INSTITUTO POLITECNICO NACIONAL
ESCUELA SUPERIOR DE INGENIERIA MECANICA Y ELECTRICA
UNIDAD PROFESIONAL "ADOLFO LOPEZ MATEOS"

SECCION DE ESTUDIOS DE POSGRADO E INVESTIGACIÓN
MAESTRIA EN CIENCIAS EN INGENIERÍA DE SISTEMAS

DISEÑO DE UN SISTEMA DE INFORMACION PARA EL MONITOREO DE EQUIPOS DE RED DE DATOS DE UNA EMPRESA DE DISTRIBUCIÓN

T E S I S

PRESENTA:

ING. BELEN CORTES RASCON

DIRECTOR DE TESIS:

DR MIGUEL ANGEL MARTINEZ

MÉXICO, CDMX, 13 DE JUNIO DEL 2022

SIP-14
REP 2017

INSTITUTO POLITÉCNICO NACIONAL

SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

ACTA DE REVISIÓN DE TESIS

En la Ciudad de México siendo las 11 horas del día 6 del mes de diciembre del 2022 se reunieron los miembros de la Comisión Revisora de la Tesis, designada por el Colegio de Profesores de Posgrado de: la SEPI ESIME Zacatenco para examinar la tesis titulada:

DISEÑO DE UN SISTEMA DE INFORMACIÓN PARA EL MONITOREO DE EQUIPOS DE RED DE DATOS DE UNA EMPRESA DE DISTRIBUCIÓN

del (la) alumno (a):

Apellido Paterno:	Cortés	Apellido Materno:	Rascón	Nombre (s):	Belén

Número de registro: B 2 0 1 0 6 1

Aspirante del Programa Académico de Posgrado: Maestría en Ciencias en Ingeniería de Sistemas

Una vez que se realizó un análisis de similitud de texto, utilizando el software antiplagio, se encontró que el trabajo de tesis tiene 15 % de similitud. **Se adjunta reporte de software utilizado.**

Después que esta Comisión revisó exhaustivamente el contenido, estructura, intención y ubicación de los textos de la tesis identificados como coincidentes con otros documentos, concluyó que en el presente trabajo **SI** ☐ **NO** ■ **SE CONSTITUYE UN POSIBLE PLAGIO.**

JUSTIFICACIÓN DE LA CONCLUSIÓN: *(Por ejemplo, el % de similitud se localiza en metodologías adecuadamente referidas a fuente original)*

El % de similitud se localiza en metodologías adecuadamente referidas a fuente original

****Es responsabilidad del alumno como autor de la tesis la verificación antiplagio, y del Director o Directores de tesis el análisis del % de similitud para establecer el riesgo o la existencia de un posible plagio.**

Finalmente y posterior a la lectura, revisión individual, así como el análisis e intercambio de opiniones, los miembros de la Comisión manifestaron **APROBAR** ■ **SUSPENDER** ☐ **NO APROBAR** ☐ la tesis por **UNANIMIDAD** ■ o **MAYORÍA** ☐ en virtud de los motivos siguientes:

La tesis es un trabajo original y cumple con los requisitos establecidos en reglamento de estudios de posgrado

COMISIÓN REVISORA DE TESIS

Dr. Miguel Angel Martínez Cruz	Dr. Jorge Armando Rojas Ramírez	Dr. Julián Patiño Ortiz
Director de Tesis Nombre completo y firma	Nombre completo y firma	Nombre completo y firma
Dr. Miguel Patiño Ortiz	Dra. Maricela Cuellar Orozco	Dr. José Martínez Trinidad
2° Director de Tesis (en su caso) Nombre completo y firma	Nombre completo y firma	Nombre completo y firma **PRESIDENTE DEL COLEGIO DE PROFESORES**

SECCIÓN DE ESTUDIOS DE POSGRADO E INVESTIGACIÓN

INSTITUTO POLITÉCNICO NACIONAL

SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

CARTA DE AUTORIZACIÓN DE USO DE OBRA PARA DIFUSIÓN

En la Ciudad de México el día 05 del mes de diciembre del año 2022, la que suscribe Belén Cortés Rascón alumna del programa de Maestría en Ciencias en Ingeniería de Sistemas con número de registro B201061, adscrita a la Sección de Estudios de Posgrado e Investigación de la ESIME Zacatenco manifiesta que es autora intelectual del presente trabajo de tesis bajo la dirección de los Doctores Miguel Ángel Martínez Cruz y Miguel Patiño Ortiz y cede los derechos del trabajo intitulado Sistema de un Sistema de Información para el Monitoreo de Equipos de Red de una Empresa de Distribución, al Instituto Politécnico Nacional, para su difusión con fines académicos y de investigación.

Los usuarios de la información no deben reproducir el contenido textual, gráficas o datos del trabajo sin el permiso expresado del autor y/o director(es). Este puede ser obtenido escribiendo a la siguiente dirección de correo bcortesr2102tmp@alumnoguinda.mx. Si el permiso se otorga, el usuario deberá dar el agradecimiento correspondiente y citar la fuente de este.

Belén Cortés Rascón

INDICE

INDICE DE TABLA

INDICE DE FIGURAS

Resumen

El proyecto que a continuación se documenta se basa en la problemática que en los últimos años en las empresas de distribución de insumos se han presentado diversas transformaciones en el acceso y uso de información de sus redes, dando lugar a la necesidad de un sistema de información para el control de distintos conceptos, donde se reflejen las funciones específicas de sus almacenes y la sede principal. En concreto, para este proyecto el objetivo es analizar los problemas que se tiene en la red de la sede principal y sus almacenes de una empresa de distribución de insumos.

Para resolver el problema en el presente documento se analizan las diferencias entre la arquitectura de red, nodos, interfaces y el protocolo que se tiene en los equipos para detectar las características como similitudes y diferencias que ambas tienen a través de la metodología Waterfall o en cascada y poder afrontar con un diseño de sistema que pueda detectar las fallas a tiempo.

Una vez definida las necesidades de la red, se empieza analizar los softwares existentes en el mercado que cumplen con los objetivos planteados para detectar las fallas. Por último, se realiza el diseño del monitoreo de la red que permite detectar cualquier falla con algún equipo de red conectado en la sede principal o en sus almacenes sin necesidad de modificar altamente su topología de su red, es decir, añadiendo interfaces y protocolos para que exista una comunicación entre ellos. Con la cual se pretende obtener los siguientes resultados, como un ahorro en el tiempo de solución de fallas.

Abstract

The project that is documented below is based on the problem that in recent years in supply distribution companies there have been various transformations in the access and use of information from their networks, giving rise to the need for an information system. for the control of different concepts, where the specific functions of its warehouses and the main headquarters are reflected. Specifically, for this project the objective is to analyze the problems that exist in the network of the main headquarters and its warehouses of a supply distribution company.

To solve the problem in this document, the differences between the network architecture, nodes, interfaces and the protocol that the equipment has in order to detect the characteristics such as similarities and differences that both have are analyzed through the life cycle model and be able to cope with a system design that can detect failures in time.

Once the needs of the network have been defined, we begin to analyze the existing software on the market that meets the objectives set to detect failures. Finally, the design of the network monitoring is carried out, which allows detecting any failure with any network equipment connected in the main headquarters or in its warehouses without the need to highly modify its network topology, that is, adding interfaces and protocols for that there is communication between them. With which it is intended to obtain the following results, as a saving in the troubleshooting time.

Introducción

En la actualidad nuestra sociedad se apoya, en distinta medida, en la tecnología, y ésta a su vez en el Internet, influyendo en las relaciones humanas y laborales, educación, en sistemas: financieros, gubernamentales, de transporte y de seguridad, en todos sus ámbitos; por lo anterior, los sistemas de información para el monitoreo de los equipos de red constituyen la parte más delicada de cualquier empresa e institución.

“Empresas, almacenes y usuarios de Internet pronostican la dinámica que tendrá la red ya que es una parte principal para su rendimiento. El conocimiento de las redes permite mejorar la planeación estratégica sobre los sistemas de monitoreo, los datos de trafico de las redes de comunicaciones se han hecho con medidas en las diferentes capas del modelo referencial” (Wetteroth, OSI Reference Model for Telecomunications, 2002).

En este trabajo se presenta un sistema de información para el monitoreo de distintos equipos de red de datos de una empresa de distribución, en el cual surge la necesidad de contar con información para el funcionamiento de los equipos de red en puntos vulnerables, donde se debe controlar el rendimiento y la eficiencia que permita garantizar la seguridad de los clientes.

El monitoreo de los equipos de red se define como la suma total de políticas y procedimientos para diseñar, planificar, configurar y controlar los elementos que forman parte de una red para certificar su uso eficaz y eficiente. Como resultado de los recursos, este proceso será reflexivo en la calidad de los servicios que la empresa presta.

Este proyecto de tesis se divide en los siguientes capítulos:

En el capítulo 1 veremos el marco contextual donde se mencionan los precedentes para administrar un sistema de información y el monitoreo de equipos de la red de datos con herramientas de software, esto para poder mejorar la administración de la red y así poder realizar un buen monitoreo de los equipos.

El capítulo 2 está constituido por el Marco Teórico aquí se describe la Teoría General de Sistemas (TGS), así como la definición de un sistema de información de la red y las funciones básicas que debe tener este sistema. Se hace referencia a la cibernética y al tipo de protocolo a utilizar con las herramientas de monitoreo, se procede a indicar la recomendación a seguir para un sistema moderno bien establecido y bien pensado. El Marco Metodológico se describe el método a utilizar para el desarrollo de esta investigación y como referencia al modelo de Cascada y su aplicación.

En el capítulo 3 se presenta la propuesta del diseño de un sistema de información para la concentración y el monitoreo de equipos de red de datos de una empresa de distribución y las principales fases.

Y en el capítulo 4 se describen los pasos para la propuesta de implementación del modelo del sistema de información.

Y finalmente, se presentan las conclusiones y recomendaciones.

CAPITULO 1 MARCO CONTEXTUAL

1.1 Antecedentes

El comienzo del análisis de la red de comunicación se origina en 1965 ya que la Advanced Research Projects Agency (ARPA) comenzó con el desarrollo de un programa para empresas y universidades a proponer proyectos, con la finalidad de construir la red del futuro, el cual termino en 1969 con la primer transferencia de datos entre dos ordenadores situados a más de 600km de distancia. En 1970, Advanced Research Projects Agency Network (ARPANET) empezó a utilizar el protocolo Host to post para su comunicación. Este protocolo se conoce como Network Control Protocol (NCP) y es el precursor de Transmission Control Protocol/Internet Protocol (TCP/IP) actualmente utilizado en Internet (Redes Informaticas, 2018).

En 1973 tuvo lugar la primera conexión internacional de ARPANET, esta conexión se realizó en Reino Unido donde Bob Metcalfe presentó sus primeras ideas para una implementación del protocolo Ethernet, uno de los protocolos más importantes utilizados en las redes de área local. Cerf y Kahn publicaron su artículo, Packet Networking Protocol, en el cual se detallaba el diseño del Protocolo de control de transmisión (TCP). En 1975, los primeros enlaces satelitales se probaron a través de dos océanos desde Hawaii hasta el Reino Unido, con las primeras pruebas de TCP.

En 1982, ARPA denominaron TCP e IP al conjunto de protocolos TCP/IP para la comunicación sobre ARPANET. En el año de 1985, se establecieron distintos puntos para la responsabilidad para el control de nombres de dominio y así el Instituto de Ciencias de la Información (ISI) asumió la responsabilidad como base para la resolución de nombres de dominio. El 15 de marzo se realizó el primer registro de nombre de dominio (Symbolics.com), seguido de cmu.edu, purdue.edu, rice.edu, ucla.edu y .uk (Redes Informaticas, 2018).

Y así en la actualidad surge la necesidad de una conexión de red que permite a los usuarios de una empresa cooperar entre sí y con usuarios de otros lugares. Hacen posible contactar nuevas formas, mientras se reduce más de lo que nunca se imaginarían, entre las personas de la oficina o de todo el mundo. Si la compañía está conectada por una red, nadie está lejos de nadie. Al implementar la red, el uso del dispositivo es efectivo, se convierte en un dispositivo de acción obligatorio en una red, ya que los dispositivos de la computadora rara vez se utilizan en su capacidad máxima y, por lo tanto, son más caros: impresoras, discos duros, unidades de disco flexibles, unidades de cinta, módems, unidades de disco compactas y otros dispositivos. Al implementar la red, el uso del software es efectivo, una red informática proporciona a los usuarios múltiples opciones de software, información y programas.

Necesitamos compartir información e información generada por los usuarios: tendencias diarias y específicas de la computadora (textos, presupuestos, gráficos, recordatorios, planes, estrategias, etc.). Al compartir software, puede ahorrar tiempo de instalación y actualización, que también es muy importante, y también se puede ahorrar espacio de almacenamiento, que de otro modo sería redundante y necesitaría un disco duro con mayor capacidad. Acerca de compartir programas (también llamado aplicaciones).

Las ventajas de utilizar redes informáticas:

Tabla 1: *Ventajas de redes informáticas*

Ahorro dinero compartiendo recursos de alto costo y no siempre productivos durante la jornada laboral: impresoras, unidades de disco duro, unidades de disquete, módems, unidades de CD, cintas de respaldo y más.
Ahorro de tiempo en la transferencia de datos o información entre nodos remotos.
Ahorro de tiempo en la instalación y actualización de software.
Incrementar la eficiencia logística, evitando la duplicidad de expedientes donde deberían ser únicos, así como facilitando las actualizaciones.
Comunicación o mensajería en tiempo real
Aumentar la productividad.

Actualmente, la empresa de transporte de distribución de insumos, se dedica al almacenaje de los productos terminados, de materia prima, al etiquetado, a la distribución de tiendas, esta empresa dispone de una infraestructura de red en la ciudad de Querétaro con una sede principal y almacenes en diferentes localidades. Los equipos de red de datos que tienen en los almacenes no presentan una comunicación con la sede principal. Por lo que si el equipo se descontenta o no tiene acceso alguna aplicación, el ingeniero de Redes que se encuentra en la sede principal tiene que trasladarse a sitio para verificar y realizar un análisis en los equipos que tienen falla, esto hace que el almacén se detenga ya que no pueden monitorear que producto sale y entra.

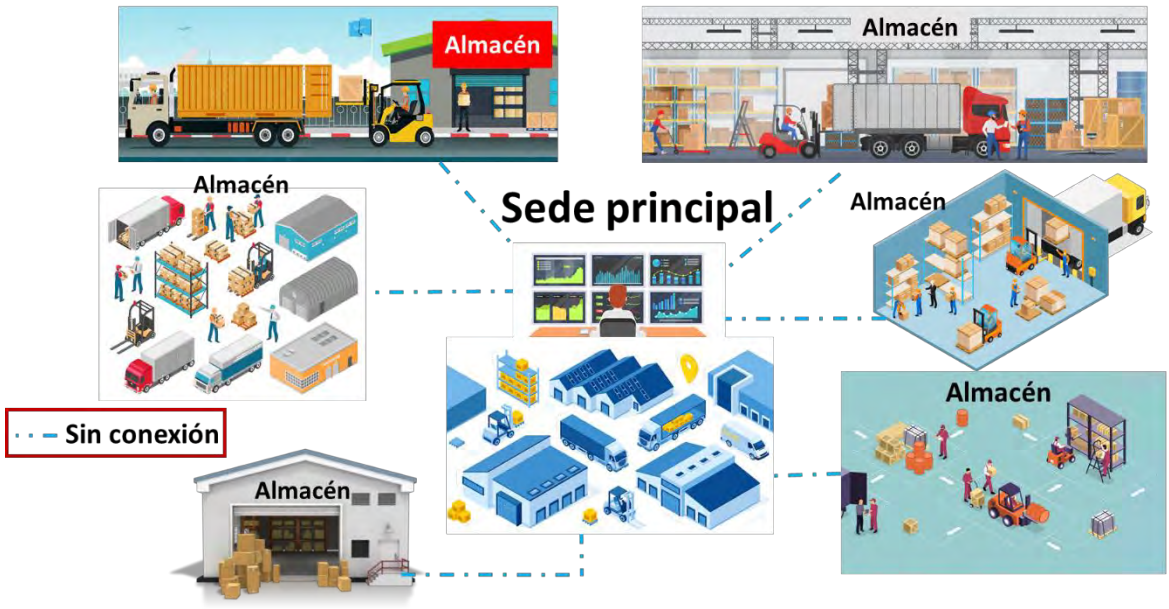


Figura 1. *Arquitectura de la sede principal y almacenes*
Fuente: *Elaboración propia*

1.2 Planteamiento del problema

La empresa de distribución de insumos cuenta con 15 almacenes, los cuales 3 son de suma importancia, ya que los productos son de excelente calidad. En la sede principal, que es donde se encuentra el departamento de Sistemas, se tienen 2 ingenieros para soporte de fallas, las cuales se presentan día a día. El principal problema, en este momento, es que no tiene una conexión de los equipos de red de datos de los almacenes desde la sede principal, y en cada almacén existe el 30% de usuarios conectados a la red con equipos personales, por lo que la calidad de internet no es suficiente. Los ingenieros de Sistemas no monitorean los dispositivos de la red de datos y no se tiene información en tiempo real para poder ir documentando los problemas que se van presentando; también no se tiene una base de datos donde se administre la información histórica y de rendimiento de las fallas que se han presentado, lo cual no permite realizar reportes estadísticos. Hoy en día, se cuenta con una tabla de direcciones de red y revisión manual en caso de que los clientes y almacenes reporten problemas.

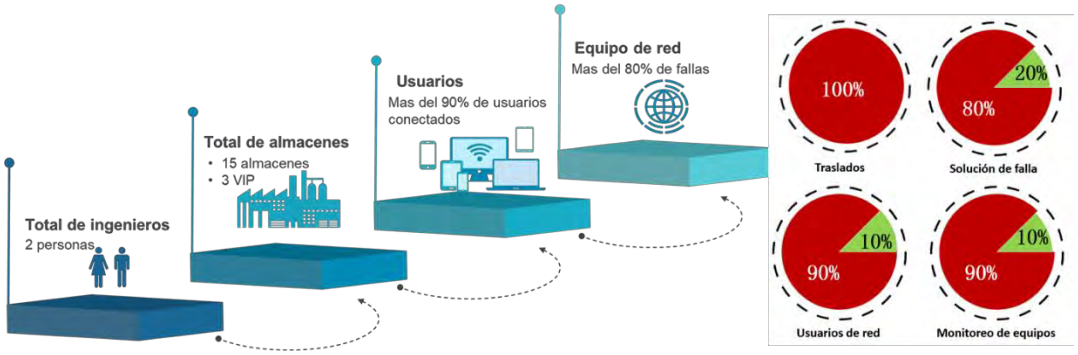


Figura 2. *Situación actual de almacenes*
Fuente: *Elaboración propia*

La empresa de distribución debe presentar a sus clientes un alto grado de confianza, para ello la necesidad de establecer reglas para el seguimiento de su red, recopilando información de incidencias cuando se presenten problemas, como congestión o lentitud del servicio, capacidad de transmisión en las redes de distribución, rendimiento de los equipos de red. Esto permite que los usuarios sean notificados con antelación de cualquier problema y sean responsables de tomar las decisiones correctas en la red de datos de la empresa de distribución.

1.3 Objetivo (s)

Objetivo General

Diseñar un sistema de información para el monitoreo de equipos de red de datos de una empresa de distribución aplicando técnicas y herramientas de la ingeniaría del software.

Objetivo Específicos:

- Definir y analizar la topología física y lógica de la red que actualmente presenta la empresa de distribución.
- Desarrollar políticas internas para monitorear, evaluar y controlar incidentes en la red de datos.
- Analizar de los equipos de redes a monitorear.
- Diseñar la arquitectura de un sistema de información.

1.4 Justificación

La dinámica del entorno y las exigentes necesidades de contar con un sistema de información para el monitoreo de los equipos de red de datos para la toma de decisiones ha generado que la empresa de transporte de distribución de insumos designe un mayor presupuesto al departamento de Sistemas para la inversión de un sistema de información. El proceso que se lleva a cabo hoy en día en el departamento de Sistemas de la empresa ha mostrado escases en la concentración y control de información de la red y una nula automatización en sus procesos, además una falta de información de los equipos de red que tienen los almacenes y una falta de rapidez de respuesta.

La empresa carece de un sistema de información que permita informar en tiempo real las fallas que día a día suceden en los equipos de red de datos en su sede principal y sus almacenes. Por lo que el departamento requiere que se tenga acceso desde la sede principal hacia cualquier equipo de red que se encuentre en un almacén. Es por ello, que es de suma importancia la propuesta de la implementación del sistema, volviéndose indispensable para el administrador de la red, debido a la inexistencia de un software de monitoreo, que cubra todos los requerimientos técnicos y que sea posible la adaptación al presupuesto. En la figura 3 se muestra el porcentaje que se lograría obtener al utilizar un sistema de información para el monitoreo de los equipos de red de datos.

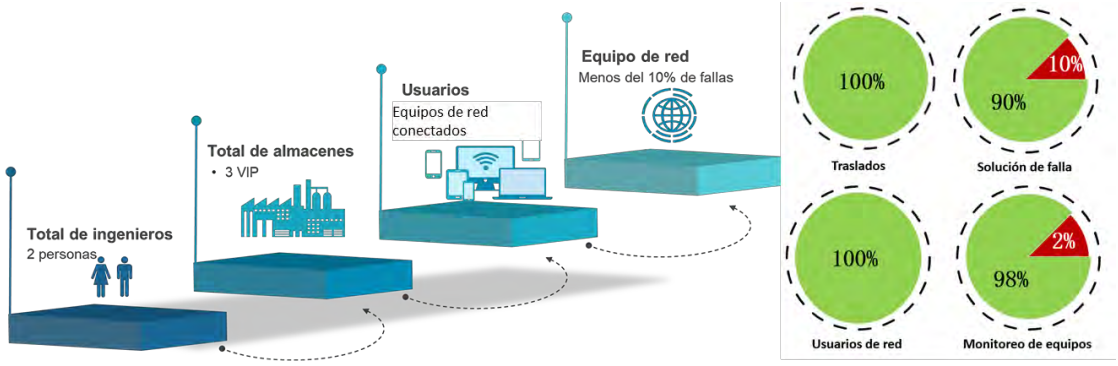


Figura 3. Situación con sistema de monitoreo en la empresa
Fuente: *Elaboración propia*

En los almacenes se tienen en ciertos puntos equipos Wireless que ayudan a que las terminales portátiles se puedan conectar y así poder realizar el inventario de los productos en los anaqueles; Sin embargo, al ir analizando el funcionamiento de los equipos de red, se obtuvo un alta capacidad de usuarios conectados a la red, lo que provoca que las terminales o computadoras presenten lentitud o problemas para conectar al WIFI.

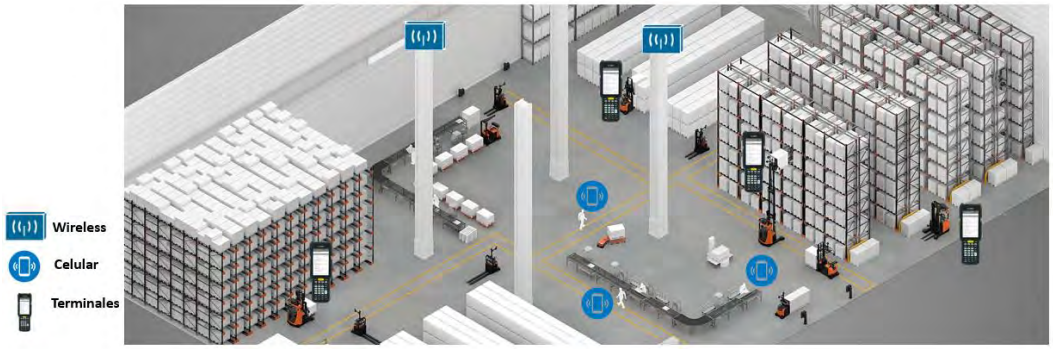
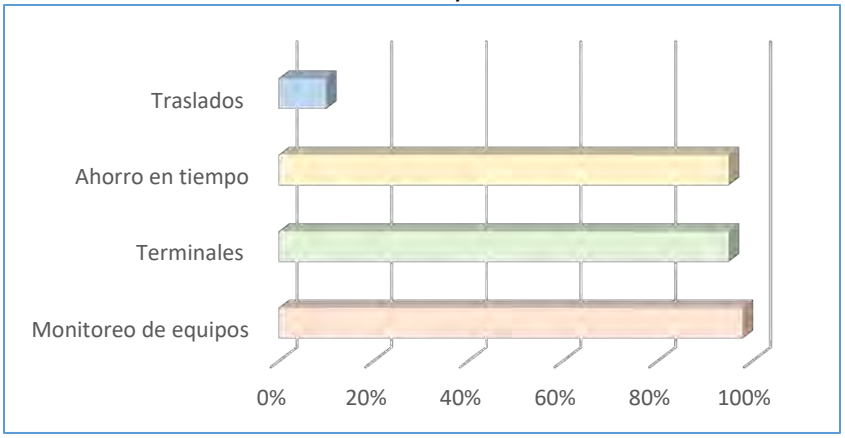


Figura 4. *Equipos en los almacenes*
Fuente: *Elaboración propia*

En la tabla 2 se muestran los resultados al implementar el sistema, en donde se muestra un 98% de monitoreo de los equipos de red, por lo que el ingeniero ahorrara tiempo y evitara traslados cuando un equipo falle, ya que podrá realizar un análisis de la red que sea oportuno, permitiendo que los almacenes no presenten desconexiones de la misma, lo anterior ayudara a definir planes y/o proporcionar las bases para estrategias a futuro.

Tabla 2: *Resultados al implementar el sistema*



CAPÍTULO 2. MARCO TEORICO

En este capítulo se abordan los conceptos teóricos con base a los cuales se desarrollará esta investigación, teniendo en cuenta las definiciones textuales de varios autores para una referencia breve y objetiva. En la tabla 3 se establecen los temas del marco teórico:

Tabla 3. *Resumen de la teoría propuesta a desarrollar*

1	**INGENIERÍA EN SISTEMAS**	Teoría General de Sistemas. Teoría de la Planeación Estratégica. Metodología.
2	**MONITOREO DE LA RED DE DATOS**	Cibernética. Conceptualización General de la Red de Datos. Conceptualización General del Monitoreo de la Red de Datos. Protocolos Simple para la Administración del Sistema de Información de Red de Datos. Tipos de Monitoreo de la Red de Datos. Sistema de Control y Administración.

2.1 MARCO TEÓRICO

2.1.1 Ciencia de Sistemas

Un sistema es un conjunto de elementos interrelacionados entre sí con el fin de alcanzar un objetivo en común. En esta definición, los aspectos importantes que se pueden considerar, es que debe haber una influencia recíproca entre los elementos del sistema, es decir, lo que afecta a un elemento afectará al otro. Y otra, que un conjunto de elementos que no persigan un mismo fin, y esto sea desde cierto ángulo, no formarán un sistema.

Hay sistemas que tienen elementos y propósitos completamente diferentes, pero tienen el mismo tipo de interacción, de los que se dice que son estructuralmente similares. Las argumentaciones extraídas del estudio de uno de estos sistemas se pueden aplicar a otro.

“Un enfoque de sistemas es un esquema sistemático que sirve como guía para resolver problemas, especialmente aquellos que surgen en la gestión de sistemas o de operaciones, cuando hay una brecha entre lo que se tiene y lo que se desea, su problema, sus componentes y su solución” (Chuchman, 1973).

El enfoque de sistemas incluye las actividades de definición de la meta general y la justificación de cada subsistema, medidas de desempeño y criterios para el objetivo principal, el conjunto de subsistemas y planes, y sus planes para un problema en particular.

La necesidad de un enfoque de sistemas es una razón común para justificar la necesidad de un enfoque de sistemas, destacando la aparición de muchos problemas hoy en día en la concentración de información. “Esta complejidad se debe a que los elementos del sistema objeto de estudio están íntimamente relacionados entre sí y el propio sistema interactúa con el entorno y con otros sistemas” (Gigch J. P., 2006).

En la figura 5 se visualizan las características de los sistemas.

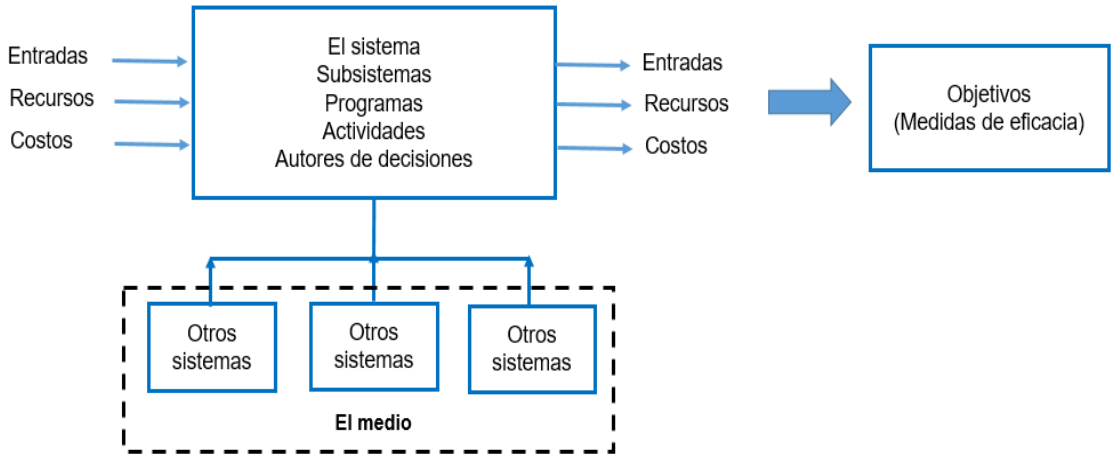


Figura 5. *El sistema y sus características*
Fuente: *TGS Van Gigch, 2006*

Los elementos son los componentes de todo sistema; Pueden ser no vivos o vivientes y la mayoría de los sistemas que tratamos son una mezcla de ambos.

Los procesos de conversión son sistemas organizados y se les da una transición en la que los elementos del sistema pueden cambiar su estado, es decir, cambiando los elementos de entrada en los elementos de salida.

La diferencia entre insumos y recursos es mínima y depende únicamente de la perspectiva y las circunstancias; los insumos son generalmente los factores a los que se aplican los recursos.

Y las salidas son el resultado de la transformación del sistema y se calculan como resultado, éxito o beneficio.

Las metas y objetivos son que la definición de estos conceptos es fundamental para el diseño de sistemas; con un nivel más bajo de abstracción, las declaraciones de intención se definen mejor y funcionan de manera más eficiente.

2.1.1.1 Teoría general de los Sistemas

"La Teoría General de Sistemas (GST) se conceptualiza como una serie de definiciones, suposiciones y cuestiones interrelacionadas según las cuales todos los fenómenos y cosas reales se ven como una jerarquía. Combinaciones completas de materia y energía. Estos grupos son sistemas. La teoría general de sistemas proporciona el poder de investigación del enfoque de sistemas. Estudia conceptos, métodos y conocimientos relacionados con el campo de los sistemas y el pensamiento" (Gigch J. P., 1990).

Una teoría general de sistemas depende de la generalización de propiedades comunes al sistema y de la capacidad de generalizar estas propiedades; también se enfoca en la atención general, el análisis y el diseño en lugar del análisis y diseño de componentes o partes; es un proceso de síntesis.

"Las TGS afirman que las propiedades de un sistema no pueden considerarse importantes para sus elementos individuales, lo cual es el caso cuando se estudian como un todo, en relación con todas las dependencias, entre sí de sus elementos o partes"(Checkland Peter, 1999).

Esta teoría fue incluida por Ludwing Von Bertalanffy como una importante actividad científica en física y biología, y proporciona la siguiente justificación para la búsqueda de una teoría cuyos principios también sean válidos.

La teoría general de sistemas dirige parte de sus esfuerzos a formular principios básicos mediante los cuales se pueda combinar el conocimiento sobre todos los sistemas vivos y no vivos.

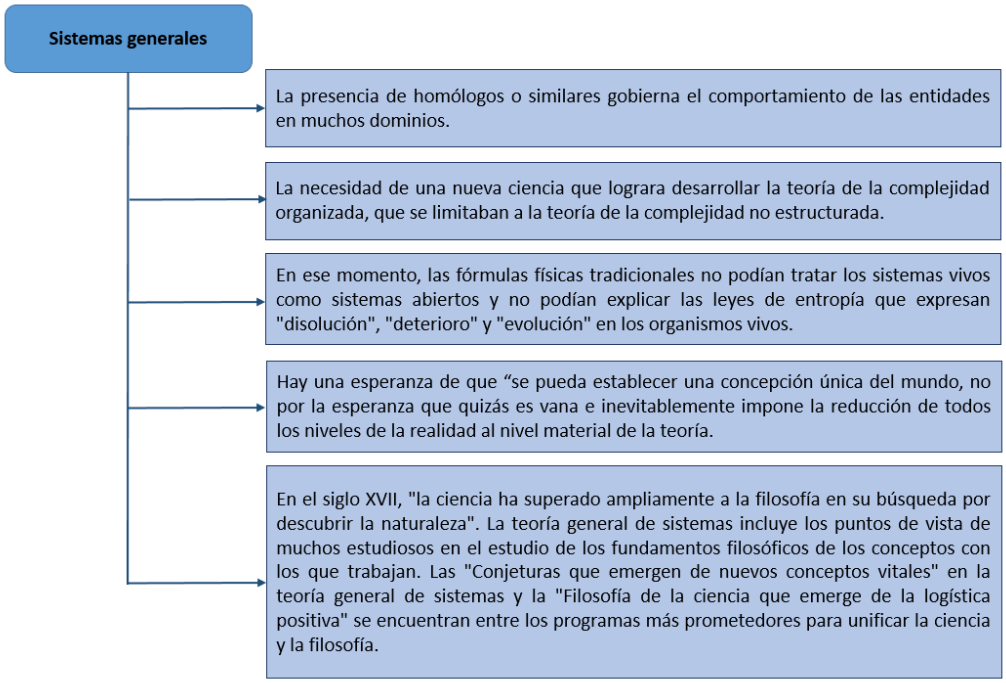


Figura 6. *Sistemas generales*
Fuente: *TGS Van Gigch, 2006*

"La Teoría General de Sistemas, es un concepto o metodología organizada que tiene como objetivo estudiar el sistema como un todo, como un todo, a partir de sus componentes y analizar las relaciones e interrelaciones entre ellos y mediante la aplicación de estrategias científicas, lo que conduce a una comprensión integral y generalizada del sistema" (Gigch J. P., 2006).

