



**UNIVERSIDAD POLITÉCNICA SALESIANA**  
**SEDE CUENCA**  
**CARRERA DE INGENIERÍA DE SISTEMAS**

“ANÁLISIS E IMPLEMENTACIÓN DE LA HERRAMIENTA NEDI PARA LA IDENTIFICACIÓN Y CATEGORIZACIÓN DE FALLOS EN UNA RED GPON; A NIVEL DE RED TRONCAL, RED DE DISTRIBUCIÓN Y DE ÚLTIMA MILLA PARA OPTIMIZACIÓN DE RECURSOS”

Trabajo de titulación previo a la obtención  
del título de Ingeniero de Sistemas

AUTORES: HERNÁN ALEJANDRO ASTUDILLO TORRES  
CRISTHIAN DAVID CABRERA GUERRERO  
TUTOR: ROBERTO AGUSTÍN GARCÍA VÉLEZ, PhD.

Cuenca - Ecuador  
2022

## **CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN**

Nosotros, Hernán Alejandro Astudillo Torres con documento de identificación N° 0104625165 y Cristhian David Cabrera Guerrero con documento de identificación N° 0105876049; manifestamos que:

Somos los autores y responsables del presente trabajo; y, autorizamos a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Cuenca, 26 de mayo del 2022

Atentamente,



---

Hernán Alejandro Astudillo Torres  
0104625165



---

Cristhian David Cabrera Guerrero  
0105876049

## **CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA**

Nosotros, Hernán Alejandro Astudillo Torres con documento de identificación No. 0104625165 y Cristhian David Cabrera Guerrero con documento de identificación No. 0105876049, expresamos nuestra voluntad y por medio del presente documento cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del Proyecto Técnico: “Análisis e implementación de la herramienta NeDi para la identificación y categorización de fallos en una red GPON; a nivel de red troncal, red de distribución y de última milla para optimización de recursos”, el cual ha sido desarrollado para optar por el título de: Ingeniero de Sistemas, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribimos este documento en el momento que hacemos la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Cuenca, 26 de mayo del 2022

Atentamente,



---

Hernán Alejandro Astudillo Torres

0104625165



---

Cristhian David Cabrera Guerrero

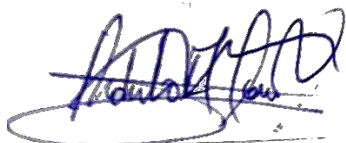
0105876049

## CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Roberto Agustín García Vélez con documento de identificación N° 0103650891, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: “ANÁLISIS E IMPLEMENTACIÓN DE LA HERRAMIENTA NEDI PARA LA IDENTIFICACIÓN Y CATEGORIZACIÓN DE FALLOS EN UNA RED GPON; A NIVEL DE RED TRONCAL, RED DE DISTRIBUCIÓN Y DE ÚLTIMA MILLA PARA OPTIMIZACIÓN DE RECURSOS”, realizado por Hernán Alejandro Astudillo Torres con documento de identificación N° 0104625165 y por Cristhian David Cabrera Guerrero con documento de identificación N° 0105876049, obteniendo como resultado final el trabajo de titulación bajo la opción Proyecto Técnico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Cuenca, 26 de mayo del 2022

Atentamente,



---

Roberto Agustín García Vélez, PhD  
0103650891

## **DEDICATORIA**

*Esta tesis está dedicada a: Mis padres Eliseo y Evelina que con su amor, crianza, educación y esfuerzo han formado un profesional más en la familia. A mis abuelos les agradezco también por siempre creer en mí y quienes con su apoyo incondicional me aconsejaron con su gran sabiduría para lograr afrontar muchos retos y adversidades.*

*A mis hermanas a quienes quiero mucho. A todos aquellos que en tiempos difíciles me han extendido la mano y me han ayudado en el pasado gracias. A mi familia en general, todos tuvieron mucha fe en mí y a aquellos que compartieron momentos en esta larga travesía, a mis amigos y futuros colegas que se han esforzado mucho para cumplir sus metas. En fin, quisiera extender un gran abrazo a todos mis allegados y recalcar mi gratitud una vez más, y desearles siempre lo mejor y muchos éxitos.*

