.

1.4. METODOLOGÍA

El método cascada, también llamado ciclo de vida básico o modelo lineal secuencial, se adoptará en la realización de este proyecto, pues se basa en el establecimiento de una serie de etapas que deben irse cumpliendo, de forma secuencial, donde el resultado de la etapa anterior se utiliza en la etapa que se está ejecutando. [9].

El modelo establecido para este proyecto seguiría la siguiente secuencia:

- Recopilación de los requisitos y la documentación: En esta etapa se realizará un levantamiento de la información que permita identificar lo requerido por la empresa.

- Diseño del sistema: Una vez realizado el análisis de la información se implementan las necesidades en el algoritmo, con el cual se construyen los procedimientos que se deben seguir y el producto final que se quiere obtener.

- Implementación: En esta etapa se realiza el montaje final de la herramienta, desarrollada con base en el diseño establecido en la etapa anterior, siguiendo los procesos y tareas establecidas.

- Pruebas: En esta etapa se busca revisar que los procesos desarrollados presenten un buen desempeño, aquí se pueden corregir los procesos con la detección de errores.

- Entrega/Implementación: En esta etapa se hace entrega final al cliente, donde se explica el funcionamiento de todos los procesos y se da la capacitación para dar un correcto uso a la herramienta.

1.5. REDELECTRON-D&S S.A.S. - Ingeniería y Soluciones

REDELECTRON-D&S S.A.S. es una empresa payanesa del sector de las telecomunicaciones y energía, fundada en el año 2018. Cuenta con cinco años de experiencia en la realización de procesos de implementación, mantenimiento y soportes sobre redes LAN, WLAN, SD-WAN, VoIP, Videoconferencia y energía, con proyectos tanto en empresas públicas como privadas en el suroccidente colombiano, para los departamentos de Cauca, Nariño, Putumayo, Huila y Valle del Cauca. Con expectativas de ampliación internacional para los próximos años, pues cuenta con aliados multinacionales de gran envergadura [4].

La misión de la empresa es ayudar a construir un desarrollo para la región, ofreciendo un amplio portafolio de productos y servicios diferenciados por su calidad y profesionalismo, con la caracterización especial por el cumplimiento de las normas vigentes aplicables para Colombia como RETIE, NTC-2050, RITEL, entre otras, para garantizar la mejor satisfacción de los clientes [5].

1.5.1. Productos.

- Citofonía Digital: La empresa REDELECTRON-D&S S.A.S. se ha ido posicionando en la inslación de productos de la empresa FERMAX S.A., por medio de la cual se comercializan equipos para comunicaciones residenciales. Es uno distribuidores autorizados en el departamento del Cauca, pues desde hace 4 años ha llevado a cabo la implementación de estos sistemas en las construcciones residenciales de la ciudad de Popayán. En la búsqueda por expandirse en la región, la empresa ofrece sus productos a departamentos del suroccidente colombiano; obteniendo una gran acogida por parte de las constructoras, debido a la calidad del portafolio ofrecido y del servicio entregado al final de la implementación. El objetivo es proveer la comunicación residencial interna, con el fin de garantizar el control de acceso a las unidades residenciales. Dentro de los productos ofrecidos se tienen videoporteros, placa-calles, conserjerías, citófonos digitales, videocitófonos y demás productos que garanticen comunicación con estos terminales [10]. La empresa ha realizado un gran despliegue de implementación de estos equipos, logrando montajes hasta en zonas de difícil implementación, como complejos industriales de bodegas, condominios con mucho usuarios, entre otros, y gracias al personal calificado con el que cuenta la empresa, se ha logrado implementar las soluciones a los clientes.

- Cableado estructurado: Debido a los procesos de implementación de cableado estructurado llevados a cabo en los últimos dos años, la empresa REDELECTRON-D&S S.A.S. se convirtió en implementador especializado con la marca Panduit

a nivel local. Se ha logrado establecer un enlace con este proveedor, logrando implementar soluciones de conectividad para instituciones educativas completas con esta marca. La realización de dichos proyectos ha logrado que la empresa brinde soluciones de alta complejidad para comunicaciones de alto tráfico, con grandes rendimientos de servicios [11]. Gracias a ello, la empresa ha tenido una gran acogida en el sector educativo para la implementación de nuevos proyectos de conectividad; buscando de igual forma expandirse hacia otros sectores de la región.

- Sistemas de domótica: Gracias a las implementaciones de domótica hechas en la ciudad de Popayán, la empresa se ha posicionado en el despliegue de soluciones con la marca Lutron, la cual brinda productos para automatización residencial. Estos dispositivos utilizan tecnologías que trabajan con protocolos de comunicación propios, lo cual impide que se generen vulnerabilidades a la privacidad por medio de ataques; la encriptación de la información es propia de la marca, entregando un servicio de alta confianza a los usuarios.

  La calidad de estos productos y la complejidad de las soluciones implementadas han permitido que el personal se epecialice en ellas, ofreciendo a los clientes finales, servicio de alta calidad con seguridad garantizada de los productos [12].

1.5.2. Servicios.

- Redes empresariales de área local: La implementación de redes empresariales de área local ha permitido que la empresa REDELECTRON-D&S S.A.S. continue escalando como organización en el sector de las telecomunicaciones, pues en los últimos años se ha realizado implementaciones de redes de todo tipo de complejidad, logrando establecer estándares altos de seguridad y disponibilidad, con equipos de gran rendimiento. Gracias a ello se ha adelantado un proceso de reconocimiento empresarial favorable, pues las organizaciones han visto en estos servicios un valor importantes para su productividad, lo cual ha permitido que se realicen despliegues en diferentes sectores empresariales en los departamentos del Cauca,Valle del Cauca, Nariño, Huila y Putumayo. De aquí ha surgido la necesidad de contratar en la empresa, personal calificado para realizar la implementación de estas redes con profesionalismo, para brindar a los clientes un valor agregado.

- Conectividad para centros educativos: A partir del año 2020, debido a la contingencia vivida a nivel mundial, se hizo muy evidente la brecha social que existe en el sector tecnológico. Con el fin de brindar solución a esta problemática, la empresa ha establecido soluciones de conectividad para los centros educativos, y ha servido de proveedor final para que dichas soluciones lleguen a los usuarios finales. La empresa ha participado en proyectos a nivel nacional para la imple-

mentación de soluciones de conectividad para instituciones educativas de carácter oficial, con los cuales se ha adquirido un reconocimiento dentro de este sector, pues se ha buscado ofrecer a los usuarios una organización mucho más cercana a ellos que brinda pronta respuesta y gran calidad del servicio. Gracias a ello, la empresa ha podido ofrecer también servicios de conectividad en el sector privado, por medio del cual se han logrado llevar a cabo proyectos de calidad, garantizando soluciones idóneas para el sector educativo, el cual tiene necesidades específicas, diferentes a otros sectores.

- Redes eléctricas residenciales: Este es un sector en el que ha iniciado la empresa desde su fundación, por medio de este servicio se han logrado llevar a cabo proyectos para brindar soluciones de energía de media y baja tensión para unidades residenciales, garantizando que se cumplan con los estándares requeridos por las certificadoras. Con ello, la empresa ha ganado nombre desde su origen en el sector, pues se ofrecen servicio de alta calidad, donde el objetivo final es que se cumplan con los requerimientos del cliente, en cuanto a certificaciones y seguridad. El personal con el que cuenta la organización se ha convertido en un gran aliado, pues su trabajo profesional le ha permitido expandirse a nivel local en el sector.

- Sistemas de seguridad y videovigilancia: En el último año, la organización se encuentra en un proceso de expansión y diversificación en el sector tecnológico, por lo cual, se han venido adelantando procesos, formación y comunicación para establecer un puente que permita que la organización pueda ofrecer servicios de seguridad residencial y videovigilancia. Gracias a ello se han logrado implementar proyectos a nivel regional de este servicio, logrando articularlo con los productos de automatización residencial. Con ello se desea brindar una solución integral a los clientes, garantizando automatización y seguridad para las viviendas, esto ha permitido que la empresa se abra campo en el sector y se pueda convertir en proveedor oficial de marcas de renombre en el sector de la videovigilancia. El valor agregado en este sector es el nivel organizacional con el que cuenta la empresa, pues se garantiza que se cumplan todos los estándares de ley que se solicitan a nivel empresarial, esto ha dado a los usuarios un nivel de confianza alto para elegir a la empresa.

- Sistemas de energías renovables: Como se dijo anteriormente, la empresa se encuentra en la búsqueda de diversificación de servicios ofrecidos, y teniendo en cuenta la calidad de personal, se han venido adelantando procesos de formación y conocimiento de energías renovables debido al auge que estas han tenido en los últimos años. La empresa ha empezado a incursionar en el sector, observando buenos resultados en la implementación de servicios de alumbrado público en unidades residenciales y en municipios del departamento del Cauca. Por el momento, se ofrecen soluciones de iluminación exterior, pero el objetivo empresarial para los próximos años en lograr posicionarse como líder en este sector a nivel regional, de la misma manera como se ha hecho con las demás tecnologías que opera la empresa. El personal con el que se cuenta, tiene amplia experiencia en el

sector de energía residencial, lo que garantiza una alta capacidad para desarrollar proyectos futuros en el sector de las energías renovables.

- Sistemas de detección de incendios: La empresa REDELECTRON-D&S S.A.S. ha brindado esta solución para el sector hotelero en la ciudad de Popayán. Estos proyectos han ido de la mano con la implementación de servicios de energía de baja tensión, y han permitido a la organización crecer en los diferentes sectores productivos locales. Estos sistemas de detección de incendios se han integrado con los sistemas videovigilancia y control de acceso, para ofrecer a los clientes soluciones integrales tecnológicas. Se han manejado pocos proyectos, pero han permitido que la organización gane renombre en los sectores productivos.

CAPÍTULO 2

DISEÑO Y ANÁLISIS DE LAS HERRAMIENTAS DE MONITOREO PARA LAS REDES ADMINISTRADAS POR LA EMPRESA REDELECTRON-D&S S.A.S.

En este capítulo se hará un análisis detallado de la infraestructura de las redes administradas por la empresa, ya que existe la necesidad de tener un monitoreo remoto constante de estas redes implementadas, y para realizar su diseño se hace necesario identificar y describir estas infraestructuras con el fin de encontrar la herramienta de monitoreo que mejor se adapte a las necesidades identificadas. La Figura 2.1 presenta el diagrama de flujo del desarrollo del proyecto basado en la metodología en cascada.

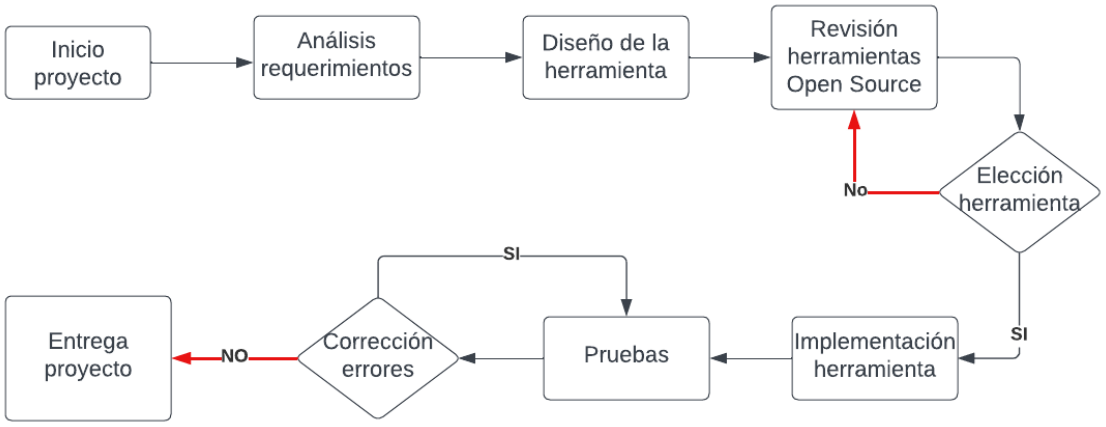

Figura 2.1: Diagrama de flujo del desarrollo del proyecto.
Fuente: Elaboración propia.

2.1. INFRAESTRUCTURA DE RED DE LAS SOLUCIONES EMPRESARIALES

2.1.1. Infraestructura de red de soluciones empresariales cableadas

La implementación de las redes de comunicación empresariales tiene diferentes grados de complejidad, pues cada red debe adaptarse a las necesidades de los clientes; para ello, antes de realizar una implementación, se realiza un estudio de campo durante el cual se busca definir las posibles ubicaciones de los cuartos de comunicaciones, las distancias que desde ellos se tiene hasta los funcionarios, las ubicaciones para las soluciones de red inalámbrica, estado en el que se pueda encontrar el cableado estructurado con el cual cuenta la empresa, entre otras tareas.

Una vez realizado el estudio de campo, y describir detalladamente las necesidades empresariales, se procede a establecer el diseño de la red, donde se definen las soluciones que se deben implementar. Dentro de los proyectos recientes se ha notado una constante y es el hecho de las redes con las que cuentan en la actualidad las empresas en la ciudad de Popayán, las cuales se encuentran obsoletas, en lo referente a equipos, cableado y demás componentes, no cumplen con el nivel mínimo de seguridad para garantizar una alta confiabilidad. Sin embargo, las soluciones llevadas a las empresas, han sido satisfactorias, se han hecho implementaciones totales de red, recategorizando el cableado estructurado, utilizando las últimas normas, montaje de equipos de alta velocidad para no tener cuellos de botella en la transmisión de datos, soluciones seguras para redes inalámbricas, con configuración de los últimos estándares de seguridad de acceso y encriptación.

Debido a la diversidad que se ha encontrado en el sector empresarial para las soluciones de conectividad, se elaborará a continuación una descripción, lo más completa posible, para lograr identificar los elementos esenciales que componen las redes implementadas por la empresa REDELECTRON-D&S S.A.S.

Según se evidencia en la Figura 2.2, la infraestructura de red a nivel empresarial cuentas con tres etapas de trabajo, en la primera etapa se encuentran los equipos que tienen salida hacia internet, allí pueden estar el *router* y el *firewall*; el primero define las rutas que deben ser utilizas para el transporte de paquetes, mientras que el segundo establecer las políticas de ingreso y salida de la red; por medio de este se obtiene la seguridad en la red, definiendo las políticas de uso de los servicios, tanto desde afuera como desde adentro de la red interna. Estos dos equipos pueden ser agrupados mediante el uso de las Redes definidas por software, *Software Defined Networks* (SDN), donde se centraliza la red de manera remota por medio del uso de controladoras de la red, eliminando las características básicas tanto del *firewall* como del *router*. Finalmente, para comunicación externa, se emplea el *router*, asignándole políticas de salida e ingreso, y se brindaría la seguridad en general, de manera remota y centralizada [13].

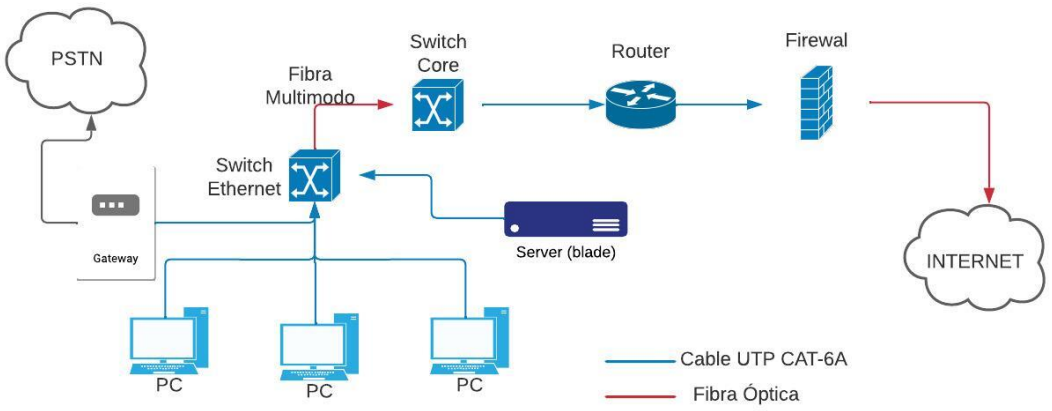

Figura 2.2: Diseño básico de red empresarial.
Fuente: Elaboración propia.

En la segunda etapa, se tienen los equipos de distribución de la red interna, también llamados *switchs*, los cuales se encargan de permitir la conexión de los terminales a la LAN. Estos equipos son de dos tipos, existe un *switch* principal el cual es llamado *switch core*, donde se establecen los segmentos de red, llamados Redes Virtuales de Area Local, *Virtual Local Area Network* (VLAN), que van a ser utilizados para los diferentes servicios que se usan dentro de la red; estos segmentos ayudan a brindar seguridad y alto rendimiento, pues logran establecer dentro de la organización una distribución de acceso de los diferentes usuarios y delimitan el acceso a las demás redes virtuales que puedan existir. Esto quiere decir que si a un usuario solo se le permite acceso a un servicio, por medio del segmento de red asignado, no podrá utilizar los demás servicios que están distribuidos a las demás redes virtuales. Esta solución es muy favorable para las organizaciones, pues se definen los roles de los usuarios y los servicios a los cuales tendrán acceso, con ello se garantiza que toda la información no va a ser manejada por todos, sino segmentada dependiendo de los roles establecidos. De igual forma, es muy favorable para el rendimiento de la red, pues los paquetes van a ser distribuidos de forma más eficiente y llegarán a los usuarios más rápido, ya que el tráfico segmentado evitará la saturación de una sola red, porque se manejarán sobre una misma red varias subredes [14].

Finalmente, se tienen los terminales de usuario y servicios, los cuales son los que utilizan la red y definen cuáles son los tipos de datos que viajan a través de ella. En la Figura 2.2 se tiene 3 tipos de terminales, los primeros son los computadores corporativos, los cuales tienen acceso a la información de la organización dependiendo de los roles establecidos, y se conectan, por medio de red cableada, a los *switchs* de distribución, quienes permitirán el acceso a los servicios. El segundo tipo de terminales son los

servidores, en ellos se definen los servicios internos con los que cuenta la empresa; estos servicios pueden ser de correo electrónico, servicios web, aplicaciones de finanzas, bases de datos, entre otros [15]. En la actualidad, estos servicios se están manejan en la nube, evitando el uso de estos terminales, pues con ello se garantiza una mayor disponibilidad y seguridad, pues la organización entrega estas responsabilidades al proveedor del servicio. Sin embargo, la organización debe establecer los mecanismos de acceso seguros a la nube para evitar al máximo las vulnerabilidades y fugas de información que puedan presentarse. Finalmente, se tiene la *gateway VoIP* o planta telefónica, la cual permite realizar la gestión del servicio de comunicación telefónica y que da la salida hacia la Red telefónica pública conmutada, *Public Switched Telephone Network* (PSTN). Estos equipos al interior de las organizaciones garantizan una comunicación telefónica interna; en la actualidad, también es posible generar comunicaciones telefónicas para empresar que tienen sedes remotas, generando canales virtuales para optimizar la cantidad de equipos [16].

Los paquetes de voz son independientes y normalmente segmentados por medio de una VLAN, con el objetivo de que la calidad de la voz no se vea afectada por el tráfico de otros servicios. Los teléfonos usados para esta tecnología van conectados de manera cableada a los *switchs*. Sin embargo, existe un avance en esta tecnología por medio de aplicaciones para Comunicaciones y Colaboraciones Unificadas, *Unified Communications and Collaboration* (UCC), en los cuales, por medio de soluciones *software* se cuenta con herramientas telefónicas a las cuales se adicionan herramientas ofimáticas de colaboración, esto eliminaría el uso de plantas telefónicas físicas, optimizando el rendimiento y disponibilidad del servicio.

2.1.2. Infraestructura de red de soluciones inalámbricas empresariales

Las soluciones inalámbricas implican un alto grado de complejidad, pues al no tener el control de la propagación de las ondas, el acceso a ellas es más vulnerable. Por este motivo, se hace necesario establecer modelos de acceso al servicio que impidan que pueden existir huecos de seguridad por donde puedan ingresar usuario no deseados. Los avances en seguridad para estas redes han permitido estableces procesos de identificación para acceso complejos para las redes corporativas, sin embargo, gran parte de esta seguridad la tienen los usuarios, pues de ellos depende que las acciones para proteger la red sean efectivas, por lo que se hace siempre necesario realizar un despliegue de información educativa para dar buen uso de las soluciones inalámbricas [17].

Por otro lado, garantizar un alto rendimiento de la red para estos servicios también es complejo, ya que, por el mismo motivo expuesto anteriormente, no se tiene control completo de las ondas propagadas, por eso se hace necesario establecer métodos de configuración que impidan que la red se deteriore para todos los usuarios. Por medio de las buenas prácticas de configuración se pueden establecer políticas de conexión tales como controlar la velocidad mínima de navegación que pueda tener un usuario, con ello,

por ejemplo, se obtendrá que los usuarios naveguen con un límite bajo de velocidad, si un usuario queda por debajo del límite, el sistema lo sacará de la red, garantizando que los recursos de propagación no sean dirigidos a ese usuario y los demás queden sin recursos, esto hace que la red se mantenga estable para todos [**?**].

Teniendo en cuenta lo anterior y las necesidades de cada cliente, se procede a realizar un estudio de campo donde se deben establecer el número de equipos que se deben utilizar para cubrir los requerimientos, garantizando seguridad y alto rendimiento. En este sentido, es importante tener en cuenta las características de propagación de las ondas, pues los equipos no deben quedar muy cerca para evitar interferencias entre ellos, ni muy lejos para garantizar *roaming* en el espacio de corporativo [18].

Adicionalmente, para estas redes deben establecerse, de forma clara, los roles corporativos para acceso a la información, pues las conexiones seguras y la configuración de los segmentos de red dependen de estas políticas. En este caso, también se usan las redes virtuales, con ellas se garantiza que se cumplan los accesos seguros de los roles establecidos.

Es importante resaltar que dentro de las soluciones empresariales que se han implementado por REDELECTRON-D&S S.A.S. (Figura 2.3) no se cuenta con un gran despliegue de redes inalámbricas. Sin embargo, poco a poco se ha visto un crecimiento en la adquisición de estos servicios, ya que los espacios empresariales han mutado hacia lugares más participativos, donde el despliegue inalámbrico garantiza la movilidad para todos los usuarios sin dejar de garantizar alto rendimiento. Este fenómeno se ha evidenciado en los últimos años, pues el deseo por mejorar el clima organizacional lo requiere [19].

En ese mismo sentido, debido a la contingencia vivida por el COVID-19, las organizaciones se vieron obligadas a cambiar sus modelos espaciales al interior de las oficinas [20], con el fin de evitar contagios y demás problemas que pudieran presentarse; para ello, las redes inalámbricas logran establecerse como una solución para este cambio, pues se convirtieron en una herramienta de fácil implementación a bajo costo, ya que un despliegue alámbrico tomaría más tiempo y un aumento de presupuesto, debido a que representarían modificaciones a la infraestructura del cableado.

Finalmente, es importante reconocer que estos equipos inalámbricos representan equipos de alta criticidad en el servicio de telecomunicaciones, ya que se encuentran mucho más expuestos a los estados ambientales, y en muchos casos, se implementan en ubicaciones con condiciones extremas; esto implica que deban ser altamente monitorizados para tratar de evitar problemas que afecten la conectividad y dar respuesta rápidamente ante fallas que puedan presentarse. Este tipo de servicios son importantes para la organización, porque gracias a ellos, se demuestra la calidad del servicio que se ofrece a los clientes.

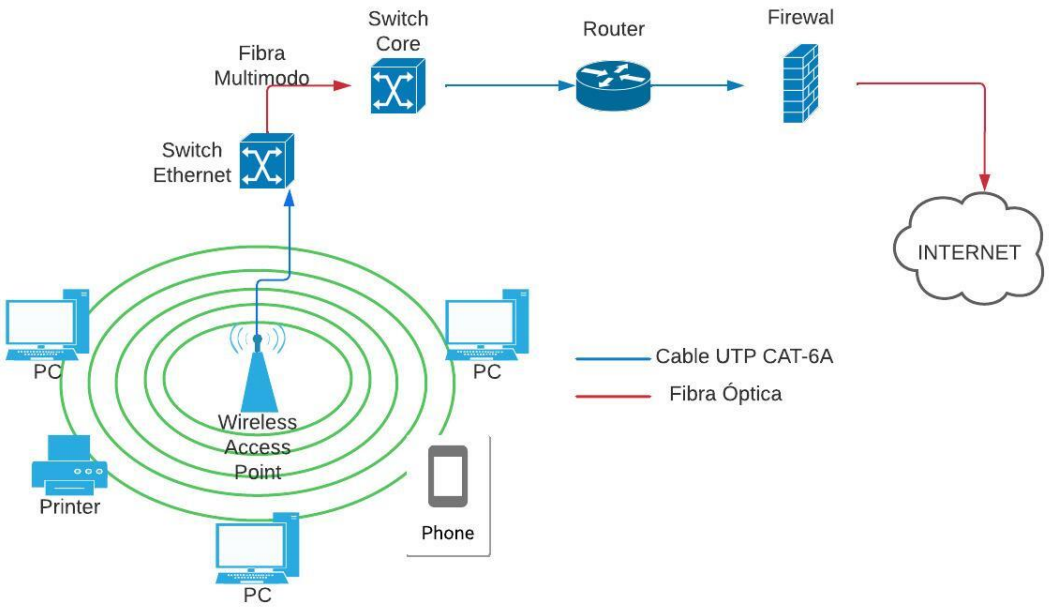

Figura 2.3: Diseño básico de red inalámbrica empresarial.
Fuente: Elaboración propia.