2.1.1.2 Enfoque de la Metodología de Sistemas

Bolding formuló dos posibles enfoques a la teoría general de sistemas, desarrollados por Oscar J. Bertoglio de la siguiente manera: "El primer enfoque es observar el universo empírico y escoger ciertos fenómenos generales que se encuentran en las diferentes disciplinas y tratar de construir un modelo teórico que sea relevante para esos fenómenos. Este método, en vez de estudiar sistema tras sistema, considera un conjunto de todos los sistemas concebibles (en los que se manifiesta el fenómeno general en cuestión) y busca reducirlo a un conjunto de un tamaño más razonable" (Bertoglio, 1982).

“Un segundo enfoque posible para la Teoría General de Sistemas es ordenar los campos empíricos en una jerarquía de acuerdo con la complejidad de la organización de sus individuos básicos o unidades de conducta y tratar de desarrollar un nivel de abstracción apropiado a cada uno de ellos. Este es un enfoque más sistemático que el anterior y conduce a lo que se ha denominado Un Sistema de Sistemas.” (Bertoglio, 1982).

2.1.1.3 Clasificación del sistema

La resolución de problemas siempre ha estado estrechamente relacionada con el trabajo de los ingenieros cuya función principal es diseñar las soluciones a las necesidades sociales, industriales o económicas.

El ingeniero usa el conocimiento científico, matemático y la experiencia relevante para localizar las mejores soluciones a problemas específicos, creando modelos matemáticos específicos del problema que les permiten realizar análisis y pruebas rigurosos para encontrar soluciones potenciales.

“La metodología Waterfall es un proceso de desarrollo de proyectos secuenciales comúnmente utilizado en el desarrollo de software. Este modelo implica trabajar un conjunto de pasos que deben ejecutarse uno tras otro. Su nombre viene dado por las diferentes etapas que componen el diseño, ya que deben colocarse una encima de otra siguiendo un orden concreto y estricto de arriba hacia abajo. Por ejemplo, no podemos comenzar la fase de diseño sin completar la fase de requisitos. Waterfall impulsa la filosofía paso a paso, por bloques de tareas” (Sampieri, 2014).

Esta metodología tiene varias ventajas, pero la más importante es de poder monitorizar el progreso del proyecto con documentación estrechamente generada. Otra ventaja del modelo Waterfall es que se puede autorizar a los clientes a las tareas, si se requieren.

2.1.2 Teoría de la Planeación Estratégica

Algunos autores asocian este concepto con la preparación para el futuro, a la hora de definir planes estratégicos.

"La planificación estratégica es un proceso que se dirige hacia la producción de uno o más estados deseados, situados en el futuro, que no es probable que ocurran si no hacemos algo al respecto" (Ackoff, 1970).

"La planificación estratégica es un proceso que comienza con la identificación de los objetivos de la organización, la definición de estrategias y políticas para lograrlos y, por lo tanto, el desarrollo de planes detallados para garantizar la implementación exitosa de las estrategias y, por lo tanto, el logro de los objetivos deseados" (Miklos, 2001).

"El modelo de planificación estratégica propuesto por Morrissey se basa en el desarrollo de una serie de actividades propuestas a través de sus tres componentes: pensamiento estratégico, planificación a largo plazo y planificación táctica. Este es un modelo de planificación estratégica. En él índica que la planificación estratégica es fundamental para el buen funcionamiento de cualquier organización, ya que a través de ella se pueden generar expectativas y cambios futuros, tomar las medidas necesarias y prepararse para afrontarlos" (Miklos, 2001).

Para desarrollar el plan estratégico de esta organización, se identificaron e implementaron las siguientes nueve fases:

Tabla 4. *Fase de Planeación Estratégica*

Fase I.	Definición de los valores.
Fase II	Definición de la misión.
Fase III	Definición de la visión.
Fase IV	Realización de un análisis interno para detectar las fortalezas y debilidades.
Fase V	Realización de un análisis externo para detectar las oportunidades y amenazas.
Fase VI	Formulación de la estrategia.
Fase VII	Formulación de los objetivos.
Fase VIII	Establecimiento de los planes estratégicos de acción.
Fase IX	Establecimiento de los planes tácticos de acción.

2.1.3 Metodología

"La metodología es un conjunto integrado de técnicas y métodos que permiten un enfoque unificado y abierto para cada actividad del ciclo de vida del proyecto de desarrollo. Es un proceso de desarrollo de software detallado y completo" (Sampieri, 2014).

Las metodologías se establecen en una combinación de modelos de procesos comunes. Identifican dispositivos, funciones y operaciones, así como las mejores prácticas y métodos.

Los principales objetivos de la metodología de desarrollo son:

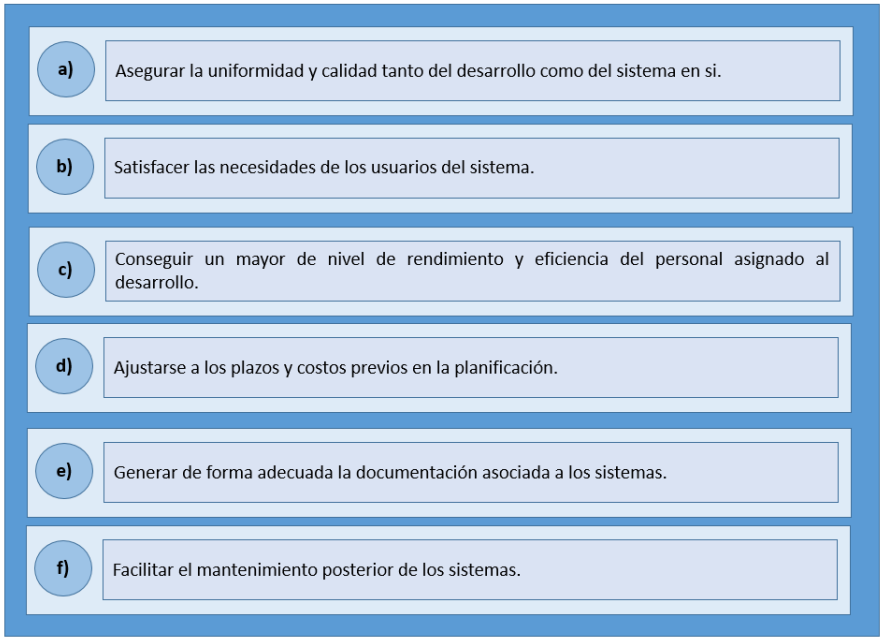


Figura 7. *Metodología de desarrollo*
Fuente: (Sampieri, 2014)

La metodología a utilizar es el modelo de Cascada de información con un enfoque sistémico y sistemático. El enfoque sistemático es global e integral y el enfoque sistémico es secuencial y con retroalimentación.

“La metodología Waterfall o cascada relaciona actividades en un diagrama cuyos entregables son necesarios para que la próxima actividad pueda dar comienzo. El proyecto se va desarrollando de una forma secuencial y se trata de una metodología tradicional frente a las cada vez más populares metodologías ágiles.” (Sampieri, 2014).

Existen sub-etapas para cada una de las fases mencionadas en el párrafo anterior, el modelo de cascada se utiliza para construir un sistema que define la secuencia de actividades involucradas y la coordinación, conexión y retroalimentación entre ellas.

2.1.3.1 Modelo Cascada

El primer modelo de desarrollo de software publicado se derivó de otros procesos de ingeniería, y tomó las actividades fundamentales del proceso de especificación, desarrollo, validación y evolución, que representa como fases separadas del proceso (Royce, 1987).

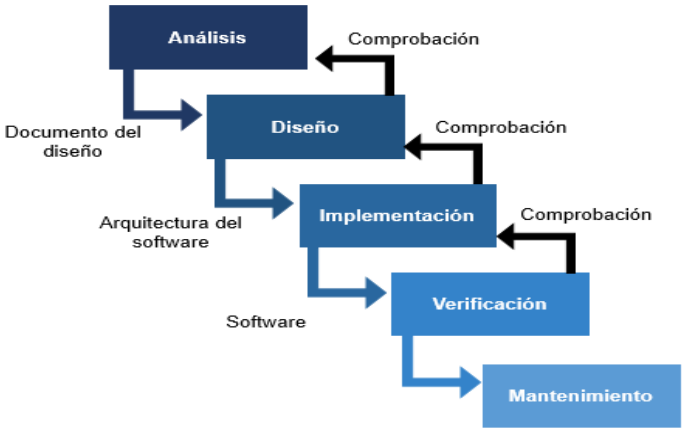


Figura 8. *Modelo de cascada*
Fuente: *(Royce, 1987)*

Una fase no comienza hasta que termine la fase anterior, y generalmente se incluye la corrección de los problemas encontrados en fases previas. En la práctica, este modelo es sistemático.

Hay diferentes versiones de este modelo disponibles. El modelo más común es el que divide el proceso de desarrollo en cinco etapas. A veces, las fases 1, 2 y 3, tal como las define Royce, se integran en una fase del proyecto como análisis de requisitos.

Tabla 5. *Etapas del Modelo de Cascada*
Fuente: *(Royce, 1987)*

Análisis	Todo proyecto de software comienza con una fase de análisis que incluye un estudio de viabilidad y definición de requisitos. Los estudios de factibilidad evalúan el costo, la rentabilidad y la factibilidad de un proyecto de software. Los resultados de los estudios de viabilidad son las especificaciones del proyecto (descripción general de los requisitos), el plan del proyecto y las estimaciones financieras y, si es necesario, las recomendaciones al cliente. Posteriormente, los requisitos se especifican en detalle, incluido el análisis de escenarios y conceptos de salida. Si bien se supone que el análisis resultante describe el problema en sí mismo, los conceptos deben definir las funciones y las características que el software debe proporcionar para cumplir con los requisitos relevantes. El resultado de definir los requisitos es una especificación, una descripción detallada de cómo se cumplirán los requisitos de diseño y un plan de prueba. Finalmente, el primer paso del modelo en cascada implica analizar la definición de requisitos donde los problemas complejos se dividen en sub-tareas y desarrollar soluciones en consecuencia.
Diseño	Se utiliza para desarrollar soluciones específicas basadas en los requisitos, tareas y estrategias identificadas en la fase anterior. En esta fase, los desarrolladores son responsables de diseñar la arquitectura del software y desarrollar un modelo, centrándose en componentes específicos como interfaces, bancos de trabajo o bibliotecas. Durante la fase de diseño, se crea un borrador preliminar del plan de diseño del software, así como planes de prueba para los diversos componentes.
Implementación	La arquitectura de software se desarrolla durante la fase de diseño realizada durante la fase de implementación, que incluye desarrollo de software, depuración y pruebas unitarias. Durante la fase de implementación, el proyecto de software se traduce al lenguaje de programación apropiado. Los diversos componentes se desarrollan por separado, se comprueban a través de las pruebas unitarias y se integran poco a poco en el producto final. El software creado en la fase de implementación se prueba primero como producto final en la siguiente fase (prueba alfa).
Prueba	Incluye la integración del software en el entorno seleccionado. Por regla general, el software se distribuye primero a usuarios finales seleccionados en versión beta (prueba beta). Las pruebas de aceptación desarrolladas durante la fase de análisis pueden determinar si el software cumple con los requisitos predefinidos. Los productos de software de prueba beta exitosos están listos para su lanzamiento.
Mantenimiento	Ésta es la fase más larga del ciclo de vida instala. El sistema se instala y se pone en funcionamiento práctico. El mantenimiento implica corregir errores no descubiertos en las etapas anteriores del ciclo de vida, mejorar la implementación de las unidades del sistema y resaltar los servicios del sistema una vez que se descubren nuevos requerimientos.
Servicio	Una vez completada con éxito la fase de prueba, se obtiene la licencia de la aplicación de producción de software. Las etapas finales del modelo en cascada incluyen la distribución, el mantenimiento y la mejora del software. El modelo en cascada tiene la ventaja de que se genera documentación en cada etapa y es consistente con otros modelos de procesos de ingeniería. Su principal problema es la falta de flexibilidad a la hora de dividir el proyecto en distintas fases. Las compensaciones deben realizarse desde el principio, lo que dificulta satisfacer las necesidades cambiantes de los clientes. Por lo tanto, el modelo en capas debe usarse solo cuando los requisitos se comprenden bien y es poco probable que se produzcan cambios fundamentales durante el desarrollo del sistema.

2.2 MARCO CONCEPTUAL

2.2.1 Cibernética

El concepto de cibernética ha sido utilizado en diversas disciplinas que parten desde un estudio de carácter propiamente derivado de la ciencia política, hasta estudios con enfoques matemáticos.

"Fue utilizado por primera vez en 1848 por el francés André Marie Ampere en una clasificación de las ciencias políticas, ya que él había creado un sistema para coordinar todo el conocimiento humano y había introducido el término cibernética para indicar el arte del gobierno entendido en sentido político. Cibernética es el vocablo griego que indica el arte del gobierno, arte de guía" (Livas, 1988).

"De hecho la cibernética se desarrolló como ciencia profundamente "transdisciplinar" que estudia el control y el autocontrol de Wiener o la ciencia de la eficacia de la acción" (Wiener, 1948).

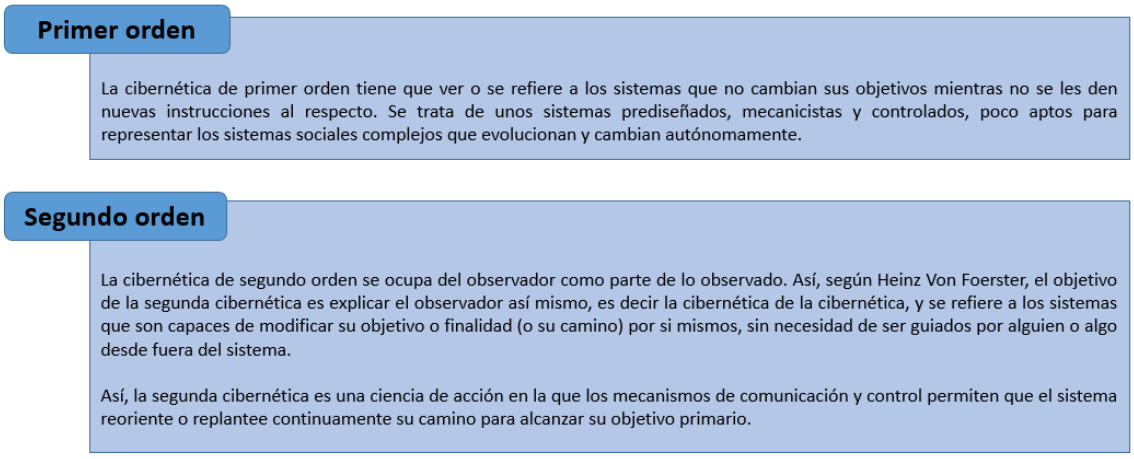


Figura 9. *Cibernética*
Fuente: *Elaboración propia*

Tal y como se concibe, del estudio de la cibernética parte un estudio análogo del sistema, o lo que en la actualidad se conoce como teoría general del sistema.

“La idea del sistema implica el hecho de ordenación y estructuración. Aunque algunos autores conciben la estructura como la anteposición del propio sistema, al respecto se ha determinado que una estructura es un conjunto de elementos entre los cuales existen relaciones tales que todo cambio de un elemento o de una relación entra a una modificación de los otros elementos o relaciones” (Wiener, Cybernetics, or Control and Communication in the Animal and the Machine, 1948).

“Puede decirse también que toda estructura supone determinadas relaciones entre los elementos, al mismo tiempo que una ordenación relativamente estable de las partes de un todo. Esto es lo que el propio Wiener estableció como isomorfismo, en el cual las partes de un sistema tienen relación entre ellas mismas sin alterar el todo” (Wiener, The Human Use of Human Beings en Cybernetics and Society, 1988).

“Por tal, podemos entender como sistema el complejo formado por diversos elementos que mantienen entre ellos relaciones de diversas índoles en aras a la conservación del todo sistemática. Se da, entonces, una aglutinación de diferenciaciones cuya misión es ir evolucionando hasta el logro de las organizaciones sistemáticas más perfectas, lo que quiere decir que todo sistema, por ser evolución organizada, posee una orientación teleológica (unos objetivos que cumplimentar) así como una conducta regularizada para tal fin; en esencia, es una unidad dinámica de acción” (Wiener, Cybernetics, or Control and Communication in the Animal and the Machine, 1948).

Consideramos un sistema como un conjunto organizado y estructurado de elementos, que tienen características similares, tienen una o más relaciones e interrelaciones entre sí, directa o indirectamente, con el fin de lograr una meta o metas específicas.

2.2.2 Conceptualización General de la Red de Datos

El término general red se refiere a un grupo de entidades interconectadas (objetos, personas, etc.). La red permite que elementos físicos o inmateriales fluyan entre entidades, según reglas definidas.

"Una red es un grupo de dispositivos comerciales interconectados, con el fin de compartir recursos como información, software o acceso a otros sistemas informáticos o bases de datos dentro de una organización, pero ubicados en un punto de conexión diferente. Y las Redes es la implementación de herramientas y tareas que conectan computadoras para que puedan compartir recursos a través de una red. Por lo tanto una red de comunicaciones es el conjunto de dispositivos físicos y lógicos (protocolos e interfaces), que nos permiten compartir recursos entre diferentes servidores; el host es cualquier dispositivo capaz de enviar y/o recibir información" (Stallings, Comunicaciones y Redes Computacionles, 2006).

2.2.2.1 Tipos de Redes

Las redes se pueden clasificar dependiendo de la cobertura del territorio.

Tabla 6. *Tipos de Redes*
Fuente: *(Wetherall, 2012)*

TIPO DE REDES	
Red de Área Local Local Área Network (LAN)	Esta red se refiere a la interconexión de muchos dispositivos o servidores, en un área pequeña, como una empresa, edificio, campus, etc., que generalmente se utilizan para compartir recursos e intercambiar datos y aplicaciones.
Red de Área Metropolitana Metropolitan Área Network (MAN)	Este tipo de red tiene mayor cobertura que LAN, se utiliza para conectar ciudades enteras o partes de ellas, suele ser utilizada por bancos, unidades de servicio público, proveedores de servicios de Internet, etc.
Red de Área Extensa Wide Área Network (WAN)	Esta red cubre un área más grande que las dos anteriores y puede cubrir áreas comerciales dentro de un país, varios países o incluso continentes. Por lo tanto, se necesitan tipos de vehículos menos comunes y utilizados por las organizaciones públicas, pero se necesita un mayor porcentaje de vehículos privados.

2.2.2.2 Modelo de Información OSI

"Modelo Open System Interconnection (OSI) es un modelo conceptual, creado por la Organización Internacional de Normalización (ISO) en 1984, que permite que diferentes sistemas de comunicación se comuniquen utilizando protocolos estándar" (Wetteroth, OSI Reference Model for Telecomunications, 2002).

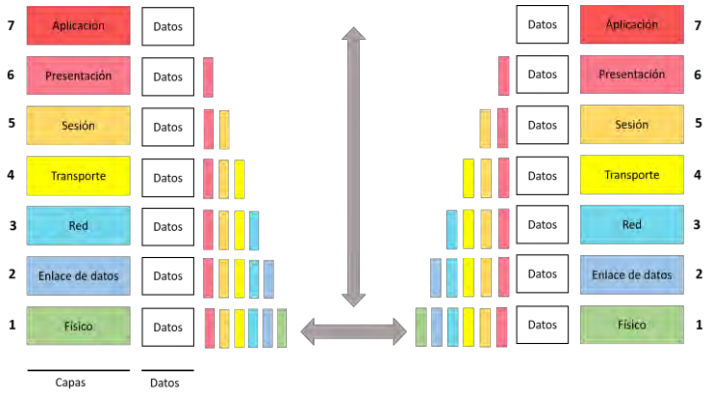


Figura 10. *Modelo OSI*
Fuente: *(Wetteroth, "OSI Reference Model for Telecomunications"., 2002)*

Tabla 7: *Capas del modelo OSI*

CAPA	FUNCION	PROTOCOLOS
Capa de aplicación	La definición de este nivel es ambigua debido a que varía. La clave es que no define una interfaz de usuario, en su lugar es una clase de caja de herramientas usadas por los desarrolladores de aplicaciones. Por ejemplo un navegador de web es una aplicación que usa HTTP, el cual se define como un protocolo de la capa de aplicación de TCP/IP para la transferencia de los contenidos de las páginas web entre el servidor y el cliente	HTTP, DNS, TFTP, TELNET, FTP, SMTP, NFS, SNMP, DHCP, etc.
Capa de presentación	Se encarga del formateo y cifrado de los datos, es decir, define el formato de los datos, la compresión y posiblemente el cifrado ("encriptación")	HTTP, DNS, TFTP, TELNET, FTP, SMTP, NFS, SNMP, DHCP, etc.
Capa de sesión	Tiene la función de establecer, administrar y finalizar las sesiones de comunicación entre hosts, además administra el intercambio de datos, sincronizando las capas de presentación de los host. Se asegura de que no sólo una comunicación se dé entre dos puntos finales, sino que sean varias.	HTTP, DNS, TFTP, TELNET, FTP, SMTP, NFS, SNMP, DHCP, etc.
Capa de transporte	Esta controla el flujo de datos entre los host que establecen comunicación, garantizando que los mensajes de entregan sin errores, provee recuperación ante errores de fin a fin si requiere, establece las conexiones de fin a fin, permite especificar que aplicaciones utilizan dichas conexiones	TCP, UDP
Capa de red	Es la que determina el direccionamiento lógico y global de cada red y host de manera inequívoca y única, establece el transporte universal (protocolos ruteados, IP, IPX). Por lo que determina las mejores rutas.	IPX, IP, RIP, RIPv2, EIGRP, OSPF, IS-IS, BGP4.
Capa de enlace de datos	Define el direccionamiento específico a un medio particular, dicho de otra forma establece el direccionamiento único y local para cada dispositivo. También establece el protocolo para determinar que dispositivo o dispositivos acceden al medio para transmitir.	CSMA/CD, CSMA/CA, TOKEN PASSING, etc.
Capa física	Es responsable de señalizar la energía codificada al medio e interpretar la energía de las señales recibidas, define los conectores y tipos de cableados.	

2.2.2.3 Modelo TCP/IP

"El acrónimo TCP/IP hace referencia al conjunto de protocolos utilizados para la transmisión de datos. Este conjunto toma su nombre de dos de sus protocolos más importantes, el Protocolo de Control de Transmisión (TCP) y el Protocolo de Internet (IP).El desarrollo del protocolo TCP/IP siempre ha estado estrechamente relacionado con el desarrollo de Internet. En 1969, la Agencia de Proyectos de Investigación Avanzada (ARPA) desarrolló un proyecto de red experimental de conmutación de paquetes al que llamaron ARPAnet" (Forouzan, 2013).

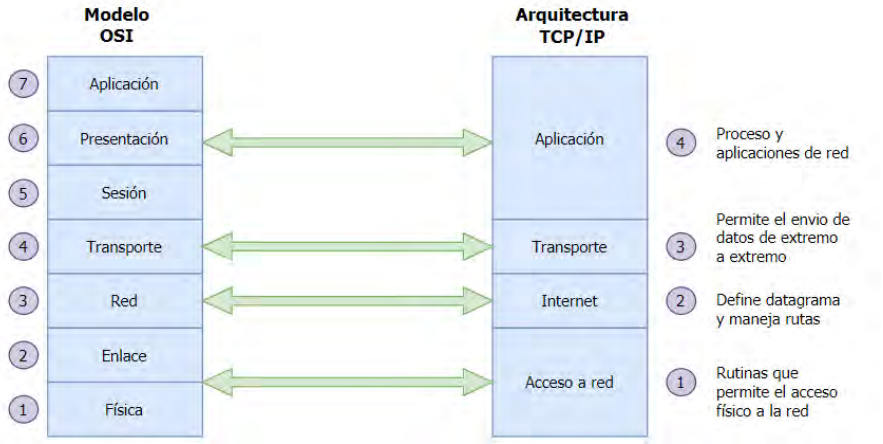


Figura 11. *Correspondencia del Modelo OSI vs TCP/IP*
Fuente: *(Wetteroth, "OSI Reference Model for Telecomunications"., 2002)*

El crecimiento que logrado el protocolo TCP/IP para ser el estándar en todo tipo de aplicaciones incluida en las redes corporativas y locales, y es precisamente en este ámbito, conocido como Intranet, donde TCP/IP adquiere cada día un mayor prestigio. TCP/IP se creó antes que el modelo de capas OSI, por lo que el nivel de TCP/IP no coincide exactamente con las siete capas establecidas por OSI. La descripción del protocolo TCP/IP define de tres a cinco niveles. La Figura muestra el modelo TCP/IP de cuatro niveles y su conformidad con el modelo de referencia OSI. Los datos enviados a la red pasan por la pila TCP/IP desde las capas superiores de la aplicación hasta las capas inferiores de acceso a la red. Una vez recibidos, se mueven a través de la pila de protocolos en direcciones opuestas.

Tabla 8. *Modelo TCP/IP*
Fuente: *(Wetteroth, "OSI Reference Model for Telecomunications"., 2002)*

CAPA	FUNCION	PROTOCOLOS
Acceso a red	Especifica la información de la red, incluida la forma en que un dispositivo de hardware conectado directamente a un medio de red (como un cable coaxial, de fibra óptica o de cobre de par trenzado) utiliza señales eléctricas para enviar bits.	Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS.
Internet	Encapsula datos en gráficos de IP que contengan información de direcciones de origen y destino con el fin de transferir gráficos de datos entre hosts y redes y poder implementar enrutamiento de datagramas IP.	IP, ICMP, ARP, RARP.
Transporte	Le permite administrar sesiones de comunicación entre servidores. Define el servicio y el estado de conexión que se utilizará al transferir datos.	TCP, UDP
Aplicación	Define el protocolo de aplicación TCP/IP y cómo los programas host se conectan a los servicios de la capa de transporte para usar la red.	HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP, X Windows y otros protocolos de aplicación.

2.2.2.4 Protocolos de transporte en TCP/IP

"El protocolo de transporte de la arquitectura TCP/IP son (Protocolo de Control de transmisión (TCP) y Protocolo de Datagramas de Usuario (UDP). Esto significa que TCP/IP proporciona dos versiones del protocolo de envío en el nivel y la aplicación. Ambos protocolos funcionan de manera muy diferente y se están enfocando en diferentes aplicaciones" (Forouzan, 2013).

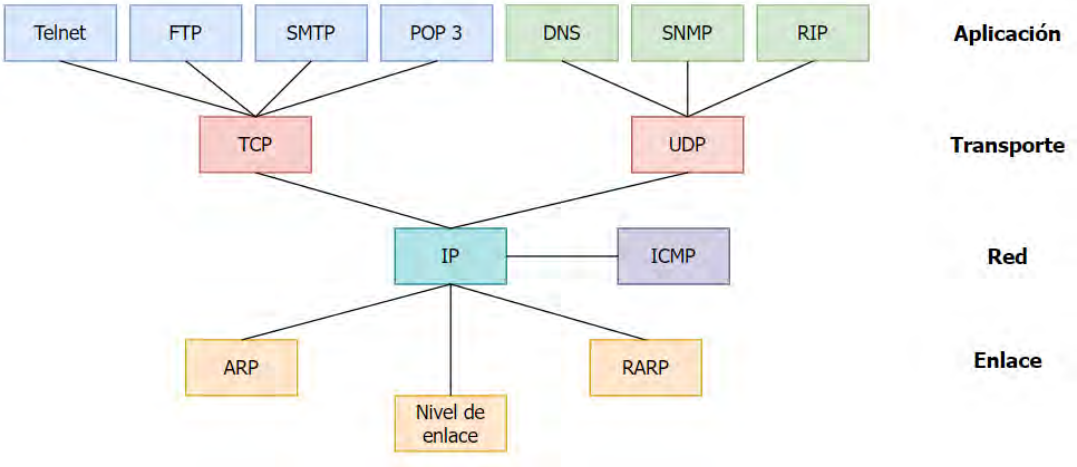


Figura 12. *Arquitectura de red TCP/IP*
Fuente: *(Forouzan, 2013)*

Como característica principal, TCP es un protocolo orientado a la conexión que brinda un servicio muy confiable, aunque implica mucho tráfico de red adicional. Por otro lado, UDP no tiene conexión y brinda un servicio poco confiable a pesar de su alta velocidad y facilidad de uso de la red.

Tabla 9. *Función y características de TCP y UDP*
Fuente: (Wetherall, 2012)

	FUNCIÓN	CARACTERISTICAS
TCP	Se establece una conexión TCP con la ayuda de un handshake de tres vías. Es un proceso de inicio y reconocimiento de una conexión. Una vez que se establece la conexión, comienza la transferencia de datos, y cuando el proceso de transmisión termina, la conexión se termina por el cierre de un	Acuse de recibo de la entrega. Retransmisión. Retrasa la transmisión cuando la red está congestionada. Fácil detección de errores.
UDP	UDP utiliza un método de transmisión simple sin diálogos implícitos de handshake para el orden, la fiabilidad o la integridad de los datos. UDP también asume que la comprobación y corrección de errores no es importante ni se realiza en la aplicación, para evitar la sobrecarga de dicho procesamiento a nivel de la interfaz de la red. También es compatible con las emisiones por paquetes y la multidifusión.	Soporta aplicaciones intensivas en ancho de banda que toleran la pérdida de paquetes. Menos retraso. Envía la cantidad de paquetes a granel. Posibilidad de pérdida de datos. Permite pequeñas transacciones (búsqueda DNS)

A continuación se muestra la tabla las diferencias entre el TCP y UDP:

Tabla 10. *Diferencia entre TCP y UDP*
Fuente: *(Wetherall, 2012)*

TCP	UDP
Es un protocolo orientado a conexión.	Es un protocolo sin previa conexión.
El TCP lee los datos como flujos de bytes, y el mensaje se transmite a los límites de los segmentos.	Los mensajes UDP contienen paquetes que son enviados uno por uno. También comprueba la integridad en el momento de la llegada.
Los mensajes TCP se abren camino a través de Internet de un computador a otro.	No está basado en la conexión, así que un programa puede enviar muchos paquetes a otro.
El TCP reorganiza los paquetes de datos en el orden específico.	El protocolo UDP no tiene un orden fijo porque todos los paquetes son independientes entre sí.
La velocidad para el TCP es más lenta.	UDP es más rápido ya que no se intenta la recuperación de errores.
El tamaño de la cabecera es de 20 bytes.	El tamaño de la cabecera es de 8 bytes.
El TCP es pesado. TCP necesita tres paquetes para establecer una conexión antes de que se pueda enviar cualquier dato de usuario.	UDP es ligero. No hay conexiones de control, ordenamiento de mensajes, etc.
TCP hace la comprobación de errores y también hace la recuperación de errores.	UDP realiza la comprobación de errores, pero descarta los paquetes defectuosos.
Segmentos de confirmación.	No hay segmentos de confirmación.
Usa el protocolo de handshake como SYN, SYN-ACK, ACK	No hay handshake
El TCP es fiable, ya que garantiza la entrega de datos al router de destino.	La entrega de datos al destino no puede ser garantizada en UDP.
El TCP ofrece amplios mecanismos de comprobación de errores porque proporciona control de flujo y reconocimiento de datos.	El UDP tiene un único mecanismo de comprobación de errores el cual es la suma de comprobación o checksum.

2.2.2.5 Puertos

Son canales utilizados por el subsistema de la red para redirigir información al programa apropiado, estos son los números lógicos asignados a las conexiones de origen y destino. No tiene significado físico. Están representados por un número de 16 bits que identifica el punto final de la conexión en el encabezado TCP o UDP. Los números de puerto oscilan entre 0 y 65,535. Se tienen tres categorías para su clasificación: Puertos bien conocidos, Puertos registrados y Puertos dinámicos o privados.