***Hernán Alejandro Astudillo Torres***

## **DEDICATORIA**

*Este logro académico de enorme importancia en mi vida, se lo dedico especialmente a mi madre Enma, a mis abuelos Roberto y Delfa, a mi hermana, Sol Anahí, a mi prima María Paz, y a todos mis tíos/as, quienes creyeron siempre que podía lograr este, y todos los objetivos que me propusiera, si le dedicaba todo el esfuerzo y perseverancia que se necesita para alcanzar algo así; lo que al final se consiguió. Pero especialmente, esta meta alcanzada se la dedico a mi hermano Israel+ que siempre me cuida y me alienta a seguir, desde el lugar especial donde se encuentra, a pesar de todos los obstáculos que se pudieran presentar. Este trabajo va dedicado para todos ustedes que han creído siempre que el apoyo entre todos nosotros es lo más importante, y que cada uno debe alegrarse por el triunfo del otro.*

***Cristhian David Cabrera Guerrero***

## **AGRADECIMIENTOS**

*A nuestros padres por enseñarnos a ser mejores personas cada día, por darnos su apoyo incondicional en todo momento, y alentarnos a cumplir con esfuerzo y sacrificio, todas las metas que nos propusimos desde un inicio. También queremos agradecer a nuestros profesores, quienes, a través de todo el proceso educativo, nos han dado las herramientas necesarias para poder culminar con éxito nuestro proyecto de investigación, y, por ende, nuestro grado académico. A nuestro tutor de tesis, Roberto Agustín García Vélez, PhD, por las observaciones y correcciones pertinentes al documento, durante todo el proceso de análisis y redacción, para lograr un trabajo de alta calidad y relevancia académica. Finalmente, queremos agradecer a todos nuestros compañeros de estudio, por brindarnos su amistad, y compartir gratos momentos que nos ha enriquecido mucho como personas. Gracias a todos ustedes, que de una u otra manera han contribuido a alcanzar uno de nuestros grandes objetivos.*

***Hernán Alejandro Astudillo Torres***

***Cristhian David Cabrera Guerrero***

## **RESUMEN**

Varias empresas de telecomunicaciones e internet están tratando de contrarrestar los efectos de los soportes a usuarios finales ocasionados por fallos en la parte de última milla de redes GPON. De la misma manera, la importancia de adoptar y seguir las practicas recomendadas en cuanto a la instalación de equipos finales y adicionalmente la instalación e integración de un sistema de monitoreo en el nodo principal para el respectivo seguimiento y resolución de problemas relacionados con los fallos en el servicio.

El objetivo de este estudio es determinar los fallos comunes en las redes de última milla, verificar las causas de caídas del servicio en ciertos puntos. Con la implementación de la herramienta de monitoreo designada, se realizar el análisis y registro de los datos de fallos detectados. Empleando una arquitectura Cliente-Servidor, desarrollar una aplicación móvil que sirva de herramienta de monitoreo y notificaciones para el departamento técnico con el fin de optimizar los tiempos de respuesta.

La verificación del funcionamiento de la aplicación se llevó a cabo mediante una fase de pruebas comprobando que se cumplieron los objetivos funcionales y no funcionales propuestos. El producto final de la aplicación operativa detecta los fallos considerando la parte física de la red de última milla y las posibles causas de la caída del servicio con su respectiva solución sugerida. Aplicaciones y mecanismos de detección de fallos y monitoreo de redes similares serán de gran utilidad para las empresas de telecomunicaciones públicas y privadas.



## **ABSTRACT**

Many Internet Service Providers and telecommunication companies are looking to overcome the negative effects of handling customer support and technical assistance due to network failures in the last mile of a GPON structured network. In like manner, the importance of following best practices and recommendations when installing network devices on the user's residence and additionally the installation and integration of an NMS and monitoring tool at the central office to keep track of network failure and handle troubleshooting whenever necessary.

The goal of this research is to determine common network failures in last mile GPON networks, establish the main causes of service outages in several areas. The designated monitoring tool will be used to carry out the analysis and collect data pertaining to network failures. Additionally, with the use of a client-server architecture, the development of a mobile application that will bolster support for monitoring and notifications so that customer service may optimize response time.