2.2. INFRAESTRUCTURA DE RED DE LAS SOLUCIONES EDUCATIVAS

2.2.1. Infraestructura de red de soluciones cableadas para instituciones educativas

Una de las soluciones que más se impulsó durante la contingencia fue la conectividad escolar [21], pues fue durante esos años que se evidenció en mayor medida la brecha que existe en Colombia y en todo el mundo. El Gobierno Colombiano inició nuevos planes para esta década con el fin de brindar conectividad a todas las escuelas en el país y con ello garantizar un crecimiento en los niveles educativos. En ese sentido, la empresa REDELECTRON-D&S S.A.S. ha servido de puente para lograr que las soluciones de conectividad lleguen a las zonas rurales de la región. Durante los últimos años se han llevado a cabo varios proyectos que han permitido desplegar recursos hacia las zonas más desfavorecidas del departamento de Cauca. Se ha observado, durante este tiempo, la calidad del servicio que se ha implementado, pues las soluciones llevadas a las escuelas han permitido que se adelanten emprendimientos que motivan a los estudiantes para optar por estudios tecnológicos.

Estas soluciones, cuando son llevadas a las zonas rurales, se han acompañado con

capacitaciones para dar buen uso. Esto ha evidenciado la calidad humana con la que cuenta la empresa, pues se ha logrado obtener buenos resultados de todos estos proyectos. Llevar soluciones tecnológicas e innovadoras a toda la región, tanto en lo rural como en lo urbano, ha sido un gran desafío para la empresa, pues el hecho de llevar nuevas tecnologías significa la necesidad de entregar a los usuarios la educación alrededor de ellas, y en ese sentido, la empresa ha cumplido a cabalidad con los objetivos.

Así las cosas, al momento de realizar la implementación de soluciones de conectividad educativa en la región, se han debido tener en cuenta todos los aspectos anteriormente mencionados. Por este motivo, se hace siempre necesario realizar un estudio en sitio que ayude a aclarar las diferentes necesidades que se presentan y establecer los requerimientos finales importantes, para poder llevar a cabo la implementación.

Con esto establecido se procede a diseñar la solución para la institución educativa, la cual normalmente cuenta con una estructura de red como en la Figura 2.4, se debe elegir un Centro de distribución principal,*Main Distribution Frame.* (MDF) donde se implementarán los equipos *firewall*, *router*, *switch core*, *transceiver*; adicional a estos equipos se podrá realizar el montaje de uno de los *stacks*, con ello se adaptaría el MDF como un centro de distribución de red primario. Los demás *stacks* se ubicarán en centros de datos secundario, que se instalarán en lugares estratégicos para cubrir el alcance de red de la institución educativa, estos *stacks* adicionales se conectan con una topología en estrella al MDF por medio de fibra óptica, llamada *backbone*

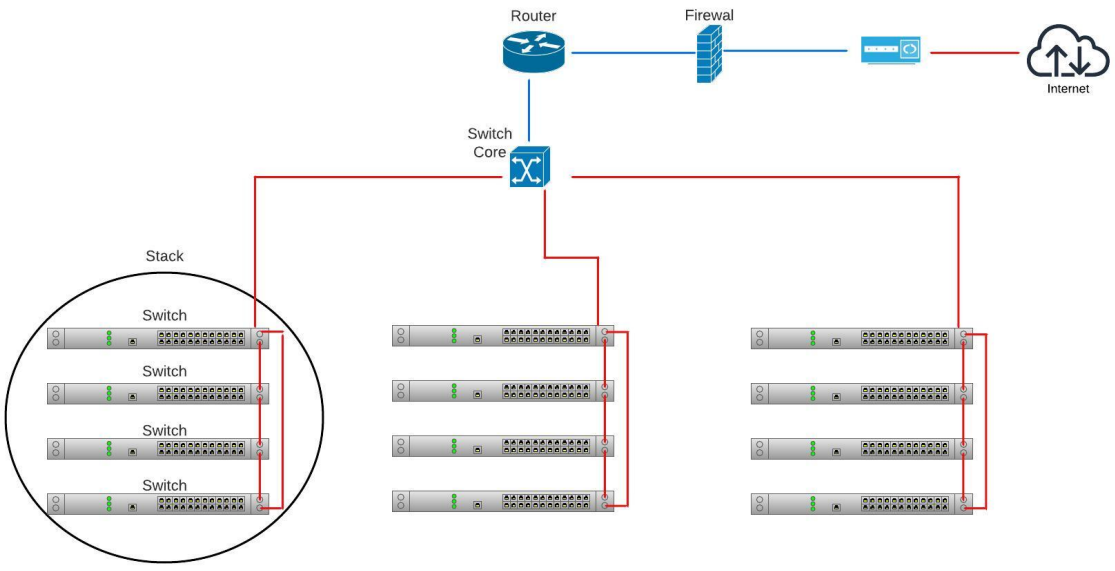

Figura 2.4: Diseño básico de red educativa.
Fuente: Elaboración propia.

Este despliegue se hace con el fin de garantizar que se cumpla que la distancia máxima de cableado horizontal sea de 90 metros, que se tenga conexión de *patch cords* máximo de 10 metros, con ello se garantizaría el cumplimiento normativo y las mejores prácticas para brindar alta calidad en el servicio [22].

La funcionalidad de cada uno de los equipos fue explicada anteriormente, pero adicional a ello, es importante tener en cuenta que en el caso de las instituciones educativas es necesario controlar el tráfico que viaja por la red, pues es un recurso limitado usado masivamente [23]. En este orden de ideas, se configura el servicio de forma segmentada, para organizar el acceso de los usuarios, y aplican políticas de acceso a servicios para cada segmento establecido. Los roles que se han identificado en estas organizaciones permite evidenciar que es necesario también evitar fugas de información y accesos no autorizados, por ello es importante establecer prácticas de control de acceso para aislar los datos según los roles establecidos.

Para lograr cumplir con la alta disponibilidad y seguridad es necesario realizar también un monitoreo a los dispositivos de red que se utilizan en esta solución, con ello se pueden evitar problemas de conectividad y posibles fallas de seguridad que puedan presentarse.

2.2.2. Infraestructura de red de soluciones inalámbricas para instituciones educativas

Como complemento de las soluciones cableadas para las instituciones educativas, se realiza el despliegue de las redes inalámbricas, con condiciones especiales, debido a la complejidad de estas instituciones (Figura 2.5). Para hacer esta implementación se realiza un análisis de las necesidades del cliente, estableciendo el alcance del servicio, las condiciones de uso y las restricciones que se deben configurar, teniendo en cuenta esta información, se realiza un diseño de red para definir la ubicación de los equipos, para cubrir las áreas de interés por parte del cliente.

Una vez definidas las ubicaciones de los equipos, cuáles se hace la implementación de la solución, y para cumplir con los requerimientos de seguridad, las redes se dividen en varias redes virtuales que permitan establecer los límites de acceso que va a tener cada uno de los usuarios finales que utilicen el servicio, de la misma manera como se explicó en la sección anterior.

Como se dijo anteriormente, los equipos utilizados en estas soluciones tienen un nivel de criticidad alto, debido al tipo de exposición, en muchos casos hostil, debido a que se implementan en lugares que, en algunas ocasiones, no cumplen con las condiciones ideales para mantener los dispositivos en buen estado.

Sin embargo, las instituciones educativas presentan características particulares, que hacen que de cierta forma el nivel de criticidad aumente en mayor medida, pues es ne-

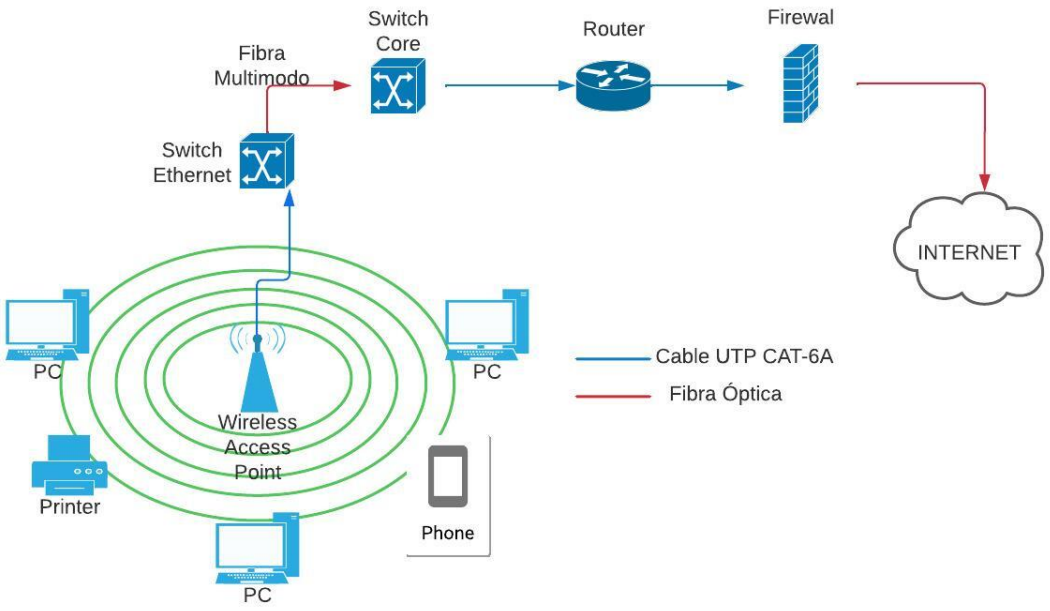

Figura 2.5: Diseño básico de red inalámbrica educativa.
Fuente: Elaboración propia.

cesario establecer un servicio constante para tráfico alto y acceso de múltiples usuarios, que hace que los recursos utilizados por los equipos crezcan y que se deban monitorear constantemente para brindar el mejor servicio a los usuarios finales.

2.3. Requerimientos de la herramienta de monitoreo

Para el desarrollo de la herramienta es importante tener en cuenta algunos criterios que logren cumplir con la necesidades de la empresa REDELECTRON-D&S S.A.S.. El primero de ellos es la capacidad de monitorear casi la totalidad de los dispositivos y servicios que son administrados por la empresa, es decir, todo lo expuesto en la Sección 2.2. El segundo criterio a tener en cuenta es que la solución sea completamente de código abierto (*Open Source*), con ello se garantiza que se puedan realizar los ajustes necesarios que permitan adaptarla a los múltiples escenarios donde se realizará el despliegue; finalmente, al no contar con el rol de administrador dentro de la empresa, es importante que se generen las alertas directamente en la herramienta de agendamiento de tareas, ya que no se pueden hacer el monitoreo constantemente, con ello se mitigaría la ausencia del administrador de red.

Ahora bien, es importante que la plataforma cuente con una interfaz amigable, que permita tener un resumen del estado general de los servicios y dispositivos, con el fin de facilitar al coordinador, la visualización e interacción con la solución.

Para lograr garantizar todos los criterios de forma óptima, es importante utilizar una plataforma ya existente, pues si se realiza un desarrollo desde cero, no se lograrían cumplir todos los criterios en los tiempos establecidos dentro del proyecto. En consecuencia, es necesario realizar un análisis de las plataformas de monitoreo ya existentes, con el fin de encontrar la que se adapte mejor a las necesidades de la empresa y con base en ella completar la generación de tareas que optimice la labor del coordinador.

2.4. Análisis de las herramientas de monitoreo

2.4.1. Zabbix

Zabbix es una herramienta de monitoreo y gestión de redes que se utiliza para medir el rendimiento y la disponibilidad de los servicios y sistemas de una organización. Esta herramienta de software libre está diseñada para monitorear y gestionar servidores, aplicaciones, servicios de red y dispositivos de red. [24]

A continuación, se exponen los diferentes componentes que permiten que sea una solución escalable para el monitoreo de redes:

- Servidor de Zabbix: El servidor es el componente principal de Zabbix y es responsable de recopilar datos, procesarlos y almacenarlos en la base de datos. El servidor también se encarga de enviar alertas cuando se detectan problemas en la red.
- Base de datos: Este componente permite almacenar los datos que son recogidos de las redes de telecomunicaciones por parte del servidor. Puede usar bases de datos como MySQL, PostgreSQL, Oracle, SQLite e IBM DB2.
- Agente de Zabbix: En las redes de telecomunicaciones, el agente se considera como un componente opcional que se instala en los equipos que deseen ser monitoreados, este componente envía los datos recopilados al servidor.
- Consola web: Esta interfaz de usuario es usada para administrar y configurar la herramienta de monitoreo; por medio de ella, los administradores pueden ver los gráficos de rendimiento, gestionar las alertas, generar informes y crear o agregar los objetos que van a ser monitoreados.

Zabbix tiene una amplia oferta de funciones y características de monitoreo y gestión de redes. Las siguientes son las características más notables incluyen:

- Monitoreo de red: Esta herramienta permite monitorear servidores, sistemas operativos, aplicaciones y terminales de red. Por otro lado, se pueden monitorear el tráfico de red, uso de CPU, la memoria, uso de los discos y demás parámetros que permiten evaluar el rendimiento de la red.

- Alertas: Zabbix permite definir y configurar las diferentes alertas, estableciendo los niveles de severidad y los canales de notificación. Los canales que tiene la herramienta son mensajes de texto, correo electrónico, entre otros.

- Automatización: Esta solución admite la automatización de acciones de monitoreo de las redes, con lo cual, los usuarios pueden programar funciones según los eventos que puedan presentarse.

- Visualización de datos: En este sentido, la herramienta ofrece una interfaz de usuario bastante completa que permite visualizar los datos obtenidos en el monitoreo, con gráficas en tiempo real y tablas de datos.

- Personalización: Zabbix es altamente personalizable y permite a los usuarios modificar la configuración para adaptarse a sus necesidades específicas de monitoreo y gestión de redes.

En resumen, Zabbix es una herramienta de monitoreo de redes altamente flexible, escalable y personalizable. Permite a los usuarios monitorear eficazmente su infraestructura de red, detectar y solucionar problemas en la red antes de que afecten la disponibilidad y el rendimiento de los servicios.

2.4.2. Nagios

Nagios es una herramienta de monitoreo de redes de código abierto que se lanzó en 1999. Inicialmente fue llamada NetSaint. Nagios fue desarrollada por Ethan Galstad y su objetivo fue otorgar una solución de monitoreo flexible y escalable para infraestructuras de red [25].

Nagios cuenta con varios componentes que se articulan para proporcionar un sistema de monitoreo bastante completo. Estos son los componentes que tiene el sistema:

- Servidor de Nagios: Como se dijo anteriormente, el servidor es componente principal de la herramienta, el cual recibe y administra los datos de monitoreo de la red.

- Complementos: Nagios utiliza una variedad de complementos para monitorear diferentes tipos de sistemas y servicios. Los complementos se ejecutan en los sistemas que se desean monitorear y envían datos al servidor de Nagios.

- Plugins: Los plugins son un componente particular de Nagios, pues realizan tareas específicas para el monitoreo. Los plugins pueden realizar tareas como verificar la disponibilidad de un servicio o enviar alertas a un sistema de gestión de tickets.
- Consola web: Esta interfaz web facilita a los administradores la lectura de datos y la generación de alertas, sin embargo, para poder manejarla se requiere un mínimo nivel de conocimientos en administración de red, pues no es muy intuitiva.

Las siguientes características son las más notables en el monitoreo de red de la herramienta Nagios:

- Monitoreo de red: Nagios permite monitorear los diferentes parámetros que determinan el rendimiento de la red y de los equipos, tales como tráfico, estado de CPU, entre otros.
- Alertas: La herramienta permite gestionar y determinar la severidad de las alertas y los canales por medio de los cuales se darán las notificaciones. Dentro de los canales se tiene correo electrónico, mensajes de texto, entre otros.
- Automatización: Nagios permite automatizar tareas para el monitoreo de las redes, por medio de las cuales se pueden programar las acciones frente a eventos que se presenten en la red.
- Visualización de datos: Nagios también ofrece la visualización de los datos por medio de gráficos en tiempo real y tablas de datos que permiten el análisis de estado.
- Personalización: Nagios es personalizable, pero se requiere un nivel mínimo de conocimientos para adaptar la herramienta a lo que se desea observar.

En resumen, Nagios es una herramienta de monitoreo que permite observar el rendimiento y disponibilidad de los servicios y equipos de una red de telecomunicaciones, para la cual se pueden configurar las alertas y el canal de notificación, sin embargo, es necesario contar con un conocimiento mínimo en administración de redes, pues la herramienta no es muy intuitiva.

2.4.3. PRTG *Network Monitor* (*Paessler Router Traffic Grapher*)

PRTG Network Monitor es una herramienta de monitoreo de redes de alto rendimiento que se utiliza para monitorear la disponibilidad y el rendimiento de los sistemas y servicios en una red de telecomunicaciones. La herramienta fue desarrollada por la empresa alemana Paessler AG y se ha convertido en una opción popular para empresas de todos los tamaños [26].

PRTG cuenta con los siguientes componentes para el monitoreo de las redes:

- Servidor de PRTG: Como se ha venido diciendo, el servidor es el componente más importante para una herramienta de monitoreo, pues se encarga de recopilar y administrar los datos que permiten analizar el rendimiento de la red.
- Sensores: PRTG utiliza una variedad de sensores para monitorear diferentes tipos de sistemas y servicios. Los sensores se ejecutan en los sistemas que se desean monitorear y envían datos al servidor de PRTG.
- Consola web: La interfaz web permite el uso de la herramienta por parte de los usuarios, por medio de la cual se admite realizar configuraciones y adaptaciones de la herramienta para personalizarla.

Las características con las que cuenta la herramienta PRTG para el monitoreo de las redes son las siguientes:

- Monitoreo de red: La principal característica de la herramienta es el monitoreo de los diferentes servicios y dispositivos que componen las redes de telecomunicaciones, dentro de las cuales se tienen servidores, terminales de red, entre otros.
- Alertas: PRTG también permite la personalización de la severidad de las alertas y definir los canales de notificación para los administradores.
- Automatización: Esta herramienta cuenta con una amplia popularidad por la automatización de sus tareas, sin embargo, muchas de estas características están privilegiadas para usuario de pago.
- Visualización de datos: PRTG tiene una interfaz web que permite observar con gráficas en tiempo real y tablas de datos el estado de los servicios, sin embargo, esta interfaz es poco intuitiva y amigable.
- Personalización: PRTG es personalizable, pero muchas de sus opciones están limitadas por las opciones de pago que tiene la herramienta.

PRTG se puede instalar en sistemas operativos Windows y Linux y es fácil de configurar y usar. La herramienta también es escalable, lo que la convierte en una opción viable para empresas.

2.4.4. CheckMK

CheckMK es una herramienta de monitoreo de red que se utiliza para administrar el rendimiento y la disponibilidad de los sistemas y servicios de una red de telecomunicaciones. Fue desarrollada por Mathias Kettner en el año 2005 y actualmente es mantenida por la empresa alemana Tribe29 [27].

Check MK está basada en Nagios y utiliza su arquitectura de plugins para realizar el monitoreo. Sin embargo, CheckMK puede considerarse como una herramienta más

avanzada que Nagios, ya que incluye una variedad de características adicionales y una interfaz web más amigable e intuitiva.

Los componentes que CheckMK utiliza para el monitoreo de la red son los siguientes:

- CheckMK Server: Es el principal componente de la herramienta de monitoreo Check MK, pues se encarga de recopilar y procesar datos de monitoreo. Este servidor también es responsable de administrar alertas cuando se detectan problemas en la red.
- Agentes: CheckMK utiliza agentes para recopilar datos de monitoreo de los sistemas que se desean monitorear. Los agentes se ejecutan en los sistemas que se desean monitorear y envían datos al servidor de CheckMK.
- Consola web: La interfaz web de la herramienta de monitoreo es bastante intuitiva y permita una alta personalización de sus características, por medio de ella se pueden gestionar los servicios y equipos que se monitorean, así como las alertas y notificaciones.

Las características relevantes de CheckMK son las siguientes:

- Monitoreo de red: CheckMK permite evaluar el rendimiento de la red, el estado de los diferentes dispositivos asociados, entre otros, de la misma manera como lo manejan las demás herramientas expuestas.
- Alertas: Esta herramienta también permite la configuración y personalización de la severidad de las alertas, así como los canales de notificación que se usarán para reportar fallas en la red.
- Automatización: En esta herramienta también se pueden automatizar procesos, los cuales permiten programar tareas que deben ejecutarse frente a eventos que sucedan en la red.
- Visualización de datos: La visualización del estado de la red es uno de los fuertes de la herramienta, pues se ha empeñado en brindar una interfaz amigable para el usuario que permita identificar con claridad posibles problemas sin dejar de lado el diseño.
- Personalización: La herramienta es altamente personalizable, pero no cuenta con documentación abundante y recomendaciones de uso suficientes para realizar un buen despliegue, por lo que se requiere un nivel de conocimiento medio para su configuración.

En resumen, CheckMK es una herramienta de monitoreo bastante moderna, que cuenta con herramientas avanzadas de monitoreo y que puede ser utilizadas en diferentes sistemas operativos, sin embargo, para poder configurarla y utilizarla de la mejor manera se debe contar con un nivel de conocimiento medio para entender sus funciones.

2.5. Análisis comparativo de las herramientas de monitoreo

2.5.1. Análisis de funcionalidad de herramientas de monitoreo de redes

Para hacer una comparación exhaustiva sobre las herramientas de monitoreo anteriormente expuestas, es importante realizar un análisis de sus funcionalidades; a continuación, se presentará una breve explicación de las herramientas una vez instaladas:

Zabbix

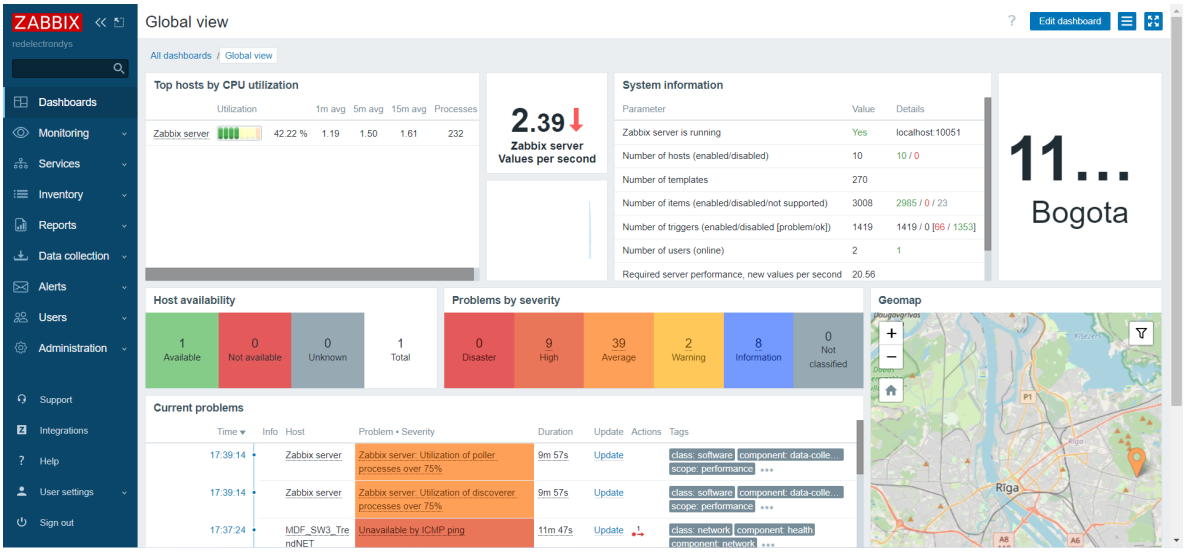

Figura 2.6: Panel principal de Zabbix.
Fuente: Elaboración propia.

Como se observa en la Figura 2.6, la herramienta de monitoreo Zabbix muestra un panel principal muy completo donde se puede obtener información general de las alertas generadas en los diferentes dispositivos, una línea de tiempo de estas, un estado general los elementos monitoreados y el estado del servidor. Todas estas opciones garantizan para el adminitrador el monitoreo completo de las redes y los elementos de la componen.

Nagios

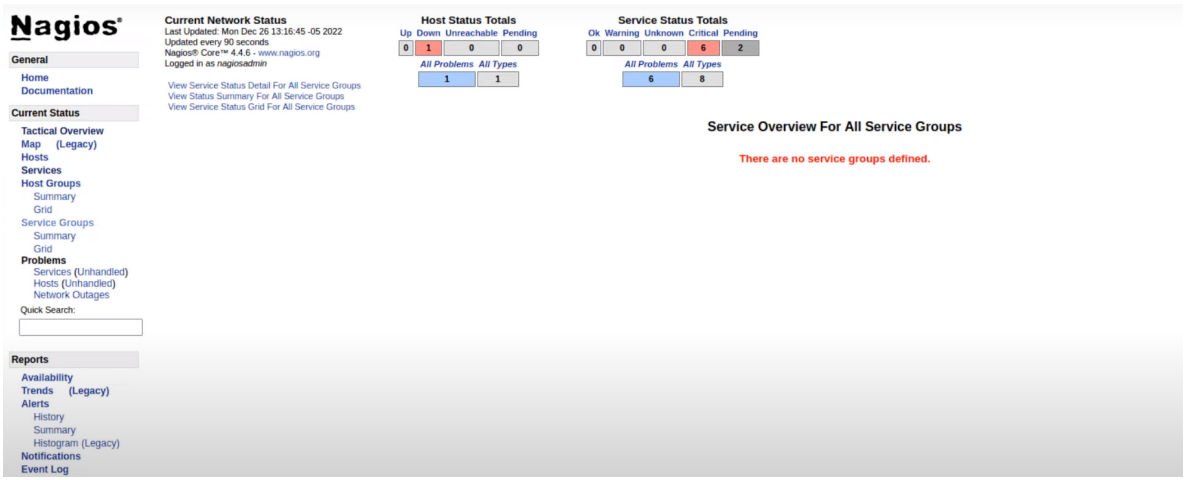

Figura 2.7: Panel principal de Nagios.
Fuente: Elaboración propia.