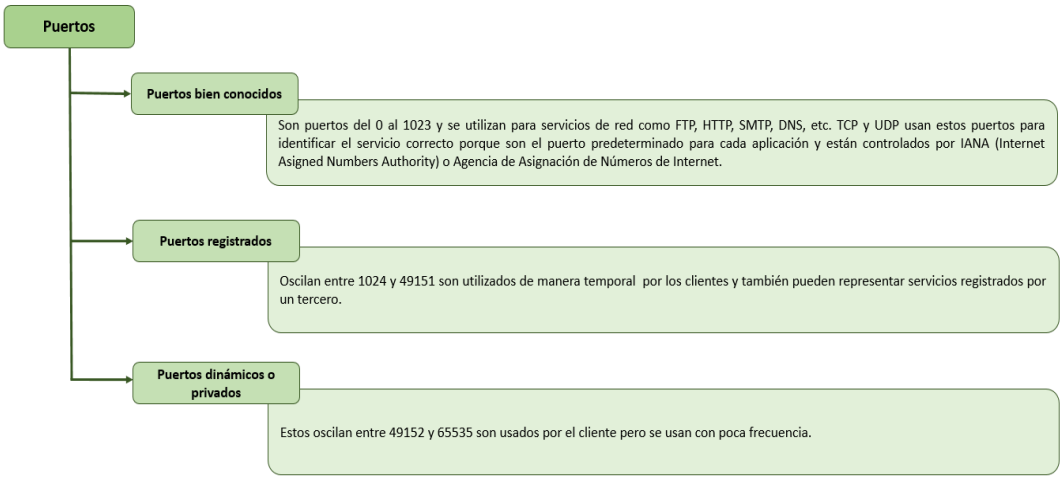


Figura 13. *Puertos*
Fuente: *Elaboración propia*

En la siguiente tabla se muestran los puertos más utilizados.

Tabla 11. *Puertos*
Fuente: (Forouzan, 2013)

PUERTO	APLICACIÓN
21	FTP (File Transfer Protocol)
22	SSH (Secure Shell)
23	Telnet
25	SMTP (Simple Mail Transfer Protocol)
53	DNS (Domain Name System)
80	HTTP (Hypertext Transfer Protocol)
110	POP3 (Post Office Protocol)
161	SNMP (Simple Network Management Protocol)
443	HTTPS (Hypertext Transfer Protocol Secure)

2.2.3 Conceptualización General del Monitoreo de la Red de Datos

"Ahora que la red es una parte esencial del éxito comercial, en el momento en que la red presenta una falla, los usuarios y empleados quedan incomunicados debido a que no se puede acceder a información corporativa crítica, sin acceso a Internet, aplicaciones de pago, servicios de correo, servidores con los bancos, acceso biométrico, lo que genera pérdidas de producción y dinero para las empresas" (Manageengine, 2020).

Dicho esto, las empresas están interesadas en lograr una infraestructura de red segura, con una excelente rapidez, fiabilidad y disponibilidad. Para lograr el objetivo, es necesario tener cuidado que el servicio de red dependa no solo de una buena infraestructura, sino también del diseño adecuado de la red y el monitoreo de la red en tiempo real.

2.2.3.1 Monitoreo de la Red

El monitoreo es de gran importancia en la prevención, seguimiento y la resolución de fallas en una red empresarial, lo que permite la detección precisa de errores, la validación del estado de los equipos y la medición del rendimiento de la red. El monitoreo de la red le permite ver información sobre la conexión que existe entre su computadora y la red, ya sea local, externa o de banda ancha.

2.2.3.2 Porque es importante monitorear la red

"Como cada empresa es diferente, tendrá distintas necesidades respecto a una aplicación de monitoreo, de modo que la empresa debe analizar qué funcionalidades necesita y con qué recursos se cuenta actualmente"(Conceptos básicos de la supervisión de la red, 2020).

A continuación se describe las razones por las cuales es fundamental el monitoreo de la red de datos.

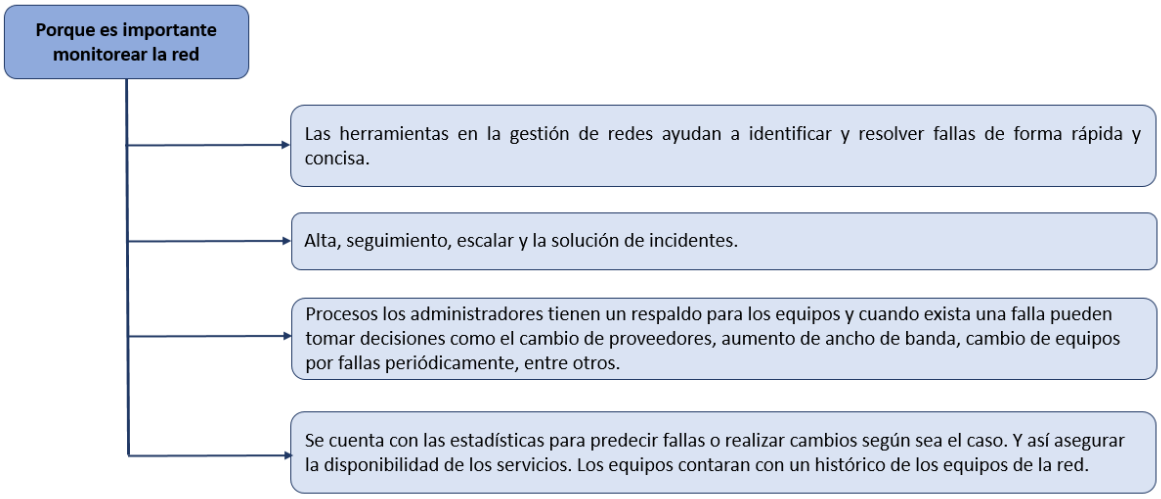


Figura 14. *Importancia del monitoreo*
Fuente: *Elaboración propia*

Las funciones de un sistema de administración y monitoreo de red incluyen descubrir o analizar lo que hay en la red. El sistema de administración de red analiza los dispositivos de red, incluidos servidores, enrutadores, conmutadores y más.

“El mapa es la capacidad de visualizar la red, sin embargo, con la escalabilidad de la red, esto limita la capacidad del administrador poder visualizar la red y retrasa la resolución de los problemas. Los mapas de red es una herramienta de retroalimentación eficaz que permite a los administradores de red visualizar incluso redes complejas. El mapa de red muestra los dispositivos y su estado más reciente” (Forouzan, 2013).

Las alertas se notifican cuando algo sale mal o está fallando. El sistema de monitoreo de red alerta al administrador cuando hay un problema con el dispositivo. Esto se puede hacer a través de notificaciones por correo electrónico, SMS, etc.

2.2.4 Protocolos Simple para la Administración del Sistema de Información de Red de Datos

"Un protocolo de red es similar a un protocolo humano, excepto en que las entidades que intercambian mensajes y llevan a cabo las acciones son los componentes hardware o software de cierto dispositivo. Cualquier actividad de Internet que implique dos o más entidades remotas que se comunican está gobernada por un protocolo. Por ejemplo, los protocolos implementados por hardware en las tarjetas de interfaz de red de dos computadoras conectadas físicamente controlan el flujo de bits a través del cable conectado entre las dos tarjetas de interfaz de red; los protocolos de control de congestión de los sistemas terminales controlan la velocidad a la que se transmiten los paquetes entre el emisor y el receptor; los protocolos de los routers determinan la ruta que seguirá un paquete desde el origen al destino" (Wetherall, 2012).

Un sistema de gestión es una unidad independiente encargada de la comunicación con los equipos de red implementados por agentes Simple Network Management Protocol (SNMP). Por lo general, esta es la computadora utilizada para ejecutar diferentes sistemas de administración de red.

SNMP se ha utilizado para la administración de redes desde 1990 y es ampliamente compatible con dispositivos de red y plataformas de monitoreo. Recopile datos de rendimiento del dispositivo mediante una herramienta de sondeo y envíelos a la plataforma de gestión. Existen tres versiones de SNMP y SNMPv3 que brindan importantes capacidades de encriptación y autenticación.

Tabla 12. *Funciones de SNMP*
Fuente: (Network Monitoring Software - ManageEngine OpManager, 2022)

COMPONENTES BASICOS	DESCRIPCION
Administrador SNMP	Es una entidad separada responsable de comunicarse con los dispositivos de red implementados por el agente SNMP. Normalmente es un equipo que se utiliza para ejecutar uno o más sistemas de administración. FUNCIONES: Agentes de consultas Obtiene respuestas de agentes Establece variables en agentes Reconoce eventos asincrónicos de agentes
Dispositivos administrados	Es una parte de la red que requiere algún tipo de monitorización y administración, por ejemplo, enrutadores, conmutadores, servidores, estaciones de trabajo, impresoras, etc.
Agente SNMP	Es un programa que está empaquetado dentro del elemento de red. La habilitación del agente le permite recopilar la base de datos de información de administración del dispositivo localmente y la pone a disposición del administrador SNMP, cuando este se la solicita. Estos agentes pueden ser estándar o específicos de un proveedor. FUNCIONES: Recopila información de administración sobre su entorno local Almacena y recupera información de gestión según se define en la MIB. Señala un evento al administrador. Actúa como proxy para algunos nodos de red administrables que no son SNMP.
Base de datos de información de administración denominada de otro modo Base de información de administración (MIB)	Cada agente SNMP mantiene una base de datos de información que describe los parámetros del dispositivo administrado. El administrador SNMP usa esta base de datos para solicitar al agente información específica y la traduce aún más la información según sea necesario para el Sistema de administración de red (NMS). Esta base de datos comúnmente compartida entre el Agente y el Administrador se denomina Base de información de administración (MIB). En resumen, los archivos MIB son el conjunto de preguntas que un administrador SNMP puede hacerle al agente. El agente recopila estos datos localmente y los almacena, según se define en la MIB. Por lo tanto, el administrador de SNMP debe conocer estas preguntas estándar y privadas para cada tipo de agente.

“La Base de información de administración (MIB) es una recopilación de información para poder administrar algún dispositivo de la red. MIB se componen de objetos administrados identificados mediante el nombre Identificador de objeto (ID de objeto u OID). Cada identificador es único e indica una característica específica del dispositivo administrado. Cuando se lo consulta, el valor de retorno de cada identificador puede ser distinto, por ejemplo, un texto, número, contador, etc.” (Network Monitoring Software - ManageEngine OpManager, 2022).

Hay dos tipos de objeto administrado: el escalar que es el nombre del proveedor del dispositivo y el resultado solo puede ser uno y el otro tipo de objeto es tabular que es el uso del CPU de un procesador cuádruple.

La simplicidad del intercambio de información ha hecho de SNMP un protocolo ampliamente aceptado. La razón principal es el breve conjunto de comandos que se enumeran a continuación:

Tabla 13. *Comandos de SNMP*
Fuente: *(Network Monitoring Software - ManageEngine OpManager, 2022)*

GET	La operación GET es una solicitud enviada por un administrador a un dispositivo que es administrado, esto para recuperar uno o más valores del dispositivo.
GET NEXT	Esta operación es similar a GET, la diferencia es que la operación GET NEXT va a recupera el valor del siguiente OID en el árbol MIB.
GET BULK	Esta operación se utiliza para poder recuperar datos de una tabla MIB grande.
SET	Esta operación es para modificar y/o asignar el valor del dispositivo administrado.
TRAPS	Es una señal al administrador SNMP por parte del agente sobre la repetición de un evento.
INFORM	Este comando es similar a TRAP iniciado por el agente, ya que incluye la confirmación del administrador SNMP al recibir el mensaje.
RESPONSE	Es el comando para transportar los valores o la señal de las acciones ejecutadas por el administrador de SNMP.

A continuación se describen las versiones SNMP

Tabla 14. *Versiones de SNMP*

VERSION	DESCRIPCION
SNMPv1	Es la primera versión del protocolo SNMP, que se define en RFC 1155 y 1157.
SNMPv2	Este es el protocolo que incluye mejoras de SNMPv1 en las áreas de tipos de paquetes de protocolo, en asignaciones de transporte y elementos de estructura MIB pero usando la estructura de administración SNMPv1 existente. Se define en RFC 1901, RFC 1905, RFC 1906, RFC 2578.
SNMPv3	Define la versión segura de SNMP, el protocolo SNMPv3 facilita la configuración remota de las entidades SNMP. Se define mediante RFC 1905, RFC 1906, RFC 3411, RFC 3412, RFC 3414, RFC 3415.

La ventaja fundamental de usar SNMP es que su diseño es simple por lo que su implementación es sencilla en redes grandes y la información de gestión que se requiere para intercambiar los recursos de la red son pocos, esto permite al usuario elegir distintas variables que se desea monitorear como el título de la variable, el tipo de datos de las variables, el valor de la variable y si la variables es solo lectura o escritura.

Tabla 15. *Ventajas y desventajas de SNMP*

VENTAJAS	DESVENTAJAS
Simplicidad	Aspectos de seguridad
Requiere menor procesamiento que el CMPI	Funcionalidad reducida
Ampliamente usado y probado	Genera mucho tráfico por la red
Está integrad en muchos productos actuales	No facilita el diseño de las MIBs

El protocolo SNMP está compuesto por dos elementos fundamentales el agente y el gestor, con una arquitectura cliente – servidor, en la que el agente desempeña el papel de servidor y el gestor de cliente.

2.2.5 Tipos de Monitoreo de la Red de Datos

Es importante para una empresa monitorear y medir continuamente la salud de esta red, independientemente de si su infraestructura es Red de área local (LAN), Red de área metropolitana (MAN) o Red de área local (WAN).

Se trata de un proceso mediante el cual un elemento generalmente centralizado que puede ser un software alojado en uno o más servidores envía mensajes a todos los demás equipos intermedios de la red para obtener suficientes datos que le ayuden a identificar su status completo. Los elementos que se pueden monitorear en una red pueden provenir de dispositivos intermedios como rutadores, conmutadores, firewalls o multiplexores, puntos finales como computadoras, servidores, telefonía celular. Por su parte, el principal componente encargado de verificar el funcionamiento de cada equipo de red, según los escenarios y métodos implementados por los administradores e ingenieros de red.

A continuación se muestran los monitoreo de forma pasiva y activa, las técnicas que presenta cada una, sus estrategias de monitoreo incluyendo las métricas y la selección de las herramientas.

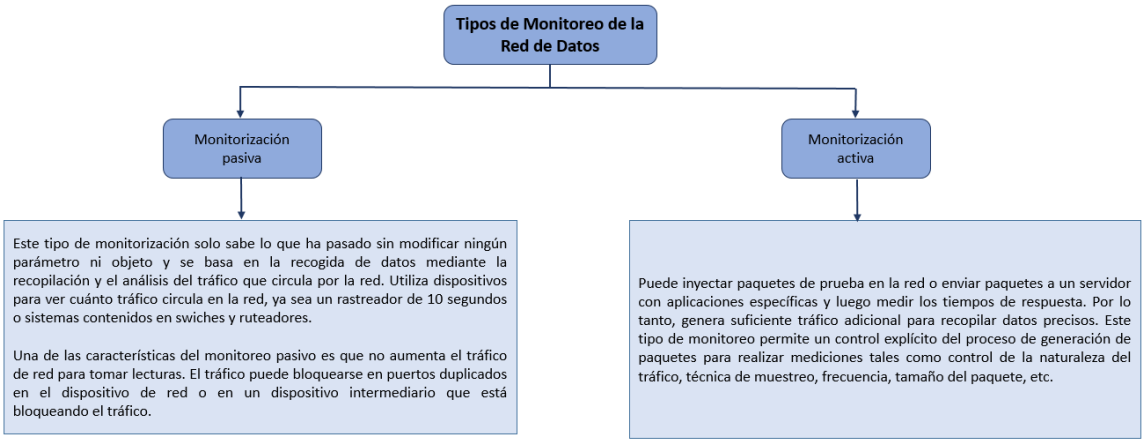


Figura 15. *Tipos de monitoreo*

Fuente: *Elaboración propia*

A continuación se muestran las técnicas de monitoreo pasivo y activo

Tabla 16. *Técnicas de monitoreo pasivo y activo*

TÉCNICAS DE MONITOREO PASIVO		
SNMP	Simple Network Management Protocol	Esta técnica se utiliza para recopilar estadísticas de uso de ancho de banda en dispositivos de red para los que se requiere acceso a dichos dispositivos. Al mismo tiempo, el protocolo genera paquetes llamados trampas que indican que ha ocurrido un evento inusual.
Otros métodos de acceso		Puede crear scripts que acceden a los dispositivos remotos para monitorear información importante.
Captura de tráfico		Se puede llevar a cabo de dos formas, una mediante la configuración de un puerto espejo en un dispositivo de red. Y mediante la instalación de un dispositivo intermedio que capture el tráfico.
Análisis del tráfico		Se utiliza para describir el tráfico de red, es decir, para identificar los tipos de aplicaciones más utilizadas. Se puede implementar con un dispositivo que envía información a través de RMON o mediante una aplicación intermedia que puede categorizar el tráfico por aplicación, direcciones IP de origen y destino, puertos de origen y destino, y más.
Flujos		Se utiliza para determinar el tipo de tráfico utilizado en la red. Un flujo es un conjunto de paquetes con La misma dirección, El mismo puerto TCP origen y destino y el mismo tipo de aplicación. Los flujos se pueden obtener de ruteadores o mediante dispositivos capaces de capturar y convertir el tráfico en flujos.

TÉCNICAS DE MONITOREO ACTIVO		
ICMP	Internet Control Message Protocol	Diagnosticar problemas en la red Detectar retardo, pérdida de paquetes RTT (Round-Trip delay Time) Disponibilidad de host y redes
TCP	Transmission Control Protocol	Tasa de transferencia. Diagnosticar problemas a nivel de aplicación.
UDP	User Datagram Protocol	Pérdida de paquetes en un sentido RTT (tracerroute)

Antes de implementar un plan de monitoreo, es importante definir la gama de dispositivos a monitorear, la cual puede ser amplia y se puede agrupar en las siguientes categorías:

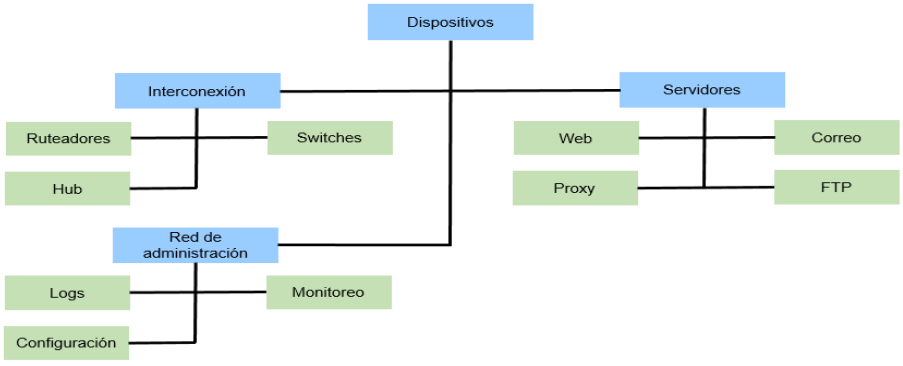


Figura 16. *Alcance de los dispositivos a monitorear*

Fuente: *Elaboración propia*

2.2.5.1 Para qué sirve el Monitoreo de Red

El análisis y monitoreo de Red lo que busca es validar en todo momento el estado de todos y cada uno de los elementos de la red para tomar acciones oportunas. Algunas de estas acciones podrían ser:

Tabla 17. *Acciones de monitoreo de la red de datos*

Preventivas	Consiste en tomar acciones concretas para evitar el impacto negativo de una posible falla que tiene cierta probabilidad de ocurrir producto de una cantidad de condiciones previamente observadas.
Correctivas	Consiste en aplicar troubleshooting o acciones que ayuden a resolver una incidencia que acaba de ocurrir y que necesita ser resuelta para no afectar el buen funcionamiento de la red y los servicios que transitan a través de ella.
Optimización	Se basa en utilizar técnicas especiales para maximizar el rendimiento de la red con los recursos existentes. En algunos casos una optimización también puede implicar la agregación o expansión de ancho de banda, memoria, capacidad de procesamiento o agregación de elementos redundantes.
Mitigación	En ocasiones las fallas son de gran impacto y no pueden resolverse en el momento, sin embargo, no podemos dejar la red afectada ya que hay usuarios y clientes cuya experiencia de navegación también se puede afectar. En estos casos se suelen usar técnicas de mitigación que lo que hacen es crear elementos alternos para que los servicios vuelvan a funcionar por otras vías, aunque la falla original todavía esté en curso y en proceso de solución.

Como sabes el monitorear la red es un proceso fundamental y desde el punto de vista de una empresa puede generar muchos beneficios. Entre las características que definen a este proceso encontramos las siguientes:

Tabla 18. *Características del Monitoreo de Red*

• Debe ser periódico y continuo en el tiempo. • Se utiliza uno o más protocolos para la comunicación e intercambio de datos entre el elemento central y los elementos de red a ser monitoreados. • Se realiza una verificación constante y en tiempo real de la salud de los equipos. • Se requiere de personal altamente calificado y entrenado para tomar acciones oportunas dependiendo de las detecciones encontradas en la fase de monitoreo. • El monitoreo se apoya posteriormente en una fase de análisis que permite identificar puntos clave en la red para determinar acciones preventivas, procesos de ampliación, optimización y mejoramiento continuo. • Ayuda a las empresas a saber qué está sucediendo en tiempo real y cómo se está comportando la red.

Existen otros tipos de alertas basadas en patrones predefinidos en nuestro indicador ya que el valor máximo se denomina umbral. Cuando se superan estos patrones, se genera una alerta porque no sigue el patrón (Stallings, 2006).

Algunos tipos de alarmas son:

Tabla 19. *Alarmas del Monitoreo de Red*

• Alarmas de procesamiento. • Alarmas de conectividad. • Alarmas ambientales. • Alarmas de utilización. • Alarmas de disponibilidad.

Para implementar un proceso de Monitoreo de Red, existen metodologías que pueden ayudarte. Todo debe comenzar con una fase de planificación en el cual debes identificar los aspectos clave en tu proceso de monitoreo. Algunos de estos pueden ser:

Figura 17. *Claves para el Monitoreo de Red*
Fuente: *Elaboración propia*

2.2.6 Sistema de Control y Administración

Los sistemas de gestión y control ayudan a optimizar al máximo los procesos logísticos. Este es un factor muy importante en la racionalización de los procesos. Tener un sistema digitalizado de control de inventario reduce el margen de error, centraliza la información y, en general, ayuda a garantizar que todo el proceso logístico se ejecute de la manera más eficiente posible.

El sistema de administración y control mejora la administración de entradas y salidas de mercancías, preparación de pedidos, gestión de pedidos, así como todas las tareas relacionadas para el control de inventarios.

Esto conduce a procesos más ágiles y con margen de error reducido. Es decir, son Sistemas de Información Logística que permiten una gestión mucho más eficiente de los flujos de información necesarios para el buen funcionamiento de los procesos logísticos.

Las características de los sistemas de administración y control pueden variar de un sistema a otro, las más comunes son:

Tabla 20. *Características de los sistemas de administración y control*

Establecen normas y protocolos concretos aplicables a la gestión de inventario.
Permiten controlar la trazabilidad de los productos.
Permiten disponer de la información histórica centralizada.
Dicha información se muestra de forma optimizada y fácil de comparar (sobre todo mediante el uso de gráficas y métricas).
Permiten conocer en tiempo real la entrada y salida de mercancías que tiene lugar en los centros logísticos.
Una de las características de los sistemas de administración y control que debería ser común a todos los sistemas es la tendencia a la automatización, lo que permite reducir los problemas derivados por el error humano.

Los tipos de sistemas de gestión y control que se pueden encontrar son muy diversos. Dependiendo de las características y necesidades específicas de cada centro logístico o almacén, se pueden encontrar diferentes tipos.

Para obtener los mejores resultados, los tipos de sistemas de administración y control deben adaptarse a las necesidades y características de cada centro logístico concreto.

Tabla 21. *Tipos de sistemas de administración y control*

Sistemas de administración y control de inventarios temporales o permanentes	Sistemas de administración y control de inventarios automáticos o manuales
Según las necesidades, estos sistemas pueden funcionar de forma continuada o solo temporal. Es decir, con protocolos aplicables siempre o protocolos que solo se aplican en situaciones o mercancías determinadas.	Dependiendo de las características de las mercancías y de los recursos disponibles, se pueden encontrar sistemas de administración y control de inventario que son ejecutados por máquinas de manera automática o que son ejecutados por trabajadores humanos. Además, también se pueden encontrar sistemas mixtos. Es decir, que combinan ambas tipologías.

La automatización y digitalización del sistema de control y gestión de inventarios es fundamental para optimizar al máximo todos los procesos logísticos del almacén. Sin embargo, esta digitalización no debe limitarse solo a los procesos internos del almacén, sino también a los procesos externos relacionados con la distribución de mercancías y la logística de última milla.

CAPÍTULO 3. DESARROLLO DEL SISTEMA DE INFORMACION POR ETAPAS

Diagnóstico general

El mecanismo de recolección de información sobre el estado actual de la empresa distribución fue creado luego de una revisión directa de la red de datos y discusiones con los encargados de los almacenes y técnicos, quienes señalaron las siguientes observaciones:

- Ninguna herramienta o aplicación de monitoreo puede garantizar el estado de la red de datos.
- Falta de información para analizar el desempeño de los equipos incluidos en la red de datos de la empresa de distribución tanto en la sede principal como en cada almacén.
- Cuando ocurre un error, no se registra ninguna advertencia ni error.

En el presente trabajo de investigación y desarrollo como se mencionó se aplicara el modelo de cascada, se tienen las principales actividades:

Recordando las etapas del modelo de cascada son:

Tabla 22. *Etapas*

Etapa de análisis y requerimientos
Etapa de diseño
Etapa de desarrollo
Etapa de pruebas
Etapa de implementación

3.1 Etapa 1. Análisis y requerimientos

En la sede principal y en los almacenes se tiene dispositivos de red de diversos proveedores y de la empresa de distribución como son: ruteadores, switches, firewall, entre otros.

La estructura de red de la sede principal es la red troncal y la red de distribución, como se muestra la figura 18.

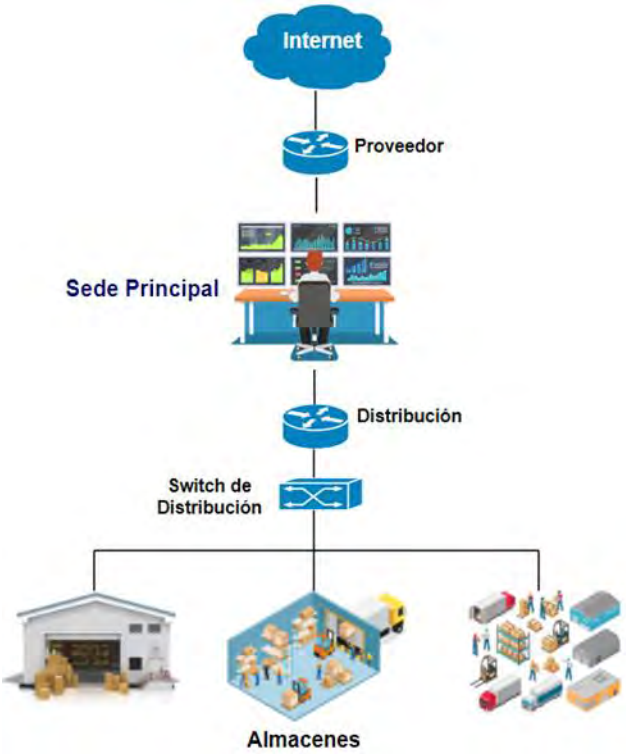


Figura 18. *Estructura de Red*
Fuente: *Elaboración propia*

El objetivo principal de la empresa de distribución de insumos es la venta, almacenamiento y distribución de productos por toda la República Mexicana por lo que en la sede principal deben tener conocimiento de cuánto producto se cuenta en cada almacén, así como las entradas y salidas de dichos productos por lo que es necesario y de suma importancia una comunicación entre la sede principal y almacenes.

Para poder acceder a los equipos a esos puntos remotos en los almacenes desde la sede principal se realiza configuración en los equipos de red como ruteo estático, dinámico o por enlaces privados como se muestra en la figura 19.

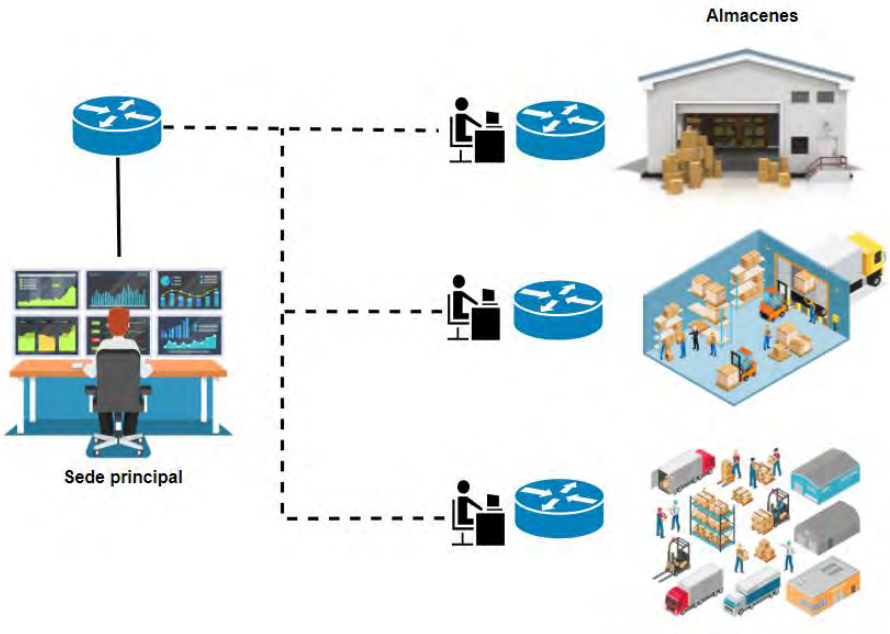


Figura 19. Configuración de la Red
Fuente: *Elaboración propia*

En los almacenes se tienen módems Wireless estos se deben conectar con los dispositivos a un switch para poder distribuir a sus terminales, celulares, computadoras, impresoras, entre, como se muestra en la figura 20.

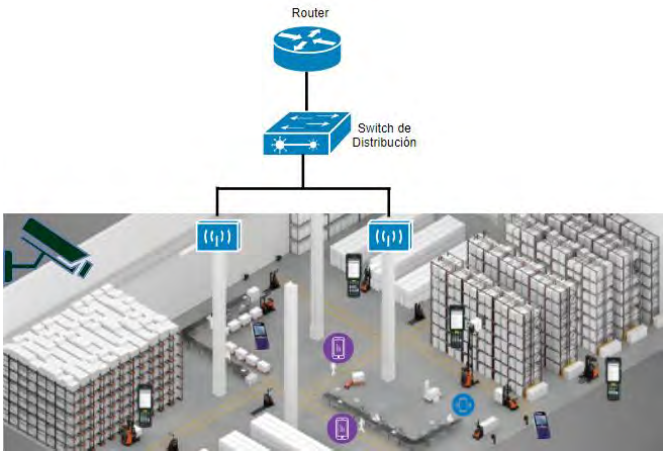


Figura 20. *Configuración de la Red en el almacén*
Fuente: *Elaboración propia*

Como se mencionó anteriormente en los almacenes se tiene un equipo donde se registran las entradas y las salidas de los productos, esta información se carga en una base de datos la cual se tiene que tener acceso desde la sede principal.

Figura 21.*Registro de productos*
Fuente: *Elaboración propia*

La empresa de distribución para tener comunicación y acceso de sus equipos de red de los almacenes en la sede principal, tiene que disponer un rendimiento alto y efectivo desde el nodo principal y el recorrido de acceso a la red. Por lo cual se debe monitorear y llevar un análisis de las fallas para poder tener un excelente servicio una red estable. En la empresa de distribución al iniciar el análisis del estado de la red de datos se encontró con diferentes marcas en los equipos de red como (cisco, meraki, entre otros).

Además, el departamento de Sistemas no cuenta con un diseño de un sistema de información para la concentración y el monitoreo de equipos de red de datos para ayudar a los ingenieros a comprender el estado, el rendimiento o la disponibilidad de los dispositivos en la red. En el departamento de Sistemas los ingenieros identifican las pruebas de falla cuando el encargado de cada área o almacén se comunican para indicarles que no tiene acceso a los equipos que presentan falla con la red, acceso a correo, impresoras, biométricos, terminales, entre otros. Y no se cuenta un ticket o una bitácora de la falla presentada.