Appropriate testing and assessment of the application will be carried out by stages or phases in which various app components, functional and non-functional goals are to be verified correctly. The final deployed application will detect several network failures considering last mile networks and possible cause for service outages providing a practical solution to each one of them as they are previously categorized. Similar applications and network fault detection mechanisms will certainly be very useful for all public and private ISPs.

## ÍNDICE DE CONTENIDO

### ABREVIATURAS Y SIMBOLOGÍA

SNMP	Simple Network Management Protocol
CDP	Protocolo de descubrimiento de Cisco.
DNS	(Domain Name System), Sistema de Nombres de Dominio.
DHCP	Dynamic Host Configuration Protocol
VPN	(Virtual Private Network), Red Privada Virtual.
VM	(Virtual Machine), Máquina Virtual.
PAN	Personal Area Network
LAN	Local Area Network
WAN	Wide rea Network
INEC	Instituto Nacional de Estadísticas y Censos.
PPPoE	Point-to-Point Protocol over Ethernet
RIP	Routing Information Protocol
IANA	Internet Assigned Number Authority

VLAN	Virtual Local Area Network
HTML	Hypertext Markup Language
OSI	Open System Interconnect
TCP/IP	Transmission Control Protocol – Internet Protocol
DMZ	Demilitarized Zone
SLA	Service Level Agreement
WMI	Window Management Instrumentation
OLT	Optical Line Termination
ONT	Optical Network Termination
ONU	Optical Network Unit
NAT	Net Address Translation
SLA	Service Level Agreement
OPM	Optical Power Meter
ODF	Optical Distribution Fibre
DBA	Dynamic Bandwidth Allocation

## **Contenido**

INTRODUCCIÓN.....	19
PROBLEMA DE ESTUDIO .....	20
JUSTIFICACIÓN.....	20
OBJETIVOS .....	21
OBJETIVO GENERAL.....	21
OBJETIVOS ESPECÍFICOS.....	21
CAPÍTULO 1 INTRODUCCIÓN AL ESTADO DEL ARTE .....	22
1.1 HERRAMIENTAS DE MONITOREO.....	22
1.1.1 NEDI.....	22
1.1.2 OBSERVIUM.....	23
1.1.3 PRTG .....	23
1.1.4 NAGIOS.....	23
1.1.5 ZABBIX .....	24
1.2 LENGUAJES DE PROGRAMACIÓN PARA MODELOS MATEMÁTICOS.....	25
1.2.1 PYTHON .....	25
1.2.2 MATLAB.....	26
1.2.3 JULIA.....	26
1.2.4 R.....	27
1.2.5 JAVA.....	27
1.3 ARQUITECTURAS DE RED. ....	28
1.3.1 MODELO OSI.....	28
1.3.2 TCP/IP .....	32
1.3.3 INTERNET.....	35
1.3.4 ARQUITECTURA CLIENTE-SERVIDOR .....	36
1.3.5 ARQUITECTURA PEER-TO-PEER.....	37
1.3.6 ARQUITECTURA DISTRIBUIDA .....	39
1.4 HARDWARE DE REDES.....	41
1.4.1 ROUTERS.....	41
1.4.2 HUBS.....	43
1.4.3 SWITCHES.....	43