En la Figura 2.7 se puede observar que la herramienta de monitoreo Nagios cuenta con una interfaz WEB bastante básica en su estado inicial, que no permite tener un monitoreo interactivo de la red y sus dispositivos, pues no cuenta con la opción de gráficas amigables que ayuden al administrador de la red en la optimización de sus labores.

PRTG Network Monitor

Figura 2.8: Panel principal de PRTG Network Monitor.
Fuente: Elaboración propia.

La Figura 2.8 muestra que PRTG Network Monitor es una herramienta de monitoreo muy interactiva que cuenta con resúmenes generales del estado de los sensores, un resumen del número de alertas generadas; sin embargo, para poder mejorar la experiencia es necesario realizar la activación de los planes de pago, con ello se podrá garantizar la completa operación de las funcionalidades que ayuden de forma integral en el monitoreo de las redes y servicios por parte del administrador.

CheckMK

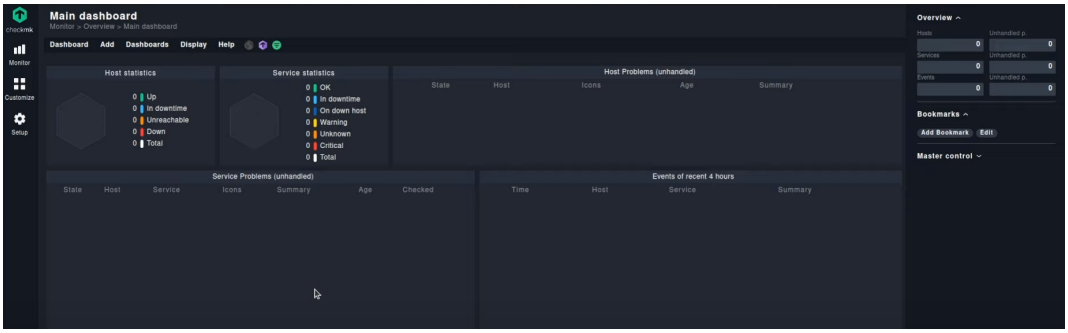

Figura 2.9: Panel principal de Check MK.
Fuente: Elaboración propia.

Como se observa en la Figura 2.9, la herramienta de monitoreo Check MK es interactiva; sin embargo, se evidencia que la herramienta viene por defecto incompleta y debe ser modulada de la misma manera que se hace con Nagios, lo que limita la interacción por parte del administrador. Las funcionalidades deben ser configuradas inicialmente para poder ser utilizadas, y para realizar un despliegue mayor es necesario realizar el pago de licencias.

2.5.2. Tabla comparativa de herramientas de monitoreo

A continuación, se presenta una tabla (Tabla 2.1) comparativa de las herramientas descritas en la sección anterior, donde se evidencian los aspectos más importantes de las herramientas, las ventajas y desventajas de cada una de ellas; ayudando a determinar la herramienta que mejor se adapte a las necesidades y requerimientos de la empresa REDELECTRON-D&S S.A.S.

Es importante tener en cuenta que todas estas herramientas tienen la capacidad de monitorear una amplia variedad de servicios y sistemas operativos, aunque algunas pueden tener una mejor integración con ciertas bases de datos. También es esencial verificar los requisitos de sistema para cada herramienta antes de implementarla, para asegurarse de que se ajuste a las capacidades de la infraestructura existente.

Finalmente, se puede concluir que cada herramienta de monitoreo tiene sus propias ventajas y desventajas en función de las necesidades y los requerimientos de la empresa.

Tabla 2.1: Tabla comparativa de herramientas de monitoreo

Herramienta	**Zabbix**	**Nagios**	**PRTG**	**CheckMK**
Cantidad de Servicios monitoreados	Cumple	Cumple.	Cumple.	Cumple.
Código abierto	Cumple.	Cumple.	No cumple.	Cumple.
Curva de aprendizaje	No cumple	No cumple.	Cumple.	No cumple.
Sistemas Operativos soportados	Cumple.	Cumple.	Cumple.	Cumple.
Bases de datos soportadas	Cumple.	Cumple.	No cumple.	Cumple.
Interfaz web	Cumple.	No cumple.	Cumple.	No cumple.
Requeri- mientos del Sistema	Cumple.	Cumple.	No cumple.	Cumple.

Zabbix es una buena opción para quienes buscan una herramienta de código abierto y escalable. Adicional a ello, se puede considerar que esta herramienta es altamente personalizable y su interfaz de usuario es muy intuitiva; los recursos computacionales requeridos para el servidor son bajos y finalmente, cuenta con un gran servicio de configuración de alertas y notificaciones; por otra parte, su amplia documentación para implementación y configuración permite que cualquiera, con conocimientos en administración de redes de telecomunicación consiga adaptar la herramienta a las necesidades futuras que puedan presentarse.

Por todo lo dicho anteriormente, además del análisis realizado en torno de las diferentes herramientas de monitoreo, Zabbix se convierte en la herramienta ideal para la implementación dentro de la empresa REDELECTRON-D&S S.A.S., pues se adapta a las necesidades actuales de la empresa y es escalable frente a los posibles requerimientos futuros que puedan presentarse, para brindar nuevos servicios.

CAPÍTULO 3

IMPLEMENTACIÓN Y CONFIGURACIÓN DE LA HERRAMIENTA DE MONITOREO

En el presente capítulo se desarrolla el proceso de implementación de la herramienta de monitoreo; para ello se inicia con la instalación del software en el servidor, que hace las veces controlador de la red. Posteriormente, se hace el análisis para establecer la matriz de riesgos para definir la criticidad de las alarmas de los equipos que se van a monitorear; con este análisis se establece la configuración correcta de la herramienta de monitoreo para que pueda generar las notificaciones necesarias frente a los incidentes, con esta configuración queda completamente implementada la herramienta.

3.1. Instalación inicial de la herramienta de monitoreo Zabbix

Para realizar la instalación del software de la herramienta de monitoreo se utilizará la guía de instalación del sitio web oficial de Zabbix [28]. Esta corresponde a la instalación para un sistema operativo Linux Ubuntu (versión 22.04, denominada Jammy). Para ello, es necesario tener en cuenta los recursos físicos mínimos del sistema para que la herramienta opere adecuadamente, los cuales son los siguientes: una CPU mínima de 2 GHz con 2 núcleos, memoria RAM de 4 GB y disco duro con 20 GB libres. Adicional a estos recursos físicos, la herramienta necesita trabajar con otros servicios adicionales, tales como, motor de bases de datos, servicio web, entre otros; los cuales, deben ser instalados en el servidor.

3.1.1. Instalación de los servicios preliminares y del software de Zabbix

Inicialmente, se debe abrir la consola en el servidor y se utiliza el comando para la descarga del instalador y su puesta en marcha del repositorio oficial de la herramienta Zabbix, con este comando se inicia la instalación del software, como se ve en la Figura 3.1.

Por medio del comando de la Figura 3.2, se inicializa la instalación que se descargó anteriormente, el cual corresponde con la versión del sistema operativo del servidor.

Posterior, se debe realizar una actualización del repositorio interno del servidor, como se muestra en la Figura 3.3, con el fin de garantizar que se tenga a disposición los

Figura 3.1: Diseño básico de red educativa.
Fuente: Elaboración propia.

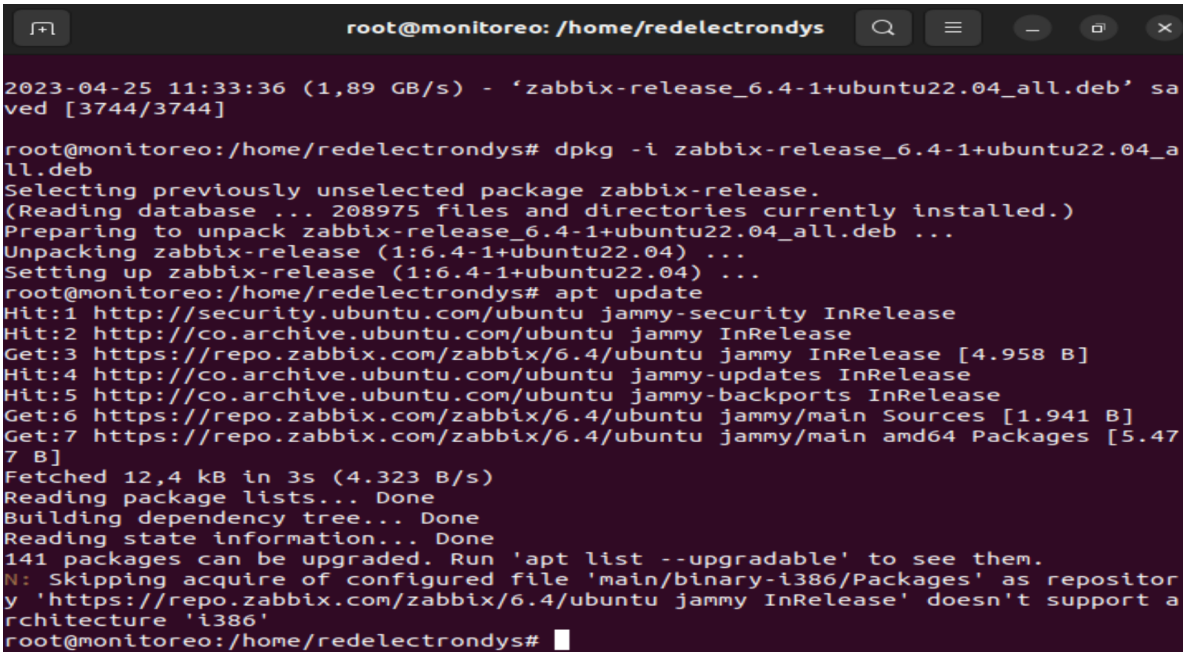

Figura 3.2: Inicialización del instalador de Zabbix.
Fuente: Elaboración propia.

últimos servicios instalados.

Como se explicó en el capítulo anterior, la herramienta de monitoreo Zabbix cuenta con ciertos componentes que permiten su funcionamiento correcto, para ello, con el comando de la Figura 3.4 se instalará el servidor, la interfaz WEB y el agente en el equipo, con ello se establece como dispositivo controlador de la herramienta de monitoreo. La

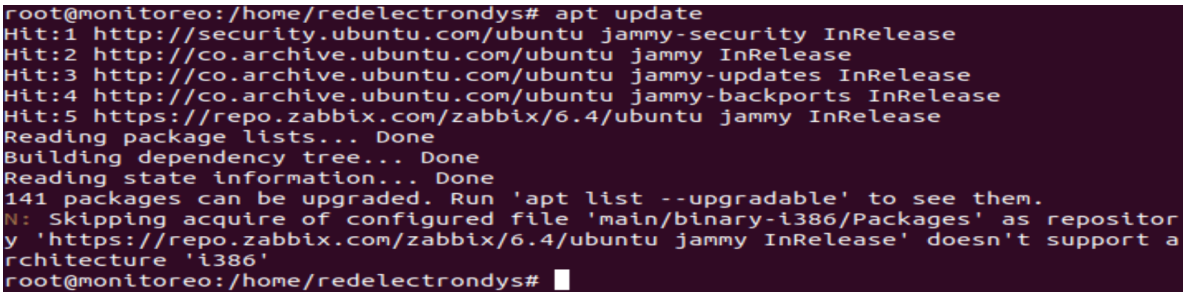

Figura 3.3: Actualización del repositorio del servidor.
Fuente: Elaboración propia.

interfaz WEB funciona con el servicio Apache, el motor de base de datos que se eligió es MySQL, el cual será instalado en el mismo servidor, para poder recolectar los datos que enviaran los dispositivos que se van a monitorear.

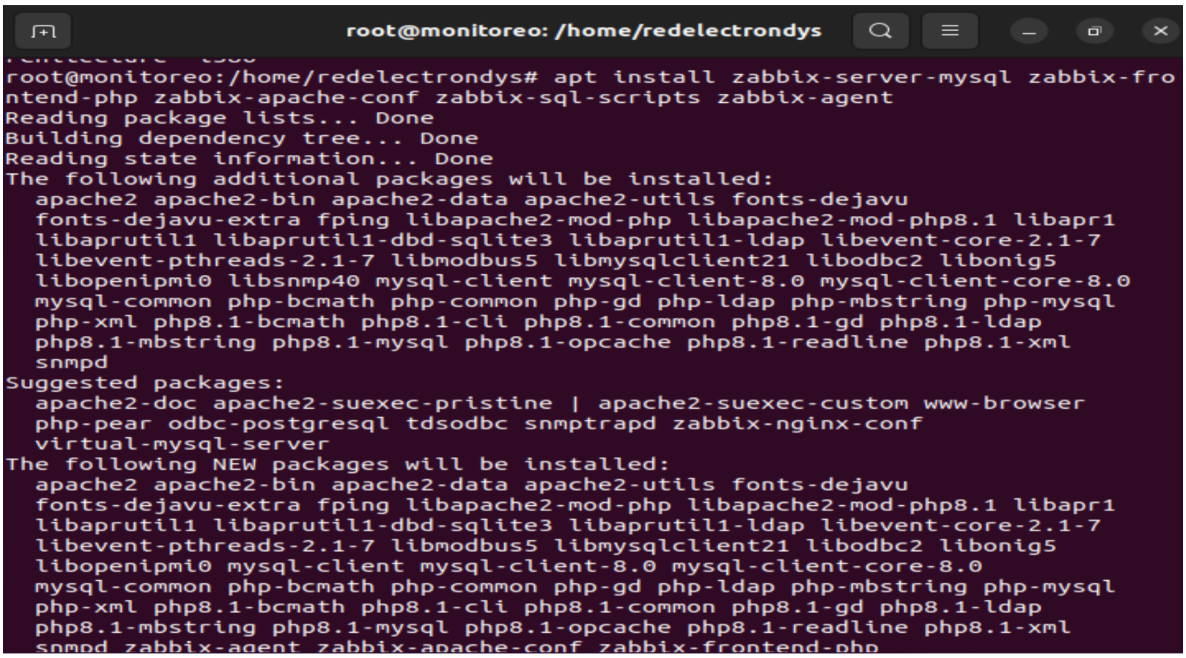

Figura 3.4: Instalación Servidor Zabbix.
Fuente: Elaboración propia.

A continuación, se realiza la instalación del servidor del motor de bases de datos que para el caso actual será MySQL (Figura 3.5), se debe realizar la instalación pues no se encuentra instalado originalmente en el sistema operativo. Para ello se utilizará la guía del sitio oficial de Ubuntu, pero la configuración se hará con las condiciones adecuadas para el servidor de monitoreo [29].

```
root@monitoreo:/home/redelectrondys# apt install mysql-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libcgi-fast-perl libcgi-pm-perl libfcgi-bin libfcgi-perl libfcgi0ldbl
  libhtml-template-perl mecab-ipadic mecab-ipadic-utf8 mecab-utils
  mysql-server-8.0
Suggested packages:
  libipc-sharedcache-perl mailx tinyca
The following NEW packages will be installed:
  libcgi-fast-perl libcgi-pm-perl libfcgi-bin libfcgi-perl libfcgi0ldbl
  libhtml-template-perl mecab-ipadic mecab-ipadic-utf8 mecab-utils
  mysql-server mysql-server-8.0
0 upgraded, 11 newly installed, 0 to remove and 140 not upgraded.
Need to get 8.483 kB of archives.
After this operation, 57,0 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://co.archive.ubuntu.com/ubuntu jammy-updates/main amd64 mysql-server
-8.0 amd64 8.0.32-0ubuntu0.22.04.2 [1.427 kB]
Get:2 http://co.archive.ubuntu.com/ubuntu jammy/main amd64 libcgi-pm-perl all 4
.54-1 [188 kB]
Get:3 http://co.archive.ubuntu.com/ubuntu jammy/main amd64 libfcgi0ldbl amd64 2
.4.2-2build2 [28,0 kB]
Get:4 http://co.archive.ubuntu.com/ubuntu jammy/main amd64 libfcgi-perl amd64 0
.82+ds-1build1 [22,8 kB]
Get:5 http://co.archive.ubuntu.com/ubuntu jammy/main amd64 libcgi-fast-perl all
 1:2.15-1 [10,5 kB]
```

Figura 3.5: Instalación del servidor del monitor de bases de datos MySQL.
Fuente: Elaboración propia.

Para poder iniciar el almacenamiento de datos en MySQL se hace necesario crear un base de datos con las condiciones iniciales para el servicio de Zabbix, en este paso se deben crear las credenciales de usuario para tener acceso, por ello es importante seguir las indicaciones que muestran en la Figura 3.6.

```
root@monitoreo: /home/redelectrondys
redelectrondys@monitoreo:~$ sudo su
[sudo] contraseña para redelectrondys:
root@monitoreo:/home/redelectrondys# mysql -uroot -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 10
Server version: 8.0.32-0ubuntu0.22.04.2 (Ubuntu)

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;
Query OK, 1 row affected (0,04 sec)

mysql> create user zabbix@localhost identified by 'password';
ERROR 1819 (HY000): Your password does not satisfy the current policy requireme
nts
mysql> create user zabbix@localhost identified by 'Monitoreo2023*';
Query OK, 0 rows affected (0,04 sec)

mysql> grant all privileges on zabbix.* to zabbix@localhost;
Query OK, 0 rows affected (0,03 sec)
```

Figura 3.6: Configuración de la base de datos inicial en MySQL.
Fuente: Elaboración propia.

Finalmente, se deben asignar los privilegios necesarios para la realización de consultas en la base de datos creada para Zabbix como en la Figura 3.7.

```
mysql> grant all privileges on zabbix.* to zabbix@localhost;
Query OK, 0 rows affected (0,03 sec)

mysql> set global log_bin_trust_function_creators = 1;
Query OK, 0 rows affected (0,00 sec)

mysql> quit
Bye
root@monitoreo:/home/redelectrondys#
```

Figura 3.7: Asignación de privilegios para la base de datos de Zabbix.
Fuente: Elaboración propia.

Con el fin de mejorar los estándares de seguridad del servicio se actualizan los componentes de seguridad del motor de bases de datos, cumpliendo con los requerimientos establecidos por el mismo servicio, por este motivo se redefine una nueva contraseña de usuario que sea validada por el servidor MySQL como se muestra en la Figura 3.8.

```
root@monitoreo: /home/redelectrondys
update-alternatives: using /var/lib/mecab/dic/ipadic-utf8 to provide /var/lib/m
ecab/dic/debian (mecab-dictionary) in auto mode
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
root@monitoreo:/home/redelectrondys# systemctl start mysql.service
root@monitoreo:/home/redelectrondys# mysql_secure_installation

Securing the MySQL server deployment.

Connecting to MySQL using a blank password.

VALIDATE PASSWORD COMPONENT can be used to test passwords
and improve security. It checks the strength of password
and allows the users to set only those passwords which are
secure enough. Would you like to setup VALIDATE PASSWORD component?

Press y|Y for Yes, any other key for No: y

There are three levels of password validation policy:

LOW    Length >= 8
MEDIUM Length >= 8, numeric, mixed case, and special characters
STRONG Length >= 8, numeric, mixed case, special characters and dictionary
            file

Please enter 0 = LOW, 1 = MEDIUM and 2 = STRONG: 2
Please set the password for root here.
```

Figura 3.8: Configuración de seguridad de la base de datos de MySQL.
Fuente: Elaboración propia.

Para poder almacenar los datos que se van a recolectar de los dispositivos Zabbix, se ha creado un esquema de base de datos, este debe ser importado como se muestra en la Figura 3.9. Con ello se garantiza un almacenamiento adecuado de la información para poder ser leído por el software y mostrados en la interfaz WEB de la herramienta.

Para finalizar la configuración del motor de bases de datos, se configuran los privilegios nuevamente a su valor por defecto para que la base de datos pueda ser gestionada

```
root@monitoreo:/home/redelectrondys# zcat /usr/share/zabbix-sql-scripts/mysql/s
erver.sql.gz | mysql --default-character-set=utf8mb4 -uzabbix -p zabbix
Enter password:


root@monitoreo:/home/redelectrondys#
root@monitoreo:/home/redelectrondys#
root@monitoreo:/home/redelectrondys#
```

Figura 3.9: Importación del esquema de bases de datos de Zabbix.
Fuente: Elaboración propia.

por el servicio de Zabbix y con ello poder realizar las consultas necesarias para el monitoreo de los equipos de red (Figura 3.10).

```
root@monitoreo:/home/redelectrondys# mysql -uroot -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 8.0.32-0ubuntu0.22.04.2 (Ubuntu)

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql> set global log_bin_trust_function_creators = 0;
Query OK, 0 rows affected (0,00 sec)

mysql> quit;
Bye
root@monitoreo:/home/redelectrondys#
```

Figura 3.10: Configuración de privilegios de usuario.
Fuente: Elaboración propia.

Se procede a configurar la contraseña de usuario para ingreso a la base de datos del servicio de Zabbix, para la Figura 3.11 se utilizará una contraseña de ejemplo para efectos prácticos, la cual será cambiada por motivos de seguridad. La contraseña se cambia en el archivo de configuración propio del servidor de la herramienta.

Posteriormente, se debe configurar la zona horaria del servidor, ya que tiene valores por defecto diferentes a la ubicación real. Con ello se garantiza que el servicio cumpla con las condiciones ideales de funcionamiento, pues todos los datos recolectados son dependientes de la hora de recolección y una configuración diferente haría variar los parámetros recolectados (Figura 3.12).

Finalmente, es necesario hacer un reinicio de los servicios de la herramienta como se ve en la Figura 3.13, esto se realiza para que puedan ser cargadas de forma exitosa todas las configuraciones iniciales que se han realizado; una vez realizado el restablecimiento de los servicios se procede a habilitarlos para que puedan entrar en funcionamiento y se integren a la herramienta de gestión para poder pasar a la configuración en interfaz WEB, como se explicará en la siguiente sección.

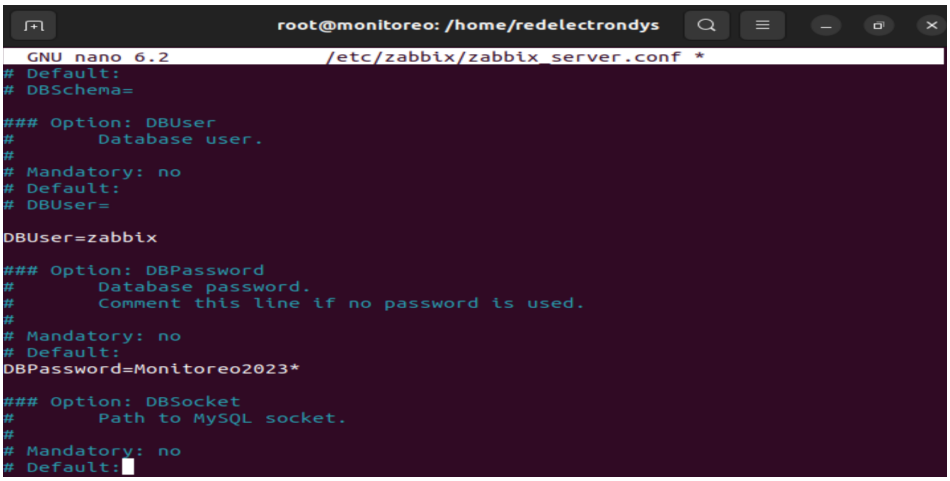

Figura 3.11: Cambio de contraseña de acceso a la base de datos del servicio Zabbix.
Fuente: Elaboración propia.

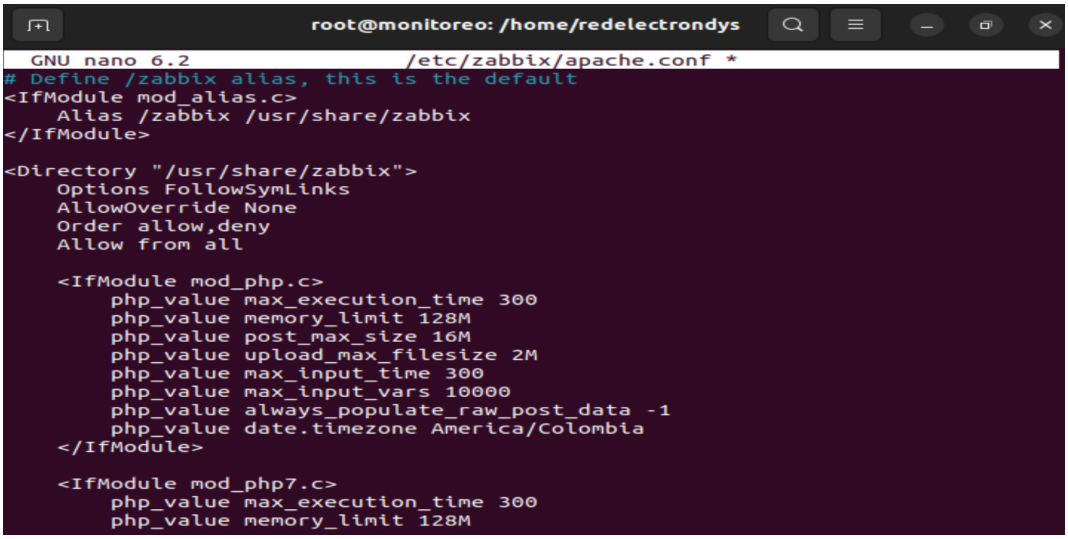

Figura 3.12: Definición de la zona horaria de la ubicación del servidor.
Fuente: Elaboración propia.