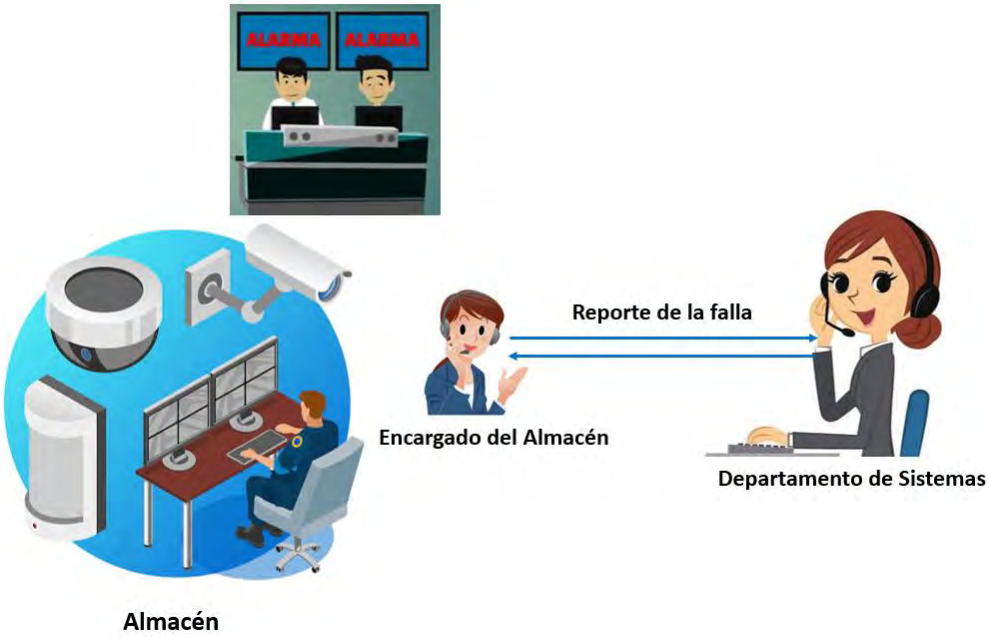
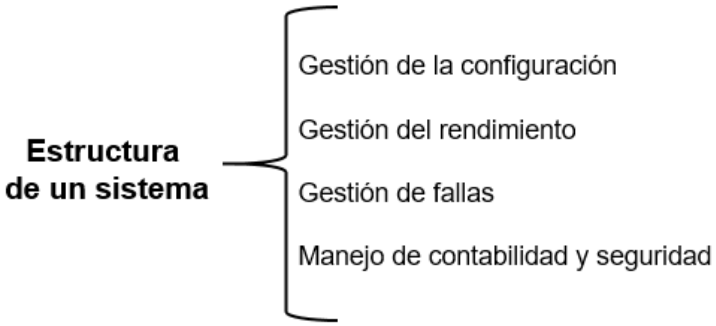


Figura 22. *Reporte de falla*
Fuente: *Elaboración propia*

3.2 Etapa 2. Diseño del sistema de información

En esta etapa, es necesario encontrar una manera de abordar este requisito para alcanzar la solución, por lo que se utilizan modelos funcionales descritos en el capítulo anterior.

El sistema debe estructurarse de la siguiente manera:



3.2.1 Gestión de configuración

Aquí se debe ejecutar conforma a las actividades que se realizaran en el seguimiento y proceso de la configuración para la gestión de los equipos de red de datos.

3.2.1.2 Diseño de Red

(Barba Martí, Gestion de Red, 1999), “define que el objetivo es satisfacer las necesidades a corto plazo y futuras de la infraestructura de la red como se refleja en su diseño a través de la implementación completa”.

a) El proceso de diseño y planificación de la red implica una serie de tareas, algunas de las cuales incluyen:

- Configuración VPN
- Ruteo estático y dinámico
- Calidad de servicio

Algunos requisitos de cuantificación podrían ser:

- La cantidad de nodos en cada almacén
- Cantidad de equipos de capa 3 y capa 2 para cubrir la demanda de los nodos en los almacenes.

Estos tipos de requisitos cubren solo adaptaciones del diseño de la red y no requieren un rediseño completo. Por ejemplo, a medida que se implementan nuevas

tecnologías, surgen necesidades comunes, como cambiar de puertos o de protocolos de enrutamiento interno.

b) Diseñar y analizar la topología de los equipos de red de datos.
c) Identificar la configuración de los equipos de red y la infraestructura con base a los requisitos técnicos de cada almacén y por lo tanto en la topología sugerida.
d) Para redes grandes como en la sede principal, la distribución se diseña utilizando un mecanismo de enrutamiento que puede ser estático o dinámico. Y para los almacenes utilizaremos VPNs hacia la sede principal.
e) Si el diseño e instalación propuestos cumplen con los requisitos, se debe continuar con la ejecución, de lo contrario se deben repetir los pasos anteriores hasta obtener los resultados recomendados.

3.2.1.3 Selección de la infraestructura de red de datos

La elección de la infraestructura depende de los requisitos y de la topología sugerida. Si se recomienda un diseño jerárquico, se deben determinar los dispositivos apropiados para los niveles de acceso, distribución y gestión. Además, la infraestructura de la red debe cumplir con la mayoría de los requisitos. Se realizaran maquetas o pruebas en el programa GNS3 que es un laboratorio que no ayuda para verificar los requisitos antes de implementarlos en la infraestructura de red de datos.

3.2.1.4 Instalación de software y hardware

El objetivo de esta tarea es lograr una buena gestión de los recursos de hardware y software en la red.

Para la instalación de hardware existen varias tareas a considerar, ya sea ingresos o reemplazo de hardware, debemos considerar que el hardware integro como un router o switch o solo una parte de estos.

El proceso de la instalación de hardware consta de las siguientes etapas:

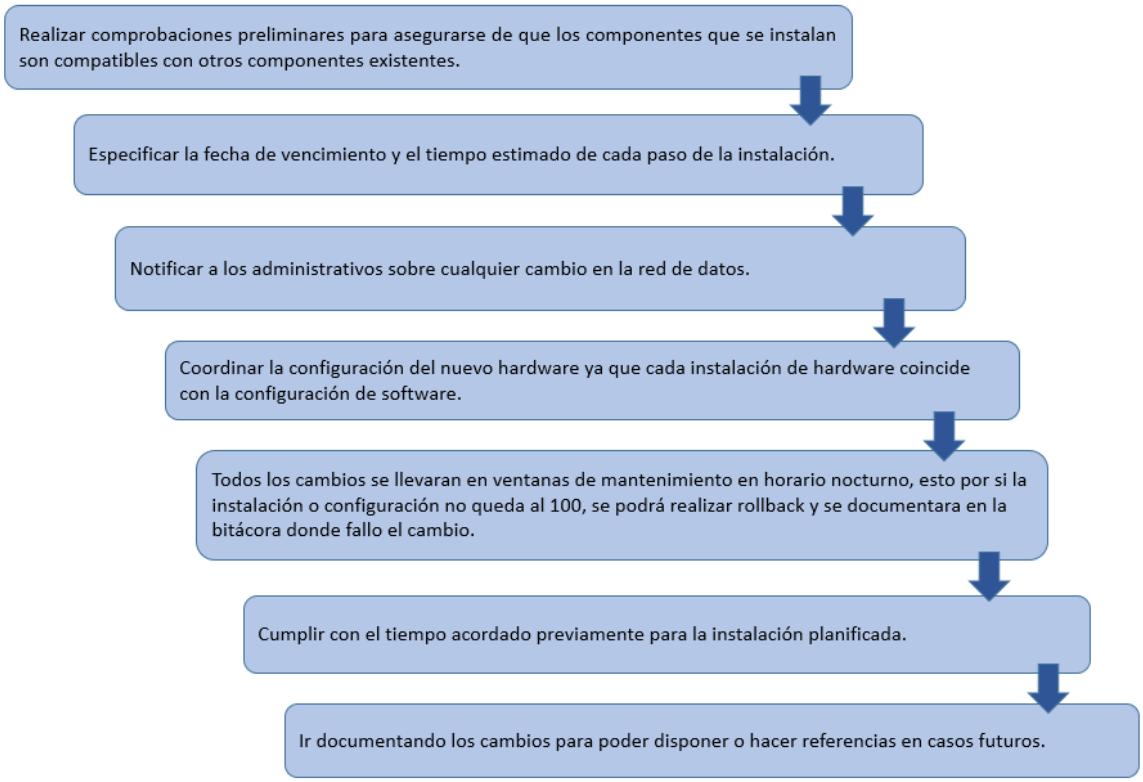


Figura 23. *Proceso de instalación de hardware*
Fuente: *Elaboración propia*

Pala la instalación del software, es un proceso el cual se deberá llevar un comportamiento responsable al momento de instalar, desinstalar y actualizar las aplicaciones, sistemas operativos o dispositivos de red. Además, un control sobre las herramientas utilizadas para obtener información específica del dispositivo de la red de datos.

Antes de iniciar la instalación, se debe tener en cuenta:

Figura 24. *Datos importantes para una instalación*
Fuente: *Elaboración propia*

3.2.1.5 Gestión de la configuración

De manera similar (Barba Martí, Gestion de Red, 1999), determinan que el objetivo principal de la gestión es recolectar y analizar el tráfico de la red para determinar cómo se comporta durante los períodos de tráfico normal o pico como

histórico o en tiempo real para poder tener ya un análisis y así poder tomar decisiones.

Para gestionar el rendimiento habrá dos fases: monitoreo y análisis

3.2.1.6 Monitoreo

El monitoreo su principal responsabilidad es observar, analizar y poder recolectar la información necesaria que corresponde al comportamiento de los equipos o de la red de datos con los siguientes aspectos:

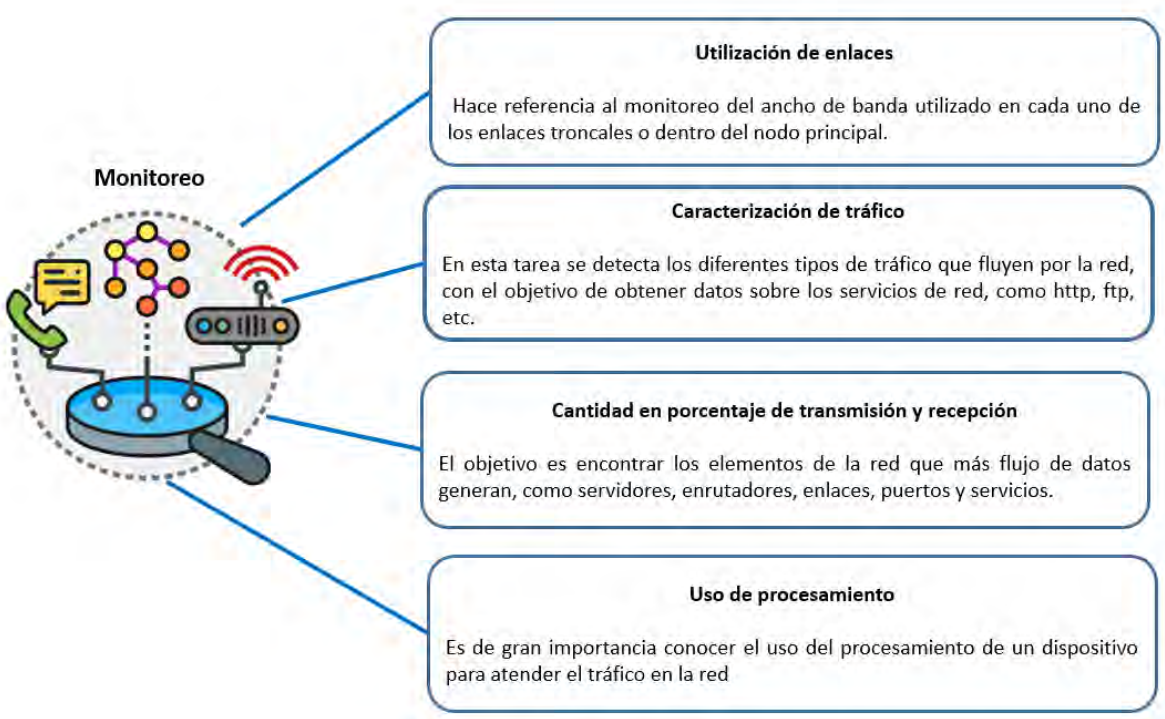


Figura 25. *Monitoreo*
Fuente: *Elaboración propia*

3.2.1.7 Análisis de información

Después de obtener la información de monitoreo, debemos saber realizar un buen análisis una buena interpretación para poder identificar como se encuentra la

red y así lograr tomar las decisiones correctas a un buen tiempo el cual ayudará a mejorar el rendimiento de la red y brindar soluciones en caso de problemas.

Las tareas para el análisis se pueden encontrar resultados relacionados con:

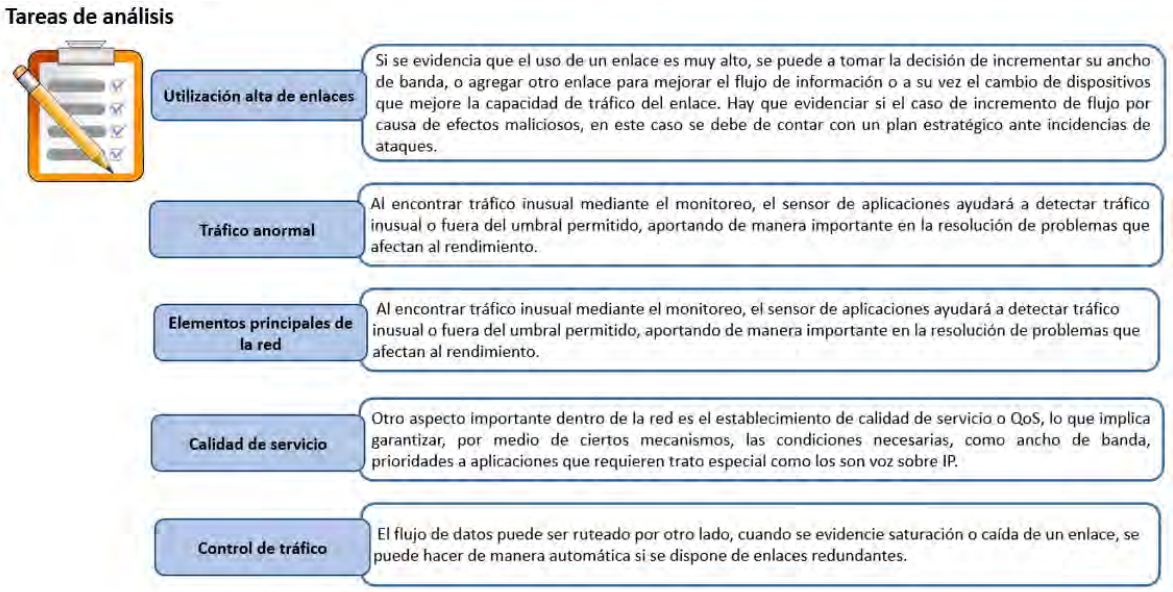


Figura 26. *Tarea de análisis*
Fuente: *Elaboración propia*

3.2.1.8 Gestión de fallas

(Barba Martí, Gestion de Red, 1999), menciona que el objetivo principal de la gestión de fallas es detectar y corregir rápidamente los eventos de la red de datos. Esto tiene que hacerse en varios pasos. Primero, los errores deben detectarse e informarse de inmediato. Después de recibir la notificación, se continúa detectando la fuente para tomar una decisión. Algunas pruebas para diagnosticar problemas relacionados con la ubicación del origen del evento. Una vez descubierto, se tomarán medidas correctivas para resolver el problema y minimizar su impacto.

El proceso consiste de varias etapas.

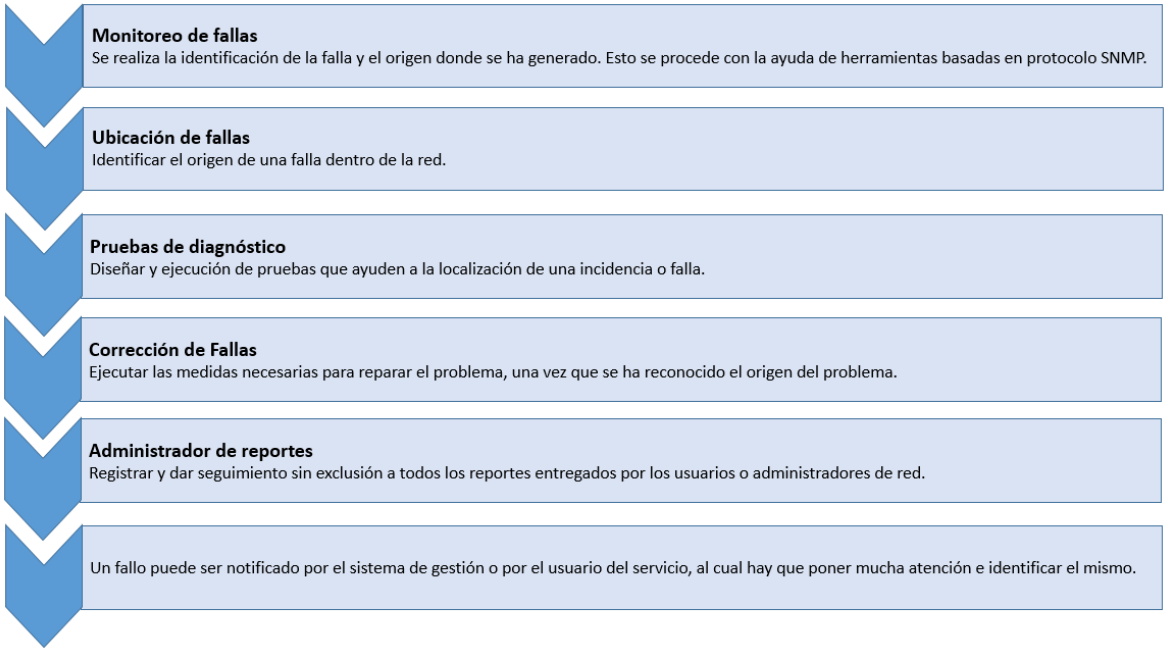


Figura 27. *Gestión de fallas*
Fuente: *Elaboración propia*

3.2.1.9 Monitoreo de alarmas

También (Barba Martí, Gestion de Red, 1999) señalan que las alertas son importantes en el monitoreo de la infraestructura en caso de presentar fallas. Por ello, se recomienda contar con un sistema de monitoreo de alarmas, es decir, una herramienta que trabaje directamente con los responsables de la gestión, de seguimiento, y que la aplicación cuente con mecanismos que permitan la notificación de problemas en la red de datos. La conclusión se basa en el uso de herramientas fundamentales en el protocolo de monitorización estándar SNMP, ya que este protocolo está incluido en la mayoría de los dispositivos de comunicación. Las alarmas deben activarse en el momento de su aparición para que el problema pueda resolverse inmediatamente, incluso antes de que el cliente se dé cuenta del problema. Debido al tipo y la gravedad de las advertencias es decir la severidad, existen al menos dos ejemplos de alarmas.

3.2.1.10 Tipo de alarmas

Como describen (Barba Martí, Gestion de Red, 1999), las alarmas son muy importantes en el entorno de gestión y este contribuyen a mejorar la calidad de la gestión de la red de datos.

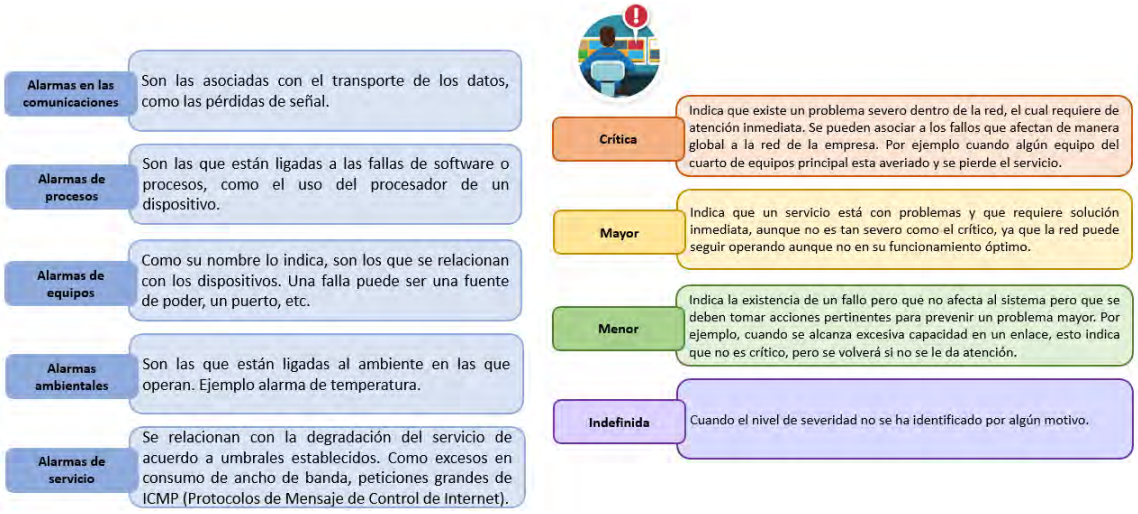


Figura 28. *Monitoreo y severidad de alarmas*
Fuente: *Elaboración propia*

3.2.1.11 Pruebas de diagnóstico

Este elemento de la gestión de errores es importante para determinar la causa dela falla. Las alarmas se deben identificar donde se encuentra el problema, y así poder realizar distintas pruebas para poder logara un diagnóstico, esto nos ayuda a identifican el origen del mismo. Una vez que se ha identificado el problema, se deben tomar medidas para resolver el problema informado.

Se deberán realizar pruebas de diagnósticos que es el proceso para identificar donde está el incidente, para llegar a este punto se pueden realizar estas pruebas como son:

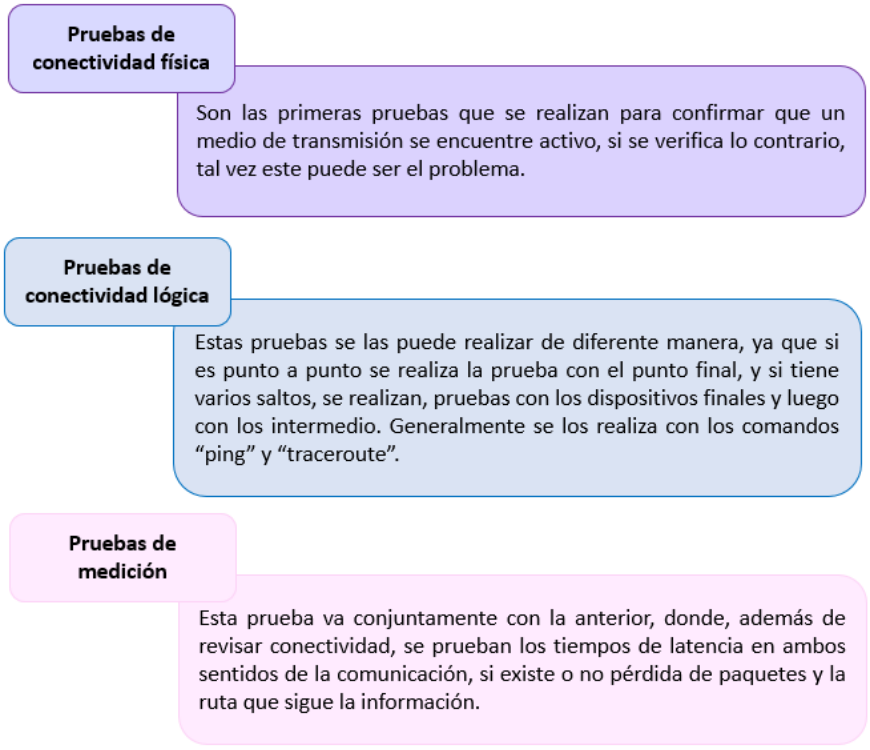


Figura 29. *Pruebas de conexión*
Fuente: *Elaboración propia*

Después de esto, la etapa de corrección de las fallas es donde todo depende de la tecnología de la red. Este proyecto solo enumera los errores a nivel de red de datos de la empresa de distribución.

Los mecanismos más comunes para gestionar redes conmutadas que manejan routers y switches son:

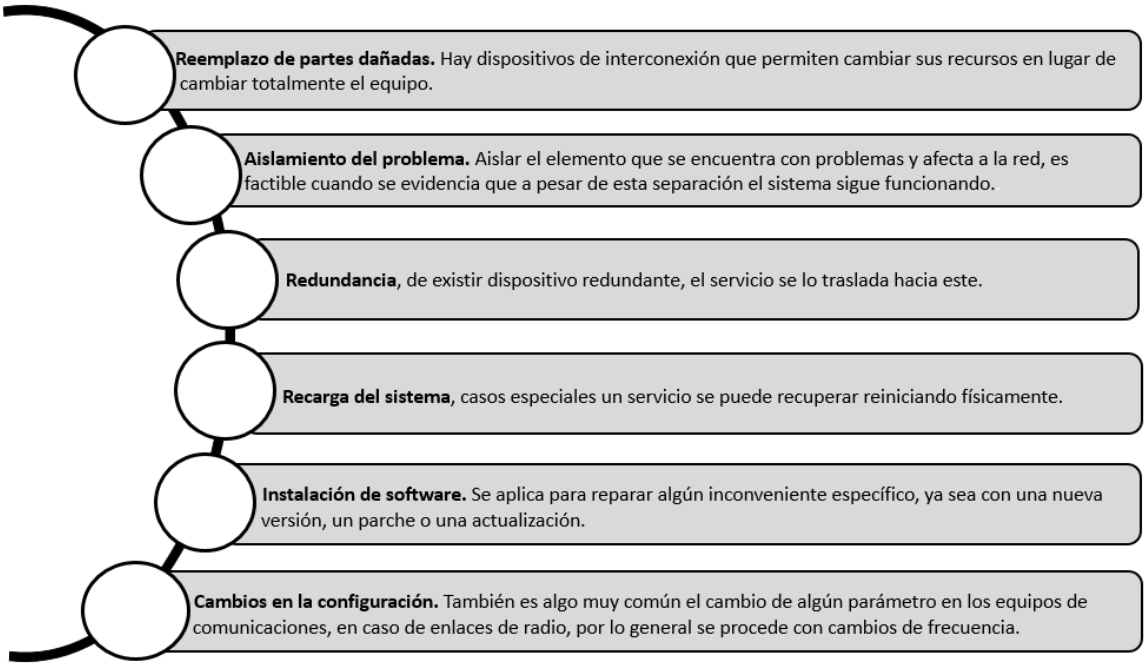


Figura 30. *Corrección de fallas*
Fuente: *Elaboración propia*

3.2.1.12 Administración de reporte de fallas

Siguiendo el modelo ITU X.700 (Modelo de referencia de interconexión de sistemas abiertos, 1998), esta fase describe la documentación de fallas. En caso de inconveniente es reportado, se deberá asignar un reporte para el seguimiento, en este punto el ticket permanecerá abierto hasta que se resuelva. De esta manera, los usuarios del servicio pueden ver el estado de los problemas informados.

De acuerdo al (Modelo de referencia de interconexión de sistemas abiertos, 1998) el ciclo de vida de informes en el sector de gestión se divide en cuatro tareas: creación, seguimiento, manejo y finalización de reporte.

Figura 31. *Ciclo de vida de informes*
Fuente: *Elaboración propia*

Para la creación de reportes es generado cuando se le notifiquen problemas de red de datos a través de alertas, llamadas telefónicas de usuarios, correo electrónico u otros medios. Al crear un informe, debe contener al menos la siguiente información.

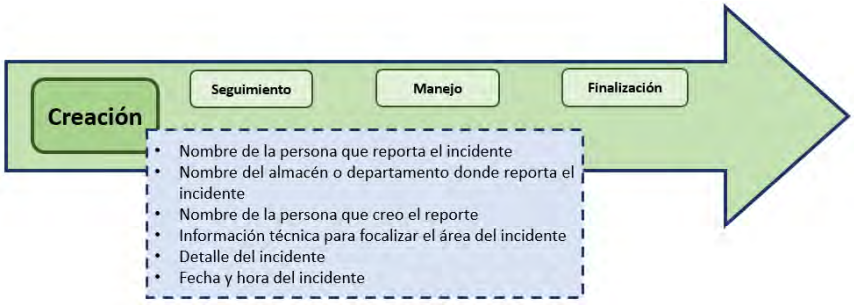


Figura 32. *Creación*
Fuente: *Elaboración propia*

La gestión de informes debe permitir a los administradores realizar un seguimiento de las acciones para encontrar una solución a un problema y tener un historial de lo que se va realizando sobre la falla reportada.

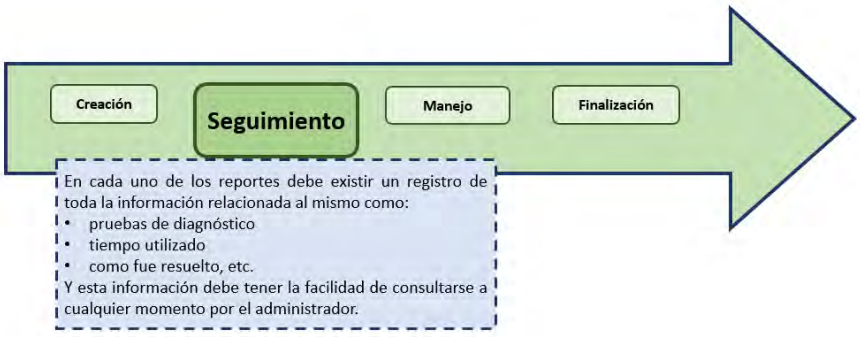


Figura 33. *Seguimiento*
Fuente: *Elaboración propia*

El personal de Sistemas o el ingeniero debe poder tomar decisiones cuando el reporte este en curso.

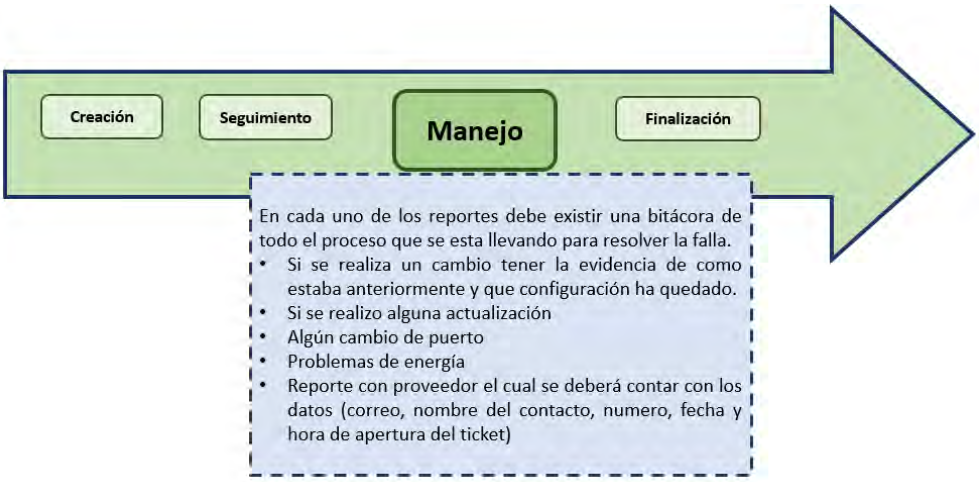


Figura 34. *Manejo*
Fuente: *Elaboración propia*

Cuando la falla fue resulta, procedemos a finalizar el reporte.

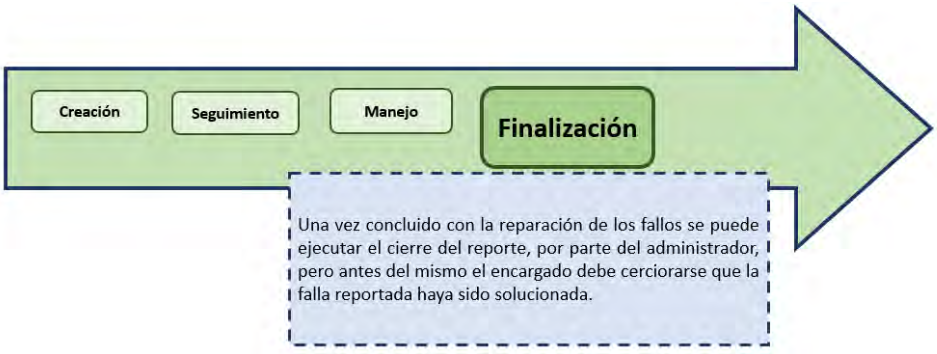


Figura 35. *Finalización*
Fuente: *Elaboración propia*

3.2.1.13 Administración de equipos y seguridad

Se ocupa del proceso de recopilación de información de los equipos utilizados por los dispositivos de la red, como la infraestructura central así como con los usuarios finales. Esto se lleva acabo con el fin de ejercer cobros hacia los proveedores en cierre de tarifas específicas si el servicio falla por parte de ellos, este proceso es conocido como facturación, es muy común entre los proveedores de servicios de Internet. Para la administración de seguridad el objetivo es brindar estabilidad y confianza en los equipos que constituye la red y así establecer estrategias para prevenir y detectar problemas en la red.

Tabla 23. *Administración de seguridad*

Prevención de ataques	Detección de intrusos	Respuesta a incidentes
El objetivo es mantener los dispositivos sin acceso de usuarios maliciosos. Un ejercicio puede ser una barrera de control de acceso. Y cabe destacar que los ataques se reducen más nunca se eliminan del todo.	El objetivo de esta tarea es detectar el momento en que se está realizando el ataque. Este proceso se puede lograr mediante un sistema de detección de intrusos que esté vigilante ante el tráfico que circula en la red, el mismo que debería generar alarmas en el momento que se detecte alguna anormalidad.	El objetivo es tomar acciones ante un posible ataque dentro de la infraestructura de la red, además que una vez presentado el riesgo de seguridad, se deberá tratar de eliminar dichas causas.

Políticas de seguridad	Mecanismos de seguridad
Indican que la tarea principal de las políticas de seguridad es señalar los requerimientos recomendados para proteger de forma adecuada a la infraestructura de la empresa y a la información que se sostiene en la misma. Una política debe especificar los mecanismos para que se cumplan los requerimientos. El grupo de gestión debe generar las políticas una vez realizado un análisis profundo de las necesidades.	En esta tarea se deben definir herramientas necesarias para poder implementar servicios de seguridad. Algunas pueden ser: control de acceso, firewall, Servidor Radius, Secure Shell para accesos remotos, mecanismos de integridad, entre otros.

Algunas de las políticas que se puede recomendar son:

Políticas de uso aceptable.
Políticas de cuentas de usuario.
Políticas de configuración de puntos de acceso.
Políticas de configuración enrutadores.
Políticas de accesos remotos.
Políticas de contraseñas.
Políticas de respaldos.