1.4.4 Adaptadores de Red .....	45
1.4.5 Servidor .....	45
1.5 SERVICIOS Y PROTOCOLOS .....	46
1.5.1 DNS .....	46
1.5.3 PPPoE.....	48
1.5.4 ETHERNET.....	49
CAPÍTULO 2 ANÁLISIS, REQUERIMIENTOS.....	51
2.1 ELICITACIÓN DE REQUERIMIENTOS .....	51
2.4.1 REQUERIMIENTOS.....	52
2.4.2 REQUERIMIENTOS FUNCIONALES.....	52
2.4.3 REQUERIMIENTOS NO FUNCIONALES.....	52
2.2 HERRAMIENTAS.....	52
2.2.1 NEDI.....	52
2.2.2 SNMP .....	54
2.2.2.1 COMPONENTES DE SNMP .....	55
2.2.3 REDES PRIVADAS VIRTUALES (VPN) .....	55
2.2.4 FIREWALL.....	56
2.2.4 Node.js .....	57
2.2.5 FLUTTER.....	58
2.2.6 HERRAMIENTAS DE MONITOREO COMUNES.....	58
2.3 TRABAJOS RELACIONADOS.....	60
CAPÍTULO 3 DISEÑO DE LA ARQUITECTURA .....	61
3.1 Diagrama de hilos de la empresa FINETIC.....	61
3.2 DEFINICIÓN DE LA ARQUITECTURA.....	61
3.1.1 ANÁLISIS DE DATOS RELEVANTES .....	62
3.3 ARQUITECTURA Y COMPONENTES.....	63
3.2.1 Modulo de monitoreo .....	65
3.2.2 Modulo de Categorización .....	68
3.2.3 Interfaz de Acceso .....	69
CAPÍTULO 4 IMPLEMENTACIÓN DE LA ARQUITECTURA .....	71
4.1 Diferentes fallos de red existentes.....	71
4.2 PRERREQUISITO DE INSTALACIÓN DE NEDI .....	75
4.3 INSTALACIÓN Y CONFIGURACIÓN DE NEDI.....	76
4.4 CODIGO RELEVANTE DE LA APLICACIÓN EN NODE.JS.....	76
4.5 CODIGO RELEVANTE DE LA APLICACIÓN EN FLUTTER. ....	78
4.6 RESULTADOS .....	81

4.7 RESULTADOS OBTENIDOS EN LAS PRUEBAS DE LA APLICACIÓN MÓVIL. ....	87
CAPÍTULO 5 CONCLUSIONES, RECOMENDACIONES Y TRABAJOS FUTUROS .	94
5.1 CONCLUSIONES .....	94
5.2 RECOMENDACIONES .....	95
5.3 TRABAJOS FUTUROS.....	95
ANEXOS .....	97
Anexos 1 Configuración de Nedi .....	97
Anexo 2 Graficas de pruebas realizadas.....	100
Referencias .....	112

## INDICE DE ILUSTRACIONES

Ilustración 1.1.1 Arquitectura de NeDi.....	22
Ilustración 1.1.2 Arquitectura de Observium. ....	23
Ilustración 1.1.3 Capas del modelo OSI.....	28
Ilustración 1.3.4 Esquema general de la arquitectura Cliente-Servidor .....	37
Ilustración 1.3.5.a Esquema general de la arquitectura P2P .....	38
Ilustración 1.3.5.b Esquema general de una arquitectura P2P centralizada .....	39
Ilustración 1.3.6: Esquema general de una arquitectura distribuida. ....	40
Ilustración 1.4.1: Ejemplo de un Router Dual band de alta para mayor ancho de banda .....	42
Ilustración 1.4.2: Un concentrador o Hub.....	43
Ilustración 1.4.3.a: Un switch simple para hogares o pequeños negocios.....	44
Ilustración 1.4.3.b: Un switch más avanzado para empresas, medianos y grandes negocios .....	44
Ilustración 1.4.5: Un ejemplo ilustrativo de servidores y su representación en diagramas de red.....	46
Ilustración 1.5.1: Árbol jerárquico de dominios.....	47
Ilustración 1.5.4: Ethernet y el modelo OSI.....	50
Ilustración 2.2.6: El comando ping que sirve para enviar paquetes a un host determinado.....	59
Ilustración 2.2.7: Comando tracert que muestra el número de hops o saltos hacia un destinatario.....	59
Ilustración 3.1 Diagrama de hilos de la red troncal del ISP.....	61
Ilustración 3.1.1: Reporte de problemas de conectividad.....	62
Ilustración 3.1.2: Reporte de problemas determinados por parte de la empresa.....	63
Ilustración 3.3.1: Árbol jerárquico de los módulos en la arquitectura del proyecto.....	64
Ilustración 3.3.2 Arquitectura propuesta para el proyecto.....	65
Ilustración 4.2.1. Instalación de paquetes para instalar la aplicación NeDi.....	76
Ilustración 4.2.2 Descarga de la aplicación de NeDi.....	76
Ilustración 4.2.3 Permisos para acceder a NeDi.....	76
Ilustración 4.2.4 Enlace simbólico para acceder a la aplicación.....	76
Ilustración 4.2.5 Permisos de la base de datos.....	76
Ilustración 4.3.1 Conexión a la base de datos MySQL.....	77
Ilustración 4.3.2 Método para la inserción de datos de LOS en la base de datos.....	77
Ilustración 4.3.3 Método para la inserción de datos de LOS en la base de datos.....	78
Ilustración 4.4.1 Código del servicio de LOS en flutter.....	78
Ilustración 4.4.2 Código del servicio de LOS en flutter.....	79
Ilustración 4.4.3 Código de la página principal del fallo LOS.....	79
Ilustración 4.4.4 Código de la página principal del fallo PowerFail.....	80