3.1.2. Configuración inicial de la interfaz WEB

Una vez terminada la configuración inicial por consola, es necesario realizar algunos ajustes sobre la interfaz. Inicialmente, como se ve en la Figura 3.14, se establece el idioma con el que trabajará la herramienta. Se escoge el idioma inglés, pues no se tiene la opción en español y es el lenguaje más conocido con el que cuenta la herramienta [30].

Posterior a ello, la herramienta realiza un análisis del servidor donde está instalado, con el fin de verificar si se cuenta con los requisitos previos para poder lanzar el programa, en la Figura 3.15. se evidencia que no existe ninguna restricción inicial para proceder con la configuración de la herramienta.

```
root@monitoreo:/home/redelectrondys# systemctl restart zabbix-server zabbix-age
nt apache2
root@monitoreo:/home/redelectrondys# systemctl enable zabbix-server zabbix-agen
t apache2
Synchronizing state of zabbix-server.service with SysV service script with /lib
/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable zabbix-server
Synchronizing state of zabbix-agent.service with SysV service script with /lib/
systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable zabbix-agent
Synchronizing state of apache2.service with SysV service script with /lib/syste
md/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2
Created symlink /etc/systemd/system/multi-user.target.wants/zabbix-server.servi
ce → /lib/systemd/system/zabbix-server.service.
root@monitoreo:/home/redelectrondys#
```

Figura 3.13: Restablecimiento y habilitación de los servicios.
Fuente: Elaboración propia.

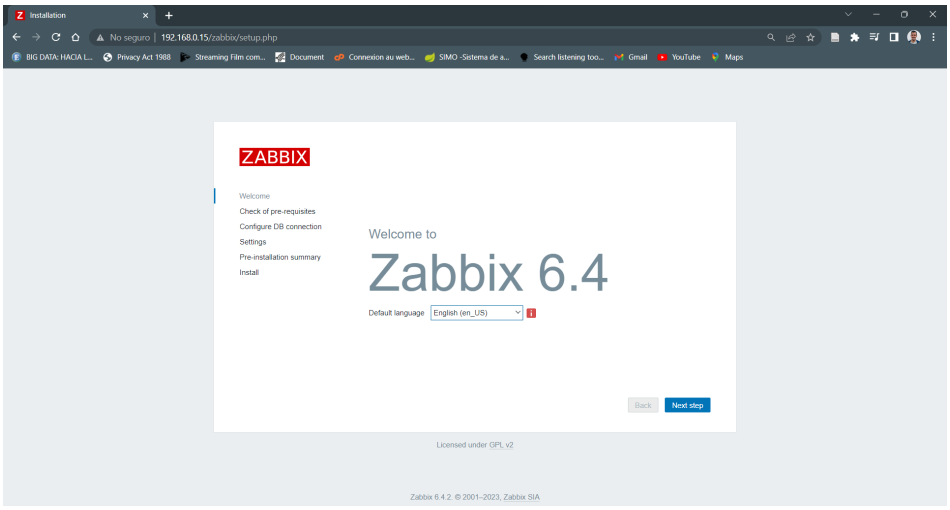

Figura 3.14: Inicio de interfaz WEB Zabbix.
Fuente: Elaboración propia.

Después de realizar el chequeo, se debe configurar la conexión a la base de datos, como anteriormente se definió el motor de base de datos y las credenciales de acceso, entonces en este caso se deben colocar estos datos para poder acceder al motor de base de datos y empezar a guardar la información en ella, este acceso se realiza como se muestra en la Figura 3.16.

Ahora se inicia la configuración del servidor de Zabbix, se define el nombre, la zona horaria donde va a trabajar la herramienta, para que no exista errores en la programación de tareas y generación de alertas, y el color de la interfaz de usuario, para el caso actual, se colocará en oscuro, como se ve en la Figura 3.17.

Se muestra un resumen de la configuración que tendrá la herramienta, donde se observa el motor de base de datos, la ubicación del mismo, el usuario que ingresa a la base de

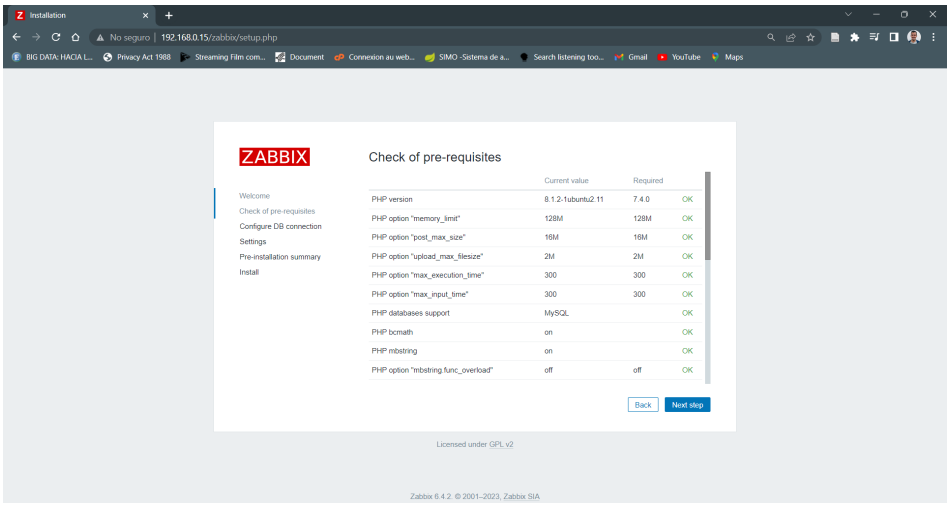

Figura 3.15: Verificación de requisitos.
Fuente: Elaboración propia.

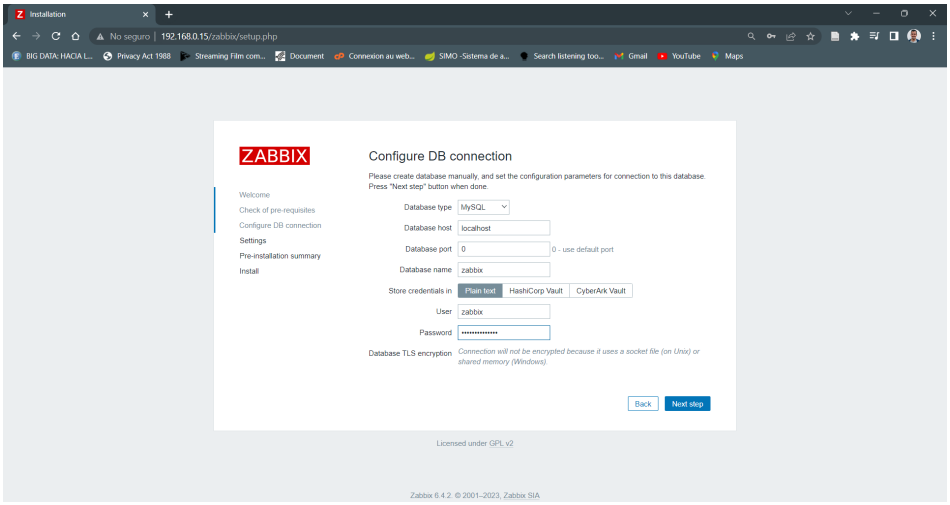

Figura 3.16: Verificación de la correcta instalación.
Fuente: Elaboración propia.

datos y el nombre del servidor de Zabbix, como se ve en la Figura 3.18.

Finalmente, si todo se ha hecho de manera correcta, la herramienta dará la bienvenida como en la Figura 3.19. pudiendo iniciar así con el acceso a la interfaz WEB.

En la Figura 3.20, se puede observar la pantalla principal de la interfaz WEB de la herramienta, con su configuración inicial y sin haber personalizado ninguna de las opciones de monitoreo.

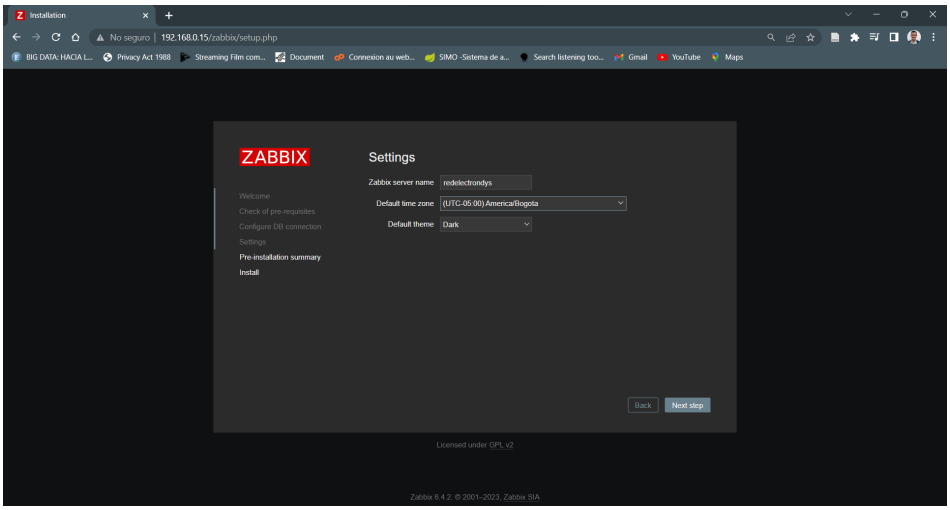

Figura 3.17: Configuración del nombre del servidor.
Fuente: Elaboración propia.

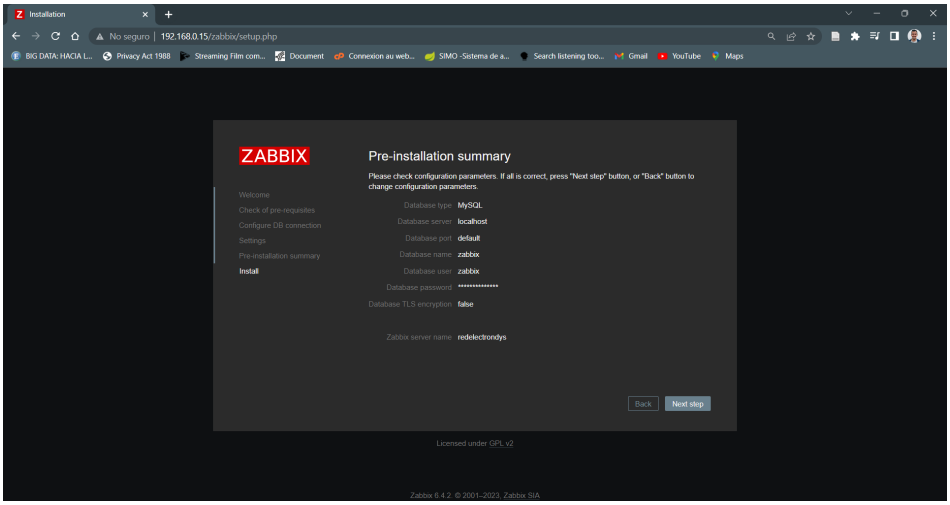

Figura 3.18: Sumario de preinstalación.
Fuente: Elaboración propia.

3.1.3. Análisis de riesgos para la configuración de alertas en la herramienta de monitoreo

Dentro de las buenas prácticas que deben llevarse a cabo en el despliegue de sistemas de telecomunicaciones, debe tenerse en cuenta un aspecto importante, que es el gobierno de las tecnologías de la información [31]. La necesidad de salvaguardar a las organizaciones del uso inadecuado de estas tecnologías, ha dado como resultado la creación de políticas que permitan definir cómo se debe operar la gobernanza [32]. En este mismo sentido, la gestión de los riesgos juega un papel muy importante, pues ayuda a definir, por medio de análisis cualitativos y cuantitativos, las decisiones que deben ser tomadas dentro de las organizaciones para mitigar las amenazas que puedan llegar a

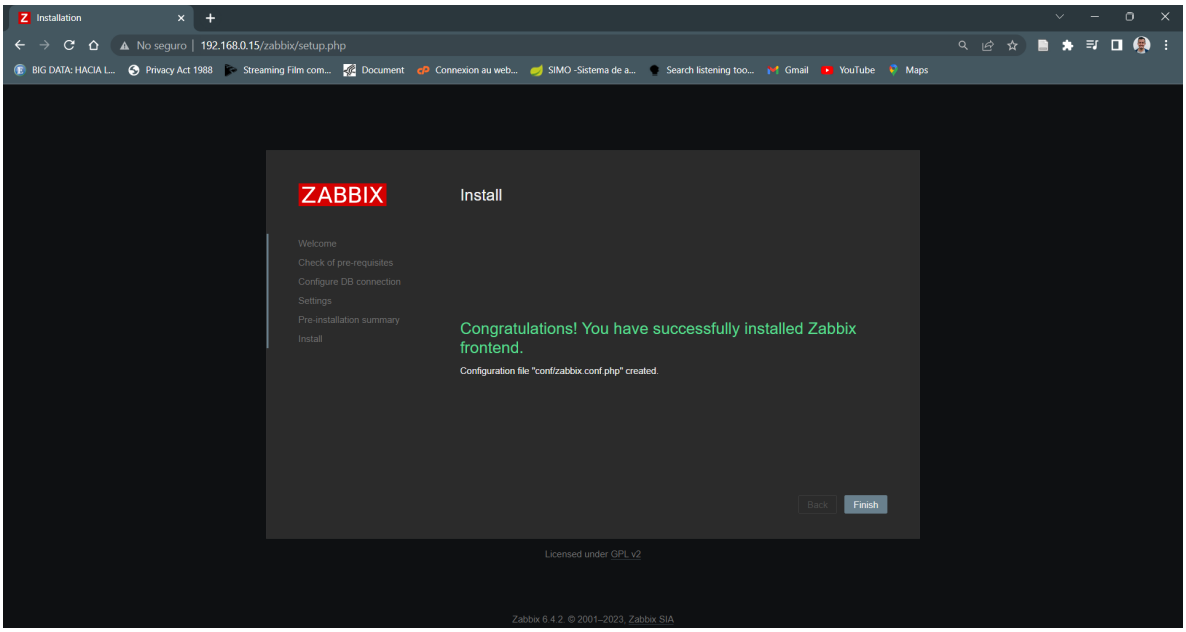

Figura 3.19: Instalación de la interfaz WEB.
Fuente: Elaboración propia.

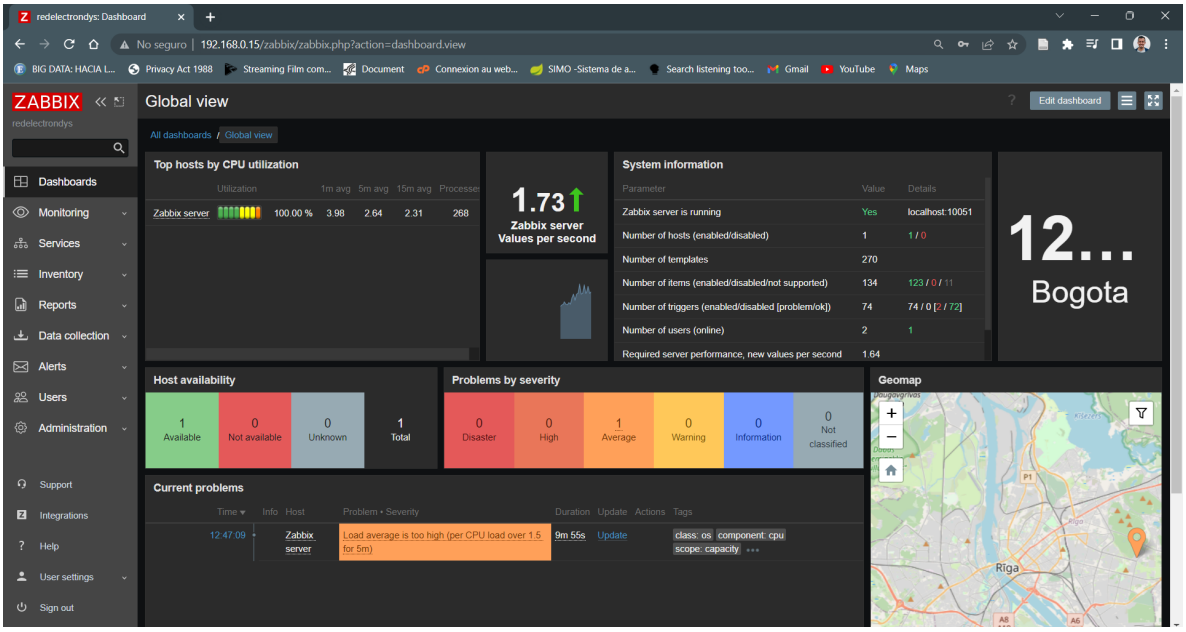

Figura 3.20: Panel principal de Zabbix.
Fuente: Elaboración propia.

presentarse a los servicios de información.

Por este motivo, se hace primordial realizar un análisis detallado de las diferentes tec-

nologías que componen los sistemas de comunicaciones de la empresa REDELECTRON-D&S S.A.S., para establecer el nivel de criticidad que cada uno de los componentes juega en la prestación de servicios, y con ello, configurar los niveles de alarmas que debe arrojar la herramienta de monitoreo.

Para ello, se utilizará la metodología MAGERIT, elaborada por el entonces Consejo Superior de Administración Electrónica de España, actualmente conocido como la Secretaría General de Administración Digital. Esta metodología busca establecer un proceso de gestión de riesgo, como lo define la ISO 31000 [8]; para poder contrarrestar las constantes amenazas a las que podrían estar expuestos los sistemas de información y comunicación en las diferentes organizaciones [33].

Con base en la guía técnica de la metodología MAGERIT versión 3, se procede a realizar la implementación del análisis de riesgo de la siguiente manera: en un primer momento se realiza la planificación de la implementación de la metodología, donde se adelanta un diagnóstico del estado general de los sistemas de comunicación, para poder definir el alcance que tiene el análisis. En un segundo momento, se lleva a cabo un proceso de identificación de activos, donde por medio de tablas se resaltan cada uno de los componentes del sistema de comunicaciones que se va a monitorear, aquí se definen los valores que cada uno de los activos tiene dentro del sistema. Finalmente, establecer la matriz de riesgos con la que se va a trabajar para la configuración de la herramienta.

Planificación

La implementación de esta, surge de la necesidad de establecer valor de criticidad de alarmas en los equipos de red que van a ser monitoreados por la herramienta Zabbix implementada. Para ello es importante definir, por medio de una matriz de riesgos, las diferentes amenazas a las que podrían estar expuestos los equipos; amenazas que puedan ser cualificadas y cuantificadas por la herramienta y que permitan proveer posibles fallas en los servicios prestados por la empresa REDELECTRON-D&S S.A.S.

Basándose en las experiencias del equipo de trabajo de la empresa, y teniendo en cuenta la función de cada dispositivo de red, realizará una descripción detallada de los componentes del servicio, así como sus valores de riesgo ante posibles fallas. Para el análisis se tendrá en cuenta una de las redes educativas que ha sido implementadas por la empresa, donde se ofrecen servicios de conectividad de alto rendimiento, y que es una de las redes más completa para ser monitoreada.

Análisis de riesgo

Para poder implementar el análisis de riesgo se tendrá en cuenta el diagrama que se ve en la Figura 3.21. donde se muestran los diferentes componentes que se deben tener

en cuenta a la hora de establecer el análisis. Los activos representan el elemento más importante del análisis, pues son ellos quienes están expuestos a las amenazas, las cuales causan degradaciones en el servicio y que tienen una cierta frecuencia de ocurrencia, por lo que se convierten en un riesgo para la organización. Estos activos también interesan por su valor, pues tienen un impacto dentro del sistema para que todo funcione adecuadamente, de manera que, cuando no es así, ellos mismos se convierten en un factor de riesgo para la óptima operación [34].

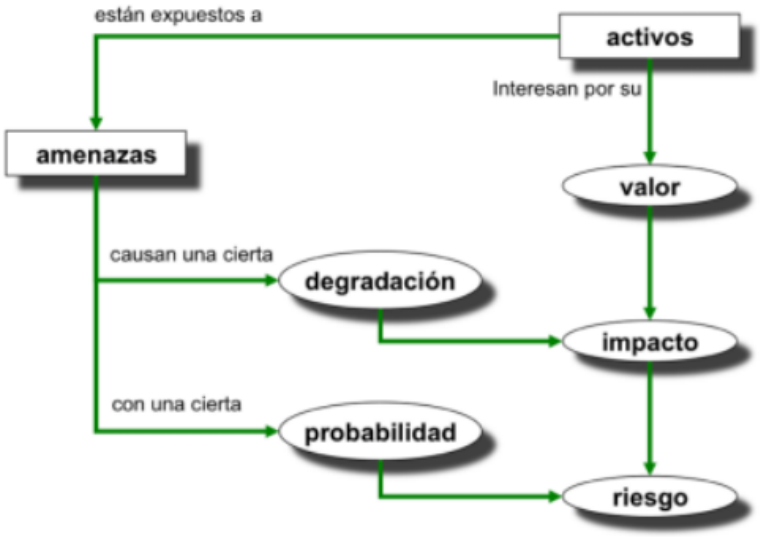

Figura 3.21: Diagrama de la metodología MAGERIT.
Fuente: Tomado de [34].

Por este motivo, lo primero que se debe realizar es una caracterización de los activos, donde se da una explicación detallada de su función dentro del sistema. Con base en el segundo libro de la metodología de MAGERIT versión 3, se hace inicialmente una identificación de los activos que componen la infraestructura de red, en conjunto con sus servicios prestados.

Tabla 3.1: Activos en una infraestructura de red en la empresa REDELECTRON-D&S S.A.S.

TIPO	**NOMBRE DEL ACTIVO**
SERVICIOS	1. [TOIP] Servidor Telefonía IP. 2. [CCTV_IP] Servidor Cámaras IP. 3. [ER] Servicio de Energía Regulada.

DISPOSITIVOS DE RED	4. [ROUTER] Router del proveedor del servicio. 5. [FW_UTM] Firewall, Equipo Unificado centro Amenazas. 6. [SW_CORE] Switch Core, principal de la red. 7. [SW_ACC] Switch de acceso de red para los centros de cableado. 8. [SW_DIS] Switch de distribución para redes menores. 9. [AP_IN] Dispositivo de red inalámbrico para interiores. 10. [AP_OUT] Dispositivo de red inalámbrico para exteriores.
REDES DE COMUNICACIONES	11. [WAN] Red de área extendida, ofrecida por el proveedor de servicio. 12. [LAN] Red de área local cableada. 13. [WLAN] Rede de área local inalámbrica.
CABLEADO ESTRUCTURADO	14. [BB_FO] Backbone de fibra óptica. 15. [ST_FO] Stack de fibra óptica.
PERSONAL	16. [EN_TI] Encargado de TI en sitio. 17. [ADM_RED] Administrador de red remoto, experto en redes. 18. [TEC_SOP] Técnico de soporte asistente.

Valoración de los activos

Para poder hacer un proceso de valoración de los activos antes identificados, se tomará como referencia la metodología MAGERIT, donde se utilizan las siguientes dimensiones:

- Disponibilidad [D]
- Rendimiento [R]
- Accesibilidad [A]
- Capacidad [C]
- Integridad [I]

Para valorar las posibles fallas que puedan presentarse en los equipos y el nivel de afectación que puede presentar esta falla al interior de la red, es necesario generar una escala de dimensiones que permita determinar la importancia de cada uno de los equipos (Tabla 3.2).

A continuación, se procede con la valoración de la importancia de cada uno de los activos que están arriba descritos (Tablas 3.3 a 3.7), esto se realiza con el fin de identificar cuáles de los activos se verían más afectados a la hora de presentarse alguna de las amenazas que se presentarán posteriormente. Los valores se dan con base en el rol

Tabla 3.2: Escala de valoración de activos [33]

Valor			Criterio
10	Extremo	E	Falla extremadamente grave
9	Muy alto	MA	Falla muy grave
6-8	Alto	A	Falla grave
3-5	Medio	M	Falla importante
1-2	Bajo	B	Falla menor
0	Despreciable	D	Falla irrelevante

Tabla 3.3: Valoración de activos tipo: Servicios.

Activo	Dimensiones de criticidad				
	[D]	[R]	[A]	[C]	[I]
[TOIP] Servidor Telefonía IP	[B]	[B]	[B]	[B]	[B]
[CCTV IP] Servidor Cámaras IP	[MA]	[B]	[B]	[B]	[MA]
[ER] Servicio de Energía Regulada	[E]	[MA]	[MA]	[B]	[MA]

Tabla 3.4: Valoración de activos tipo: Dispositivos de red.

Activo	Dimensiones de criticidad				
	[D]	[R]	[A]	[C]	[I]
[ROUTER] Router del proveedor del servicio	[E]	[MA]	[MA]	[MA]	[MA]
[FW UTM] Firewall, Equipo Unificado centro Amenazas	[A]	[B]	[MA]	[B]	[E]
[SW CORE] Switch Core, principal de la red	[E]	[MA]	[MA]	[MA]	[B]
[SW ACC] Switch de acceso de red para los centros de cableado	[A]	[B]	[M]	[B]	[B]
[SW DIS] Switch de distribución para redes menores	[M]	[B]	[B]	[B]	[B]
[AP IN] Dispositivo de red inalambrico para interiores	[A]	[B]	[B]	[B]	[B]
[AP OUT] Dispositivo de red inalambrico para exteriores.	[A]	[B]	[B]	[B]	[B]

Tabla 3.5: Valoración de activos tipo: Redes de comunicaciones.

Activo	Dimensiones de criticidad				
	[D]	[R]	[A]	[C]	[I]
[WAN] Red de área extendida, ofrecida por el proveedor de servicio	[MA]	[MA]	[MA]	[MA]	[MA]
[LAN] Red de área local cableada	[A]	[A]	[B]	[A]	[B]
[WLAN] Rede de área local inalámbrica	[A]	[B]	[B]	[B]	[B]

Tabla 3.6: Valoración de activos tipo: Cableado estructurado.