3.2.1.14 Protocolo para la gestión de red de datos

La disponibilidad de distintos fabricantes, el tipo de equipos, el aumento del número y expectativas de los clientes, logran hacer más compleja la red de datos de la empresa de distribución. Y así se obliga a tener una configuración y un protocolo al mismo tiempo estándar que pueda permitir que las herramientas de diferentes proveedores sean manejadas por el personal de dirección.

Para lo anterior se selecciona el equipamiento de cada dispositivo de comunicación de la red, y el dispositivo más importante y más utilizado en el mundo de las telecomunicaciones es el protocolo SNMP, el cual ya se encuentra soportado en el equipo, así como la función SNMP se puede ejecutar en cualquier sistema operativo.

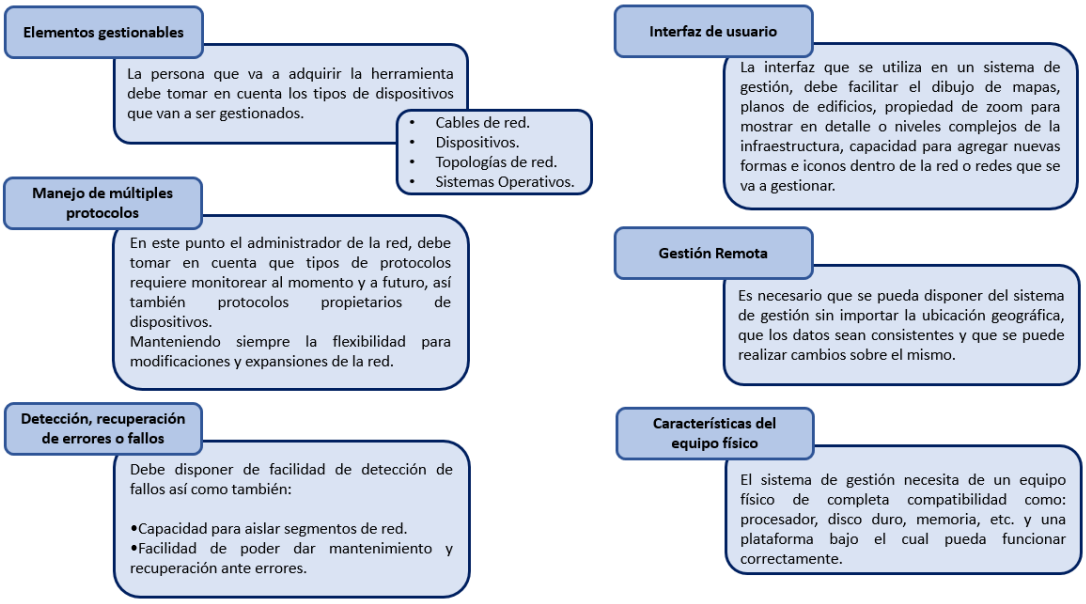
Existen distintos mecanismos para la administración de redes de datos empresariales en el mercado, en el caso de la empresa de distribución, el presupuesto financiero no se ahorra como resultado, por lo que optó por un software gratuito disponible en Internet. Para la herramienta de búsqueda, estos deben cumplir con el número máximo requerido anteriormente.

3.3 Etapa 3. Desarrollo del sistema

Las herramientas existentes son de diferentes niveles, y cada uno de estos niveles permite observar algunos tipos de equipos de redes que generalmente no están conectados a un solo sistema que podrá mostrar una visualización completa de los datos obtenidos del sistema que consta de equipos de red. Los siguientes factores se tienen en cuenta al seleccionar las siguientes herramientas: primero, se evalúan las necesidades del departamento de Sistemas de la empresa de distribución, luego se consideran los factores relevantes en el proceso de adquisición y en los detalles técnicos finales y el equipo proporcionado por la herramienta para el análisis.

Se deber analizar las necesidades de la empresa de distribución ya que él administrador de la red del departamento de Sistemas, es responsable de determinar lo que se requiere, las necesidades actuales y futuras, los límites y las limitaciones con respecto al tamaño del sistema de la red de datos. En la primera fase del proceso de apropiación de herramientas, cabe señalar que todos los requisitos, limitaciones y restricciones se aplican, entre otros a estos factores:

Tabla 24. *Administración de seguridad*



La empresa de distribución de insumos de la sede principal cuenta con 61 equipos de Cisco de diversos modelos y versiones, en cada almacén aproximadamente cuenta con 10 equipos de red.

Tabla 25. *Cantidad de equipos de red*

NOMBRE	MODELO	CORPORATIVO	SITE	VIGILANCIA	ALMACEN SITE	DIESEL	LLANTAS	TALLER	ALMACEN 1	ALMACEN 2	ALMACEN 3
Meraki	MX67-HW								2	2	2
Cisco Router	ISR4351/K9		2								
Cisco Router	CISCO1921/K9			1					1	1	1
Cisco Router	C892FSP-K9		1								
Cisco Wireless Controller	AIR-CT3504-K9								1	1	1
Cisco Punto de acceso	C9117AXI-A					3			5	5	5
Cisco Punto de acceso	AIR-AP2802E-A-K9	3	1		2						
Cisco Punto de acceso	AIR-AP1230B-A-K9		1								
Cisco Wireless Controller	AIR-SAP2702I-N-K9		1			1	1	1			
Cisco Firewall	WS-C3560X-24		1								
Cisco SW	WS-C2960X-48TS-L	2	2								
Cisco SW	WS-C2960X-24TS-L	2	3		2		1	1			
Cisco SW	WS-C2960CG-8TC-L	1		1							
TOTAL		8	12	2	4	4	2	2	9	9	9

Después de analizar el hardware en la red troncal, se puede obtener el porcentaje de presencia de cada marca en la infraestructura, como se muestra en el diagrama a continuación.

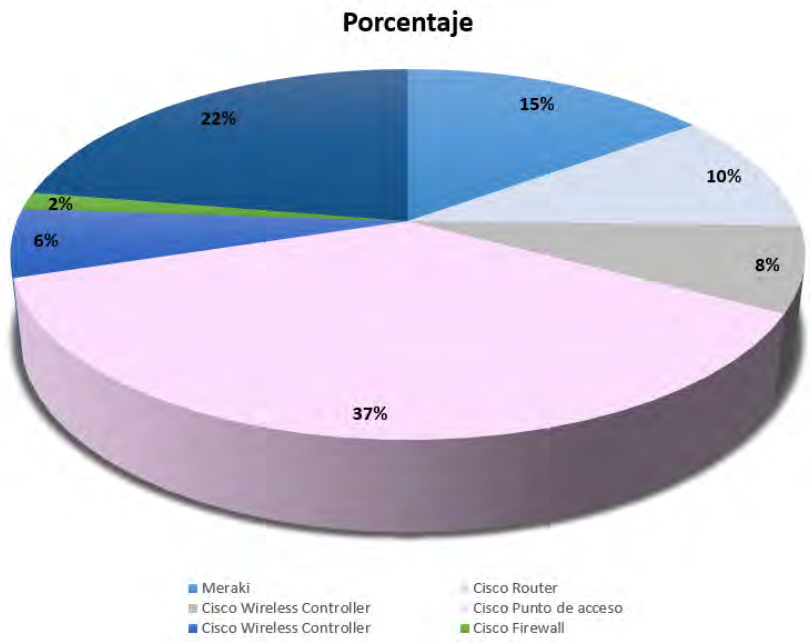


Figura 36. *Porcentaje de equipos de red*
Fuente: *Elaboración propia*

Se pudo validar que la marca Cisco domina en infraestructura de red de datos y por conocimiento personal existe un software que se puede usar para administrar la infraestructura con las necesidades anteriores, con el nombre Paessler Router Traffic Grapher (PGRT) Network Monitor. Es una herramienta gratuita se puede adquirir en el sitio web (https://www.paessler.com/es/prtg) donde se puede descargar o analizar los precios conforme a los dispositivos a monitorear.

3.3.1 Factores para la selección de herramientas

El software es el hardware lógico e intangible de un sistema informático, que consiste en un conjunto de elementos lógicos necesarios para realizar tareas específicas, a diferencia de los elementos físicos conocidos como hardware. En otras palabras, es una colección de programas informáticos, procedimientos, reglas, documentos y datos relacionados que forman parte del funcionamiento de un sistema informático. Debemos tener en cuenta todos los factores importantes para elegir las herramientas del sistema como:

Tabla 26. *Factores de herramienta del sistema*

Capacidad de soportar todo tipo de dispositivos	El sistema de gestión debe preparado para integrar diferentes dispositivos y sistemas de interconexión. Cuando se dispone de diferentes redes, protocolos, y marcas de dispositivos, existe la necesidad de que el sistema lo integre sin ningún percance.
Diseño a la medida	Es muy importante que el sistema se pueda implementar dinámicamente y modificar de acuerdo a las necesidades del usuario, adicional se pueda dar de alta de baja o modificar los dispositivos graficados. Se podría decir que la solución de software escogida para el sistema de gestión debe cubrir en su totalidad los ítems expuestos. La topología de la red implementada en la empresa es de tipo estrella como se indicó anteriormente, es decir que existe un nodo principal y de este se desprenden enlaces hacia otros repetidores. Se ha diseñado la red con el fin de propagar la señal de manera inalámbrica, usando como medio de transmisión radio enlaces, los cuales transportan todo tipo de tráfico que se genera en Internet. El equipamiento que se usará dentro de la infraestructura de red depende de su tarea o servicio como son: • **Enlace punto a punto**, como mínimo deben cumplir con estándares 802.11, para poder obtener alta capacidad de tráfico desde el nodo principal hacia un repetidor. • **Router de borde** con interfaces gigabit que soporte la capacidad contratada y el transporte del tráfico interno en la red. • **Router de distribución** con interfaces gigabit, y soporte una gran cantidad de reglas de configuración lógica como: firewall, vlans, cache DNS, etc. • **Switching** que disponga de interfaces gigabit dentro del nodo principal y como mínimo fast- ethernet en los repetidores, pero para interconexión se obligue a que se vinculen por puertos gigabit. • **Los Puntos de Acceso (APs)** en su mayoría deben tener propiedades de enrutadores para que se conviertan en equipos de acceso, de la misma forma deben cumplir con estándares 802.11. • Por **situación económica** en la empresa se manejan con CPUs clones para servidores, estos deben tener garantía en su funcionamiento con propiedades que solicite una implementación. • Los **repetidores** debe disponer de respaldo eléctrico para el caso de falla de energía. • Se debe **disponer** de equipos para ser reemplazados en caso de fallo físico en un dispositivo.

3.3.2 Especificaciones Técnicas

Se enfatiza la economía de la empresa para encontrar herramientas de código abierto que aseguren el sistema de gestión y al mismo tiempo ayuden a mantener la infraestructura. Se ha encontrado y analizado la manera de encontrar el software que aporte a la empresa con los siguientes requisitos específicos:

Figura 37. *Requisitos para los equipos de red*
Fuente: *Elaboración propia*

Las aplicaciones principales que tienen algunas de las funciones anteriores se describen a continuación. A continuación se analizan los tres primeros analizando sus características, ventajas, desventajas, precio entre otras.

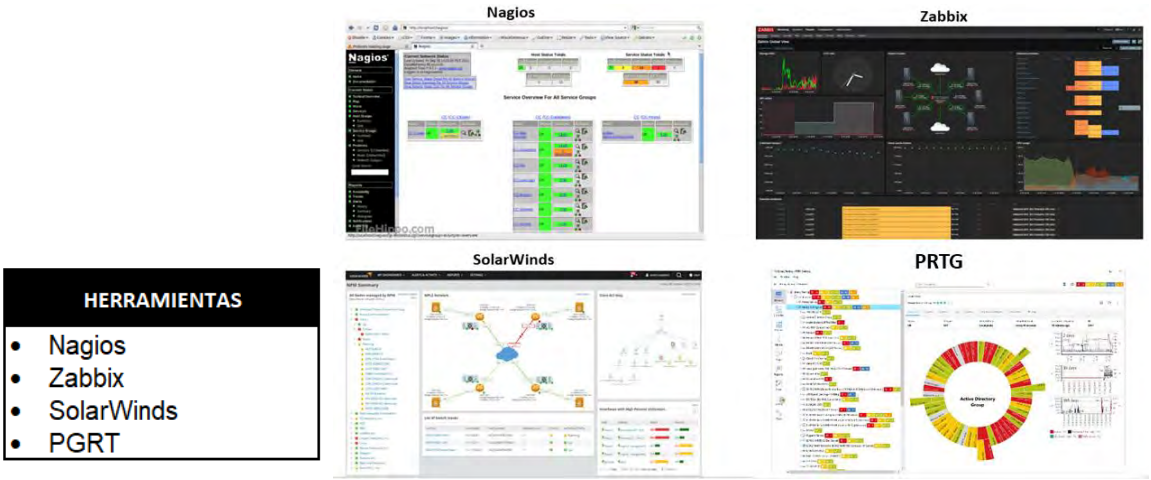


Figura 38. *Aplicaciones para el monitoreo de los equipos de red*
Fuente: *Elaboración propia*

Tabla 27. *Nagios*
Fuente: *(Nagios, 2018)*

Nagios
Nagios es la herramienta libre más conocida, desde 1996 están trabajando en USA para construir este software de monitorización. El core de Nagios es la parte más importante de la herramienta y se pueden construir plug-ins para monitorear elementos particulares. Es interesante ver cómo la tendencia de su demanda en Internet ha ido disminuyendo con el paso del tiempo. Lo que antes fue una de las herramientas de red más potentes y conocidas, está ahora perdiendo terreno.
CARACTERÍSTICAS
Monitorización de servicios de red (SMTP, POP3, HTTP, HTTPS, NTP, ICMP,SNMP, FTP,DNS, etc). Monitorización de los recursos de equipos hardware (carga del procesador, uso de los discos, procesos del sistema) en varios sistemas operativos. Monitorización de equipos remotos, a través de túneles SSL cifrados o SSH. Diseño simple de plugins, que permiten a los usuarios desarrollar sus propios chequeos de servicios dependiendo de sus necesidades, usando sus lenguajes de programación preferidos (Bash, C++, Perl, Ruby, Python, PHP, C#). Posibilidad de definir la jerarquía de la red, permitiendo distinguir entre host caídos y host inaccesibles. Notificaciones a los contactos cuando ocurren problemas en servicios o hosts, así como cuando son resueltos. Rotación automática del archivo de registro. Soporte para implementar hosts de monitores redundantes. Visualización del estado de la red en tiempo real a través de interfaz web, con la posibilidad de generar informes y gráficas de comportamiento de los sistemas monitorizados, y visualización del listado de notificaciones enviadas, historial de problemas, archivos de registros.

VENTAJAS	DESVENTAJAS
• Hay muchos perfiles con experiencia Nagios. • Si se tiene gran conocimiento de la herramienta, la configuración manual puede darle mucha potencia para monitorizar casos aislados y particulares. • Ofrece muchos plugins para adaptar Nagios a las necesidades del usuario. • Su configuración configuración básica resulta muy fácil.	• Informes simples y sencillos. • Cada instalación adicional resulta un "puzzle" en el que más que un producto estándar tenemos una implementación propia, con cientos de parches y código propio o de terceros, que la convierten en una herramienta complicada de evolucionar o de mantener. • Configuración y edición avanzada compleja, debido a la necesidad de hacer muchas modificaciones manuales. • El interfaz gráfico carece de una buena usabilidad. • Coste de aprendizaje elevado. • Muy pobre en su tratamiento de SNMP

El precio de este software es de $1,995.00 costo único. Nagios XI es el software de monitorización de red más potente y fiable del mercado

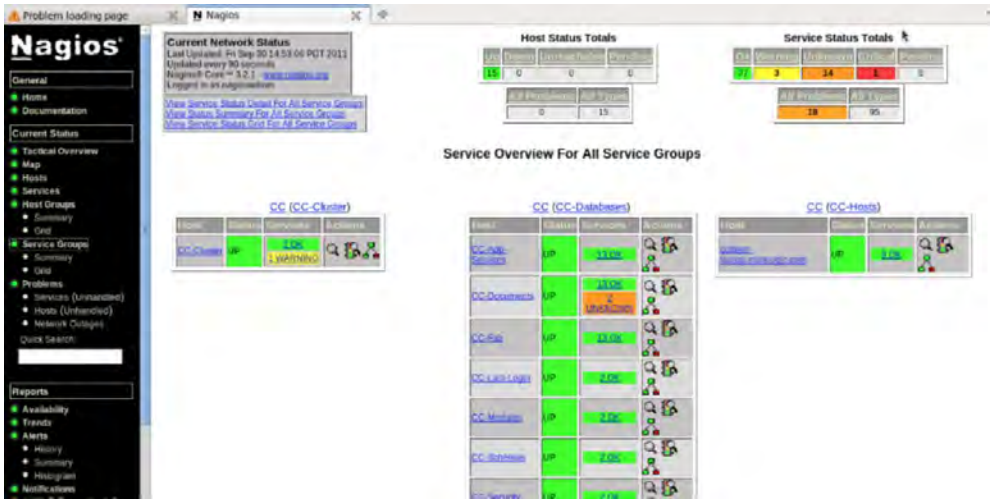


Tabla 28. *Zabbix*
Fuente: *(Capterra, 2017)*

Zabbix	
Es una plataforma madura de nivel empresarial y sin compromisos, diseñada para la supervisión en tiempo real de millones de métricas recopiladas de decenas de miles de servidores, máquinas virtuales y dispositivos de red, que se pueden escalar fácilmente a entornos aún más grandes. Reúne y analiza estadísticas precisas y métricas de rendimiento, visualízalas, recibe notificaciones sobre problemas actuales y potenciales sin demora y aprovecha la asistencia y el desarrollo profesional comprobados con el tiempo.	
CARACTERÍSTICAS	
Alto rendimiento y alta capacidad (posibilidad de monitorizar cientos de miles de dispositivos) Auto descubrimiento de servidores y dispositivos de red Monitorización distribuida y una administración web centralizada Agentes nativos en múltiples plataformas Posibilidad de monitorización sin agentes Monitorización Web Configuración de permisos por usuarios y grupos	
VENTAJAS	**DESVENTAJAS**
• Su comunidad es bastante activa. • Es potente a bajo nivel.	• Aunque se ha utilizado en grandes instalaciones, a partir de 1000 nodos disminuye su rendimiento. • Pobre tratamiento de traps. • No posee informes en tiempo real. • Es difícil de depurar cuando hay errores. • Difícil crear y definir plantillas de informes y alertas. Las configuraciones pueden requerir muchos clics y pasos para completarlas.

El precio de Zabbix comienza en $ 1,600 para la instalación de 1 servidor y 300 sensores con una licencia perpetua.

Tabla 29. *SolarWinds*
Fuente: *(SolarWinds , 2019)*

SolarWinds
Es un sólido y asequible software de monitoreo de redes que le permite detectar, diagnosticar y resolver rápidamente cortes y problemas de rendimiento de la red.
CARACTERÍSTICAS
Monitoreo de fallas: Detecte, diagnostique y resuelva rápidamente problemas de rendimiento de la red y evite el tiempo de inactividad con software de optimización de redes. Análisis salto por salto en rutas críticas: Loss detalles de desempeño, tráfico y configuración de dispositivos y aplicaciones que están en instalaciones locales, en la nube o en entornos híbridos Asignación y detección de redes inalámbricas y cableadas dinámicas: Detecte y asigne automáticamente dispositivos, métricas de desempeño, utilización de enlaces y cobertura inalámbrica. Previsión, alertas e informes de capacidad automatizados: Calcule automáticamente las fechas de agotamiento usando umbrales personalizables en función del uso promedio y máximo. Informes personalizables de desempeño y disponibilidad: Programa y genera informes personalizados del rendimiento de la red mediante una de las más de 100 plantillas listas para usar.

VENTAJAS	DESVENTAJAS
• La interfaz web es completamente personalizable, lo que permite que diferentes miembros de su equipo de TI utilicen una vista que les convenga. Por ejemplo, los administradores del sistema pueden usar una vista que se enfoca en los hosts VMware mientras que la vista del administrador de la red se enfoca en los conmutadores de red y el tráfico. • NPM tiene alertas excelentes y fácilmente configurables. Incluso podría crear una alerta para notificarle cuándo se conecta un dispositivo que se supone que debe estar desconectado de la red. Las posibilidades son infinitas. • Puede crear sondeos de dispositivos combinados con mediciones personalizadas que prácticamente pueden devolver cualquier información que necesite.	• La configuración del correo electrónico, aunque altamente flexible y personalizable, podría ser más fácil. • NetFlow Traffic Analyzer (un módulo de análisis de red cualitativo) no está integrado en el producto y debe comprarse por separado, lo que aumenta el precio del producto. • Algunos usuarios se han quejado de la falta de opciones de filtrado y búsqueda en syslogs y alertas.

El precio de solarwinds comienza en $ 2,656 para hasta 25 dispositivos.

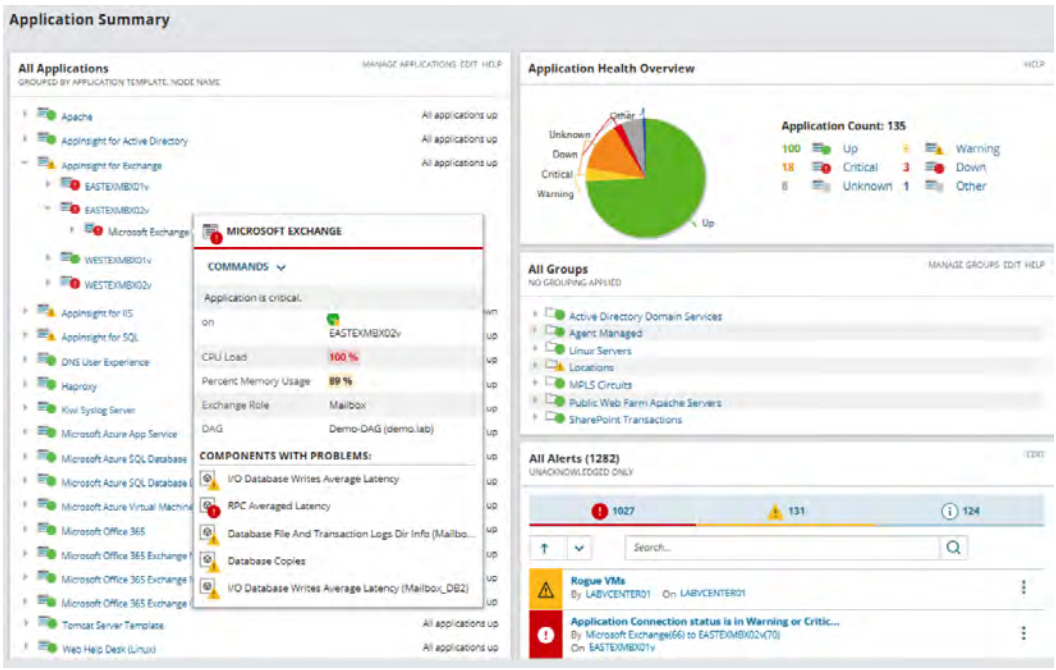


Tabla 30. *PGRT Network Monitor*
Fuente: *(https://www.paessler.com/es/prtg, 2022)*

PRTG Network Monitor
Es una herramienta de monitoreo de red que destaca por su gran interfaz y de fácil manejo. Tiene una gran flexibilidad a la hora de configurar alertas y su capacidad de generación de informes es admirable. La versión gratis (que no open) está limitada a 100 tipos de aplicaciones a monitorizar. PRTG es una aplicación que solo se ejecuta en máquinas Windows como Microsoft Network Monitoring. De todas formas, destacamos que su monitorización es multi plataforma y además es capaz de monitorizar sistemas virtuales y aplicaciones en la nube. Permite mostrar informes en tiempo real.
CARACTERÍSTICAS
Tecnologías compatibles: admite SNMP, WMI, SSH para macOS, Linux o Unix, y análisis de tráfico mediante protocolos de flujo y rastreo de paquetes, solicitudes HTTP, Ping, SQL y API REST para devolver JSON y XML Mapas y paneles: PRTG utiliza mapas en tiempo real, incluido el estado en vivo, para ver su red. Cree paneles de control personalizados e integre componentes de red a través de más de 300 objetos de mapa como gráficos de tráfico, iconos de estado, listas principales, etc Las alertas flexibles ofrecen muchos mecanismos incorporados para alertas como solicitudes HTTP, notificaciones push o correos electrónicos. Una interfaz de usuario con todas las funciones: su interfaz web está construida en AJAX mientras mantiene alta seguridad, rendimiento y diseño receptivo Solución de conmutación por error: cuando el nodo principal está inactivo o no está conectado, otro nodo se hace cargo de inmediato para proporcionar el manejo de la conmutación por error automáticamente Informes detallados: obtenga estadísticas, números y gráficos que contienen sus datos de monitoreo. Exporte información histórica de monitoreo en archivos PDF, CSV, XML y HTML y ejecute informes a pedido o prográmelos mensualmente, semanalmente o diariamente.

VENTAJAS	DESVENTAJAS
• Interfaz con grandes posibilidades para navegar • Se puede acceder a la monitorización desde sistemas móviles. • Informes en PDF/HTML. • Muy potente y flexible sistema de alertas.	• Escalabilidad limitada. • Muy rígida a la hora de implementar chequeos propios. • Muy pobre para monitorización de servidores o aplicaciones. • Ciertos plugins requieren licencias adicionales

El precio de PRTG comienza en $ 1,750 para la instalación de 1 servidor y 500 sensores con una licencia perpetua.

3.3.3 Selección de Software

Al seleccionar herramientas, los requisitos para el servidor en el que se instalará la aplicación también son importantes, ya que se deben tener en cuenta consideraciones de presupuesto, rendimiento y escalabilidad. El servidor elegido para diseñar la solución se selecciona con base a la tabla de comparación y la información proporcionada por los desarrolladores.

Tabla 31. *Tabla de comparación entre herramienta*

NOMBRE	CACTI	ZABBIX	NAGIOS	PRTG
LICENCIA	GPL	GPL	GPL	Comercial
GRÁFICAS	SI	SI	SI	SI
INFORMES SLA	SI	SI	SI	SI
ESTADÍSTICAS	SI	SI	SI	SI
AUTODESCUBRIMIENTO	A través de plugin.	SI	SI	SI
SNMP	SI	SI	A través de plugin.	SI
EVENTOS	SI	SI	SI	SI
APLICACIÓN WEB	SI	SI	Solo visualización.	SI
MAPA DE RED	A través de plugin.	SI	SI	SI
MAPA GEOGRÁFICO	NO	NO	NO	SI
APLICACIÓN MÓVIL IOS	SI (PAGA)	SI (Gratis versión trial)	SI (Gratis versión trial)	SI (Gratis app oficinal)
APLICACIÓN MÓVIL ANDROID	SI (Viewer)	SI (Cliente Gratis)	SI (Cliente Gratis)	SI (Gratis app oficial)

Paessler Router Traffic Grapher (PGRT) fue el único proveedor para detallar toda la información para una oferta de trabajo completa, aunque no es un software Licencia Pública General (GLP) y solo se puede instalar en PC con Windows en su sitio web aquí encontrará toda la documentación y el soporte necesarios para recrear el escenario del servicio, así como la posibilidad de descargar una versión de prueba con todas las características y funciones.

Los requisitos de hardware dependen principalmente del tipo de transductor y el ámbito de uso. Los siguientes valores se proporcionan como guía para casos de uso típicos de PRTG.

Si bien hay muchos parámetros que afectan el funcionamiento de PRTG, la siguiente guía de tamaño de hardware de clave de servidor de PRTG debería funcionar para la mayoría de los usuarios.

Tabla 32. *Tabla de parámetros de PGRT*

Sensores por instalación de servidor central de PRTG	Núcleos de CPU	RAM	Espacio en disco	Sesiones de administrador	Número de sondas remotas	Virtualización	Cluster	Licencia recomendada
Hasta 500	4	4 GB	100 GB	< 30	< 30	✓	✓	PRTG 500
Hasta 1000	6	6 GB	500 GB	< 30	< 30	✓	✓	PRTG 1000
Hasta 2500	8	8 GB	750 GB	< 20	< 30	✓	✓	PRTG 2500
Hasta 5000	8	12 GB	1000 GB	< 20	< 60	✓	!	PRTG 5000
Hasta 10000	10-12**	16 GB	1500 GB	< 15	< 80	✓	!	PRTG XL1
> 10000	Le recomendamos que configure instalaciones adicionales de servidor central de PRTG o que se ponga en contacto con el equipo de preventas de Paessler para obtener más información sobre el escalado.							PRTG Enterprise Monitor

✓	OK
✓	OK
!	no recomendado
!	no apoyada oficialmente, por lo que se requiere antencion directa

3.3.4 Equipos para ser monitoreados

Para determinar qué se controlará, es necesario tener en cuenta las características de cada dispositivo. Cuanta más información pueda recopilar, más efectiva será la resolución de problemas. Los dispositivos y servicios a monitorear se enumeran en la tabla 33.

Tabla 33. *Tabla de parámetros de PGRT*

Dispositivo	Parámetros	Especificaciones
Servidor/equipo	Memoria	Cantidad de memoria utilizada
	Estado	Si está activo o no el equipo
	Procesamiento	Estadística del uso del Procesamiento
	Disco Duro	Cantidad de uso del disco duro
	Procesos	Cantidad de procesos ejecutándose
	Interfaces de red	Capacidad que usa cada interfaz
Enlace	Capacidad	Cantidad que ocupa, picos máximos y mínimos
	Estado	Activo con flujo de datos o inactivo sin flujo de datos
Switch	Procesamiento	Estadísticas del uso del Procesamiento
	Interfaces	Capacidad que usa cada interfaz
Router	Procesamiento	Estadísticas del uso del Procesamiento
	Disco Duro	Cantidad de uso del disco duro
	Memoria	Cantidad de memoria utilizada
	Interfaces	Capacidad que usa cada interfaz

Capítulo 4. PROPUESTA PARA LA IMPLEMENTACIÓN

Para llevar a cabo el diseño se tuvo en cuenta el alcance definido para la fase inicial del proyecto, incluyendo las variables de monitoreo de: tiempo de respuesta y ancho de banda que permite los dispositivos de acceso a la Red, así como como los tiempos de respuesta de los almacenes conectados a la sede principal. El número de equipos se muestra a continuación:

- Corporativo
- Equipos de almacén 1
- Equipos de almacén 2
- Equipos de almacén 3
- Departamentos (Vigilancia, Taller, Llantas)

Un diagrama de la infraestructura monitoreada en el primer perímetro se muestra en la siguiente figura 39:

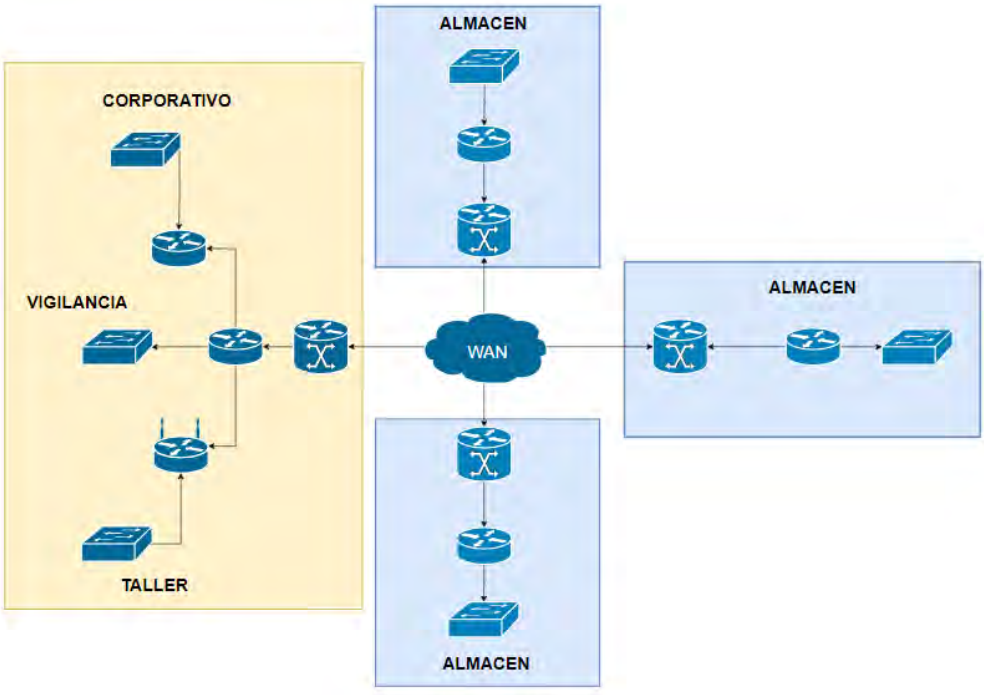


Figura 39. *Diagrama de infraestructura*
Fuente: *Elaboración propia*

El diseño de la solución de monitoreo de equipos de red de los almacenes y de la sede principal se muestra en la siguiente figura como se puede ver están conectados entre sí. Por lo que desde la sede principal se podrá accesar a los equipos de los principales almacenes. Esto beneficia a la empresa de distribución cuando se presente alguna falla, el ingeniero del departamento de Sistemas podrá acceder al equipo y realizar el análisis correspondiente.