Ilustración 4.4.5 Código de la visualización del usuario con la solución correspondiente del fallo de LOS. ....	80
Ilustración 4.4.6 Código de la visualización del usuario con la solución correspondiente del fallo de PowerFail.....	81
Ilustración 4.6.1 Grafica de la prueba 1 de ejecución de la aplicación. ....	81
Ilustración 4.6.2 Grafica de la prueba 2 de ejecución de la aplicación. ....	82
Ilustración 4.6.3 Grafica de la prueba 3 de ejecución de la aplicación. ....	82
Ilustración 4.6.4 Grafica de la prueba 4 de ejecución de la aplicación. ....	82
Ilustración 4.6.5 Grafica de la prueba 5 de ejecución de la aplicación. ....	83
Ilustración 4.6.6 Grafica de la prueba 6 de ejecución de la aplicación. ....	83
Ilustración 4.6.7 Grafica de la prueba 7 de ejecución de la aplicación. ....	84
Ilustración 4.6.8 Grafica de la prueba 9 de ejecución de la aplicación. ....	84
Ilustración 4.6.9 Grafica de la prueba 8 de ejecución de la aplicación. ....	85
Ilustración 4.6.10 Grafica de la prueba 10 de ejecución de la aplicación.....	85
Ilustración 4.6.11 Grafica de la prueba 10 de ejecución de la aplicación.....	86
Ilustración 4.6.12: Porcentaje general obtenido del muestro de pruebas de la aplicación.....	86
Ilustración 4.7.1 Muestra la base de datos, almacenados los datos de los fallos de LOS. ....	87
Ilustración 4.7.2 Muestra el resultado de los fallos LOS por rangos de tiempos al ejecutar la app móvil. ....	88
Ilustración 4.7.3 Esta página muestra al usuario con el problema y la posible solución en el fallo LOS. ....	88
Ilustración 4.7.4 Muestra el resultado de los fallos PowerFail por rangos de tiempos al ejecutar la aplicación móvil. ....	89
Ilustración 4.7.5 Esta página muestra al usuario con el problema y la posible solución en el fallo PowerFail.....	90
Ilustración 4.7.6 Aquí se muestra el resultado de los fallos PPPOE por rangos de tiempos. ....	90
Ilustración 4.7.7 Esta página muestra al usuario con el problema y la posible solución en el fallo PPPOE. ....	91



## **INDICE DE TABLAS**

Tabla 1.3.2 Capas del modelo TCP/IP.....	32
Tabla 3.2.1: Componentes principales de NeDi y sus funciones.....	67
Tabla 4.1 Prerrequisitos para la instalación de NeDi.....	75

## **INDICE DE ANEXOS**

Anexos 1 Configuración de Nedi.....	97
Anexo 2 Gráficas de pruebas realizadas.....	100

## INTRODUCCIÓN

Actualmente, existen varias empresas que brindan el servicio de internet, compiten por brindar un servicio de calidad y un mejor costo para poder incrementar el número de clientes, por lo que es necesario realizar un monitoreo de la red mediante herramientas adecuadas como pueden ser: NEDI, PRTG, etc [1] [2]. Además, deben tener un sistema de alertas para evitar que el usuario se vea afectado por fallas en la red, por lo que es necesario la implementación de una aplicación que permite alertar al administrador de la red con los fallos que se han hallados en la misma. Al categorizar las falencias, las consideradas como críticas se pueden abordar prioritariamente y, consecuentemente, adelantarse a los usuarios de manera oportuna previniendo que ellos se enteren de estos fallos.