Activo	Dimensiones de criticidad				
	[D]	[R]	[A]	[C]	[I]
[BB FO] Backbone de fibra óptica	[A]	[A]	[B]	[A]	[B]
[ST FO] Stack de fibra óptica	[A]	[B]	[B]	[B]	[B]

Tabla 3.7: Valoración de activos tipo: Personal.

Activo	Dimensiones de criticidad				
	[D]	[R]	[A]	[C]	[I]
[EN TI] Encargado de TI en sitio.	[E]	[D]	[MA]	[D]	[MA]
[ADM RED] Administrador de red remoto, experto en redes	[E]	[D]	[MA]	[D]	[E]
[TEC SOP] Técnico de soporte asistente	[MA]	[D]	[M]	[D]	[D]

que cumple cada uno de los activos dentro de la solución de conectividad general.

Una vez determinados los niveles de criticidad de los activos, es necesario establecer el nivel de impacto que tienen las fallas de los equipos sobre el servicio, con el fin de poder definir los tiempos de respuesta en los que se debe dar atención para subsanar dicha falla y afectar en lo más mínimo posible el servicio. Para ello se utiliza la tabla de valores en porcentajes de afectación establecida por la metodología MAGERIT V.3, donde un impacto muy alto sobre el servicio significa una caída total del mismo; es decir, un nivel de afectación del 100 %, mientras que un impacto muy bajo hace referencia a un nivel mínimo de afectación. El mapa de colores se establece en las Tablas 3.8 y 3.9.

Tabla 3.8: Escala de colores para nivel de afectación.

MA:	Muy alto
A:	Alto
M:	Medio
B:	Bajo
MB:	Muy bajo

3.1.4. Inclusión de los equipos a la herramienta de monitoreo

Una vez realizada la estimación de los riesgos de cada equipo para el servicio, se continúa con la configuración de la herramienta de monitoreo. Durante este paso se agregan los equipos a la herramienta para que puedan ser monitoreados, una vez realizado esto se procede con la configuración de envío de notificaciones de alertas, para finalmente, por medio de una aplicación de automatización, generar las órdenes de trabajo en la

Tabla 3.9: Escala de colores para nivel de riesgo de activos.

Tipo	Activo	Dimensiones de criticidad				
		D	R	A	C	I
SERVICIOS	1. [TOIP]					
	2. [CCTV_IP]					
	3. [ER]					
DISPOSITIVOS DE RED	4. [ROUTER]					
	5. [FW_UTM]					
	6. [SW_CORE]					
	7. [SW_ACC]					
	8. [SW_DIS]					
	9. [AP_IN]					
	10. [AP_OUT]					
REDES DE COMUNICACIONES	11. [WAN]					
	12. [LAN]					
	13. [WLAN]					
CABLEADO ESTRUCTURADO	14. [BB_FO]					
	15. [ST_FO]					
PERSONAL	16. [EN_TI]					
	17. [ADM_RED]					
	18. [TEC_SOP]					

herramienta utilizada por la empresa.

El proceso que se mostrará a continuación fue realizado durante las labores de ampliación del servicio para uno de los clientes de la empresa REDELECTRON-D&S S.A.S. Inicialmente, se procede a habilitar el protocolo de gestión Protocolo de Administración Sencilla de Red, *Simple Network Management Protocol.* (SNMP) en cada uno de los equipos (Figura 3.22), el primer equipo a configurar en LAN, es el *switch core* quien es el encargado de la gestión interna de la red, este equipo es a su vez el servidor de asignación de direcciones IP para toda la red interna. Por lo cual, la estimación del riesgo para el servicio es muy alta y en caso de falla debe darse respuesta de inmediato [35].

Una vez configurado el equipo se procede a agregarlo a la herramienta de monitoreo, es importante tener en cuenta que la información que se coloca en el equipo sobre el servicio SNMP debe coincidir con exactitud en la información con que se configura en el servidor [36].

El equipo se enlaza por medio de la dirección IP de gestión que se le haya asignado, es importante tener en cuenta que el servidor debe tener acceso a esta red de gestión, ya que de lo contrario no lograría alcanzarse el equipo que se va a monitorear. Por motivos de seguridad, en muchos casos, este segmento de red está restringido para que

```
service password-encryption
!
hostname MDF_SWCORE_x530_28GPXm
!
no banner motd
!
username manager privilege 15 password 8 $1$bJoVec4D$JwOJGPr7YqoExA0GVasdE0
!
!
service ssh
!
service telnet
!
service http
!
mail smtpserver smtp.gmail.com
mail smtpserver authentication login username soporteredelectrondys password 8 B
FRK2/ozA/aKHrg7IrDmL2KoiU9Yshh+eIkZ6uozIMw=
mail smtpserver port 587
mail from soporte.redelectron.dys@gmail.com
!
no clock timezone
!
snmp-server
snmp-server contact soporte.redelectron.dys@gmail.com
snmp-server location server Redelectron
snmp-server enable trap auth
snmp-server community Redelectron rw
!
!
!
aaa authentication enable default local
aaa authentication login default local
!
```

Figura 3.22: Configuración SNMP en *switch core*.
Fuente: Elaboración propia.

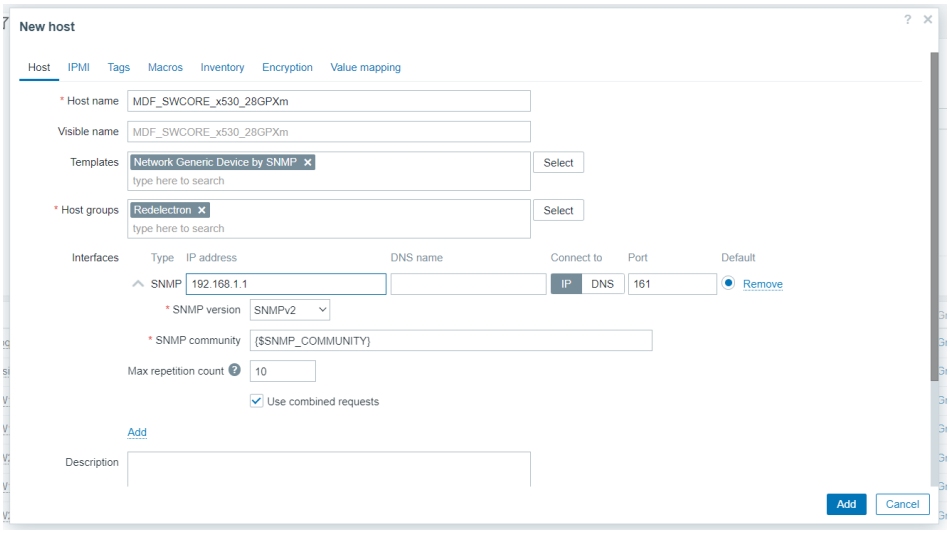

Figura 3.23: Configuración en servidor del *switch core*.
Fuente: Elaboración propia.

cualquier persona que tenga acceso a la red no pueda acceder a los equipos, por lo que se debe realizar una configuración especial y conceder permisos de acceso al segmento por parte del servidor, este paso es muy importante para garantizar el funcionamiento de la herramienta. Por otro lado, para agregar información de la comunidad, se procede a utilizar el servicio de Macros, así cuando surja la necesidad de realizar una configuración en el servicio, solo se realice el cambio de la comunidad a nivel general y no se vean afectadas las demás configuraciones (Figura 3.24).

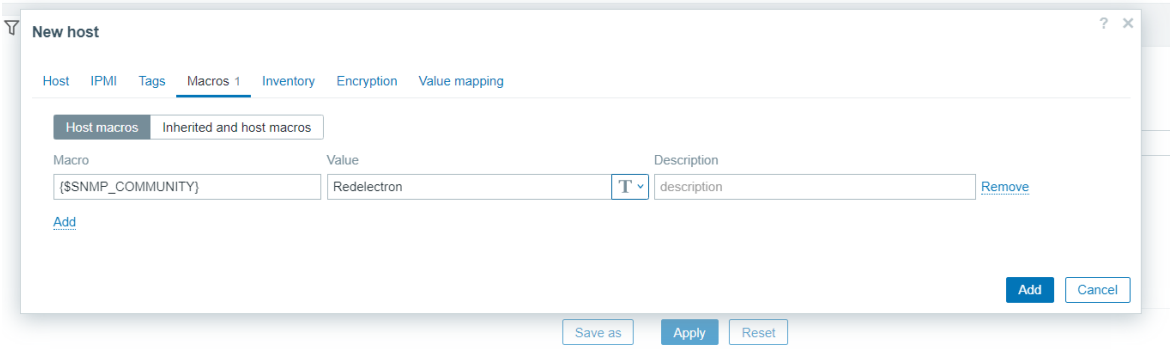

Figura 3.24: Configuración comunidad del *switch core*.
Fuente: Elaboración propia.

Con este proceso se logra establecer comunicación con el dispositivo por medio del protocolo SNMP; esto mismo se haría para los demás switch de acceso que se tienen en la red. Sin embargo, para los puntos de acceso inalámbricos se debe realizar de la siguiente forma:
Los puntos de acceso inalámbricos cuentan con una interfaz de usuario que permite realizar las configuraciones necesarias para el equipo; por lo cual, la activación y configuración del SNMP debe realizarse por medio de esta interfaz. Entonces se habilita el protocolo y se escribe la información de comunicación con el servidor, esta información debe coincidir estrictamente para que se logre establecer la comunicación, de lo contrario entraría en un conflicto y no se obtendría información del dispositivo (Figura 3.25) [37].

Para que el equipo sea agregado al servidor se procede de igual forma que con los *switches* y se accede al equipo por medio de la dirección IP, colocan la misma información del protocolo (Figura 3.26).

Para el caso de la telefonía, los dispositivos finales (teléfonos) no pueden ser monitoreados por la herramienta, debido a que ellos se comunican por medio de un protocolo llamado *syslog* (Figura 3.27), este protocolo no es soportado aún por la herramienta Zabbix. Por lo cual, se hace necesario realizar el monitoreo del servicio VoIP únicamente sobre el servidor.

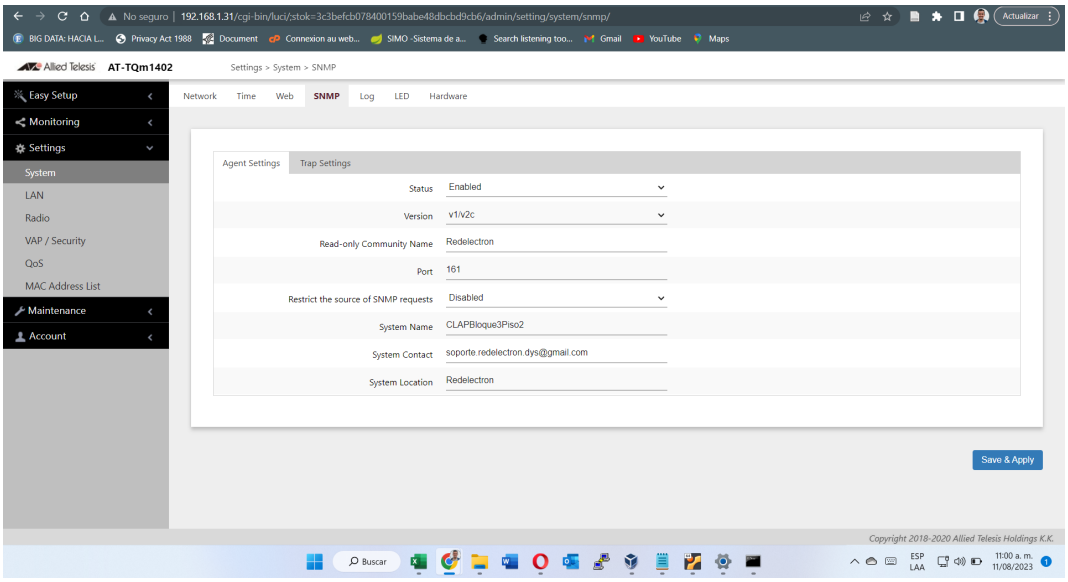

Figura 3.25: Configuración servicio de monitoreo *Access Point*.
Fuente: Elaboración propia.

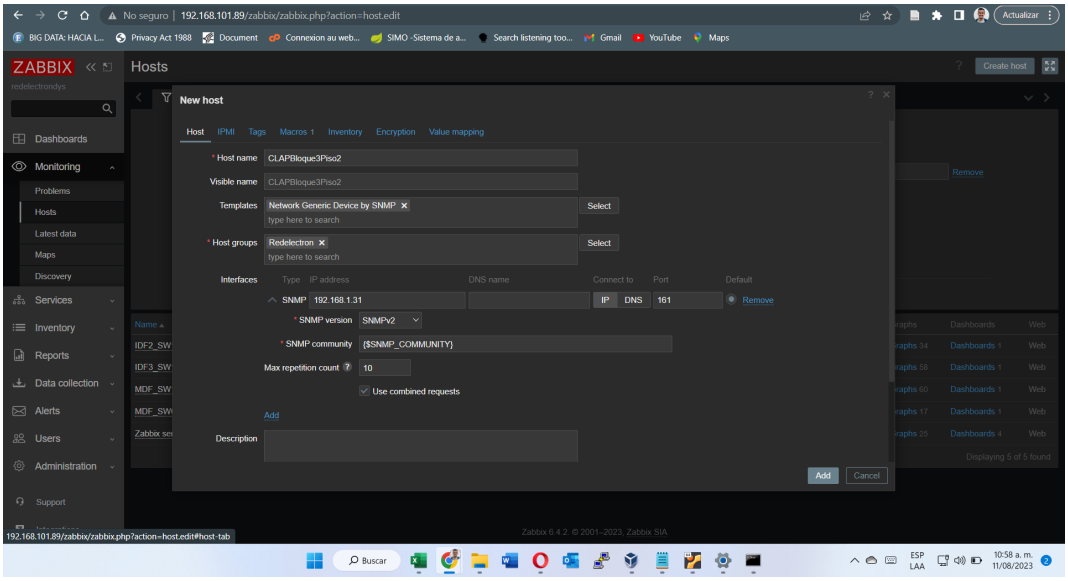

Figura 3.26: Configuración servicio de monitoreo *Access Point*.
Fuente: Elaboración propia.

Para poder monitorear el servidor, que en este caso cuenta con un sistema operativo Windows Server, se procede a realizar la instalación de un agente [38]; para ello, se realiza la descarga del instalador en la página oficial de Zabbix y se realiza la instalación como lo muestra la Figura 3.28.

Posterior a ello, es necesario validar si, dentro de las reglas de entrada del *firewall* del servidor, se ha generado automáticamente el permiso que permite escuchar al agente por el puerto 10050 (Figura 3.29).

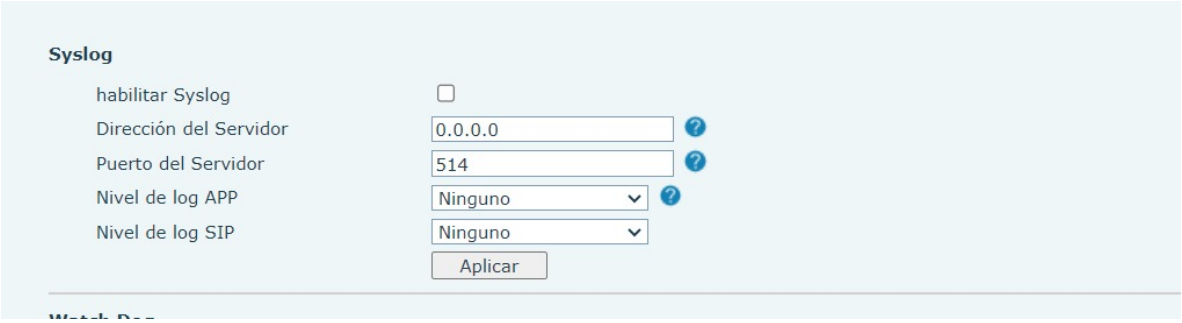

Figura 3.27: Configuración Syslog telefonía.
Fuente: Elaboración propia.

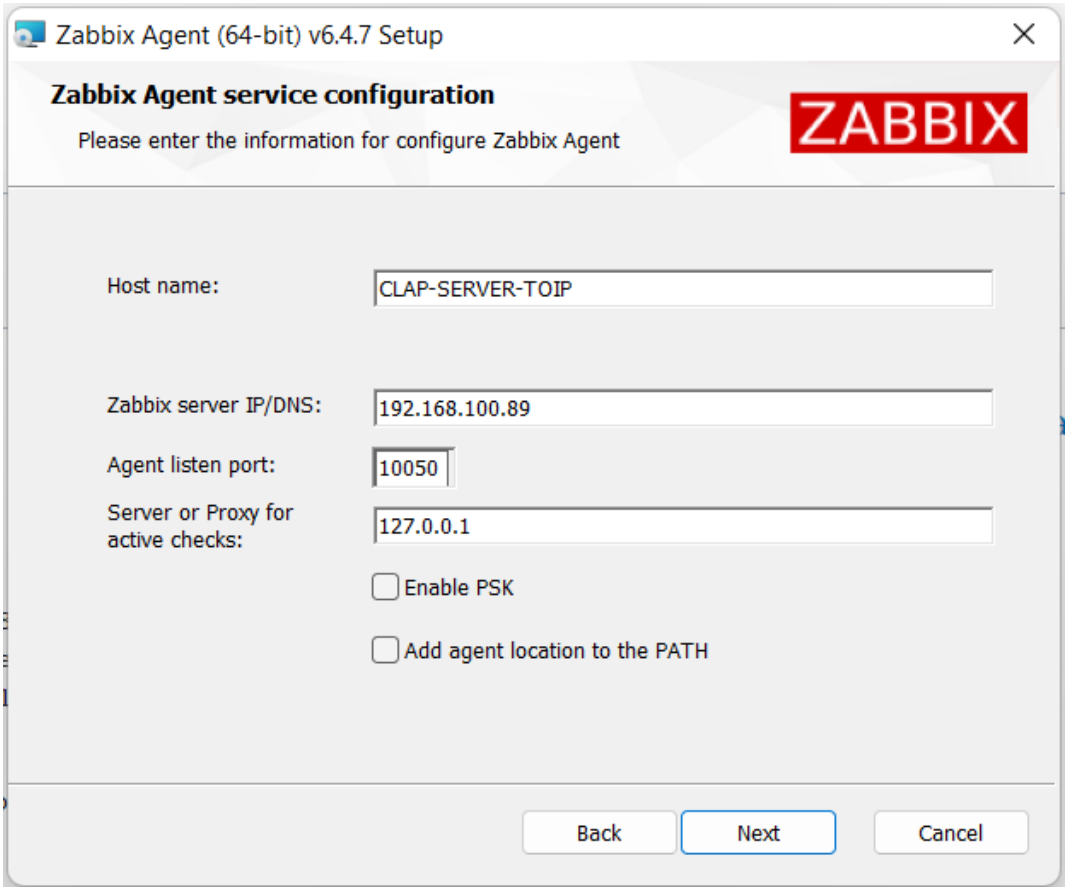

Figura 3.28: Configuración de instalación agente Zabbix.
Fuente: Elaboración propia.

Finalmente, se agrega el equipo a la herramienta de monitoreo de la misma forma que se hizo con los demás, pero se elige la opción de agente y se realiza conexión por medio de la dirección IP (Figura 3.30).

Figura 3.29: Validación puerto abierto en servidor.
Fuente: Elaboración propia.

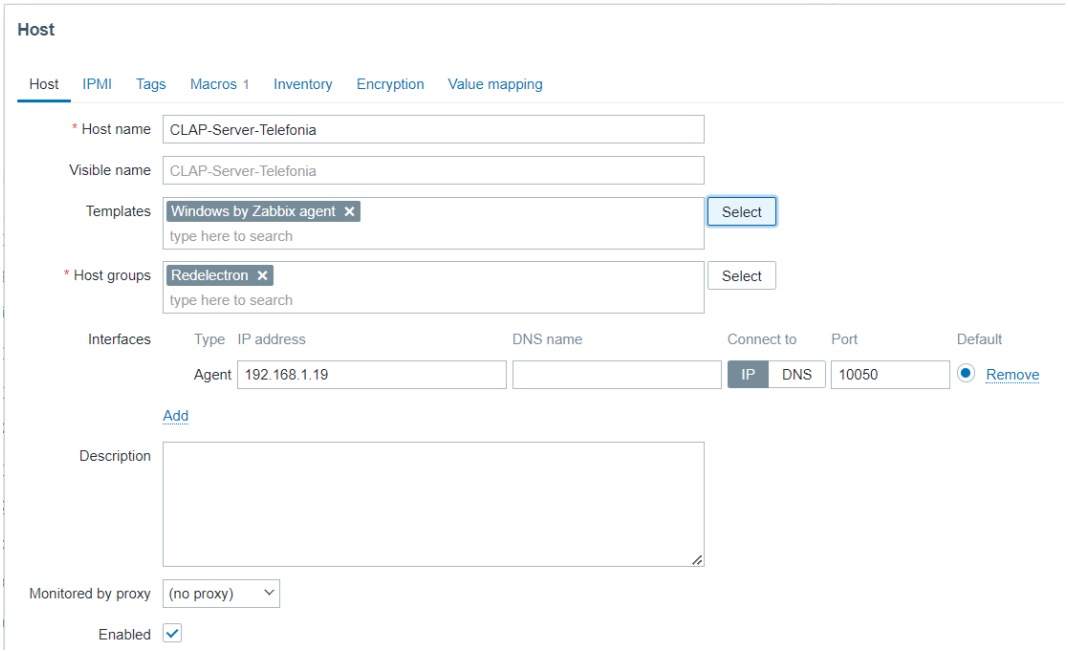

Figura 3.30: Configuración de la herramienta para agregar el servidor.
Fuente: Elaboración propia.

Una vez finalizado el proceso para cada uno de los equipos, se deben esperar unos segundos para que el protocolo establezca comunicación. Habiendo tenido éxito en la comunicación con los equipos, ya se pueden visualizar los servicios de monitoreo por medio de las herramientas de visualización con las que cuenta el servidor (Figura 3.31).

Prueba de funcionamiento de las herramientas de visualización

Con el fin de mejorar la experiencia de usuario, la herramienta de monitoreo ofrece ciertas funcionalidades de visualización que permiten tener desde una visión general del estado de los equipos, hasta una visualización específica de cada uno de los componentes del equipo.

Una de las funcionalidades de visualización es la creación de mapas, donde se puede evidenciar el estado de conexión de la red global y tener un resumen de los problemas que puedan presentar cada uno de los dispositivos de red (Figura 3.32). Para hacerlo

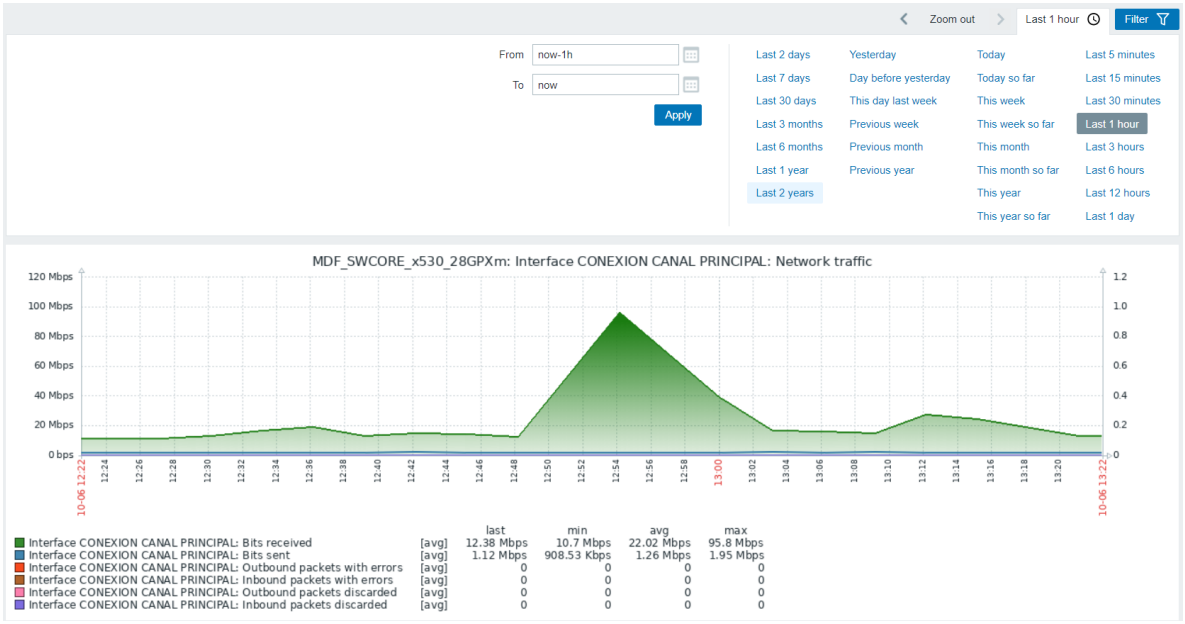

Figura 3.31: Visualización del *switch core*.
Fuente: Elaboración propia.

más interactivo, la aplicación ofrece unas plantillas genéricas para las imágenes de los equipos. A continuación, se muestra el mapa de la red de uno de los clientes de la empresa REDELECTRON-D&S S.A.S. donde se realizó la implementación de la herramienta de monitoreo.

Otra funcionalidad que se utiliza para tener una visión general del estado de los equipos es la pestaña de equipos, donde se tiene una lista general de los diferentes dispositivos monitoreados con un resumen de estado de conexión, problemas y disponibilidad, así como un menú de acceso a las gráficas específicas de cada equipo monitoreado, como se observa en la Figura 3.33.