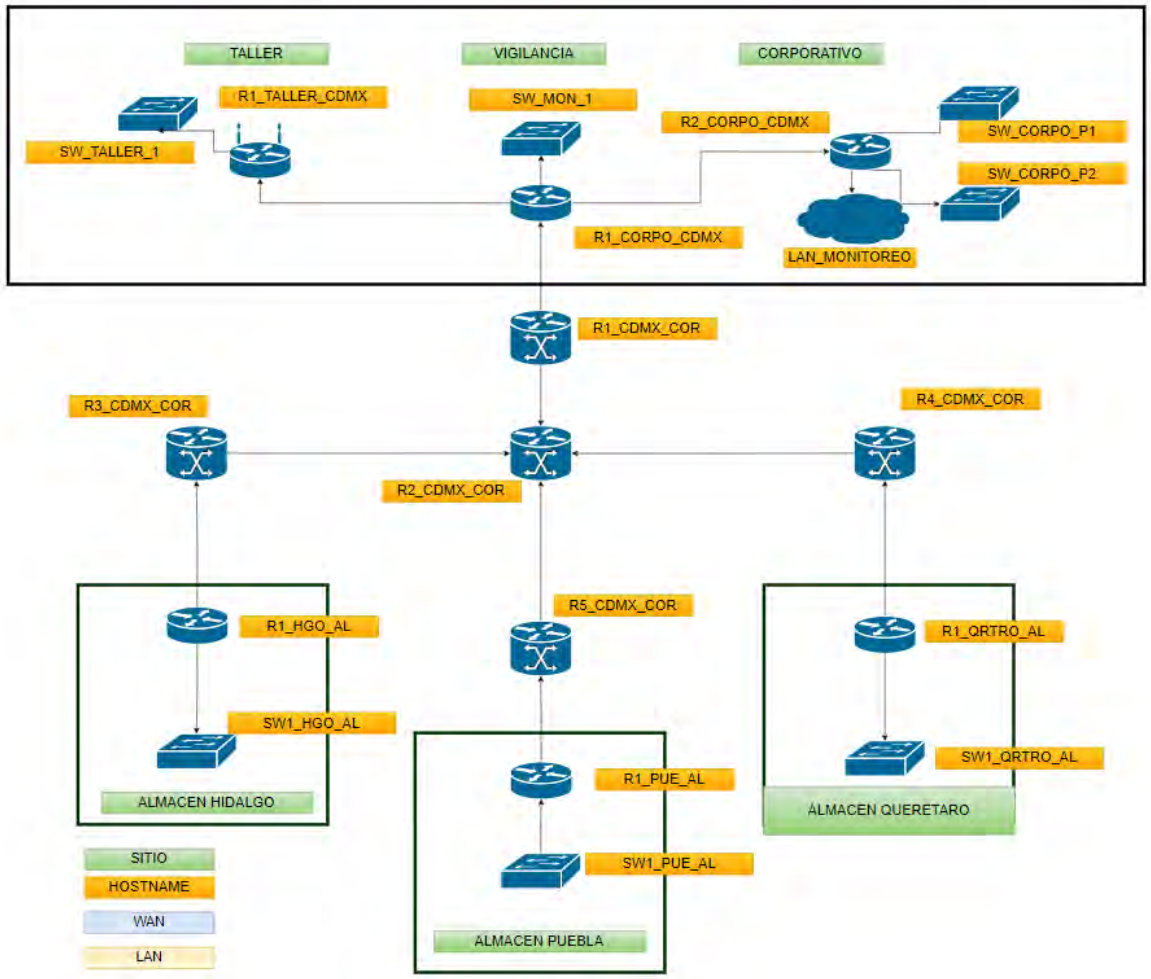


Figura 40. *Monitoreo de equipos*
Fuente: *Elaboración propia*

Con base al diseño propuesto, a continuación se explica cómo se puede monitorear toda la infraestructura de la red de la de principal y almacenes mediante el envío y la recepción de traps SNMP a todos los dispositivos.

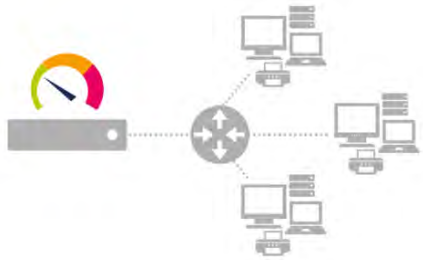


Figura 41. *Monitoreo de equipos local*
Fuente: *Elaboración propia*

Se puede observar el monitoreo con los dispositivos en la red y la aplicación puede detectar estos dispositivos automáticamente. En este caso, el monitoreo se realiza primero mediante el envío de traps o mensajes SNMP al host local y luego a los dispositivos directamente conectados.

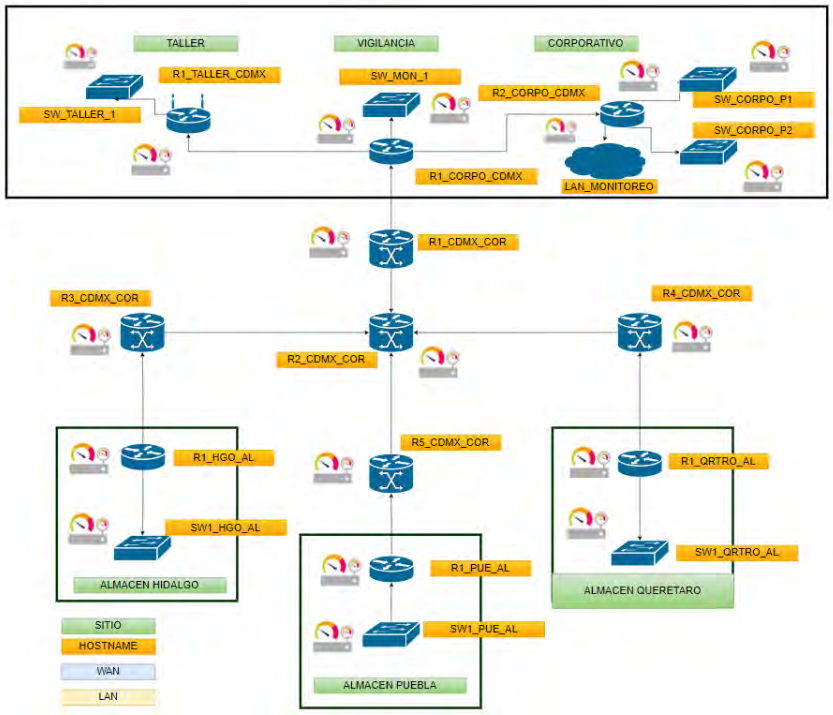


Figura 42. *Monitoreo de equipos en la sede principal y almacenes*
Fuente: *Elaboración propia*

El dispositivo de red de la sede principal, es un switch mediante el cual se interconectan los dispositivos instalados en el Centro de Datos (Firewalls, switches, servidores, etc.), una vez que las traps lleguen al destino, este enviará un mensaje de respuesta conteniendo la información del estado actual de cada dispositivo, es decir el espacio en disco de la memoria, uso de CPU, temperatura, entre otros.

De acuerdo a esto, el objetivo no es solo monitorear el dispositivo adyacente al servidor de monitoreo, para esto es indispensable crear las configuraciones requeridas en el dispositivo que conforma la red de datos y los terminales para monitorear toda la infraestructura, este proceso se muestra a continuación.

Para lograr un monitoreo extendido, las configuraciones se realizarán de la siguiente manera:

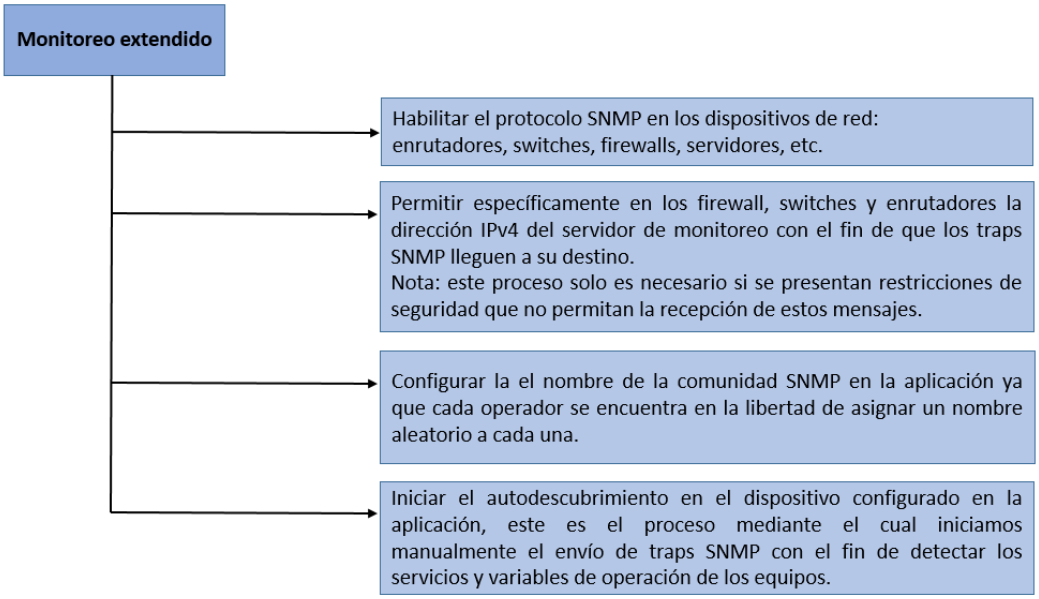


Figura 43. *Monitoreo extendido*
Fuente: *Elaboración propia*

En resumen, el diseño y la aplicación propuestos son totalmente compatibles con cualquier topología de red, lo que lo hace flexible para administrar y controlar la infraestructura de comunicación de cualquier organización, mediante la transmisión y recepción de traps o mensajes SNMP.

Por lo que nos apoyaremos en Graphic Network Simulation (GNS3) este un programa gratuito y de código abierto que se utiliza en la rama de ingeniería de Redes para poder emular, configurar, probar y solucionar problemas de redes ya sean virtuales o reales. Esta aplicación admite diferentes dispositivos de red como Cisco, Cisco ASA, Fornitet entre otros. Y tiene opciones para la parte del servidor del software un servidor local que es la misma PC donde instalo el programa y también se tiene la opción de máquina virtual remota y local se puede llevar acabo la VM GNS3 localmente en la PC usando un software de virtualización como VMware Workstation o se ejecuta la máquina virtual GNS3 de forma remota en un servidor o incluso en la nube.

Usando un navegador web con la siguiente liga https://gns3.com se puede descargar de forma gratuita la cual nos pedirá iniciar una sesión después de iniciar sesión, se seleccionara la versión de GNS3 para descargar. El archivo ejecutable tiene un tamaño aproximado de 85 MB. Si tiene problemas para descargar, tendremos que ver las políticas de seguridad, es decir las reglas de firewall o antivirus que permitan la descarga de archivos .exe. Una vez instalado la aplicación la interfaz gráfica de usuario GNS3 se muestra en la figura 44:

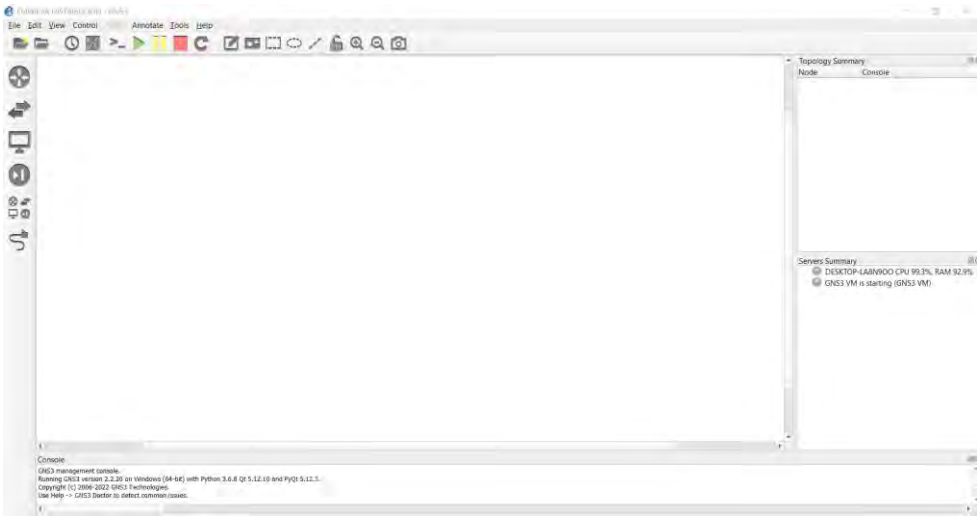


Figura 44. *Interfaz gráfica GSN3*
Fuente: *Elaboración propia*

Por lo que realizaremos el diagrama en la maqueta GNS3 de la red primeramente de la sede principal. Esto para tener una configuración de equipos y comunicación entre ellos.

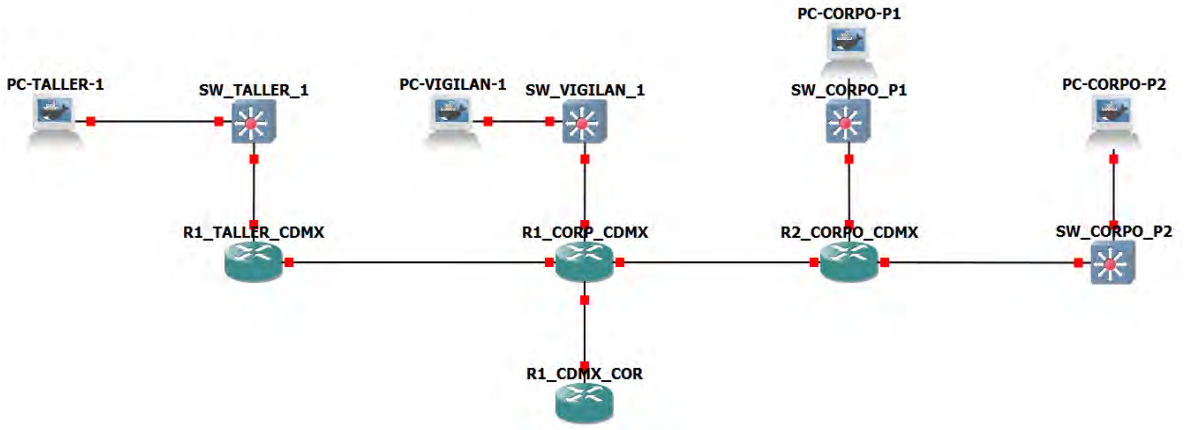


Figura 45. *Equipos de red de la sede principal en GSN3*
Fuente: *Elaboración propia*

Posteriormente, se realiza el diagrama de los almacenes como se muestra a continuación.

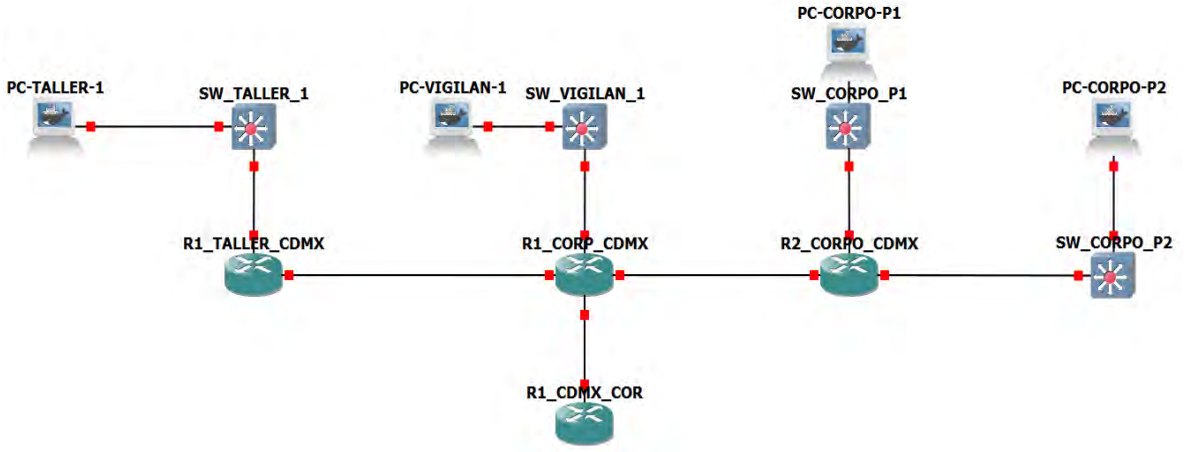


Figura 46. *Equipos de red de los almacenes en GSN3*
Fuente: *Elaboración propia*

Y a continuación se realiza la conexión de la sede principal y los almacenes.

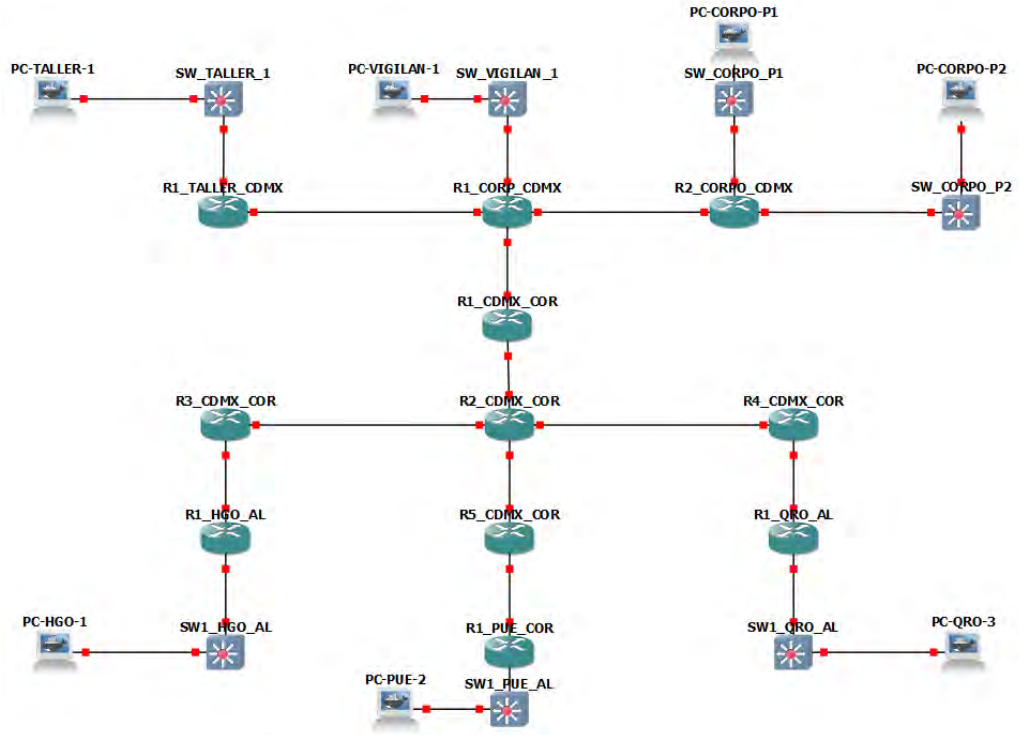


Figura 47. *Equipos de red de la sede principal y almacenes en GSN3*
Fuente: *Elaboración propia*

Se agrega el NAT para la comunicación entre el simulador y la computadora y los equipos de red y la configuración en cada uno de ellos.

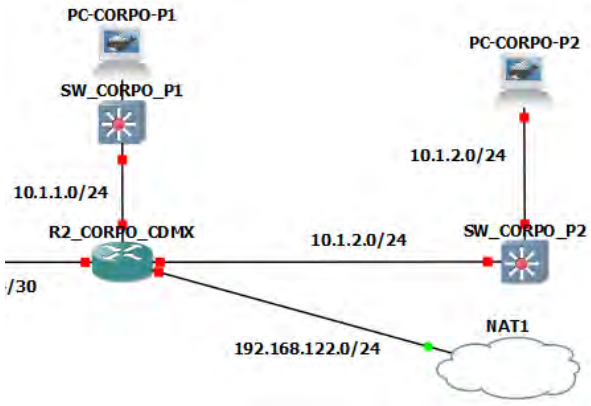


Figura 48. *Configuración de NAT*
Fuente: *Elaboración propia*

Por lo que se va a configurar los routers como indica en el Anexo A y posteriormente se encienden los routers ya configurados.

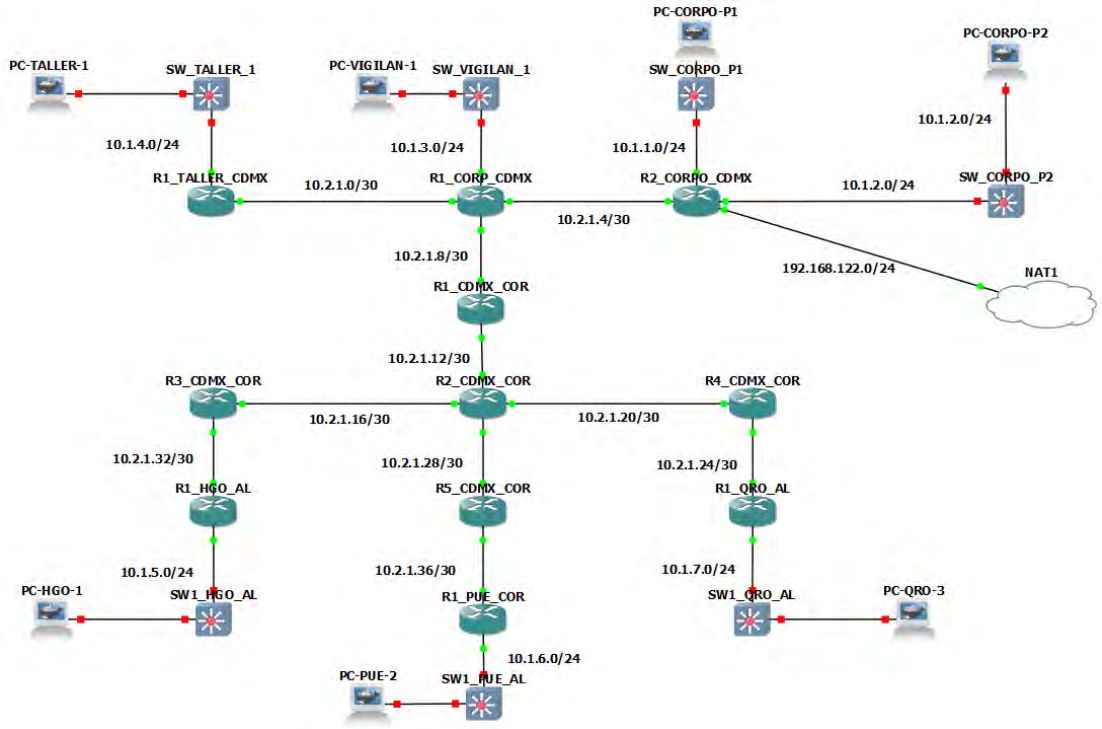


Figura 49. *Routers habilitados y configurados*
Fuente: *Elaboración propia*

Cada router se envía el comando de show ip interface brief donde se observaran las interfaces en UP, la IP de gestión y la IP que se le asigna por dhcp esto para poder tener acceso de la computadora a la red configurada.

```
R2_CORPO_CDMX#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                10.1.1.1        YES NVRAM  up                    up
Ethernet0/1                10.1.2.1        YES NVRAM  up                    up
Ethernet0/2                10.2.1.5        YES NVRAM  up                    up
Ethernet0/3                192.168.10.134  YES DHCP   up                    up
Ethernet1/0                unassigned      YES NVRAM  administratively down down
Ethernet1/1                unassigned      YES NVRAM  administratively down down
Ethernet1/2                unassigned      YES NVRAM  administratively down down
Ethernet1/3                unassigned      YES NVRAM  administratively down down
Serial2/0                  unassigned      YES NVRAM  administratively down down
Serial2/1                  unassigned      YES NVRAM  administratively down down
Serial2/2                  unassigned      YES NVRAM  administratively down down
Serial2/3                  unassigned      YES NVRAM  administratively down down
Serial3/0                  unassigned      YES NVRAM  administratively down down
Serial3/1                  unassigned      YES NVRAM  administratively down down
Serial3/2                  unassigned      YES NVRAM  administratively down down
Serial3/3                  unassigned      YES NVRAM  administratively down down
Loopback0                  10.255.255.2    YES NVRAM  up                    up
R2_CORPO_CDMX#
```

Figura 50. *Comando para interfaces*
Fuente: *Elaboración propia*

Después de validar todos las interfaces de los routers se enviara un ping a la IP 8.8.8.8 para validar la salida.

```
R2_CORPO_CDMX#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 35/67/181 ms
R2_CORPO_CDMX#
R2_CORPO_CDMX#
```

Figura 51. *Ping*
Fuente: *Elaboración propia*

Para cada dispositivo que se quiere monitorear se deberá configurar SNMP de la siguiente manera. Se configura una acl para especificar la IP del servidor del monitoreo.

```
R2_CORPO_CDMX#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2_CORPO_CDMX(config)#ip access-list standard prtg-nms
R2_CORPO_CDMX(config-std-nacl)#permit 192.168.0.11
R2_CORPO_CDMX(config-std-nacl)#exit
R2_CORPO_CDMX(config)#!
R2_CORPO_CDMX(config)#snmp-server community monitoreo ro
R2_CORPO_CDMX(config)#!
R2_CORPO_CDMX(config)#snmp-server community monitoreo prtg-nms
R2_CORPO_CDMX(config)#
R2_CORPO_CDMX(config)#!
R2_CORPO_CDMX(config)#
R2_CORPO_CDMX(config)#
R2_CORPO_CDMX(config)#
R2_CORPO_CDMX(config)#end
```

Figura 52. *Configuración SNMP*
Fuente: *Elaboración propia*

Para que exista comunicación desde la máquina hacia GNS3 es necesario configurar una ruta para el segmento de red 10.0.0.0/8 el cual es usado en la maqueta. Y se enviara un ping a las IPs de los equipos que se van a agregar para monitorear.

```
C:\WINDOWS\system32>
C:\WINDOWS\system32>route add 10.0.0.0 mask 255.0.0.0  192.168.10.134
 Correcto
```

Figura 53. *Ruta de configuración*
Fuente: *Elaboración propia*

A continuación en la imagen se muestra los pings de los equipos que se van a monitorear, las IPs que se muestras son las de gestión esto quiere decir que son las IPs para poder acceder al equipo y poder encontrar la falla o realizar alguna configuración que se tenga para una solución.

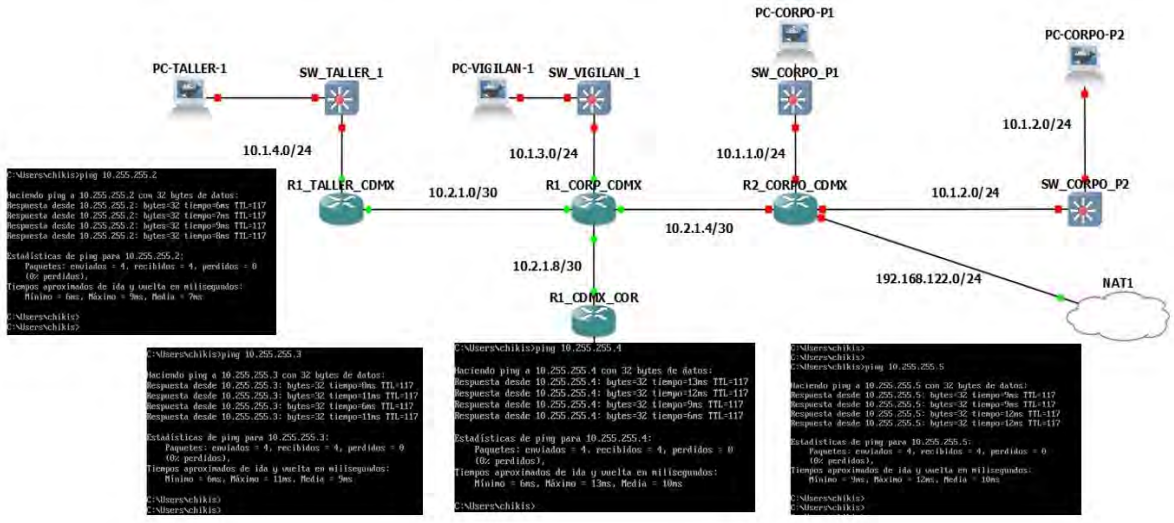


Figura 54. *Ping de los equipos de la sede principal*
Fuente: *Elaboración propia*

Y ahora enviamos los ping de los tres almacenes.

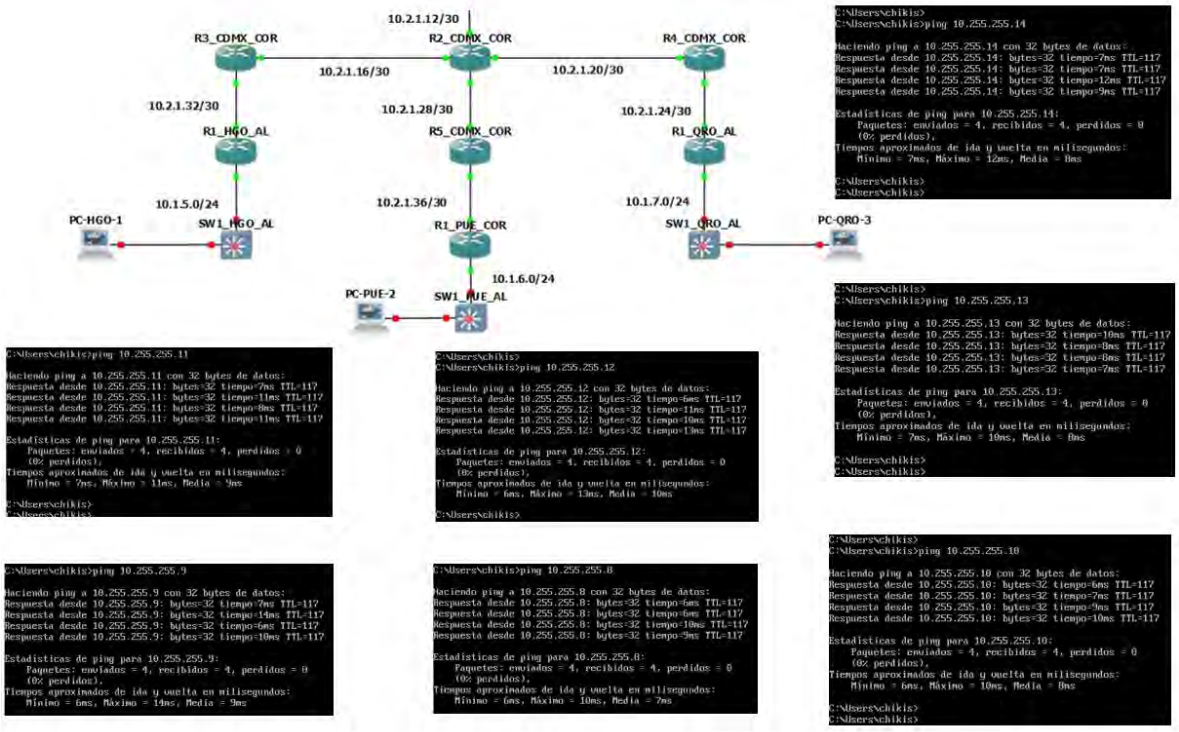


Figura 55. *Ping de los equipos de los almacenes*
Fuente: *Elaboración propia*

Una vez configurado los equipos y que se compruebe la comunicación. Se deberá instalar la aplicación Paessler Router Traffic Grapher (PGRT) que fue la que se seleccionó para el monitoreo de los equipos. Se descarga desde la liga https://www.paessler.com/es/prtg y se realiza la instalación como se muestra en el Anexo B.

Una vez instalada la aplicación podremos ingresar.

Figura 56. *Inicio de la página PRGT*
Fuente: *Elaboración propia*

Una vez que se ingresa nos encontramos con la siguiente pantalla.

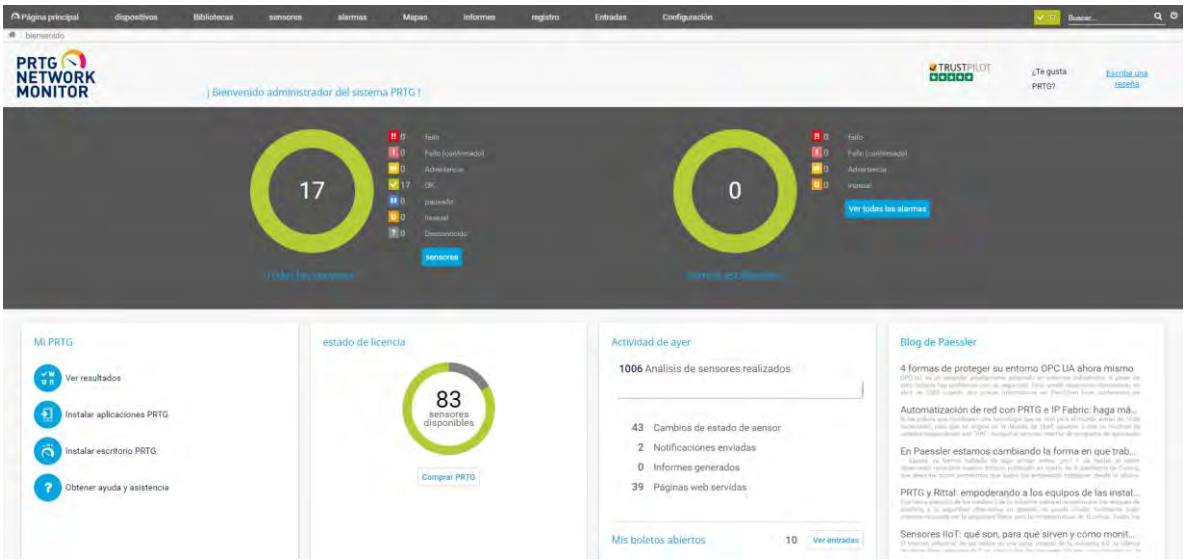


Figura 57. *Inicio de la página PRGT*
Fuente: *Elaboración propia*

Todos los equipos que vamos a monitorear los vamos agregar de forma manual de la siguiente manera.