En las redes GPON, la mayoría de las empresas de telecomunicaciones tienen la difícil tarea de garantizar un servicio de conectividad 24/7 dadas las nuevas exigencias por parte de los clientes en cuanto a video streaming, clases virtuales y teletrabajo. Todos los cambios que han ocurrido durante la pandemia a nivel global han requerido la necesidad de aumentar el ancho de banda ofertado a los clientes y migración a nuevas tecnologías más robustas, todo con el fin de brindar un servicio óptimo.

En la parte física de la red, los sistemas de monitoreo realizan un barrido de todos los equipos de red troncal, la red de distribución, pero poco se enfocan en la parte de última milla. Los inconvenientes más comunes en este contexto son: la interferencia co-canal entre los canales de las redes de domicilios adyacentes, solapamiento entre los canales del espectro radioeléctrico, inconveniente de cobertura entre el equipo de red del proveedor modem o router de internet y los equipos finales del cliente. Como se indica en [3] la manera más eficiente de resolver estas anomalías es verificar el mejor punto céntrico del domicilio para instalar el equipo principal; después, ver la posibilidad de colocar un segundo dispositivo de red vía cable Ethernet como punto de acceso para mejorar la calidad de servicio; por último, realizar un análisis espectral empleando aplicaciones como: Wifi Analyzer y Network Analyzer dentro del celular que detecten los canales disponibles. Posteriormente, configurar la red del hogar en un canal libre o con las mejores prestaciones de tal forma que se evite inconvenientes en el servicio.

## **PROBLEMA DE ESTUDIO**

El problema es que no se puede detectar o identificar los fallos dentro de la red de última milla de una manera proactiva, por lo que será difícil la identificación de fallos de la red GPON, por ende, no existe una categorización de estos, lo cual imposibilita solucionar de forma proactiva esos fallos sino de una forma reactiva con el previo aviso, reclamo u observaciones del usuario del servicio.

La falta de jerarquías y categorización de fallos de red en usuarios finales es un obstáculo para un servicio de soporte óptimo ya que cada caída de servicio puede tener un origen o motivo variado, es decir, es posible que un cliente se quede sin servicio debido a varias causas, por ejemplo, puede ser que se dio una falla de conectores SC/APC en el cable drop de la caja de distribución o bien en el dispositivo final; otra causa posiblemente es el fallo de un conector de algún Patch Cord en el OLT del ISP, así como también fallas en el Router o dispositivo final que se deben tomar en cuenta al momento de evaluar cada situación para generar algún protocolo de respuesta o solución a estas intermitencias.

En la documentación que está en [4] se establece que un ISP al carecer de un tipo de sistema de alarmas que identifiquen cada problema a solventar en cada cliente, está dejando un vacío en cuanto a los protocolos de respuesta a fallos de la red y a sus clientes. Como recomendación, es necesario implementar alguna herramienta de monitoreo de pago o gratis sirve para brindar un mejor soporte técnico, dependiendo el tipo de fallo, gestionar los recursos de la empresa de manera óptima y evaluar qué pasos se deben tomar al proceder con la solución.

## **JUSTIFICACIÓN**

Debido a que no existe una categorización de los fallos de la red, esto dificulta el soporte técnico y ocasiona demoras debido a que se desconoce los fallos que se están produciendo en ese instante, por lo que es necesario realizar un monitoreo de la red mediante alguna herramienta ya sea de pago u open source para categorizar los fallos y enviar alertas al administrador y proponer posibles soluciones a esos fallos.

Empleando técnicas de desarrollo modernas, se propone la integración de herramientas de monitoreo de red como Nedi y encontrar fallos que ocasionan problemas de navegación a los usuarios. Para ello la configuración de usuarios dentro de una base de datos del sistema a desarrollar es clave para proceder con la programación y automatización de tareas dentro de la parte de redes, por lo cual se optó para el desarrollo de una aplicación que funcione conjuntamente con la herramienta NeDi, para esto se utilizó el entorno Node.js para el levantamiento de sus respectivos servicios (Rest), y sus funcionalidades. En la parte el desarrollo de dicha aplicación será de mucha utilidad el uso de librerías incluidas en Node.js como: MySQL y Express.js, estas dos herramientas brindarán el soporte necesario para poder acceder a la base de datos y realizar el consumo de los servicios. Por otro lado, para la aplicación móvil se empleará Flutter que es un entorno que permite crear aplicaciones multiplataforma, permitiendo su uso en distintos dispositivos, programando en un único bloque de código escrito en Dart.