Finalmente, la funcionalidad de estado específico de cada uno de los equipos; en ella se pueden visualizar cada una de las alertas que puedan generarse en el equipo, estas alertas pueden ser filtradas según las necesidades que tenga el administrador, con el fin de tener reportes específicos de la actividad de cada uno de los dispositivos de red, pues son almacenadas por la herramienta en su base de datos. En la Figura 3.34, la herramienta permite visualizar estos eventos en una línea de tiempo, con ello, el administrador puede rastrear los eventos que han ocurrido en el equipo a lo largo del tiempo.

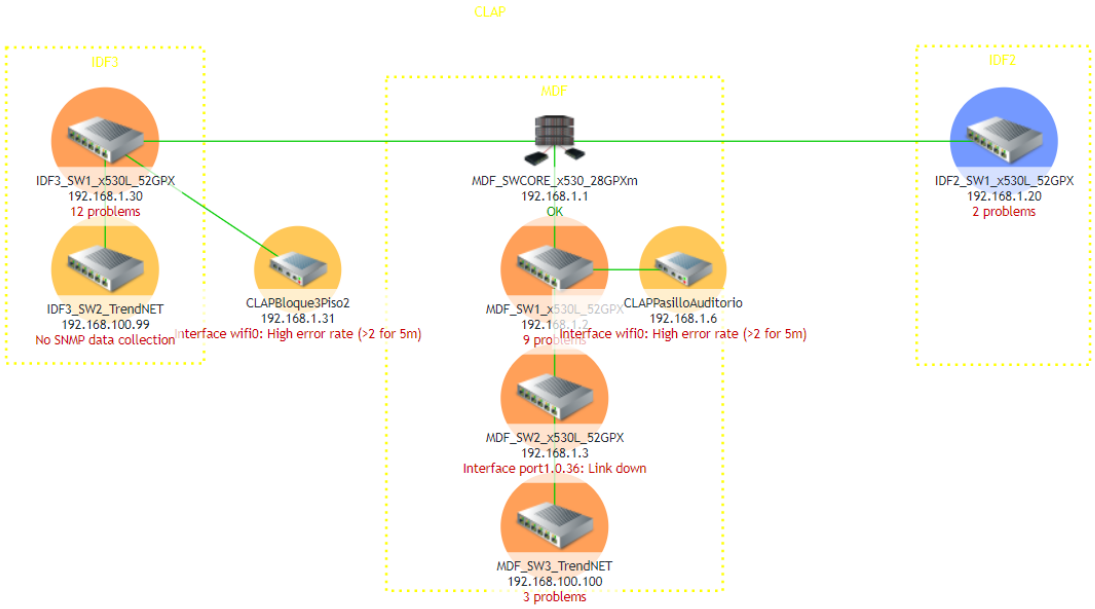

Figura 3.32: Visualización del Mapa de Red.
Fuente: Elaboración propia.

Name ▲	Interface	Availability	Tags	Status	Latest data	Problems	Graphs	Dashboards	Web
CLAPBloque3Piso2	192.168.1.31:161	SNMP	class: network target: generic	Enabled	Latest data 66	1	Graphs 6	Dashboards 1	Web
CLAPPasilloAuditorio	192.168.1.6:161	SNMP	class: network target: generic	Enabled	Latest data 66	1	Graphs 6	Dashboards 1	Web
IDF2_SW1_x530L_52GPX	192.168.1.20:161	SNMP	class: network target: generic	Enabled	Latest data 340	2	Graphs 34	Dashboards 1	Web
IDF3_SW1_x530L_52GPX	192.168.1.30:161	SNMP	class: network target: generic	Enabled	Latest data 554	5 7	Graphs 58	Dashboards 1	Web
IDF3_SW2_TrendNET	192.168.100.99:161	SNMP	class: network target: generic	Enabled	Latest data 274	2	Graphs 28	Dashboards 1	Web
MDF_SW1_x530L_52GPX	192.168.1.2:161	SNMP	class: network target: generic	Enabled	Latest data 582	8 1	Graphs 60	Dashboards 1	Web
MDF_SW2_x530L_52GPX	192.168.1.3:161	SNMP	class: network target: generic	Enabled	Latest data 544	1	Graphs 58	Dashboards 1	Web
MDF_SW3_TrendNET	192.168.100.100:161	SNMP	class: network target: generic	Enabled	Latest data 278	2 1	Graphs 28	Dashboards 1	Web
MDF_SWCORE_x530_28GPXm	192.168.1.1:161	SNMP	class: network target: generic	Enabled	Latest data 170	Problems	Graphs 17	Dashboards 1	Web
Zabbix server	127.0.0.1:10050	ZBX	class: os class: software target: linux •••	Enabled	Latest data 134	2 1	Graphs 25	Dashboards 4	Web

Displaying 10 of 10 found

Figura 3.33: Tabla de visualización de equipos.
Fuente: Elaboración propia.

Generación de alertas y tiempos de respuesta ante incidentes

Una de las funcionalidades más importantes dentro de las herramientas de monitoreo es la generación de alertas; esto sucede cuando uno de los equipos que se está monitoreando presenta un evento de cualquier tipo, el cual puede afectar o no su operación. En la herramienta Zabbix se cuenta con un listado de servicios por medio de los cuales se notifica la alerta generada. Por defecto la herramienta presenta seis tipo de alerta [39]:

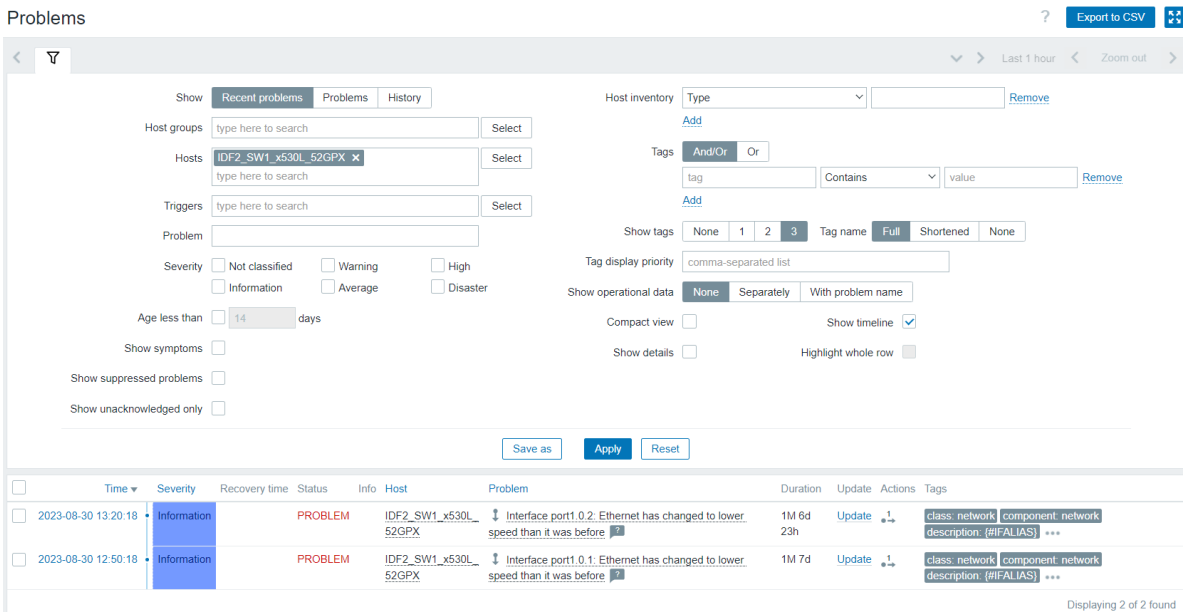

Figura 3.34: Tabla de problemas de un equipo.
Fuente: Elaboración propia.

- *Not classified*: Los cuales corresponden a alertas que no influyen en nada en los procesos de operación de los equipos, pero que deben ser reportados de manera informativa. Este tipo de alertas son poco comunes, debido a que la mayoría de las alertas corresponden a servicios que han sido clasificados.

- *Information*: Este tipo de alertas son meramente informativas, ya que corresponden a mensajes de estado de funcionamiento de los equipos, a manera de actualización del estado de los mismos, o cuando suceden acciones que no afectan en nada su operación.

- *Warning*: Corresponden a las alertas que se activan cuando uno de los servicios o funcionalidades físicas del equipo se encuentra en riesgo, normalmente se activan cuando un equipo ha sobrepasado los límites de uso de sus componentes hardware, tales como: uso de memoria, uso de CPU, eso podría poner en riesgo el funcionamiento del equipo.

- *Average*: Este tipo de alertas son las que se generan cuando uno de los componentes de red del equipo deja de funcionar; un ejemplo de ello es cuando deja de operar uno de los puertos del equipo, generando reporte de inoperación.

- *High*: Estas alertas son las más importantes a la hora de evaluar la operación de los equipos; se dan cuando los equipos son inaccesibles o uno de sus componentes principales de operación deja de funcionar.

- *Disaster*: Es el nivel más alto de alerta y se genera cuando uno de los dispositivos ha tenido un daño que representa pérdidas económicas, es decir, daño total en equipo de red que pueda ser cuantificado por la herramienta.

Adicionalmente, en las alertas, la herramienta asigna un nombre el problema que está ocurriendo, a continuación se da una explocación general de nombres de problemas comunes (Tabla 3.8):

Tabla 3.10: Nombres de problemas comunes.

Tipo de problema	**Nombre del problema**	**Interpretación**
Information	Interface X. Ethernet has changed to lower speed than it was before.	Conexión al puerto de red con una tarjeta de Base baja.
Warning	Interface X. Link down	Desconexión de equipo conectado al puerto de red.
Warning	Interface X. High error rate (>2 for 5m)	Equipo inalámbrico con navegación lenta para los usuarios.
High	Unavailable by ICMP ping	Equipo no alcanzado desde el servidor por ping.

Como se dijo en capítulos anteriores, para garantizar una óptima prestación de servicios, es necesario poder asistir al cliente en el menor tiempo posible cuando se presenten fallas en los diferentes equipos, por lo cual, es indispensable definir los tiempos de respuesta mínimos para atender los incidentes dependiendo del nivel de importancia que tenga el equipo dentro de la red. Así las cosas, basándose en el análisis de criticidad, se definen en la Tabla 3.10 los tiempos máximos de respuesta de la siguiente manera:

Tabla 3.11: Tiempos de respuesta.

Dispositivo de red	Tiempo de respuesta
[ROUTER]	2 Horas
[FW_UTM]	2 Horas
[SW_CORE]	2 Horas
[SW_ACC]	4 Horas
[SW_DIS]	8 Horas
[AP_IN]	8 Horas
[AP_OUT]	8 Horas
[VoIP]	8 Horas

Los tiempos se establecen para garantizar fluidez en la asistencia, ya que pueden presentar inconvenientes de desplazamiento que pueden afectar la llegada del personal técnico. Estos tiempos, de igual forma, serán pactados con los clientes y plasmados en

los contratos de prestación de soportes una vez se haya dado aviso por parte de ellos para atender algún incidente.

Integración de la herramienta de monitoreo y aplicación de asignación de tareas

Una vez definidos los tiempos de respuesta, se procede a realizar la integración de la herramienta de monitoreo con la aplicación de asignación de tareas utilizada por la empresa REDELECTRON-D&S S.A.S. En la actualidad, se cuenta con el servicio de Google Calendar, por medio del cual, cada uno de los colaboradores recibe las órdenes de trabajo que deben ejecutarse y la hora en la cual se deben realizar. El coordinador de proyectos se encarga de definir cuál de las cuadrillas estás disponible para atender el incidente y la agrega al evento que se ha creado en la aplicación.

Según lo anterior, surge la necesidad de que se realice la generación de eventos una vez recibida la alerta enviada por la herramienta de monitoreo, para garantizar una respuesta en los tiempos establecidos ante el incidente que se presenta. Para ello, se define en primera medida que el nivel mínimo de alerta que puede generar una visitar es el nivel 5 (*High*), ya que esta alerta se da ante una indisponibilidad de uno de los equipos monitoreados.

Habiendo establecido lo anterior, se procede entonces con la integración de la siguiente manera:

- **Elección del medio de notificación**: Debido a que la herramienta de asignación de tareas utilizada hace parte del conjunto de servicios de Google, se decide establecer un canal de comunicación con un correo Gmail, dedicado principalmente para el monitoreo de las redes. Al hacer esta elección se garantizaría una completa utilización del ecosistema de servicios de Google para la implementación de la aplicación. Para que la herramienta pueda realizar notificaciones hacia un correo Gmail, se debe realizar la integración de la aplicación otorgando permisos de acceso para aplicaciones desconocidas por medio de la generación de una contraseña dedicada para dicha aplicación, esto se realiza con la opción de Contraseñas de aplicaciones como se muestra en la Figura 3.35 [40].

  Una vez generada la contraseña se procede a realizar la autenticación con la herramienta Zabbix para el envío de correos a la cuenta seleccionada, este proceso debe realizarse como se muestra en la Figura 3.36 [41].

  Posteriormente, se procede a realizar la configuración del cuerpo del mensaje que será enviado por correo electrónico. Se decide entonces entregar la mayor cantidad de información posible en el asunto del correo, con el fin de facilitar la obtención de información del problema, y utilizar el cuerpo del correo para brindar mayores

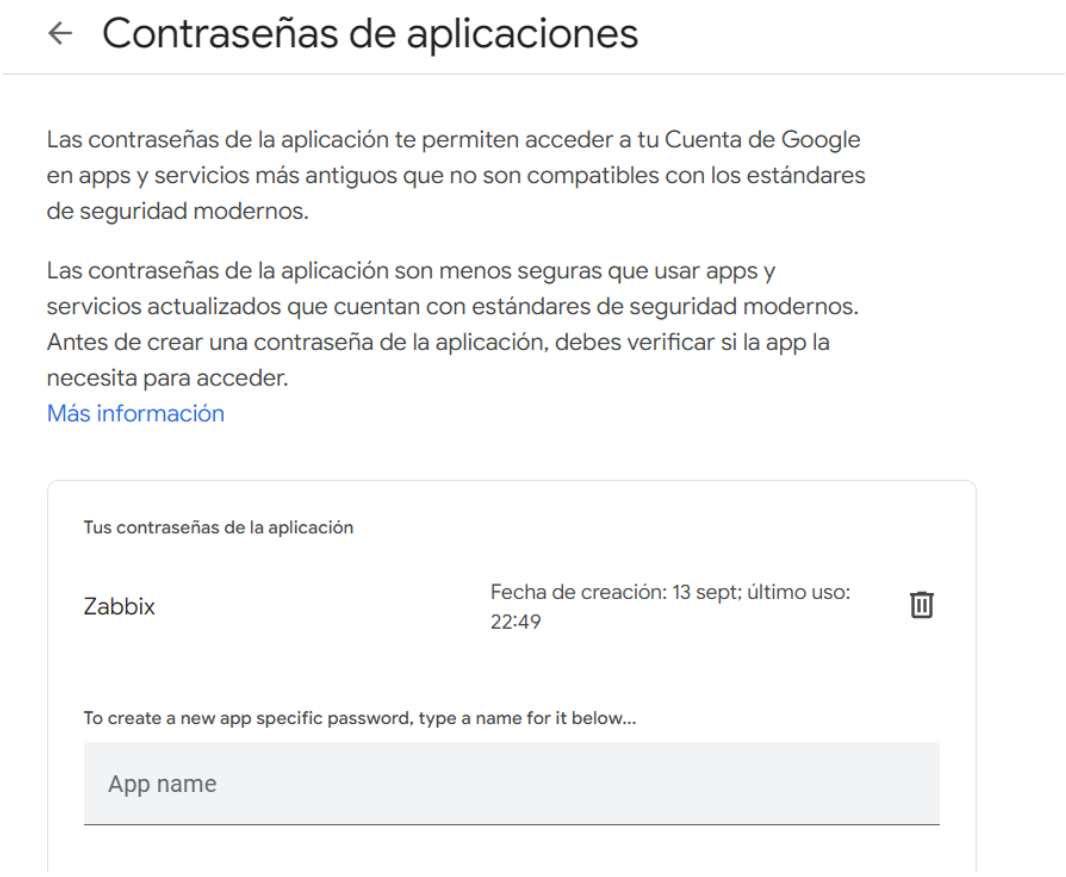

Figura 3.35: Configuración de permisos de cuentas de Google.
Fuente: Elaboración propia.

especificaciones sobre la alerta. Esta configuración se realiza como en la Figura 3.37 [42].

- **Generación de eventos en Google Calendar**: Habiendo realizado la configuración para el envío de correos, es necesario iniciar la automatización de generación de eventos según los criterios definidos para asistir al cliente en caso de incidentes con los equipos monitoreados. Para ello es necesario utilizar los servicios de computación en la nube ofrecidos por Google. Para iniciar este proceso se debe crear un proyecto en la consola de Google Cloud, donde se definen las Interfaz de programación de aplicaciones, *Application Programming Interfaces.* (API) que van a ser utilizadas por la aplicación; para este caso las dos API que serán utilizadas son Gmail API, para realizar la lectura de los correos que llegan desde la herramienta de monitoreo, y Google Calendar API para generar los eventos a partir de los correos leídos, como se muestra en la Figura 3.38 [43].

Posterior a ello, se deben establecer los permisos a los cuales va a tener acceso la

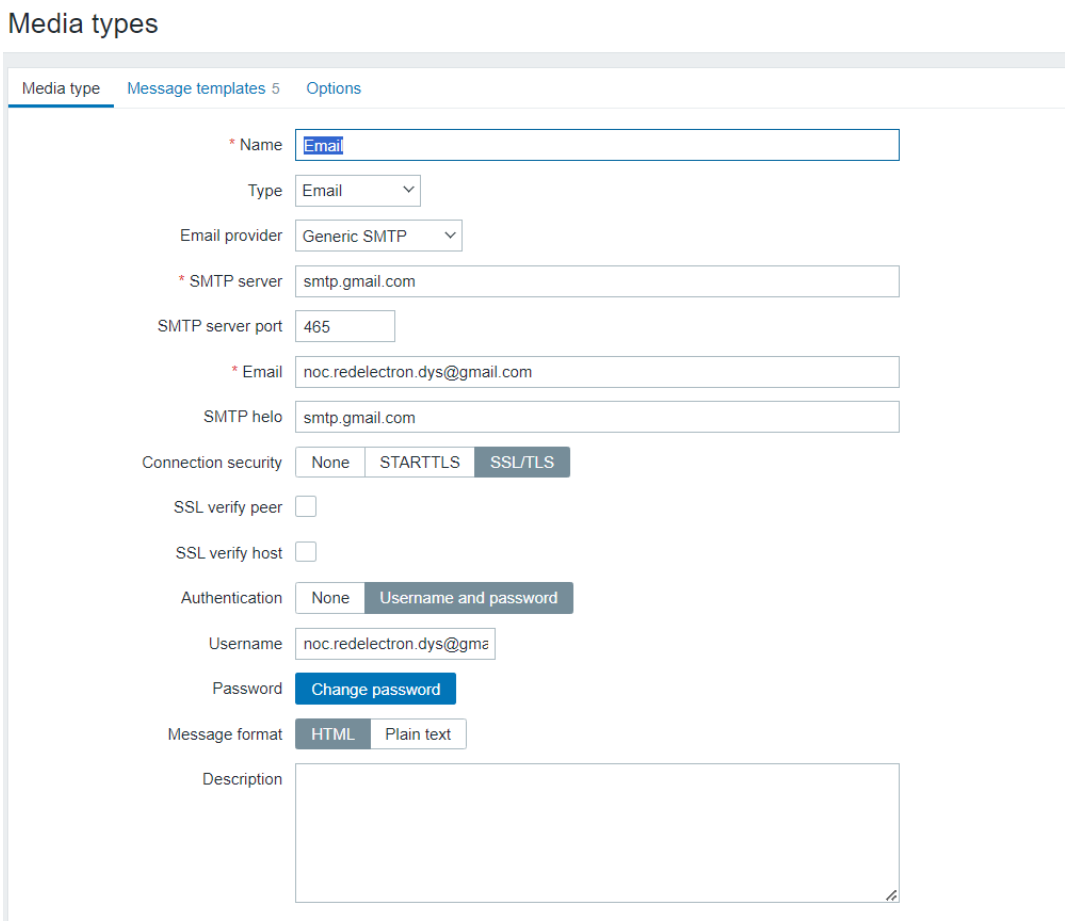

Figura 3.36: Configuración de acceso a correo desde Zabbix.
Fuente: Elaboración propia.

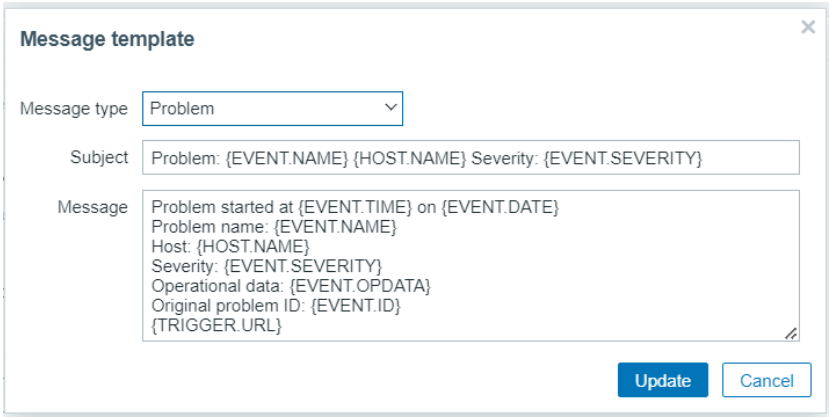

Figura 3.37: Configuración del correo desde Zabbix.
Fuente: Elaboración propia.

aplicación por medio de las API, para este caso, se define que la aplicación tendrá un rol de solo lectura para poder obtener información de los correos y un rol de

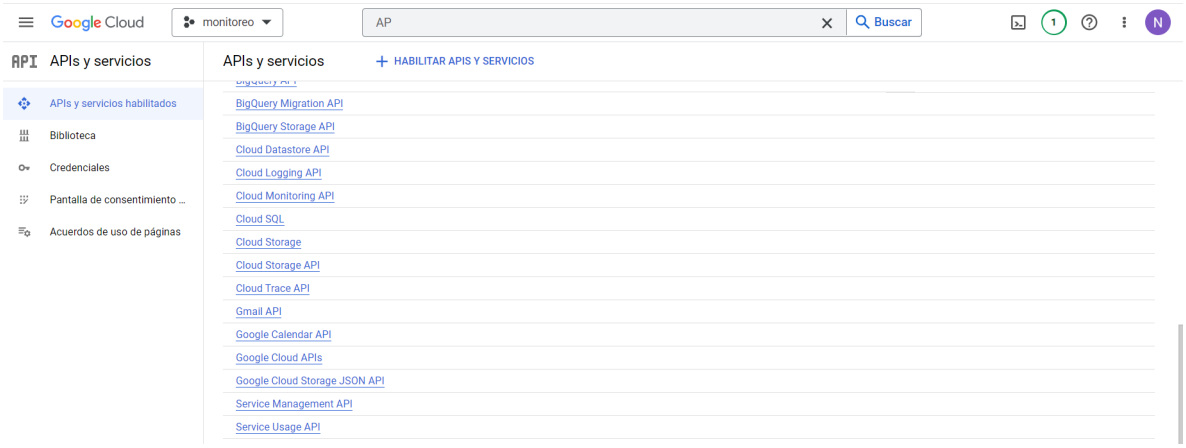

Figura 3.38: Habilitación de API en Google Cloud.
Fuente: Elaboración propia.

escritura para la generación de eventos en el calendario, estos permisos se definen como se muestra en la Figura 3.39.

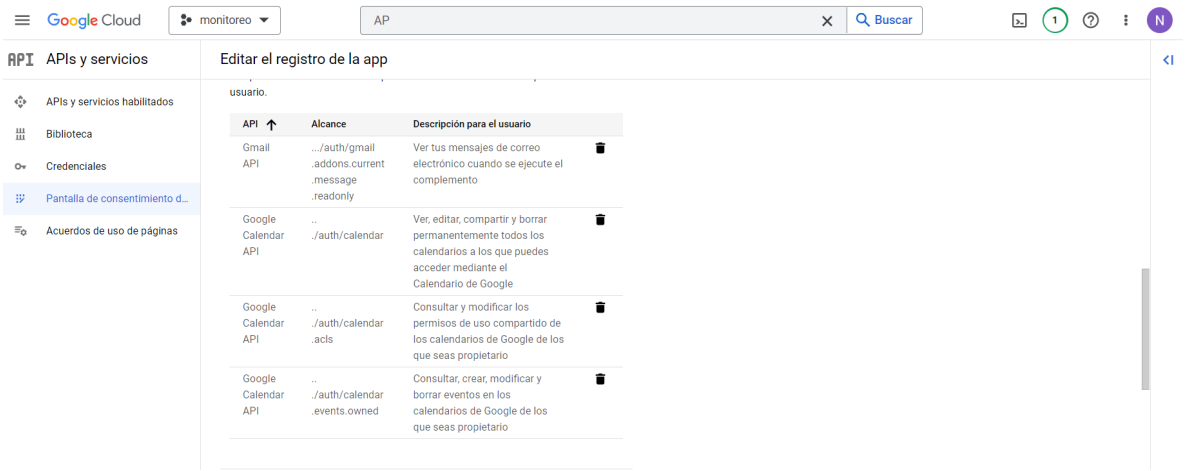

Figura 3.39: Configuración de permisos de la aplicación.
Fuente: Elaboración propia.

Se procede entonces crear una cuenta de servicio, la cual tendrá el rol de propietario del proyecto, pues con este rol se le entregan altos privilegios para realizar configuraciones en las API. Esta cuenta de servicio tiene a su vez las funciones de un correo electrónico, con lo cual se permite realizar la generación de eventos en la API de Google Calendar. La configuración de permiso se realiza como se muestra en la Figura 3.40 [44].