- Nos colocamos en el menú de Dispositivos.

Figura 58. *Dispositivos*
Fuente: *Elaboración propia*

- Seleccionar y hacer clic en el grupo donde se desea agregar el dispositivo.
- Dar clic derecho sobre el grupo y seleccionar la opción de Añadir dispositivo.

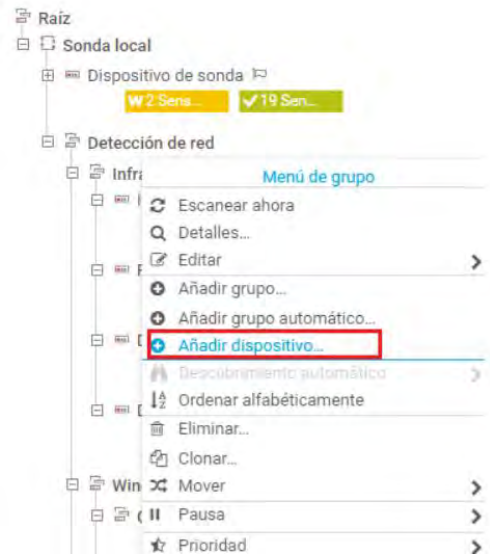


Figura 59. *Añadir Dispositivos*
Fuente: *Elaboración propia*

- En la siguiente ventana se deberán a completar la siguiente información.

Nombre del dispositivo:	El nombre que tendrá el dispositivo.
Versión de IP:	Si es IPv4 o IPv6.
Dirección IP o nombre del dispositivo:	Para conectarse al dispositivo (reconocerlo).
Etiqueta (opcional):	Para reconocer el dispositivo.
Ícono de dispositivo (opcional):	Ícono para el dispositivo.

Figura 60. *Añadir Nombre del Dispositivo*
Fuente: *Elaboración propia*

En esta parte se tendrá que añadir la IP de gestión de cada equipo que se va a monitorear. En esta ocasión son las siguientes:

Tabla 34. *IPs a Monitorear*

Sede principal	Almacenes
10.255.255.2	10.255.255.8
10.255.255.3	10.255.255.9
10.255.255.4	10.255.255.10
10.255.255.5	10.255.255.11
	10.255.255.12
	10.255.255.13
	10.255.255.14

- El tipo de gestión del sensor también es importante, ya sea que desee realizar la detección automática o no, y si la está ejecutando, el tipo de detección automática, porque esto determina qué tipo de reconocimiento de dispositivo y reproducción automática son en ese momento. Cuando haya terminado, haga clic en Aceptar.

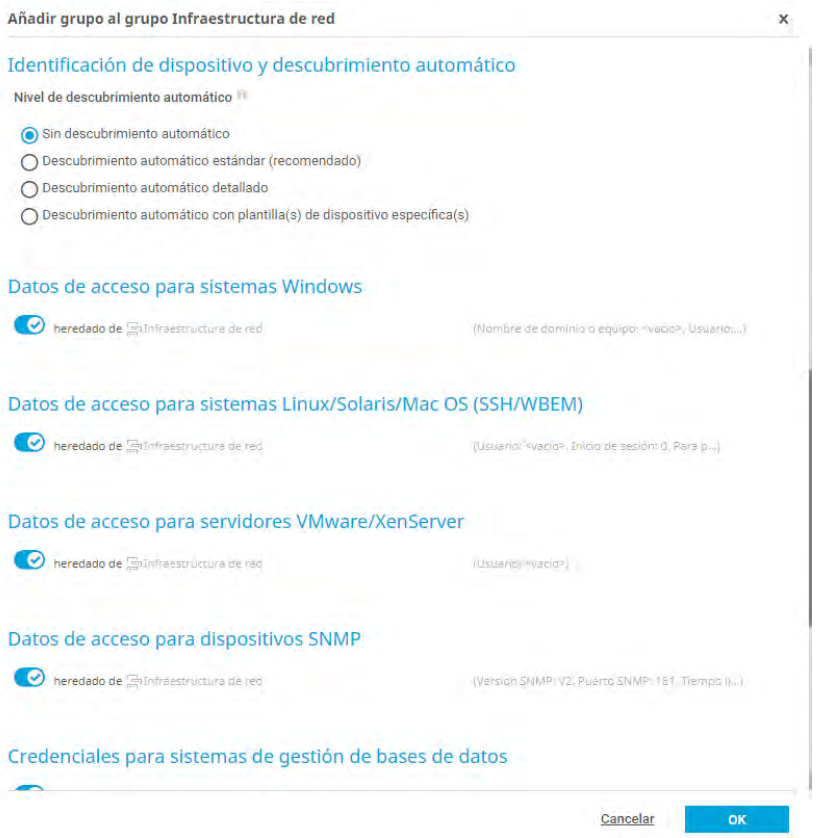


Figura 61. *Añadir grupo*
Fuente: *Elaboración propia*

El tipo de sensor que se seleccione ayudara para el monitoreo del equipo de red.

- Finalmente, debe esperar a que el dispositivo comience a detectar automáticamente y agregará automáticamente el sensor Ping.

Figura 62. *Selección de sensor*
Fuente: *Elaboración propia*

Si se requiere añadir algún sensor distinto se realiza de la siguiente manera:

- Se da clic en el botón Añadir sensor.

Figura 63. *Añadir de sensor*
Fuente: *Elaboración propia*

En esta ventana nos pregunta qué tipo de sensor queremos agregar al monitoreo del dispositivo.

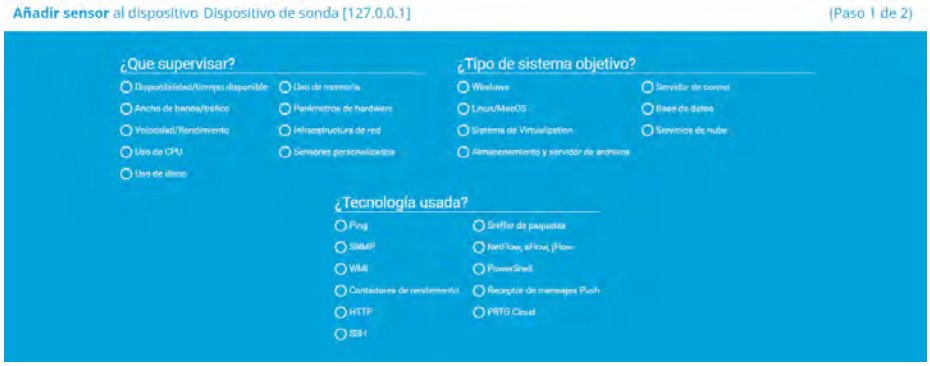


Figura 64. *Selección y búsqueda del sensor*
Fuente: *Elaboración propia*

Si se requiere buscar el sensor solo se ingresa el nombre de él.

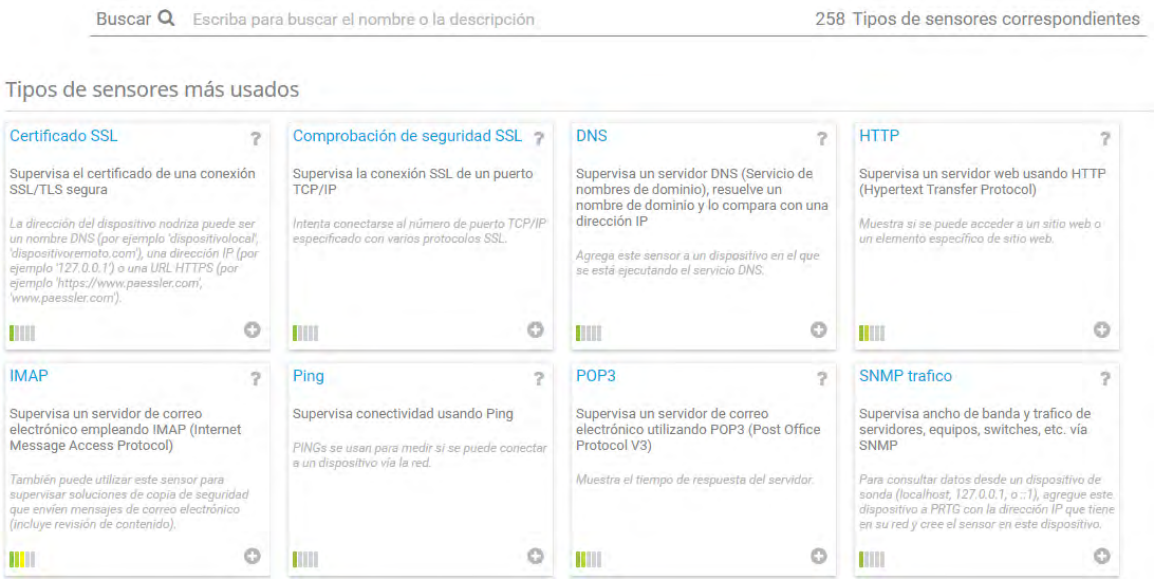


Figura 65. *Tipos de sensores*
Fuente: *Elaboración propia*

- Y se da clic en el sensor requerido.

Como un administrador de la red debemos tener en cuanta un monitoreo sobre el tráfico de la red. Y una dirección IP puede utilizar tanto ancho de banda que pueda tener alguna consecuencia negativa en toda la red. Por lo que se puede evitar los problemas de tráfico a largo plazo y optimizará el rendimiento de su red.

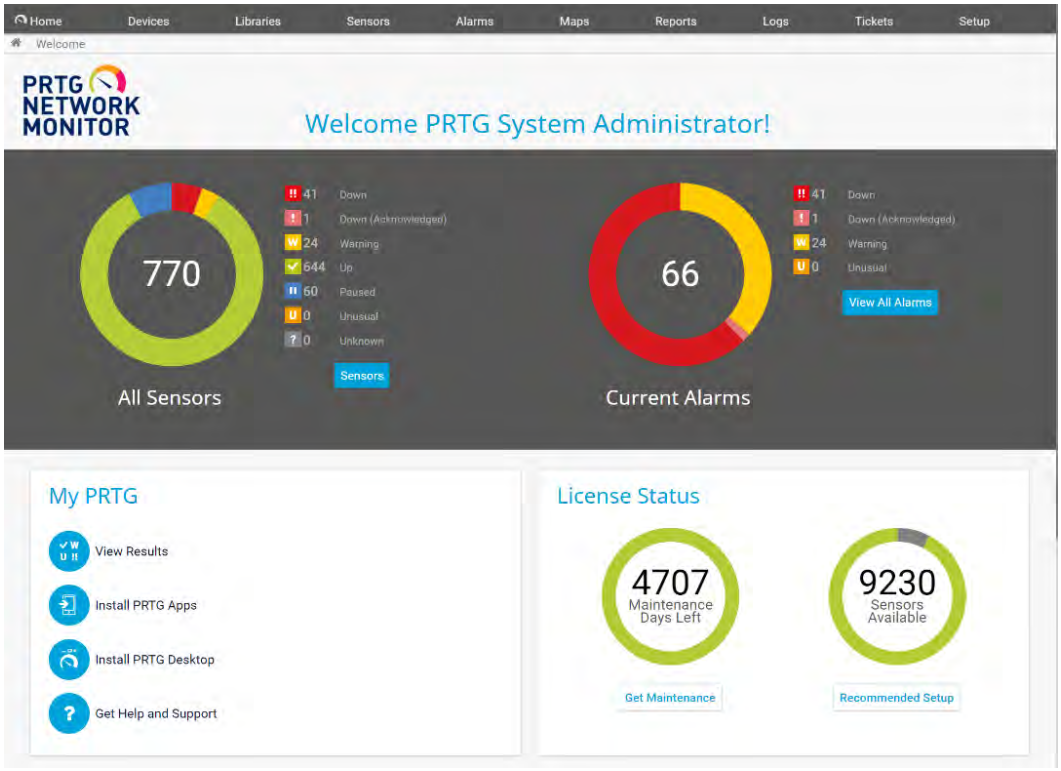
Una vez que se agregan los dispositivos para el monitoreo, la página principal se observa de la siguiente manera donde se encuentra la Sede principal con los equipos y sus tres almacenes Querétaro, Puebla e Hidalgo.

Figura 66. *Monitoreo de la sede principal y almacenes*
Fuente: *Elaboración propia*

Una vez implementadas las herramientas de monitoreo de los equipos de red se debe verificar y probar el cumplimento de los requerimientos mencionados. También se desarrollan políticas de monitoreo, evaluación y control de fallas en la red de datos para la empresa de distribución.

Para la supervisión de la actividad de la red, la herramienta PGRT tiene plug-ins el cual se puede convertir en un tablero, agregando ventajas como visualización de estado, capacidad, tolerancias, alertas y más. Además de la pantalla de inicio, el complemento crea pestañas con servicios adicionales como:

Consola: Esta es la parte más grande e importante de la herramienta PGRT, se proporciona de forma predeterminada y admite la configuración completa del software. Desde el menú del panel de control, puede realizar las siguientes acciones.



- Agregar, modificar y eliminar, nuevos dispositivos para monitoreo.
- Importar, generar y exportar plantillas para casi todos los complementos.
- Administrar cada uno de los plug-in, instalación, desinstalación.
- Crear los árboles de las gráficas y gestionar los mismos.
- Editar cualquier parámetro que se requiera de configuración de complemento o dispositivo ingresado a monitoreo.
- Ingreso de indicadores para realizar toma de medidas, umbrales, y reportes.

Figura 67. *Consola de PGRT*
Fuente: *Elaboración propia*

Gráficas: Con esta opción se pueden encontrar gráficas de dispositivos importados para monitoreo, gráficas similares dependiendo del tipo y modelo de dispositivo, de manera que se represente gráficamente mayor cantidad de información, como es el caso de los dispositivos cisco, se obtiene mucha información como se muestra en la Figura 68, donde datos como:

- Capacidad de tráfico por interfaces.
- Usabilidad de procesamiento.
- Cantidad de uso de memoria.
- Capacidad de almacenamiento y disponibilidad.
- Voltaje y temperatura del equipo.
- Tiempo de disponibilidad de un dispositivo (uptime), entre otros.

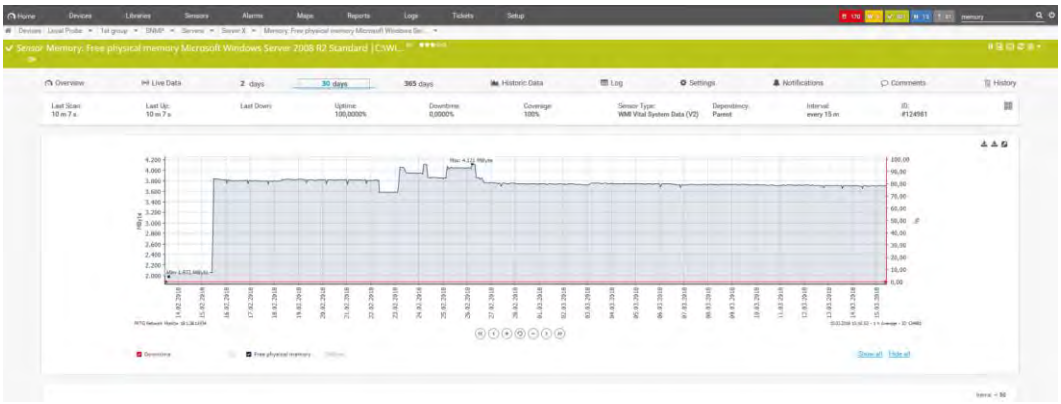


Figura 68. *Gráficas de PGRT*
Fuente: *Elaboración propia*

Se ingresa a un gráfico en particular puede ver el historial de la instalación y el dispositivo que se está monitoreando, por ejemplo si ingresa a la configuración de tráfico de la interfaz Ethernet puede ver claramente su progreso desde que se creó. Además, existe la posibilidad de visualizar el estado del tráfico o parámetros en tiempo real.

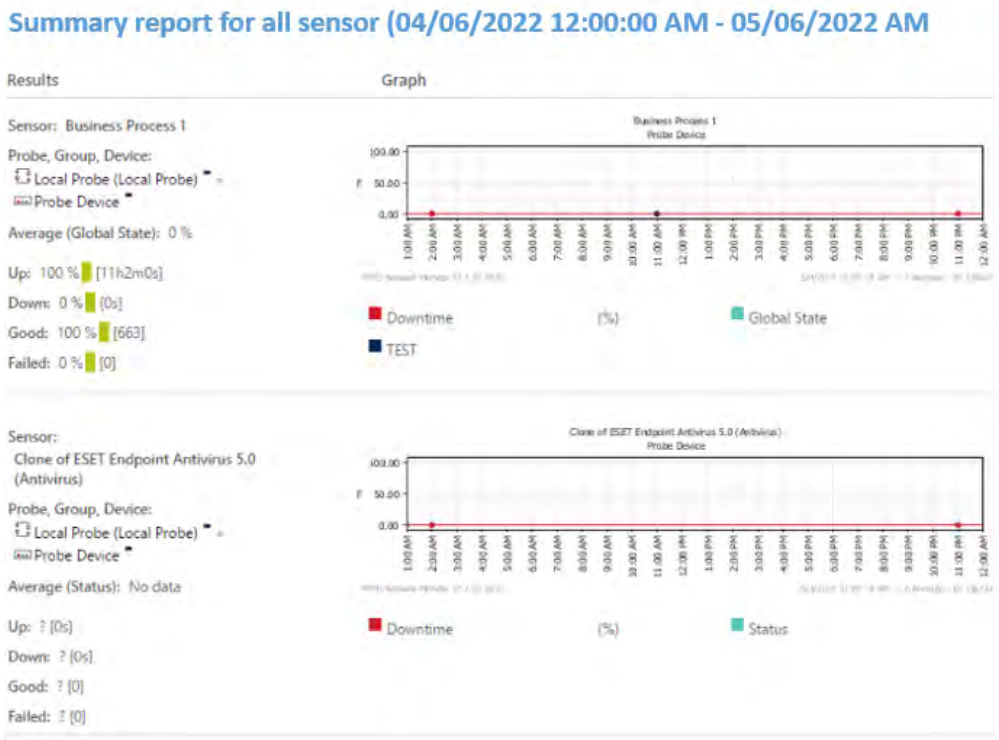


Figura 69. *Estado del tráfico del equipo*
Fuente: *Elaboración propia*

Registro del sistema: En este complemento permite centralizar todos los eventos que ocurren en cada dispositivo, y cada dispositivo debe configurarse para que envíen esta información a esta tienda.

Como en el ejemplo de la Figura 70, se puede ver el almacenamiento de información sobre eventos que han ocurrido en el dispositivo base o un punto de acceso, tiene varios eventos y se envía a este colector de datos con estos eventos puedes aplicar diferentes filtros y crear alarmas si es necesario.

Figura 70. *Registro en el sistema del equipo de red*
Fuente: *Elaboración propia*

Monitor: Este complemento muestra un diagrama con los dispositivos ingresados en la configuración para monitorear, pero solo aquellos que han sido seleccionados para mostrar en esta sección, ya que se puede configurar de tal manera que los dispositivos puedan estar o no en esta sección, en la siguiente figura se muestra un ejemplo.

Figura 71. *Monitoreo de los equipos de red*
Fuente: *Elaboración propia*

Alarmas: su principal función para configurar los equipos es que se deben de realizar ciertas notificaciones de alarmas esto informará inmediatamente que sucede algún comportamiento extraño sobre cualquier dispositivo.

Las notificaciones se configuran directamente sobre cada sensor debido a que cada uno registra una información diferente. PRTG tiene dos tipos de notificaciones, uno que informe si cambia el estado del sensor.

Es decir si el sensor deja de recibir información o cambia su comportamiento normal se alarma o queda en estado de “alerta” e informa inmediatamente sobre lo que puede estar sucediendo y el otro que informe cuando llegue a un umbral de operación anormal.

Nos apoyamos con esta aplicación para la simulación de fallas esto con el fin de validar si la notificación se realiza adecuadamente. Para esto nos colocamos donde está el sensor y damos clic en “Simular estado de error” el sensor cambiara de color verde a amarillo y por lo tanto rojo.

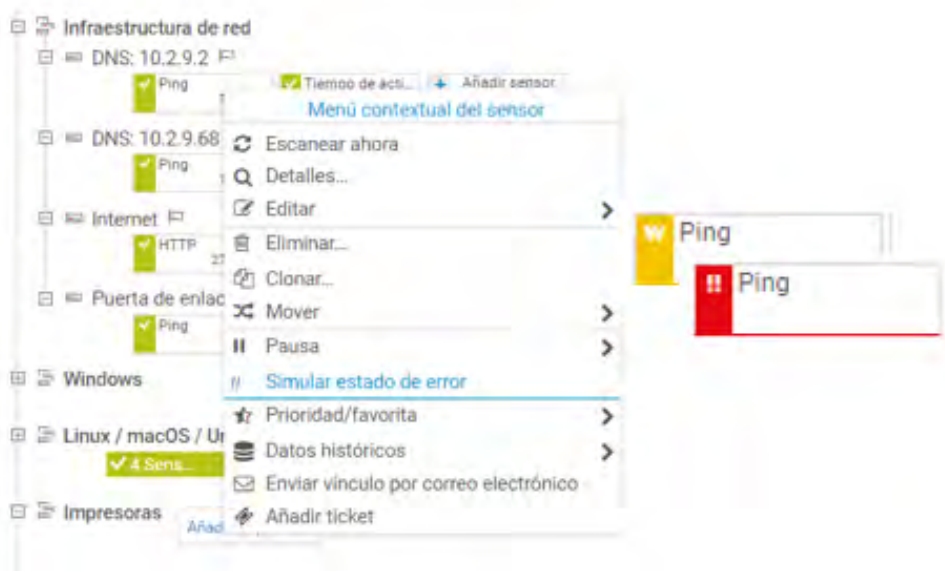


Figura 72. *Simulación del estado de error de equipos de red*
Fuente: *Elaboración propia*

Cuando se realiza esta simulación de error podemos ver como la aplicación de monitoreo nos ayuda inmediatamente a identificar en que equipo se está presentando el problema y así poder obtener un log para realizar un análisis del porque se está perdiendo la comunicación con el equipo, también nos ayuda a validar cuanto tiempo se tarda en que el equipo identifique que tiene un problema.

Donde se observa la gráfica con pérdida el equipo y se puede obtener su log.

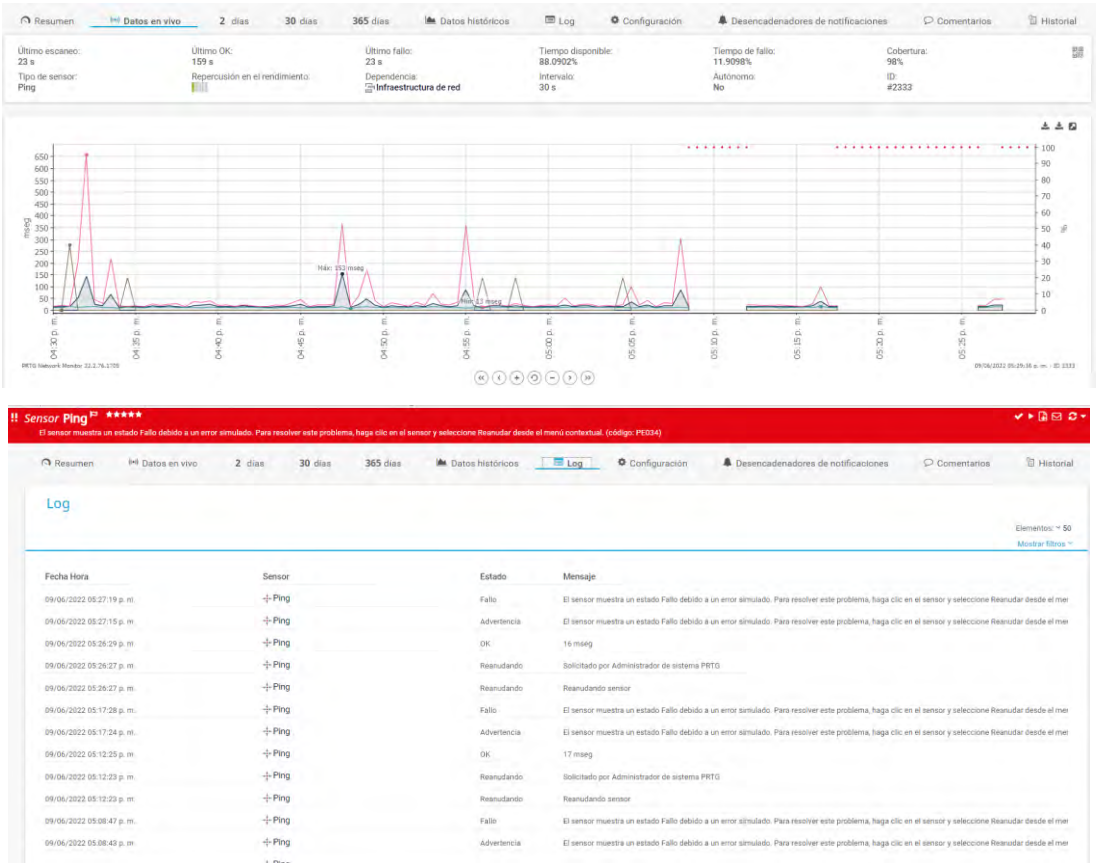


Figura 73. *Logs de equipos de red*
Fuente: *Elaboración propia*

Cada que un dispositivo se alarme se podrá adjuntar el ticket con el cual se llevará acabo para la solución de la falla.

Figura 74. Añadir ticket para el dispositivo
Fuente: *Elaboración propia*

En esta opción nos solicita el asunto y el grupo asignado para esta solución y se enviara un correo de notificación del ticket.

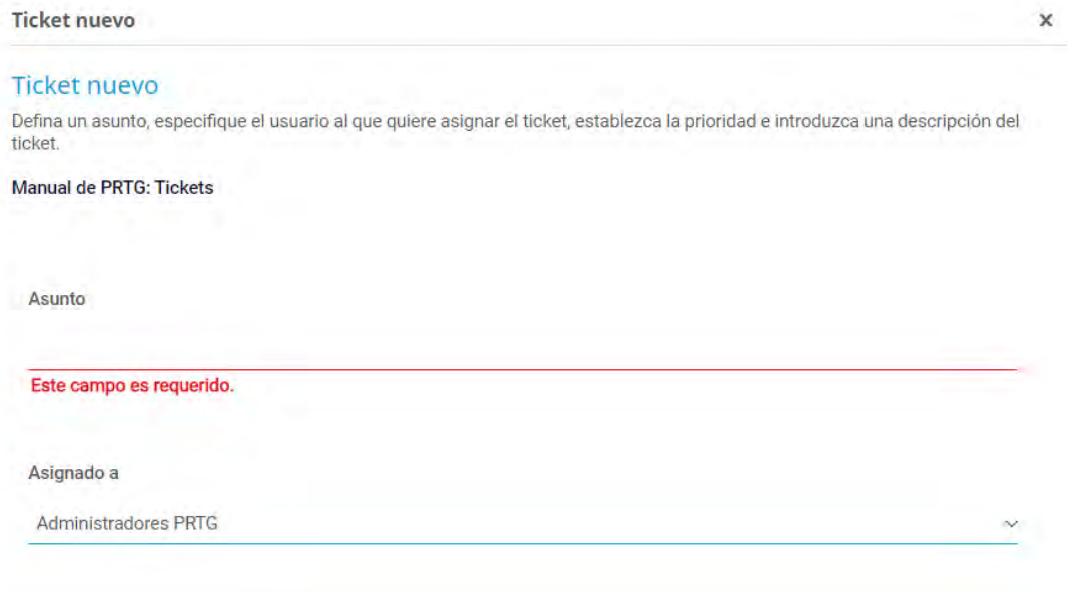


Figura 75. *Ticket nuevo*
Fuente: *Elaboración propia*

Las direcciones IPv4 de los dispositivos que respondió al envío del traps SNMP durante 1 minuto se resume en el nombre del dispositivo al que pertenecen, que corresponde a todas las unidades que forman parte de la sede y almacén.

Tabla 35. *Resumen de dispositivos*

Sede principal	Almacenes
10.255.255.2	R2_CORP_CDMX
10.255.255.3	R1_CORP_CDMX
10.255.255.4	R1_TALLER_CDMX
10.255.255.5	R1_CDMX_COR
10.255.255.8	R4_CDMX_COR
10.255.255.9	R1_QRO_AL
10.255.255.10	R2_CDMX_COR
10.255.255.11	R5_CDMX_COR
10.255.255.12	R1_PUE_COR
10.255.255.13	R3_CDMX_COR
10.255.255.14	R1_HGO_AL

La información consignada en la Tabla 34 son los dispositivos que se integraron en la maqueta para validar la implementación tanto de los equipos de la sede principal como de sus almacenes esta tabla ayudara al departamento de Sistemas para que pueda identificar la IP, el equipo y su ubicación que es una prioridad.

El resumen de todo el proceso de Implementación para el monitoreo de los equipos de red y las actividades que con lleva como el resultado, el costo y el tiempo empleado se observa a continuación:

Tabla 36. *Resumen del proceso de implementación*

ACTIVIDAD	RESULTADO	TIEMPO EMPLEADO	COSTO
Comprar Licencia Windows server	Compra aprobada	30min	$1,750
Instalación Servidor Virtual	Instalación exitosa	60min	NA
Ingresar a la página web del proveedor	Ingreso correctamente	10min	NA
Descargar la versión de prueba	Descarga exitosa	10min	NA
Instalar la aplicación	Instalación completa	30min	NA
Configurar la cuenta de correo del administrador	Configuración correcta	10min	NA
Ingresar la clave o key-id	Ingreso exitoso	1min	NA
Seleccionar la ubicación de los archivos de instalación	Selección correcta	5min	NA
Crear Usuario Administrador	Creado correctamente	5min	NA
Ingresar los equipos a monitorear	Ingreso exitoso	10min c/u	NA
Configurar los Grupos	Configuración correcta	10min c/u	NA
Configurar los Aparatos	Configuración correcta	10min c/u	NA
Configurar los Sensores	Configuración correcta	10min c/u	NA
Crear notificaciones y alertas	Creación exitosa	20min c/u	NA
Agregar la ubicación física de los equipos	Agregación exitosa	20min c/u	NA
Configurar la Comunidad SNMP	Configuración operativa	10min c/u	NA
Simulación de prueba	Simulación exitosa	20min c/u	NA
Monitoreo del ingeniero	Ingeniero de Sistemas	480min	$26,000 c/meses
Integración de equipos por almacen	Ingeneiro de Sistemas	57,600 min	$210,000 c/6 meses
Total	19 actividades	58,351 min	$237,750

Como se observa en la tabla anterior hay actividades que solo se realizaron una sola vez como la compra y su instalación, también especifica el costo y el tiempo que se requiere para la integración de los equipos de red por cada almacén y el monitoreo que tendrá que desempeñar el ingeniero de Sistemas por mes. Se agrega el tiempo que se requiere en agregar un dispositivo y el sensor esto con lleva la configuración en el router o switch de la comunidad SNMP. En el monitoreo del ingeniero desempeña la realización de tickets y seguimiento de las fallas que se vayan presentando.

TRABAJOS A FUTUROS

A nivel general este proyecto se puede implementar este proyecto y poder contribuir con la mejora continua en el área de Sistemas de la empresa de distribución. Para ello se recomienda realizar esta implementación e ir integrando los almacenes cada seis meses e ir obteniendo reportes constantes de los equipos de la sede principal para poder validar su comportamiento de la aplicación y poder capacitar al ingeniero de Sistemas sobre cómo utilizar la aplicación y poder identificar los equipos y realizar un análisis.

En primer lugar se recomienda gestionar la mayor cantidad de dispositivos que conforman la red de la sede principal, de esta manera se podrán realizar un proceso de gestión. En segundo lugar se recomienda empezar a realizar las configuraciones de los equipos de algún almacén cercano para poder irlo agregando a la aplicación de monitoreo e ir solucionando inconvenientes que se vayan presentando en la configuración de router y switches.

A medida que crecen sus operaciones e infraestructura, se recomienda comprar una licencia más grande que le permita aumentar la cantidad de sensores, instalar sondas o administración en varios servidores y poder recibir soporte y actualizaciones ilimitadas. De esta forma, es posible no solo monitorear más dispositivos, sino también establecer un proceso operativo general en el área del sistema.

Finalmente, para mejorar el proceso de operaciones del servicio, se recomienda que se implemente el siguiente proceso de gestión de incidentes basado en la información obtenida de su aplicación. Esto no solo minimiza la falla de uno o más servicios, sino que también aumenta los valores de disponibilidad y calidad del servicio.

Este proceso se muestra en la siguiente imagen.