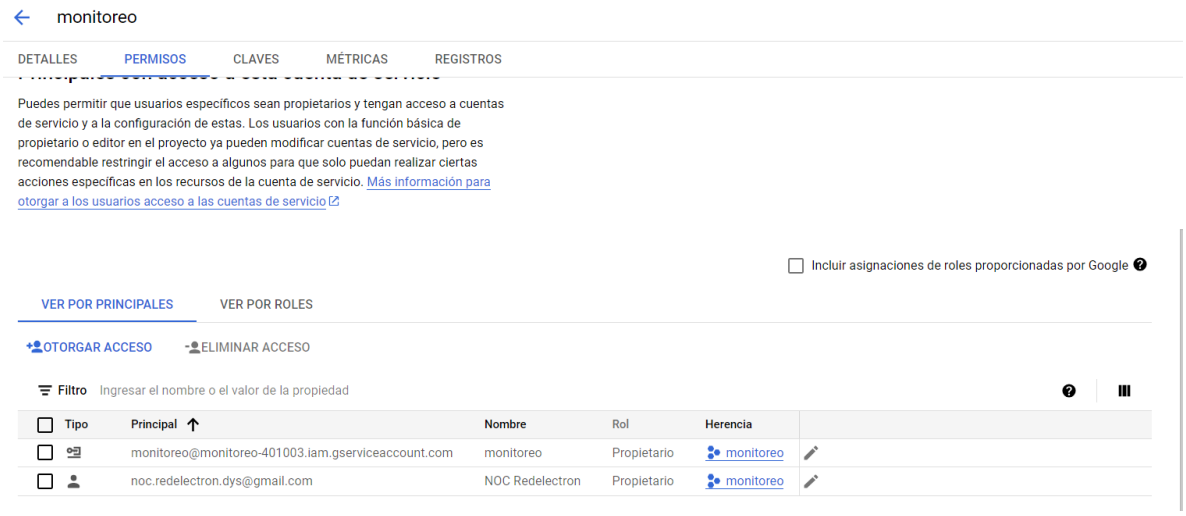

Figura 3.40: Configuración de cuenta de servicio.
Fuente: Elaboración propia.

Para finalizar las configuraciones del proyecto en la consola de Google Cloud, se procede a generar una clave privada para que se pueda realizar la autenticación de la aplicación con la cuenta de servicio por medio de un *script*. Para obtener esta clave privada se genera un archivo JSON que contiene toda la información de la cuenta de servicio. Una vez finalizadas las configuraciones de Google Cloud, se procede a compartir el calendario donde van a ser agendados los eventos con la cuenta de servicio. Este proceso se realiza en las configuraciones del calendario en la aplicación WEB del servicio, según como se muestra en la Figura 3.41. Al compartir calendario se deben asignar a la cuenta de servicio privilegios de escritura para poder realizar configuraciones en el calendario compartido y poder agendar los eventos en él.

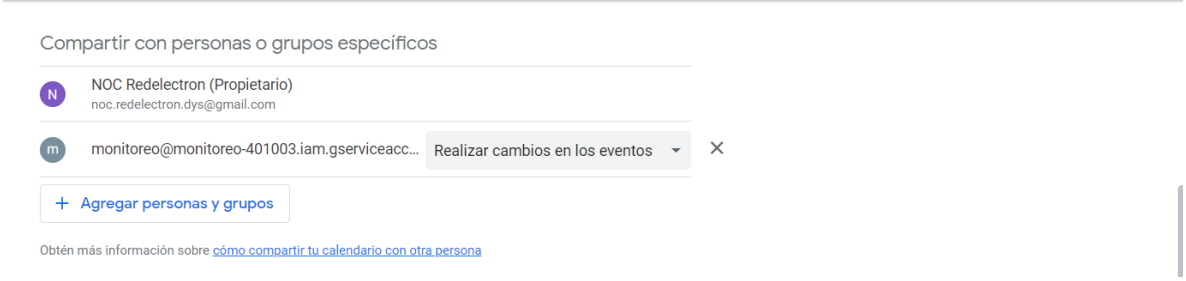

Figura 3.41: Configuración para compartir calendario con la cuenta de servicio.
Fuente: Elaboración propia.

La última etapa del desarrollo de la aplicación de integración entre Zabbix y la

Suite de Google, la cual se realiza mediante un *script* de Java (Anexo I) que permite obtener la información de los asuntos de los correos, realizar una comparación de estos asuntos con los asuntos que indican una falla en algún equipo, establecer el tiempo de respuesta requerido para dicho equipo y registrar finalmente el evento en el calendario según el tiempo establecido; en caso que ninguno de los asuntos cumpla con los criterios; el *script* cumpliría con el diagrama de flujo de la Figura 3.42. El código debe ser escrito en la plataforma Google App Script y debe ser integrado con el proyecto de Google Cloud.

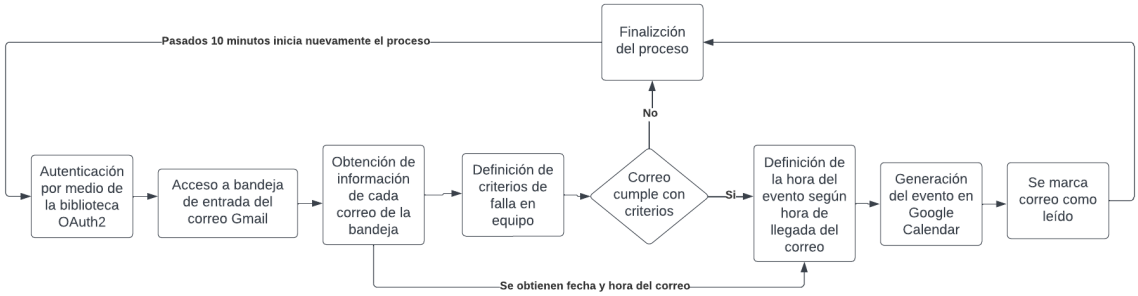

Figura 3.42: Diagrama de flujo del *script*.
Fuente: Elaboración propia.

- **Implementación de la aplicación**: Habiendo finalizado el proceso de configuración y generación del *script*, se procede a realizar la implementación de la aplicación en conjunto con la herramienta de monitoreo, para ello, se utilizan inicialmente las implementaciones de prueba que ofrece la plataforma de Google App Script, donde se puede hacer una depuración del código para descartar errores en el proceso y verificar que todas las solicitudes estén operando con normalidad. Una vez calibrado el código con las implementaciones de prueba, se procede a realizar la implementación definitiva de la aplicación y pasarla a producción. La herramienta debe ejecutarse cada 10 minutos, por medio de un desencadenador, y durante su ejecución realiza una revisión completa de los correos para verificar los que cumplan con los criterios establecidos.

Todo el proceso descrito anteriormente permite que la herramienta de monitoreo se integre de manera adecuada con la aplicación de asignación de tareas Google Calendar, utilizada por la empresa REDELECTRON-D&S S.A.S. De esta forma, cuando uno de los equipos monitoreados entre en falla y no pueda ser alcanzado por la herramienta; esta generará una notificación por correo electrónico indicando el nombre del equipo afectado, lo cual permitirá, por medio de la aplicación de integración, generar un evento en Google Calendar, basándose en los tiempos de respuesta para cada uno de los equipos, dependiendo de su importancia dentro de los servicios de red.

CAPÍTULO 4
PRUEBAS Y RESULTADOS

En este capítulo se presentarán las pruebas realizadas que ayudarán a verificar el correcto funcionamiento de la solución implementada. Con ello, se establecerán los resultados obtenidos con el fin de comprobar el cumplimiento del alcance del proyecto.

4.1. Prueba de operación de la herramienta de monitoreo

4.1.1. Prueba de instalación

Siguiendo el procedimiento detallado en la Sección 3.1, se puede observar en la Figura 4.1, la correcta instalación de la herramienta de monitoreo. De otra parte, se puede evidenciar la operación de la herramienta con los equipos asociados a ella. Lo que se muestra en la interfaz principal de usuario es un resumen de todo lo que se está monitoreando; se pueden observar los problemas ocurridos en los equipos, un resumen de uso de los recursos de cada equipo, rendimiento de la herramienta del servidor donde se encuentra alojada la herramienta, para establecer si se encuentra funcionando correctamente, resumen de cantidad de equipos monitoreados con los detalles de las alertas generadas y cantidades totales de las alertas que se encuentran activas. Esta interfaz de usuario puede ser modificada según las necesidades que tenga el administrador de la red.

4.1.2. Pruebas de generación y notificación de alertas

Como se observa en la Figura 4.2, la herramienta genera una secuencia de alertas con diferentes tipos de criticidad, con los cuales se puede observar el comportamiento de los dispositivos al interior de la red. Esta función brinda información sobre el origen del problema y la acción que se generó a partir de cada una de las alertas.

Prueba de generación de alertas para un *switch* de acceso

Para realizar la prueba de funcionamiento con un *switch* de acceso, se procederá a hacer una desconexión del cable de fibra. Para esta prueba se desconecta el equipo del *switch* principal, como se ve en la Figura 4.3. Con ello, se simulará una caída del servicio por posibles fallas en el equipo, no se realizará un apagado del equipo, pues

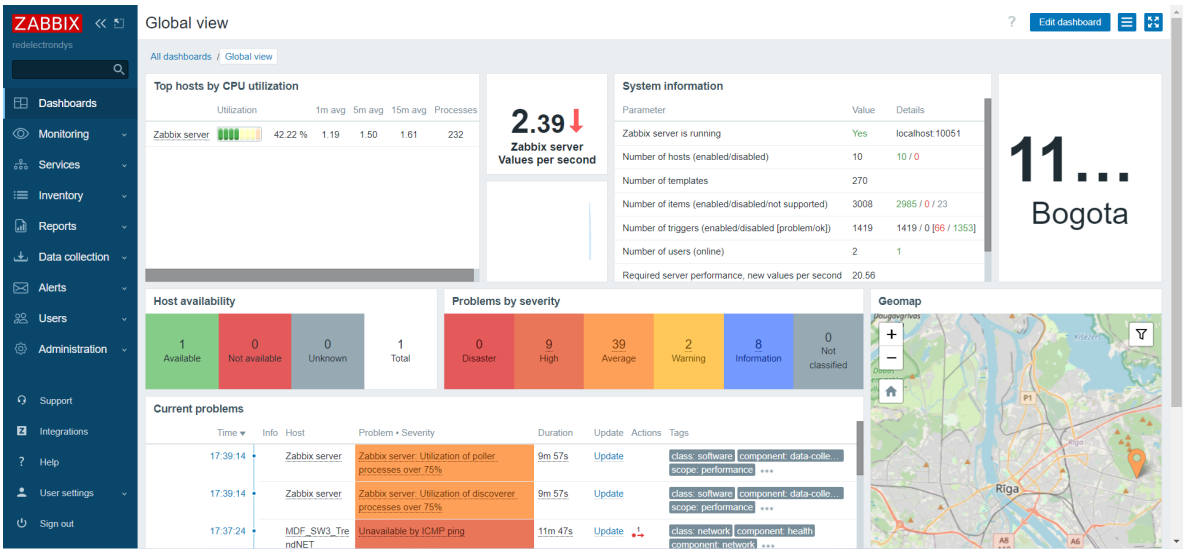

Figura 4.1: Herramienta de monitoreo en operación.
Fuente: Elaboración propia.

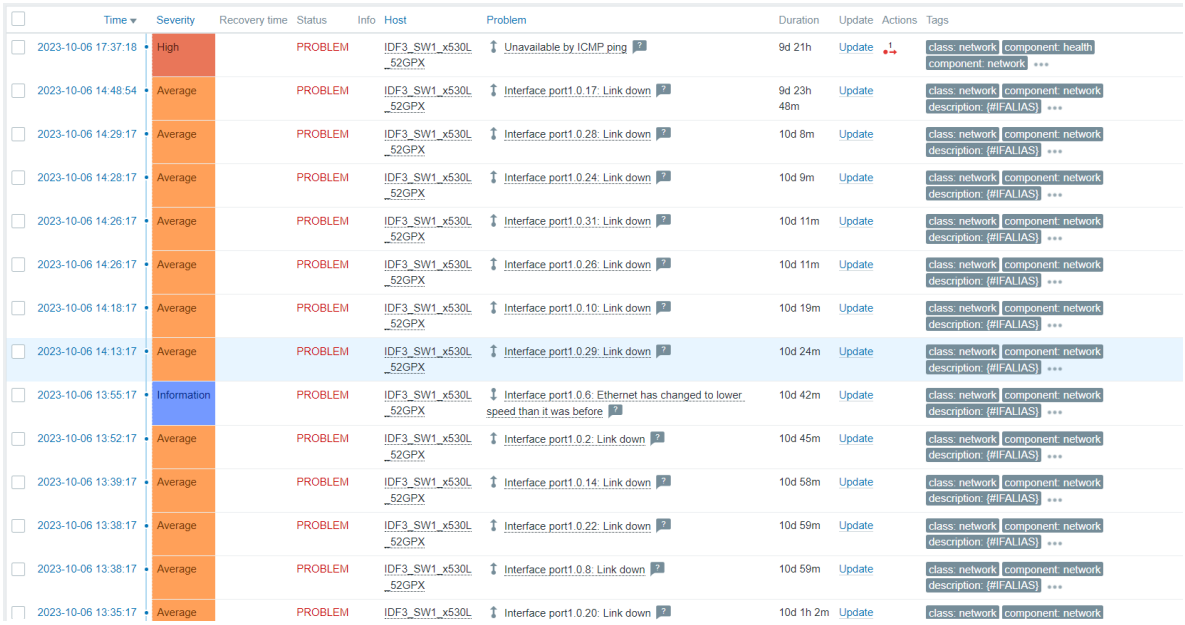

Figura 4.2: Generación de alertas de la herramienta.
Fuente: Elaboración propia.

por políticas del contrato con el cliente no se pueden apagar los equipos de red, debido a que esta acción podría causar daños irreversibles en el equipo, dejándolo fuera de producción.

Figura 4.3: Desconexión física del *switch* de acceso.
Fuente: Elaboración propia.

Una vez realizada la desconexión física del equipo, la herramienta intentará establecer comunicación con él, sin poder lograrlo; cuando la herramienta confirma que no se tiene alcance, se generará una alerta, como se muestra en la Figura 4.4, esto permitirá al personal encargado de vigilar el estado de la red, detectar cuál fue el origen del problema y poder así identificar cuáles podrían ser sus posibles causas.

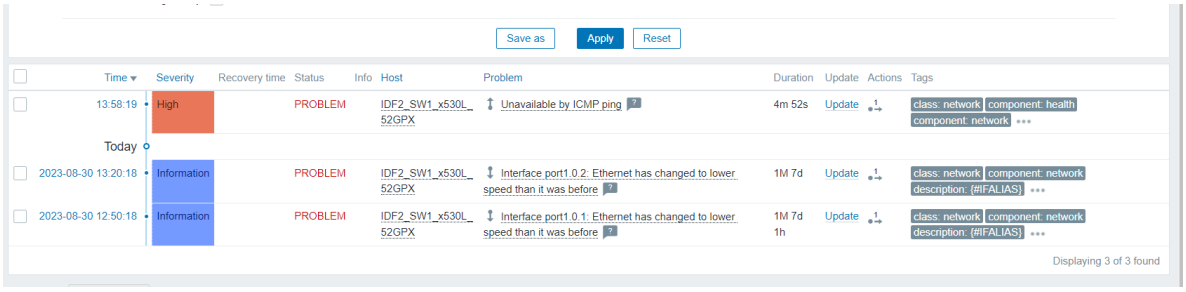

Figura 4.4: Alerta de la herramienta por fallas en el *switch* de acceso.
Fuente: Elaboración propia.

Ahora bien, inmediatamente generada la alerta por la herramienta implementada, se envía un mensaje por correo electrónico con información de lo ocurrido. Este mensaje es

enviado al correo de la empresa REDELECTRON-D&S S.A.S. destinado para recibir las alertas de monitoreo y poder agendar las visitas al cliente, en caso de que sea necesario. La Figura 4.5 muestra el mensaje de correo electrónico generado por la herramienta de monitoreo, el cual contiene información como, la hora de detección del evento, equipo afectado, tipo de falla detectada, estos datos son valiosos para el administrador, pues ayudan a generar un diagnóstico más específico sobre el evento ocurrido. El asunto del correo contiene la información necesaria para determinar el equipo con falla y cuál es la su importancia dentro de la red. Se observa en este caso que, según el nombre del dispositivo, es un *switch* de acceso, el cual no es alcanzado por la herramienta de monitoreo y que por ello tiene una criticidad alta.

Figura 4.5: Mensaje de correo electrónico generado por la herramienta de monitoreo. Fuente: Elaboración propia.

Prueba de generación de alertas para un *Access Point* tipo interior

Para realizar esta prueba, el cliente ha permitido realizar la desconexión del equipo desde el puerto del *switch* de acceso que le brinda energía y conectividad. La Figura 4.6 evidencia la desconexión física realizada al equipo.

Cuando ocurre un fallo por desconexión del equipo, la herramienta actúa como se explicó anteriormente, comienza a ejecutar intentos de conexión, una vez verificado que no tiene alcance, se genera una alerta en la herramienta, como se muestra en la Figura 4.7.

Finalmente, la herramienta realiza una notificación inmediata hacia el medio seleccionado, que para este caso es el correo electrónico. Como se observa en la Figura 4.8, el mensaje de correo electrónico muestra información relacionada con el incidente, que permite tener un resumen detallado de lo ocurrido con el equipo. El asunto, en este caso, corresponde a un dispositivo inalámbrico que igualmente no es alcanzado por la herramienta de monitoreo y por ello tiene una alerta con criticidad alta.

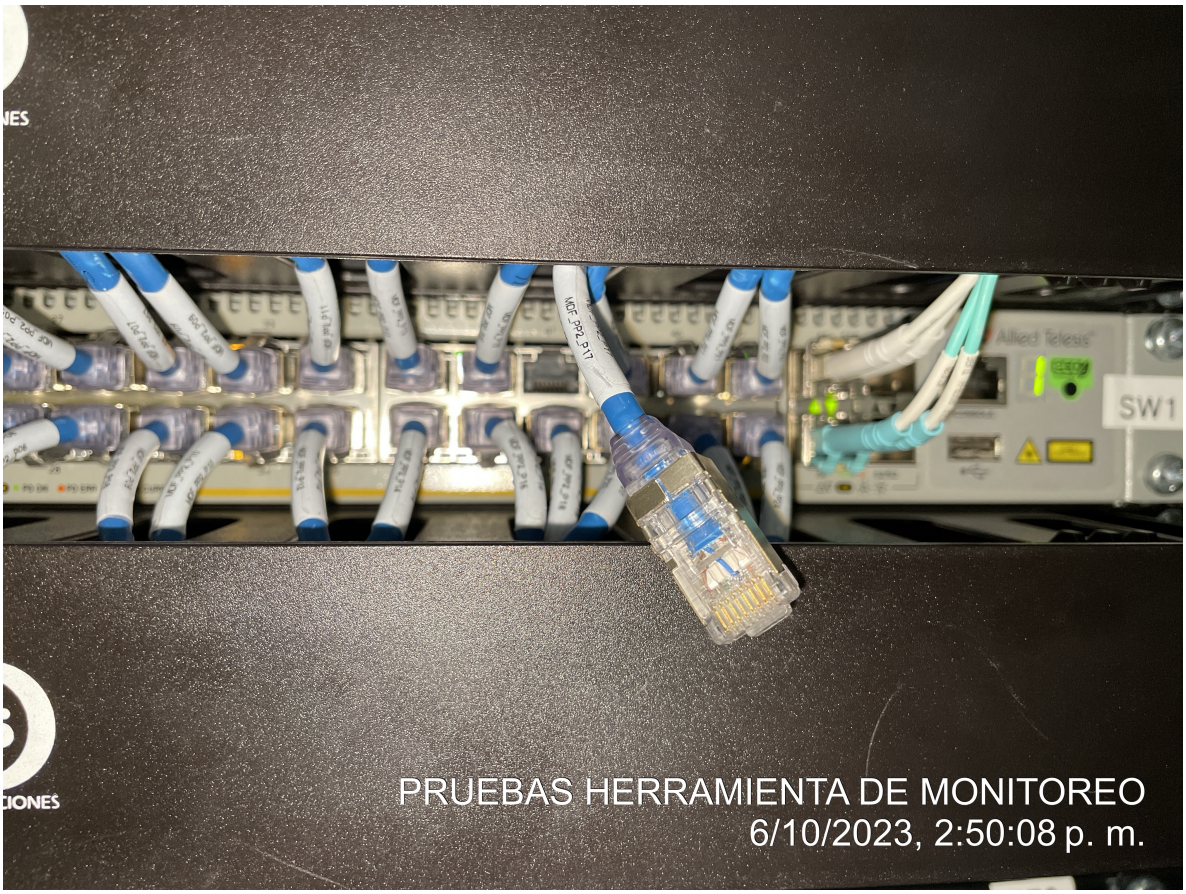

Figura 4.6: Desconexión física del *Access Point* tipo interior.
Fuente: Elaboración propia.

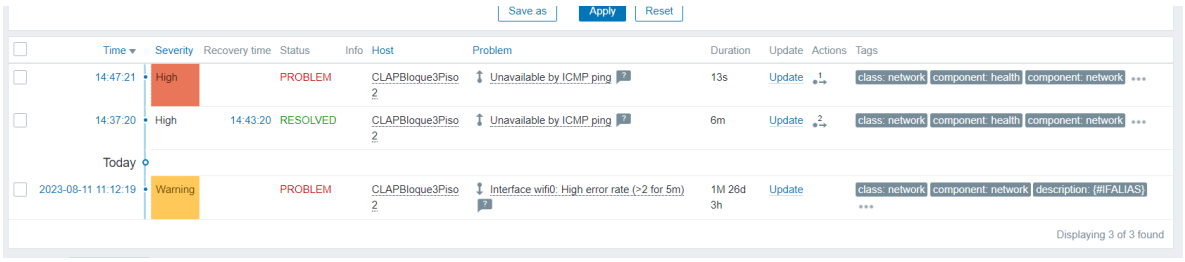

Figura 4.7: Alerta por fallas en el *Access Point* tipo interior.
Fuente: Elaboración propia.

Prueba generación de alertas para el servidor VoIP

Para realizar la prueba con el servidor se hace una desconexión física del cable de red, lo cual impedirá la comunicación para generar las alertas dentro de la herramienta (Figura 4.9).

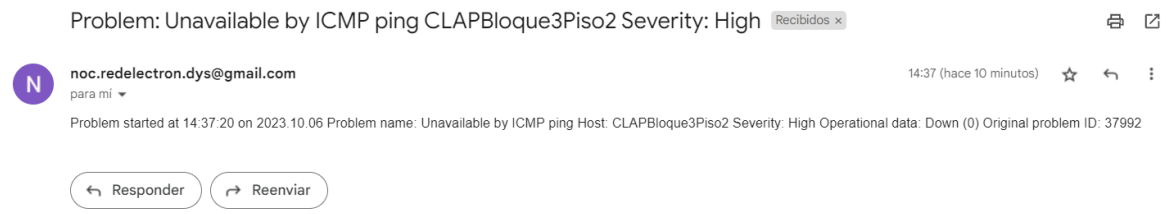

Figura 4.8: Mensaje de correo electrónico generado por la herramienta de monitoreo. Fuente: Elaboración propia.

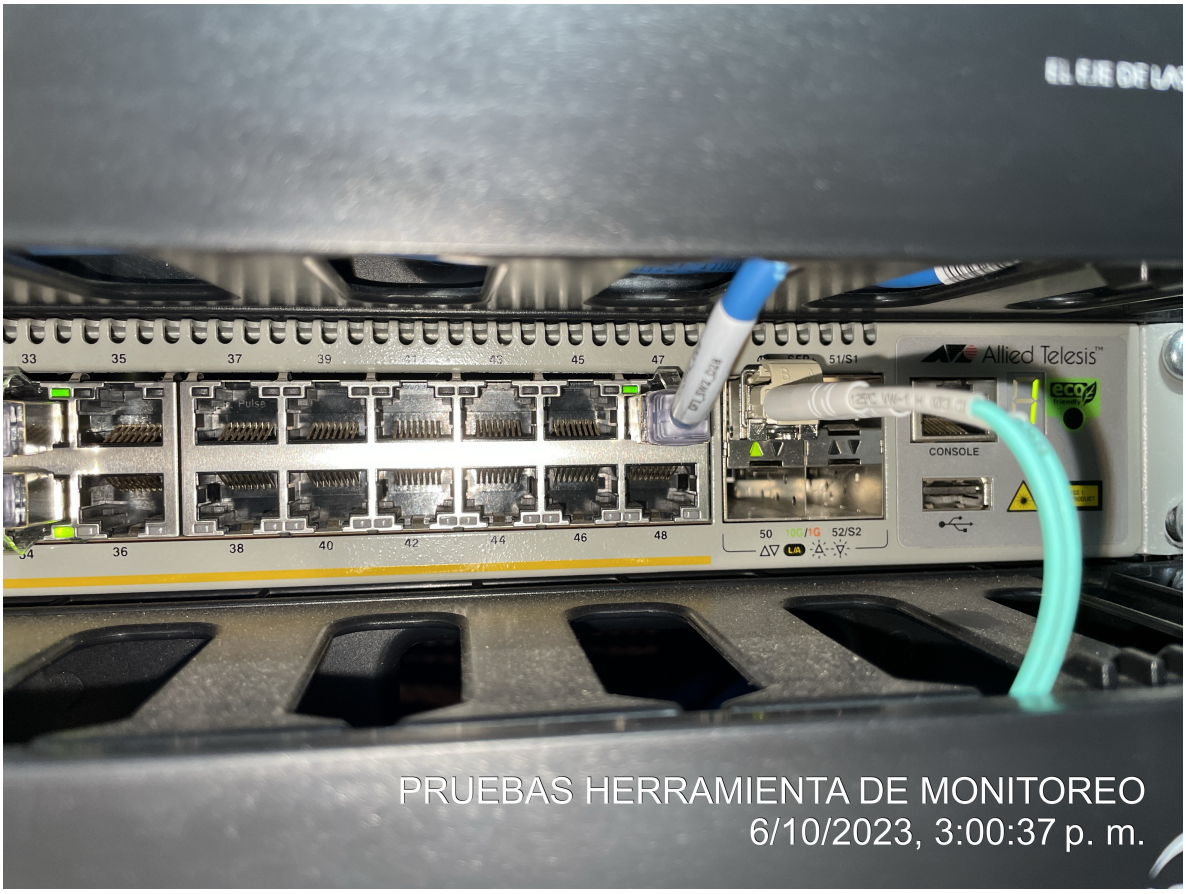

Figura 4.9: Desconexión del cable de red del servidor de telefonía. Fuente: Elaboración propia.

La herramienta intenta comunicarse con el servidor, pero no tiene alcance, entonces genera una alerta de falla de conexión (Figura 4.10).

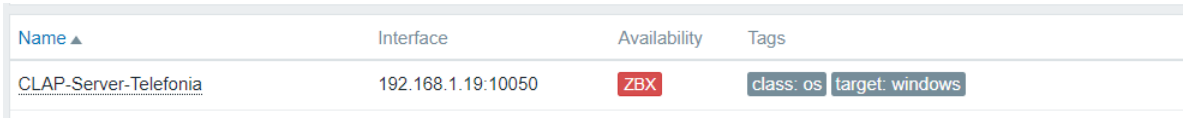

Figura 4.10: Creación de problema en la herramienta de monitoreo.
Fuente: Elaboración propia.

Se realiza el envío del correo con información del problema generado en el servidor de telefonía. Como se ve en la Figura 4.11, el asunto contiene información de que no se alcanza el dispositivo, así como el nombre del equipo dentro de la herramienta y una criticidad alta.

Figura 4.11: Envío del correo del problema en el servidor de telefonía.
Fuente: Elaboración propia.

4.1.3. Prueba de la aplicación de agendamiento

Adicional a la herramienta de monitoreo, se hizo necesario desarrollar una aplicación que permitiera generar agendamiento de visitas, frente a fallas presentadas, a partir de las notificaciones vía mensajes de correo electrónico enviadas. Esto permite al coordinador de proyectos de la empresa REDELECTRON-D&S S.A.S. un menor tiempo de respuesta frente a los incidentes, pues la única actividad que debería realizar de forma inmediata, sería definir la cuadrilla que atendería la visita. La aplicación que realiza el agendamiento de la visita en Google Calendar entra en ejecución cada 10 minutos, en ese momento valida la bandeja de correos recibidos para verificar si alguno cumple con las características necesarias para generar el agendamiento, es decir, que el correo no haya sido leído y que el asunto contenga información de que un equipo no ha sido alcanzado, el nombre de dicho equipo y un nivel de criticidad alto. La Figura 4.12 muestra la evidencia de ejecución de la aplicación cada 10 minutos para realizar la validación de correos.

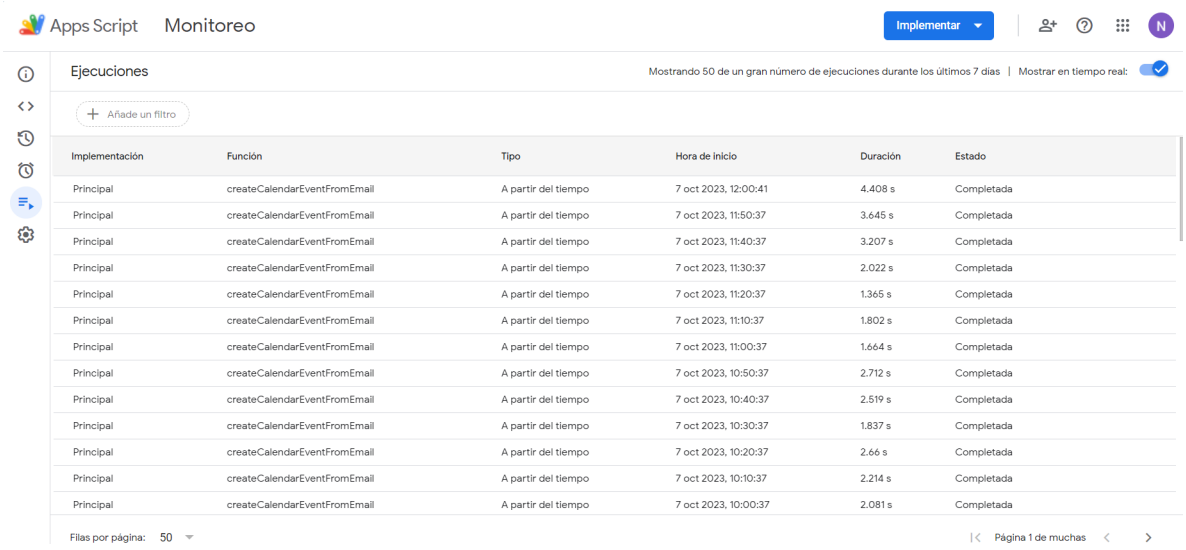

Figura 4.12: Prueba de ejecución de la aplicación cada 10 minutos.
Fuente: Elaboración propia.

4.1.4. Prueba de agendamiento en Google Calendar

Agendamiento para un *switch* de acceso

Como se puede observar en la Figura 4.13, cuando se genera la alerta por caída del servicio en un *switch* de acceso, se agenda una visita al cliente cuarto horas después de la notificación del evento, cumpliendo así con los tiempos de respuesta máximos, contratados con el cliente. El agendamiento en Google Calendar brinda a su vez detalles de lo ocurrido con el equipo notificado, de manera que la cuadrilla sepa qué equipo revisar en el momento de la visita.

Agendamiento para un *Access Point* tipo interior

La Figura 4.14 muestra el agendamiento de visita para una alerta generada por fallas en un *Access Point* tipo interior. En ella se observa cómo la alerta es generada para el día siguiente de la notificación, a las 8 de la mañana, cumpliendo así con los tiempos máximos de respuesta contratados con el cliente para atender fallas en equipos de conectividad inalámbrica.

Agendamiento para el servidor de telefonía

En la Figura 4.15 se observa el agendamiento de una visita para revisión del servidor de telefonía al día siguiente de la generación de la alerta, a las 8 de la mañana. Cumpliendo así con la generación de visitas, según el tiempo contratado con el cliente

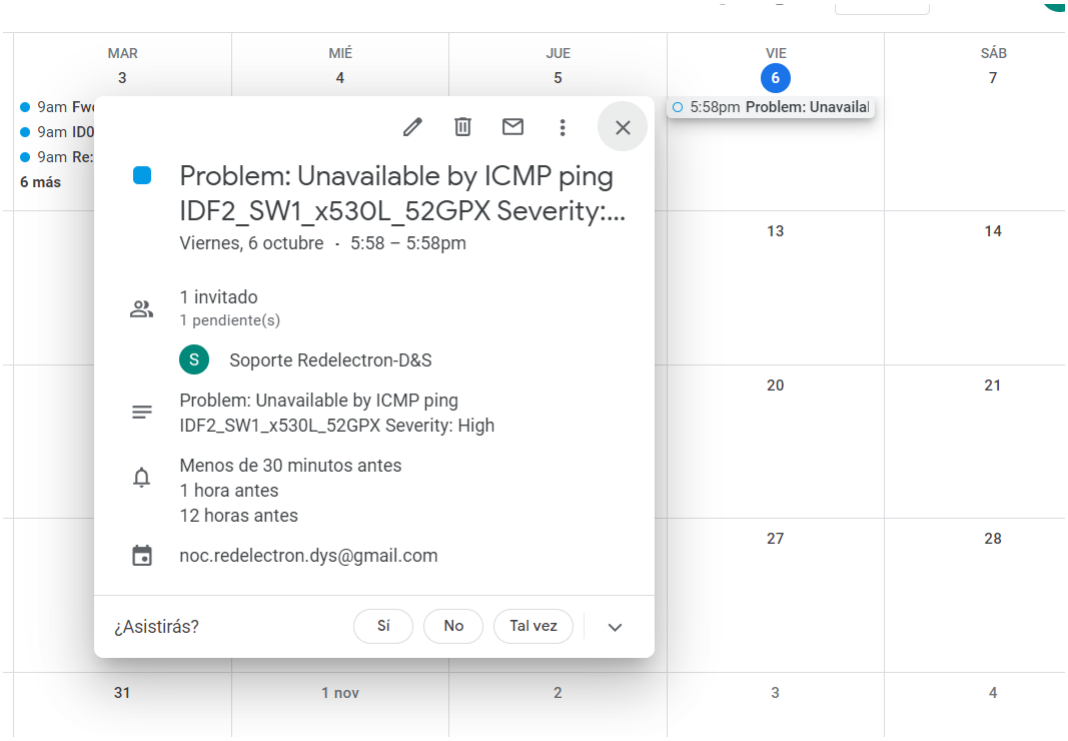

Figura 4.13: Agendamiento de visita para *switch* de acceso.
Fuente: Elaboración propia.

para este tipo de servicio y según el nivel de criticidad dentro de la red.

Finalmente, se evidencia el correcto funcionamiento de la solución planteada, pues se cumplen con las tres tareas proyectadas. En primera medida se cumple con el monitoreo de los dispositivos de red instalados y soportados por la empresa REDELECTRON-D&S S.A.S. En segunda instancia, se logra realizar notificación vía correo electrónico de la alerta que se presentan en los equipos de red, estas notificaciones contienen información valiosa para establecer un diagnóstico preliminar sobre lo ocurrido con el equipo. Por último, se genera el agendamiento de visitas a partir de la notificación de correo electrónico por medio de una aplicación en la nube que integra el servicio de monitoreo con la herramienta de asignación de tareas utilizada por la empresa.

La empresa REDELECTRON-D&S S.A.S. se encuentra conforme con la solución desarrollada y los resultados obtenidos (Anexo 1).

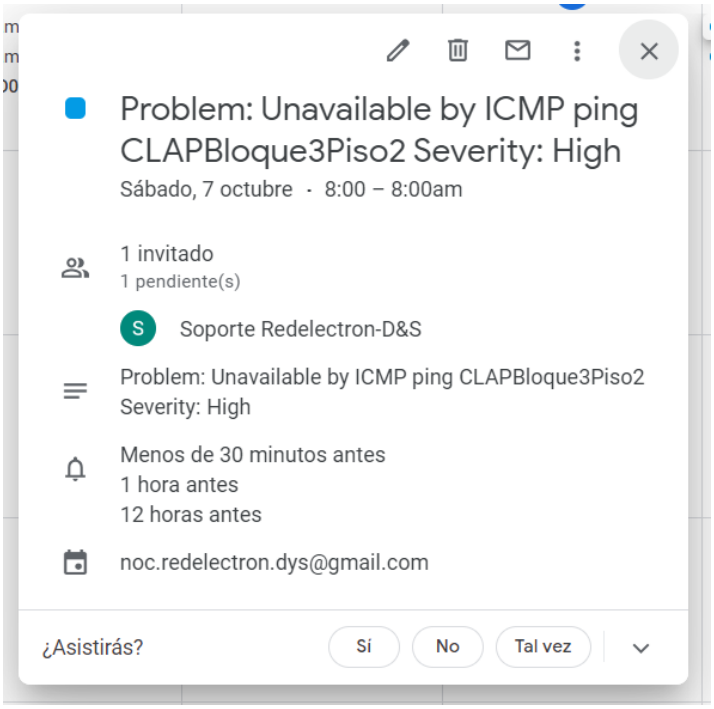

Figura 4.14: Agendamiento de visita para *Access Point* tipo interior.
Fuente: Elaboración propia.

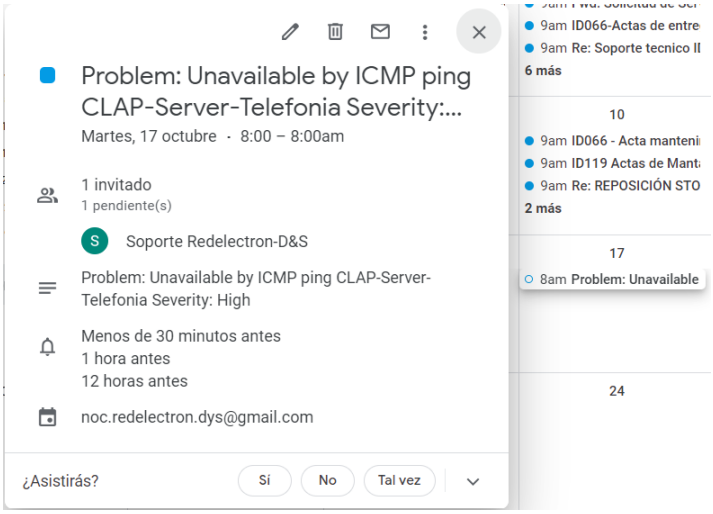

Figura 4.15: Agendamiento de visita para el servidor de telefonía.
Fuente: Elaboración propia.

CAPÍTULO 5

CONCLUSIONES, RECOMENDACIONES Y TRABAJOS FUTUROS

En el presente proyecto se realizó el desarrollo de una herramienta de monitoreo articulada con el programa de asignación de tareas utilizado por la empresa REDELECTRON-D&S S.A.S., para lo cual, en un primer momento se hizo la implementación de la herramienta de monitoreo para las redes que se encuentran a cargo de la empresa. A continuación, se realizó una aplicación en la nube que verifica la notificación realizada por la herramienta de monitoreo para realizar el agendamiento de visitas cuando se presentan fallas en los equipos. Finalmente, se evaluó el desempeño de la solución desarrollada, verificando que se cumpliera el alcance establecido y se diera respuesta a los clientes según los tiempos contratados para el soporte de las redes.

5.1. CONCLUSIONES

Una vez finalizada la implementación y puesta en producción de la herramienta de monitoreo para la empresa REDELECTRON-D&S S.A.S., se concluye que:

5.1.1. Conclusiones sobre los resultados

- El despliegue de la solución logra mitigar la ausencia del administrador de red, ya que el agendamiento se genera de forma automática notificando al coordinador de proyectos sobre el incidente ocurrido.
- La automatización de generación de visitas permite ofrecer al cliente un servicio de atención óptimo el cual se basa en respuesta rápidas frente a incidentes y realización de actividades objetivas gracias a la información obtenida por la herramienta.
- Se logra garantizar el funcionamiento de la herramienta en todos los dispositivos para los servicios que se habían planteado inicialmente, cumpliendo con los objetivos planteados.

5.1.2. Conclusiones sobre la implementación

- El análisis de los requerimientos para el desarrollo de la herramienta de monitoreo, permitieron establecer las necesidades reales de la empresa REDELECTRON-D&S S.A.S. para garantizar una puesta el despliegue de la solución de manera correcta.

- El análisis de la criticidad de los equipos permite definir tiempos de respuesta basados en las necesidades de los clientes, con ello se logran establecer mejoras en los tiempos de asistencia de los colaboradores frente a fallas.
- El monitoreo del servicio de VoIP se realizó sobre el servidor que alberga la planta, ya que en la actualidad los teléfonos utilizan el protocolo SysLog para monitoreo, el cual no es soportado por la herramienta Zabbix. Adicional a ello, el sistema de UCC no permite monitoreos directos, pues se trata de una aplicación y no de un servidor.
- La utilización de una herramienta *Open Source* y APIs de baja de demanda de recursos, permitió realizar una implementación austera para la empresa REDELECTRON-D&S S.A.S. logrando el mejor porcentaje del índice calidad sobre servicio posible.

Finalmente, se concluye que la implementación de la primera herramienta de monitoreo de equipos y servicios de red para la empresa REDELECTRON-D&S S.A.S., como respuesta al crecimiento de redes soportadas, permite brindar un mejor servicio de respuesta ante incidentes a los clientes, logrando así su satisfacción y la posibilidad de ofrecer este servicio a muchas más empresas. Adicionalmente, gracias al desarrollo de bajo costo logrado, se obtuvo el mejor índice de costo beneficio posible, permitiendo así mejoras financieras para la empresa al ofrecer un producto de buena calidad.

5.2. RECOMENDACIONES

Con el fin de que se logre obtener los mejores resultados con la solución implementada, es importante tener en cuenta las siguientes recomendaciones:

- Establecer, dentro de la empresa REDELECTRON-D&S S.A.S., la figura de administrador de redes y servicio para los clientes, para que este colaborador realice el correcto manejo de la herramienta. Con ello se evita daños en la implementación y malas prácticas.
- Realizar el escalamiento del *script* implementado, estableciendo bases de datos con los nombres de todos los equipos de clientes que se van a monitorear, con el fin de que se pueda mejorar la experiencia de asignación de tareas. Esta implementación no fue realizada en el presente trabajo, pues implicaba costos de almacenamiento que no fueron incluidos al inicio del proyecto.
- Realizar actualización constante del servidor de monitoreo, con ello se podrá disfrutar de mejoras en seguridad y en rendimiento de la herramienta.

5.3. TRABAJOS FUTUROS

- Implementar del Centro de operaciones de red, *Network Operation Center.* (NOC) físico en la empresa REDELECTRON-D&S S.A.S. que permita realizar monitoreo

en tiempo real de las redes soportadas, en un lugar establecido para este fin.

- Desarrollar una aplicación de asignación de tareas que permita definir las cuadrillas que está libre para atender el incidente presentado, y articularla con la aplicación ya existente.
- Realizar la implementación de la herramienta para monitorear los servicios en la nube en los cuales la empresa está incursionando.
- Acondicionar la herramienta Zabbix con las plantillas sobre las que está trabajando Zabbix, para poder monitorear los servicios de UCC con el fin de brindar un mejor monitoreo al servicio de VoIP.

REFERENCIAS

[1] S. Kemp. Digital 2023: Global overview report. [Online]. Available: https://datareportal.com/reports/digital-2023-global-overview-report

[2] ——. Informe digital 2022: las nuevas estadísticas de redes sociales. [Online]. Available: https://blog.hootsuite.com/es/informe-digital-estadisticas-de-redes-sociales/

[3] Colombia el segundo país con más ciberataques en 2022 - novedades tecnología - tecnología - ELTIEMPO.COM. [Online]. Available: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/colombia-el-segundo-pais-con-mas-ciberataques-en-2022-746276

[4] REDELECTRON DS S.A.S. Nosotros. [Online]. Available: https://www.redelectrondys.com/nosotros/

[5] ——, "Misión y visión de la empresa REDELECTRON D&S S.A.S." [Online]. Available: https://www.redelectrondys.com/nosotros/

[6] U. I. de Telecomunicaciones, "MANTENIMIENTO: INTRODUCCIÓN y PRINCIPIOS GENERALES." [Online]. Available: https://www.itu.int/rec/dologin_pub.asp?lang=s&id=T-REC-M.20-199210-I!!PDF-S&type=items

[7] ——, "SERIE m: RGT y MANTENIMIENTO DE REDES: SISTEMAS DE TRANSMISIÓN, CIRCUITOS TELEFÓNICOS, TELEGRAFÍA, FACSÍMIL y CIRCUITOS ARRENDADOS INTERNACIONALES." [Online]. Available: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-M.3010-200002-I!!PDF-S&type=items

[8] ISO 31000:2018(es), gestión del riesgo — directrices. [Online]. Available: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

[9] Los pros y los contras de la metodología de cascada. [Online]. Available: https://www.lucidchart.com/blog/es/pros-y-contras-de-la-metodologia-de-cascada

[10] FERMAX. Sobre FERMAX. [Online]. Available: https://www.fermax.com/spain/sobre-fermax

[11] Panduit | perfil de la empresa. [Online]. Available: https://www.panduit.com/latam/es/about/company-profile.html

[12] History of lutron - growth & prosperity of the light control industry. [Online]. Available: https://www.lutron.com/es-LA/Company-Info/Paginas/AboutUS/OurStory.aspx

[13] Infraestructura de red siempre a la vista con PRTG. [Online]. Available: https://www.paessler.com/es/network-infrastructure

[14] Infraestructura de red con red hat y sus partners. [Online]. Available: https://www.redhat.com/es/partners/network-infrastructure

[15] Servidor: definición y detalles. [Online]. Available: https://www.paessler.com/es/it-explained/server

[16] ¿qué es un gateway VoIP? [Online]. Available: https://quarea.com/es/?post_type=page&p=639

[17] Productos WLAN para empresas - huawei. [Online]. Available: https://e.huawei.com/es/products/enterprise-networking/wlan

[18] Z. Fangfang. What is WiFi roaming? how does WiFi roaming work? - huawei. [Online]. Available: https://info.support.huawei.com/info-finder/encyclopedia/en/WiFi+Roaming.html

[19] "las WLAN proporcionan movilidad y ahorro de costes". Section: Movilidad. [Online]. Available: https://www.computerworld.es/movilidad/las-wlan-proporcionan-movilidad-y-ahorro-de-costes

[20] O. I. del Trabajo, "Herramienta de 10 pasos para un retorno al trabajo seguro y saludable en tiempos de COVID-19." [Online]. Available: https://www.ilo.org/wcmsp5/groups/public/---americas/---ro-lima/documents/publication/wcms_745842.pdf

[21] Semana. De 46.645 escuelas en el país, solo el 36,63 % tendría acceso a internet. Section: Educación. [Online]. Available: https://www.semana.com/educacion/articulo/de-46645-escuelas-en-el-pais-solo-el-3663-tendria-acceso-a-internet/202152/

[22] Q. D. T. D. Company, "Cabling standard - ANSI-TIA-EIA 568 b - commercial building telecommunications cabling standard." [Online]. Available: https://www.csd.uoc.gr/~hy435/material/Cabling%20Standard%20-%20ANSI-TIA-EIA%20568%20B%20-%20Commercial%20Building%20Telecommunications%20Cabling%20Standard.pdf

[23] D. A. León, J. G. M. Cuenca, I. A. A. Sánchez, and D. J. M. Palacios, "Inteligencia artificial para el control de tráfico en redes de datos: Una revisión," vol. 16, no. 31, pp. 17–24, number: 31. [Online]. Available: https://revistas.ucp.edu.co/index.php/entrecienciaeingenieria/article/view/2655

[24] 2 what is zabbix. [Online]. Available: https://www.zabbix.com/documentation/current/en/manual/introduction/about

[25] About nagios. what is nagios? nagios.ORG. [Online]. Available: https://www.nagios.org/about/

[26] PRTG network monitor – all-in-one network monitoring tool. [Online]. Available: https://www.paessler.com/prtg/prtg-network-monitor

[27] The official checkmk user guide. [Online]. Available: https://docs.checkmk.com/latest/en/

[28] Descargar zabbix 6.4 for ubuntu 22.04 (jammy), MySQL, apache. [Online]. Available: https://www.zabbix.com/la/download?zabbix=6.4&os_distribution=ubuntu&os_version=22.04&components=server_frontend_agent&db=mysql&ws=apache

[29] Install and configure a MySQL server. [Online]. Available: https://ubuntu.com/server/docs/databases-mysql

[30] Zabbix. 6 instalación de la interfaz web. [Online]. Available: https://www.zabbix.com/documentation/current/es/manual/installation/frontend

[31] ISO/IEC standard for corporate governance of information technology. [Online]. Available: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/news/2008/06/Ref1135.html

[32] "Buen gobierno de las tecnologías de la información según la normas ISO/IEC 38500."

[33] PAe - MAGERIT v.3 : Metodología de análisis y gestión de riesgos de los sistemas de información. [Online]. Available: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=en

[34] MAGERIT 3.0: MÉTODO DE ANÁLISIS DE RIESGOS. [Online]. Available: https://interpolados.wordpress.com/2020/10/07/magerit-3-0-metodo-de-analisis-de-riesgos/

[35] A. Telesis, "SNMP feature overview and configuration guide." [Online]. Available: https://www.alliedtelesis.com/sites/default/files/documents/configuration-guides/snmp_feature_overview_guide.pdf

[36] Zabbix. 1 configuración de un equipo. [Online]. Available: https://www.zabbix.com/documentation/current/es/manual/config/hosts/host

[37] A. Telesis, "At-tq5403 wireless access point management user's guide." [Online]. Available: https://www.alliedtelesis.com/sites/default/files/documents/configuration-guides/ati-tq5403series_ug.pdf

[38] Descargar agentes zabbix. [Online]. Available: https://www.zabbix.com/la/download_agents

[39] Zabbix. 4 severidad del disparador. [Online]. Available: https://www.zabbix.com/documentation/current/es/manual/config/triggers/severity

[40] Cómo acceder con contraseñas de aplicaciones - ayuda de cuenta de google. [Online]. Available: https://support.google.com/accounts/answer/185833?hl=es-419

[41] Zabbix. 1 email. [Online]. Available: https://www.zabbix.com/documentation/current/en/manual/config/notifications/media/email

[42] ——. 1 configuring a user. [Online]. Available: https://www.zabbix.com/documentation/current/en/manual/config/users_and_usergroups/user

[43] Cómo habilitar una API en tu proyecto de google cloud | cloud endpoints frameworks para app engine. [Online]. Available: https://cloud.google.com/endpoints/docs/frameworks/enable-api?hl=es-419

[44] IAM service account credentials API | IAM documentation. [Online]. Available: https://cloud.google.com/iam/docs/reference/credentials/rest