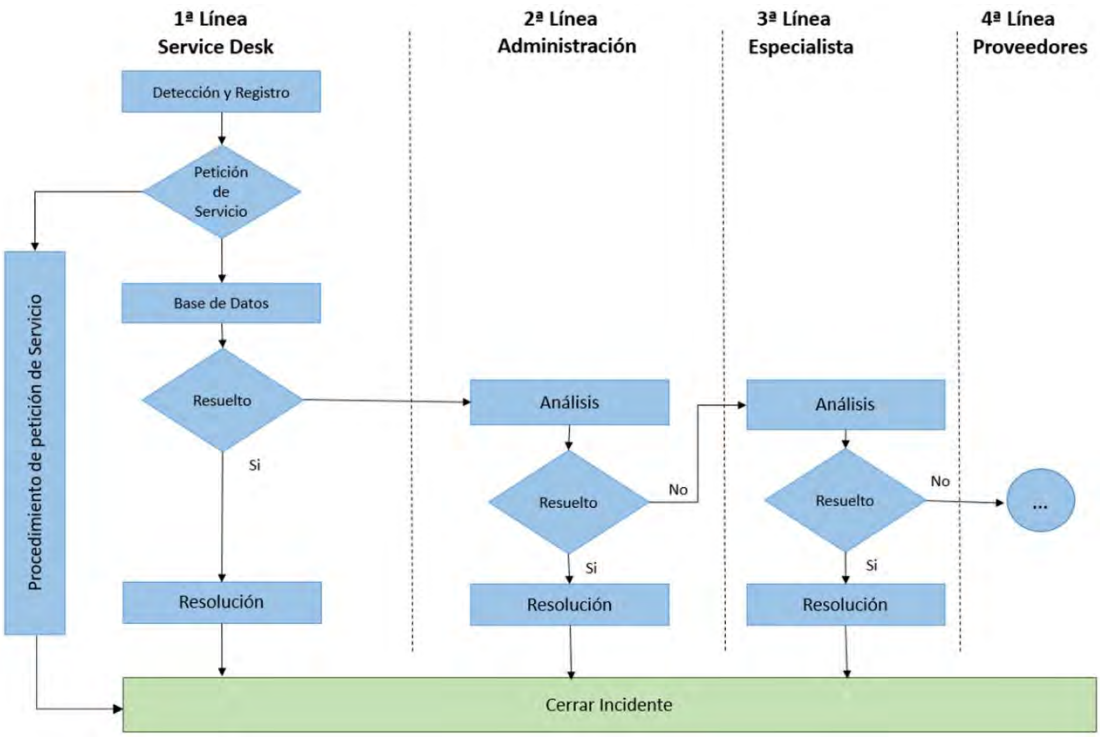


Figura 76. *Diagrama del proceso de Gestión de Incidentes*
Fuente: *Elaboración propia*

En la tabla 37 se describe brevemente el proceso propuesto para poder ser implementado en la empresa de distribución.

Tabla 37. *Descripción del proceso*

Registro	El proceso inicia con la detección del incidente que puede ser ocasionado por una falla en un dispositivo, un servicio o un error humano, por esta razón el registro es la primera actividad que se debe realizar para iniciar con las labores pertinentes para solucionar el incidente. La información que contiene el registro generalmente es la hora, una descripción breve de lo que sucede, sistemas afectados, entre otros. El registro también funciona como mecanismo para informar a la organización y los clientes acerca del incidente.
Clasificación	El objetivo de la clasificación es determinar el impacto y la urgencia del incidente con el fin de realizar el despliegue adecuado de los recursos y capacidades que requiera para darle solución eficazmente, por lo general son clasificados dependiendo si afecta o no uno o más servicios de la organización. También en la clasificación se establece si el incidente debe ser escalado con un cliente o proveedor dependiendo del caso.
Análisis	Dependiendo si afecta o no uno o más servicios. En esta fase la idea es consultar la base de datos con la información de otros incidentes con el fin de verificar si anteriormente sucedió alguno igual o similar y ejecutar el procedimiento realizado. De no ser el caso se procede a realizar las pruebas para establecer la causa. Si no se logra establecer la causa se recomienda escalarlo con el siguiente nivel o grupo de expertos en el caso.
Solución	Es la fase donde finaliza el incidente, las actividades incluyen documentar las acciones realizadas por los encargados o proveedores e informar a la organización y a los clientes que el incidente ya fue solucionado.
Cierre	El cierre incluye un informe detallado de todo lo referente a la causa, actividades realizadas y como se solucionó el incidente. Este informe debe ser almacenado en una base de datos con el fin de consultar el procedimiento realizado a fin de solucionar un nuevo incidente en un tiempo menor.

CONCLUSIONES

Se analizaron los procesos de gestión de redes y servicios de las operaciones de una empresa de distribución, donde se conocieron las principales razones por las que la empresa en su sede principal y almacenes requiere implementar un sistema de monitoreo de equipos y distribución que permita lograr una gestión eficaz de los elementos de la infraestructura de telecomunicaciones y, en consecuencia, de las actividades económica de la empresa.

El protocolo SNMP implementado en los equipos contribuye significativamente a obtener información relevante de los dispositivos incluidos en la infraestructura de comunicación de los equipos de la sede principal y almacenes, lo que da como resultado logs históricos de fallas en los equipos de la red.

El establecimiento de PRTG NETWORK MONITOR como una herramienta adecuada para la implementación empresarial permitió un marco funcional, adaptable y extensible para cumplir con los requisitos de mejorar la red.

El sistema de información en el monitoreo de los equipos para una empresa de distribución permitió mejorar el desempeño del dominio técnico y en general alcanzar un rendimiento en los almacenes que se traduce en un ahorro en tiempo y dinero, y una mayor eficiencia en los procesos que se llevan a cabo.

GLOSARIO

A

ARPANET (Advanced Research Projects Agency Network)

Fue una red de computadoras creada por encargo del Departamento de Defensa de los Estados Unidos para utilizarla como medio de comunicación entre las diferentes instituciones académicas y estatales.

ADMINISTRADOR

El administrador principal de una red. Normalmente el administrador tiene permisos para realizar cualquier tarea en una red y acceder a cualquier recurso, además puede asignar permisos a los usuarios nuevos.

ANCHO DE BANDA

Capacidad de un cableado en bits por segundos. También se utiliza este término para describir la capacidad de rendimiento medida de un medio o un protocolo de red específico.

B

BACKUP/RESPALDO

Copia de archivos virtuales, configuraciones o bases de datos a un sitio secundario para su preservación en caso de falla del equipo.

BANDA ANCHA

Modalidad de transmisión de red que utiliza la señalización análoga para enviar información sobre un amplio rango de frecuencias.

C

CLIENTE

Estación de trabajo de una red que solicita y recibe servicios de un servidor de red. Los clientes de red solicitan los servicios del servidor de la red.

CLOUD/NUBE

Servicios o capacidades de gestión de forma remota desde internet, en el aspecto de equipos para WiFi puede hacer referencia al control y administración de las redes inalámbricas desde internet por medio de un controlador.

D

DEFAULT IP

Dirección IP que tiene por defecto un equipo en valores de fábrica.

DIRECCIÓN IP (PROTOCOLO DE INTERNET)

Es la dirección de red o lógica de un nodo. Está compuesta de hasta cuatro números de ocho bits (cada uno de ellos llamado octeto) que se combinan para identificar no solo la estación de trabajo o nodo, sino también su red. La dirección IP identifica una estación de trabajo con la LAN, WAN e Internet.

E

ENRUTAMIENTO

Proceso utilizado para determinar la mejor ruta y hacer avanzar la información a lo largo de esa ruta, a partir de una red fuente o segmento de red, hacia una dirección de red de destino.

ETHERNET

Estándar de redes de área local para computadoras, define las características de cableado y señalización; de nivel físico y los formatos de tramas de datos del nivel de enlace de datos del modelo OSI.

EXTENSOR WIFI

Dispositivo que puede tomar la señal de un WiFi principal y extenderlo a zonas donde no alcanzaba cobertura.

F

FIREWALL

Router o servidor de acceso o varios routers o servidores de acceso designados como búfer entre cualquier red pública conectada y una red privada. Un router firewall utiliza listas de acceso así como otros métodos para garantizar la seguridad de la red privada.

G

GRUPO DE TRABAJO

Conjunto de estaciones de trabajo y servidores de una LAN que se designan para comunicar e intercambiar datos entre sí.

H

HARDWARE

Parte física de un equipo.

HTTP HYPERTEXT TRANSFER PROTOCOL

Es el protocolo de comunicación que permite las transferencias de información en la World Wide Web.

HTTPS HYPERTEXT TRANSFER PROTOCOL SECURE

Es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto.

I

IP

Protocolo de capa de red de la pila TCP/IP que ofrece un servicio de internetwork no orientada a la conexión. El IP brinda funciones de direccionamiento, especificación del tipo de servicio, fragmentación y re ensamblaje, y seguridad.

IP DINÁMICA

Dirección IP obtenida de forma automática desde un servidor DHCP.

IPv4

Protocolo de Internet utilizado actualmente para las direcciones IP de los dominios y dispositivos.

L

LAN (LOCAL AREA NETWORK):

Red de área local que consiste en dos o más nodos, generalmente en un área relativamente pequeña (local). Las estaciones de trabajo de una LAN se conectan con el propósito principal de compartir información y recursos locales. Típicamente, una red casera es una LAN, así como la red de una oficina pequeña o la red de una planta manufacturera.

M

MASCARA DE DIRECCIÓN

Combinación de bits utilizada para describir cuál es la porción de una dirección que se refiere a la red o subred y cuál es la que se refiere al host. A veces se la llama simplemente máscara.

MODELO OSI

Modelo de referencia de interconexión de sistemas abiertos, un estándar que define las diversas funciones denominadas capas, que un paquete de red transmite al trasladarse desde una fuente hasta su destino. El modelo OSI de siete capas se aplica tanto a las redes locales como a las extensas, entre ellas Internet.

N

NCP (Network Control Program)

Fue la base de las comunicaciones entre sistemas pertenecientes a ARPANET hasta 1981, cuando se diseñó TCP/IP para permitir un mejor crecimiento de la red.

NODO

Una estación de trabajo en red o cualquier otro dispositivo unido a la red. Un nodo, término derivado de la palabra nódulo, es de hecho el punto de referencia que utiliza la red para identificar lo que esté unido a la red.

NTP Network Time Protocol.

Protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes.

P

PAQUETE

Un pequeño haz de información de longitud variable, que generalmente tiene de 256 a 2,000 bytes de longitud.

PROTOCOLO

Reglas de comunicación bajo las cuales opera la red. Un protocolo prescribe la manera como se formatean y transmiten las solicitudes, los mensajes y otras señales a través de la red.

PING

Utilidad de diagnóstico en redes de computadoras que comprueba el estado de la comunicación del anfitrión local con uno o varios equipos remotos de una red que ejecuten IP.

PUERTO FÍSICO

Ranura que porta una computadora personal. Esta ranura tiene la capacidad de que se le introduzca un cable de red con el cual el dispositivo se conectará a la señal del router.

R

RED

Dos o más computadoras o dispositivos periféricos, como impresoras, torres de CD-ROM, escáners y dispositivos semejantes, que están directamente conectados con el propósito de compartir el hardware, el software y los recursos de información de los dispositivos conectados.

S

SEGMENTO DE RED

Sinónimo de LAN; es un conjunto de equipos (computadoras y periféricos) conectados en red, pertenecen al mismo segmento de direccionamiento IP.

SNMP

Simple Network Management Protocol, es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red, normalmente para el monitoreo de un equipo.

T

TCP

Protocolo de la capa de transporte orientado a conexión que proporciona una transmisión confiable de datos de full dúplex. TCP es parte de la pila de protocolo TCP/IP.

TCP/IP

Probablemente el protocolo más común utilizado en las redes modernas. El TCP/IP es de hecho una pila de protocolos, cada uno de los cuales establece las reglas y los estándares para una acción de red específica.

TOPOLOGÍA

Organización física de la red. De bus, de anillo y de estrella son las topologías más comunes de las redes.

V

VLAN VIRTUAL LOCAL AREA

Es un método para crear redes lógicas independientes dentro de una misma red física.

W

WLAN WIRELESS LOCAL AREA NETWORK

Es un sistema de comunicación inalámbrico.

REFERENCIAS

(06 de 01 de 2022). Obtenido de Network Monitoring Software - ManageEngine OpManager: https://www.manageengine.com/es/network-monitoring/what-is-snmp.html#snmp-manager

Ackoff, R. L. (1992). *Rediseñando el futuro,.* México: Limusa Editores.

Barba MArtí, A. (1999). *Gestion de Red.* Venezulea: UPC.

Barba Martí, A. (1999). *Gestión de Red.* Venezuela: UPC.

BERTOGLIO, O. J. (1994). *Introducción a la Teoría General de Sistemas.* Noriega: Limusa.

Capterra. (12 de 1 de 2017). Obtenido de https://www.capterra.mx/software/135902/zabbix-monitoring-solution#features

Checkland Peter, S. J. (1999). Soft Systems Methodology in Action. En *Soft Systems Methodology in Action.* Wiley.

Chuchman, C. W. (1993). *El enfoque de sistemas para la Toma de Decisiones .* CDMX: Diana. Obtenido de http://dicyg.fi-c.unam.mx:8080/sistemas/publicaciones/TEMAII.5.pdf.

Conceptos básicos de la supervisión de la red. (2 de 12 de 2020). Obtenido de https://www.motadata.com/es/what-is-network-monitoring/

Forouzan, B. A. (2013). *TCP/IP Protocol Suite.* McGraw-Hill.

Gigch, J. P. (2006). *TEORIA GENERAL DE SISTEMAS.* CDMX: Trillas.

Gigch, J. P. (2006). Teoría General de Sistemas. En J. P. Gigch, *Teoría General de Sistemas.* Mexico: Trillas.

https://www.paessler.com/es/prtg. (10 de 01 de 2022). Obtenido de https://www.paessler.com/es/prtg: https://www.paessler.com/es/prtg

Livas, L. (1988). *Cibernética, Estado y derecho .* México: Gernika.

Manageengine. (12 de 11 de 2020). Obtenido de https://download.manageengine.com/network-performance-management.html?pos=MEhome&loc=SecondScroll&cat=AllSol&prev=AB2

Miklos, T. (2001). *Criterios básicos de planeación.* México: Siglo XXI.

(1998). *Modelo de referencia de interconexión de sistemas abiertos.* Recomendación X.200 del CCITT.

Morrisey, G. L. (1996). *Pensamiento estratégico.* México: Prentice Hall.

Nagios. (15 de 1 de 2018). Obtenido de https://www.nagios.org/

Pandora FMS. (02 de 01 de 2022). Obtenido de https://pandorafms.com/blog/es/herramientas-de-monitoreo-de-redes/

Planificación y Gestión de Red. (2010). Obtenido de https://www.urbe.edu/info-consultas/web-profesor/12697883/archivos/planificacion-gestion-red/Unidad-I.pdf

Redes Informaticas. (10 de Abril de 2018). Obtenido de http://redesinformaticas4to.blogspot.com/p/origen.html

Samperieri, H. R. (1991). Metodología de la Investigación. En H. R. Samperieri, *Metodología de la Investigación.* Mc. Graw Hill.

SolarWinds . (02 de 11 de 2019). Obtenido de https://www.solarwinds.com/es/server-application-monitor

Stallings, W. (2006). *Comunicaciones y Redes Computacionles.* Mexico: Prentice Hall.

Wetherall, T. |. (2012). *REDES DE COMPUTADORAS.* CIUDAD DE MEXICO: PEARSON.

Wetteroth, D. (2002). “OSI Reference Model for Telecomunications”. USA: Mc Graw Hill.

Wetteroth, D. (2002). OSI Reference Model for Telecomunications. En D. Wetteroth, *OSI Reference Model for Telecomunications.* USA: Mc Graw Hill.

Wiener, N. (1948). *Cybernetics, or Control and Communication in the Animal and the Machine.* Cambridge: MIT Press.

BIBLIOGRAFIA

(06 de 01 de 2022). Obtenido de Network Monitoring Software - ManageEngine OpManager: https://www.manageengine.com/es/network-monitoring/what-is-snmp.html#snmp-manager

Ackoff, R. L. (1992). *Rediseñando el futuro,.* México: Limusa Editores.

Barba MArtí, A. (1999). *Gestion de Red.* Venezulea: UPC.

Barba Martí, A. (1999). *Gestión de Red.* Venezuela: UPC.

BERTOGLIO, O. J. (1994). *Introducción a la Teoría General de Sistemas.* Noriega: Limusa.

Capterra. (12 de 1 de 2017). Obtenido de https://www.capterra.mx/software/135902/zabbix-monitoring-solution#features

Checkland Peter, S. J. (1999). Soft Systems Methodology in Action. En *Soft Systems Methodology in Action.* Wiley.

Chuchman, C. W. (1993). *El enfoque de sistemas para la Toma de Decisiones .* CDMX: Diana. Obtenido de http://dicyg.fi-c.unam.mx:8080/sistemas/publicaciones/TEMAII.5.pdf.

Conceptos básicos de la supervisión de la red. (2 de 12 de 2020). Obtenido de https://www.motadata.com/es/what-is-network-monitoring/

Forouzan, B. A. (2013). *TCP/IP Protocol Suite.* McGraw-Hill.

Gigch, J. P. (2006). *TEORIA GENERAL DE SISTEMAS.* CDMX: Trillas.

Gigch, J. P. (2006). Teoría General de Sistemas. En J. P. Gigch, *Teoría General de Sistemas.* Mexico: Trillas.

https://www.paessler.com/es/prtg. (10 de 01 de 2022). Obtenido de https://www.paessler.com/es/prtg: https://www.paessler.com/es/prtg

Livas, L. (1988). *Cibernética, Estado y derecho .* México: Gernika.

Manageengine. (12 de 11 de 2020). Obtenido de https://download.manageengine.com/network-performance-management.html?pos=MEhome&loc=SecondScroll&cat=AllSol&prev=AB2

Miklos, T. (2001). *Criterios básicos de planeación.* México: Siglo XXI.

(1998). *Modelo de referencia de interconexión de sistemas abiertos.* Recomendación X.200 del CCITT.

Morrisey, G. L. (1996). *Pensamiento estratégico.* México: Prentice Hall.

Nagios. (15 de 1 de 2018). Obtenido de https://www.nagios.org/

Pandora FMS. (02 de 01 de 2022). Obtenido de https://pandorafms.com/blog/es/herramientas-de-monitoreo-de-redes/

Planificación y Gestión de Red. (2010). Obtenido de https://www.urbe.edu/info-consultas/web-profesor/12697883/archivos/planificacion-gestion-red/Unidad-I.pdf

Redes Informaticas. (10 de Abril de 2018). Obtenido de http://redesinformaticas4to.blogspot.com/p/origen.html

Samperieri, H. R. (1991). Metodología de la Investigación. En H. R. Samperieri, *Metodología de la Investigación.* Mc. Graw Hill.

SolarWinds . (02 de 11 de 2019). Obtenido de https://www.solarwinds.com/es/server-application-monitor

Stallings, W. (2006). *Comunicaciones y Redes Computacionles.* Mexico: Prentice Hall.

Wetherall, T. |. (2012). *REDES DE COMPUTADORAS.* CIUDAD DE MEXICO: PEARSON.

Wetteroth, D. (2002). “OSI Reference Model for Telecomunications”. USA: Mc Graw Hill.

Wetteroth, D. (2002). OSI Reference Model for Telecomunications. En D. Wetteroth, *OSI Reference Model for Telecomunications.* USA: Mc Graw Hill.

Wiener, N. (1948). *Cybernetics, or Control and Communication in the Animal and the Machine.* Cambridge: MIT Press.

ANEXO A

A continuación se muestra la configuración en los routers en cada uno cambia las IPs y se adjunta la configuración de SNMP y el protocolo OSPF

Tabla 38. *Configuración de los router*

```
R1_CORPO_CDMX#sh run
Building configuration...

Current configuration : 2425 bytes
!
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1_CORPO_CDMX
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
bsd-client server url
https://cloudsso.cisco.com/as/token.oauth2
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
no ip icmp rate-limit unreachable
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!

cts logging verbose
!
redundancy
!
ip tcp synwait-time 5
!
interface Loopback0
 description IP_GESTION
 ip address 10.255.255.1 255.255.255.255
!
interface Ethernet0/0
description A_LAN_SW_VIGILAN_1
 ip address 10.1.3.1 255.255.255.0
!
interface Ethernet0/1
 description A_R1_CDMX_COR
 ip address 10.2.1.9 255.255.255.252
!
interface Ethernet0/2
 description A_R1_TALLER_CDMX
 ip address 10.2.1.1 255.255.255.252
!
interface Ethernet0/3
 description A_R2_CORPO_CDMX
 ip address 10.2.1.6 255.255.255.252
!
interface Ethernet1/0 -----3
 no ip address
 shutdown
!
router ospf 1
 router-id 10.255.255.1
 network 10.1.3.1 0.0.0.0 area 1
 network 10.2.1.1 0.0.0.0 area 1
 network 10.2.1.6 0.0.0.0 area 1
 network 10.2.1.9 0.0.0.0 area 1
 network 10.255.255.1 0.0.0.0 area 1
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip access-list standard prtg-nms
 permit 192.168.0.11
!
snmp-server community monitoreo RO prtg-nms
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
 transport input none
!

end
```

A continuación se muestra la configuración en los switches en cada uno cambia las IPs y se adjunta la configuración de SNMP.

Tabla 39. *Configuración de los switches*

SW_TALLER_1#sh run		
Building configuration...	no ip icmp rate-limit unreachable	line con 0
	!	exec-timeout 0 0
Current configuration : 1368 bytes	no ip domain-lookup	privilege level 15
!	ip cef	logging synchronous
! Last configuration change at 13:08:38 UTC Fri Jun 10 2022	no ipv6 cef	line aux 0
!	!	exec-timeout 0 0
version 15.2	spanning-tree mode rapid-pvst	privilege level 15
service timestamps debug datetime msec	spanning-tree extend system-id	logging synchronous
service timestamps log datetime msec	!	line vty 0 4
no service password-encryption	vlan internal allocation policy ascending	login
service compress-config	!	!
!	ip tcp synwait-time 5	!
hostname SW_TALLER_1	!	end
!	interface Ethernet0/0	
boot-start-marker	!	
boot-end-marker	interface Ethernet0/1	
!	!	
!	ip access-list standard prtg-nms	
logging discriminator EXCESS severity drops 6	permit 192.168.0.11	
logging buffered 50000	!	
logging console discriminator EXCESS	snmp-server community monitoreo RO prtg-nms	
!	!	
no aaa new-model	control-plane	
!	!	

ANEXO B

A continuación se describirá el proceso de la instalación de la aplicación para el monitoreo de la red. La cual incluye imágenes paso a paso del procedimiento, el tiempo empleado en cada actividad.

Este proceso es realizado comúnmente cuando descargamos alguna versión de prueba gratuita y temporal de cualquier software que lo permite a través de una página web.

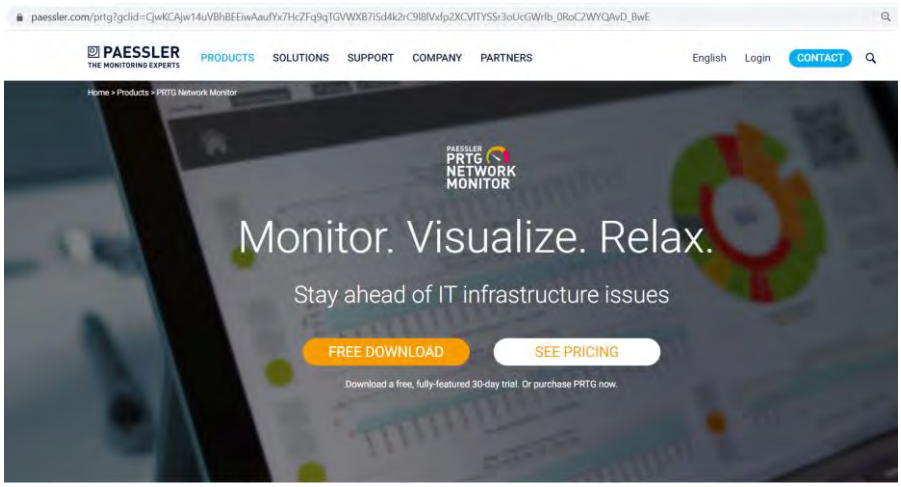


Figura 77. *Proceso de descarga*
Fuente: *(https://www.paessler.com/es/prtg, 2022)*

Para instalar aplicación luego de finalizar la descarga, en el Escritorio encontraremos el instalador que indica que ya es posible iniciar la instalación.

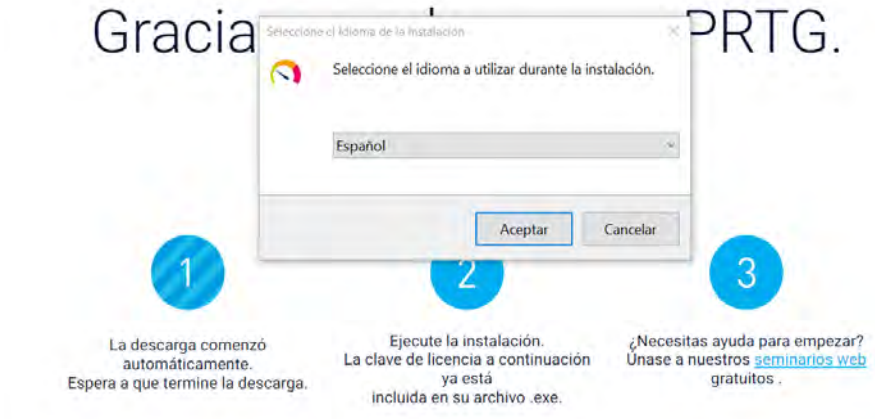


Figura 78. *Instalar aplicación*
Fuente: *(https://www.paessler.com/es/prtg, 2022)*

En este caso es la cuenta del ingeniero de Sistemas que podrá realizar los servicios y el modo de instalación

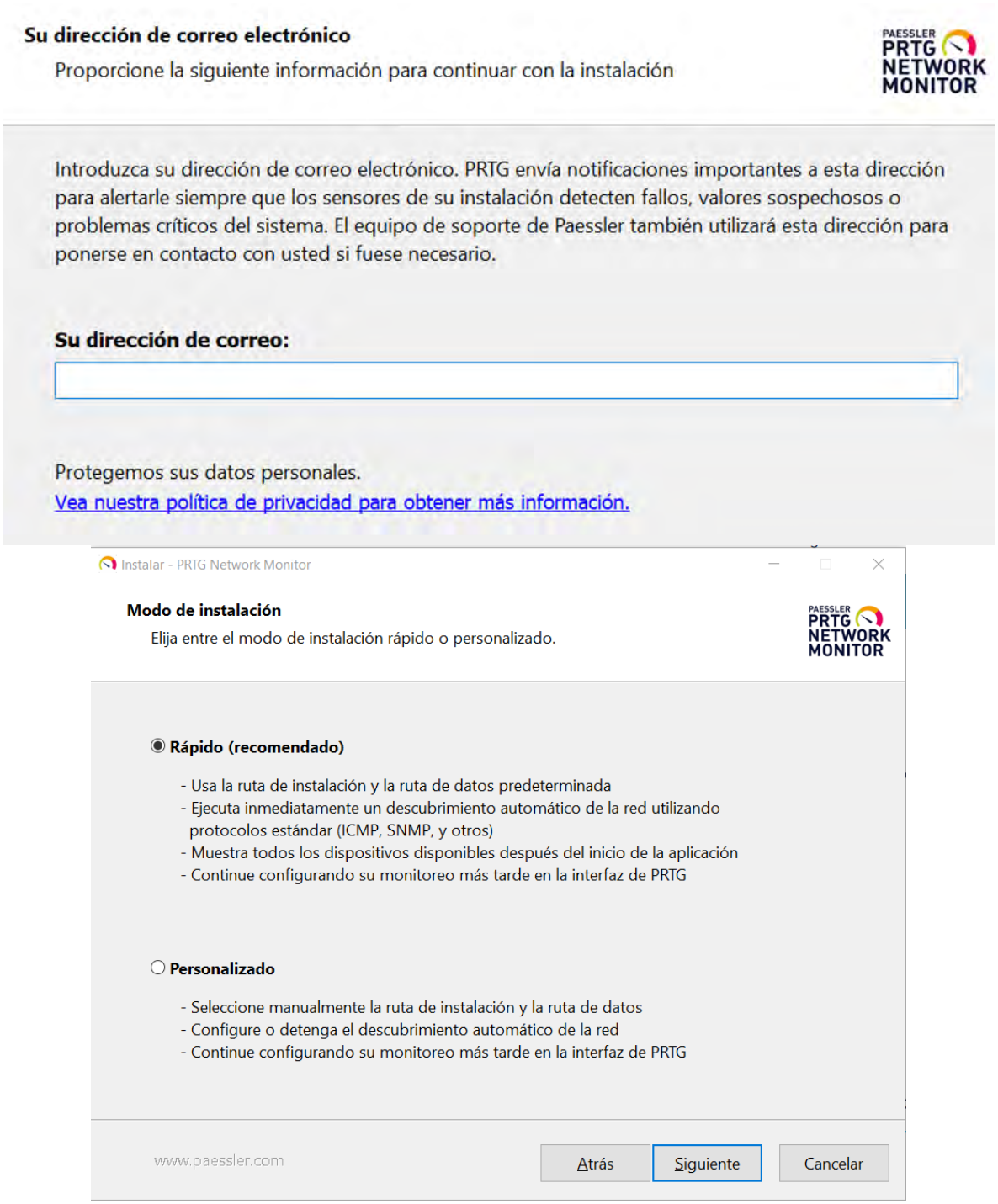


Figura 79. *Configuración de cuanta de correo*
Fuente: *(https://www.paessler.com/es/prtg, 2022)*

Nos debe mostrar el iniciode sesión de la aplicación, como se ilustra en la siguiente figura.

Figura 80. *Inicio de sesión PRTG NETWORK MONITOR*
Fuente: *(https://www.paessler.com/es/prtg, 2022)*

ANEXO C

EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA

Instituto Politécnico Nacional
"La Técnica al Servicio de la Patria"

XXI CONGRESO NACIONAL DE INGENIERÍA ELECTROMECÁNICA Y DE SISTEMAS

Otorga el presente

DIPLOMA

a

Cortés Rascón Belen

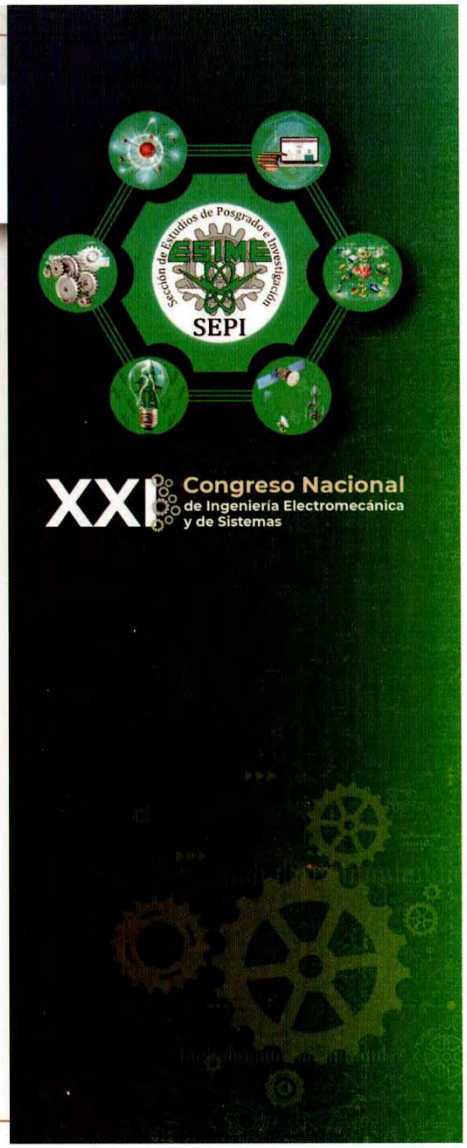
Por su participación como:

ASISTENTE

Ciudad de México, del 24 al 26 de octubre de 2022

DR. DAVID SEBASTIAN BALTAZAR
Coordinador General del CNIES 2022

DR. MAURO ALBERTO ENCISO AGUILAR
Director de la ESIME Unidad Zacatenco



EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA

Instituto Politécnico Nacional
"La Técnica al Servicio de la Patria"

XXI CONGRESO NACIONAL DE INGENIERÍA ELECTROMECÁNICA Y DE SISTEMAS

Otorga el presente

DIPLOMA

a

Belén Cortés Rascón, Miguel Ángel Martínez Cruz, Miguel Patiño Ortiz, Julián Patiño Ortiz, Eduardo Hernández Hernández

Por su participación como:

PONENTE

Con el trabajo:

Sistema de Información para el Monitoreo de Equipos de Red de datos de una Empresa de Distribución

Ciudad de México, del 24 al 26 de octubre de 2022

DR. DAVID SEBASTIÁN BALTAZAR
Coordinador General del CNIES 2022

DR. MAURO ALBERTO ENCISO AGUILAR
Director de la ESIME Unidad Zacatenco

EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA

Instituto Politécnico Nacional
"La Técnica al Servicio de la Patria"

XXI CONGRESO NACIONAL DE INGENIERÍA ELECTROMECÁNICA Y DE SISTEMAS

Otorga el presente

DIPLOMA

a

Belén Cortés Rascón, Miguel Ángel Martínez Cruz, Miguel Patiño Ortiz, Julián Patiño Ortiz, Eduardo Hernández Hernández

Por su participación como:

PONENTE

Con el trabajo:

Sistema de Información para el Monitoreo de Equipos de Red de datos de una Empresa de Distribución

Ciudad de México, del 24 al 26 de octubre de 2022

DR. DAVID SEBASTIÁN BALTAZAR
Coordinador General del CNIES 2022

DR. MAURO ALBERTO ENCISO AGUILAR
Director de la ESIME Unidad Zacatenco