## **OBJETIVOS**

### **OBJETIVO GENERAL**

Desarrollar una aplicación que permita adquirir una categorización de fallos de la red GPON y en efecto, mediante la herramienta monitoreo, realizar un sistema de recomendaciones en base a los resultados obtenidos.

### **OBJETIVOS ESPECÍFICOS**

- Identificar fallos usando la herramienta NEDI open-source.
- Categorizar los fallos según niveles o jerarquías existentes.
- Generar advertencias y posibles soluciones a las fallas por nivel o por jerarquías existentes.
- Generar registros y almacenarlos en una base de datos.

# CAPÍTULO 1 INTRODUCCIÓN AL ESTADO DEL ARTE

## 1.1 HERRAMIENTAS DE MONITOREO

### 1.1.1 NEDI

En [5] “se indica que es una herramienta para facilitar la gestión y descubrimiento de dispositivos de infraestructura como enrutadores y conmutadores. Es un software de código abierto que está diseñado para que los administradores puedan monitorear y administrar sus dispositivos de infraestructura”. Está formado por un backend SQL y una interfaz web fácil de usar, donde se puede realizar búsquedas y visualización de toda la información descubierta por la herramienta. Utiliza diferentes tecnologías de descubrimiento para el monitoreo de las redes usando el protocolo SNMP. Se maneja también CDP (Protocolo de descubrimiento Cisco); de acuerdo con la ilustración 1.1.1, se emplean otros tipos de tecnologías para el sondeo y consulta de los dispositivos encontrados y luego los datos se almacenan en un base de datos dinámica. Desde la aplicación web, los administradores están en capacidad de mostrar la información obtenida de los dispositivos y cómo se relacionan entre ellas, además de agregar diferentes gráficas de consumo de ancho de banda y de las tecnologías que se incluyen dentro de la empresa.

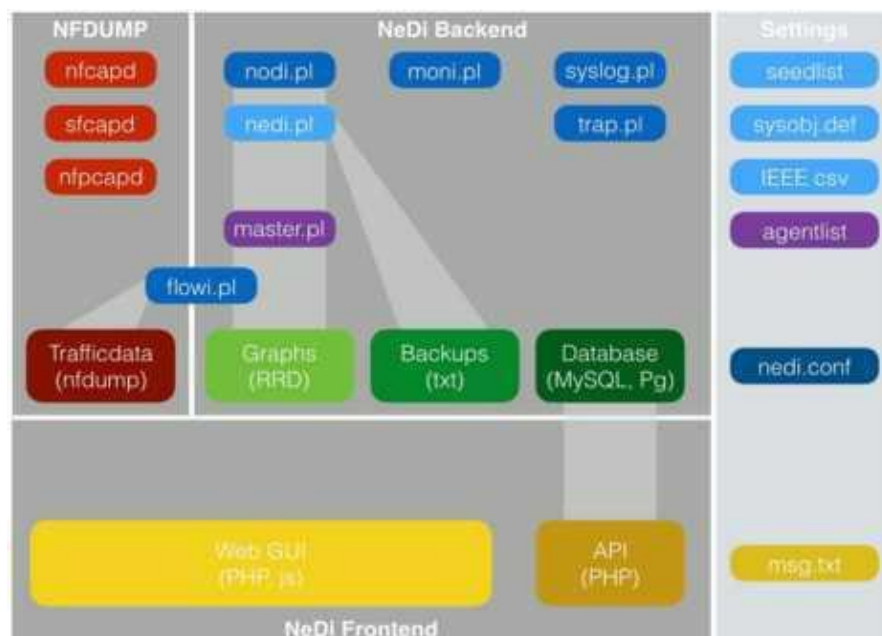


Ilustración 1.1.1 Arquitectura de NeDi. [2]

### 1.1.2 OBSERVIVUM

En el documento [6] indica que es un software que está enfocado en el monitoreo de redes, que permite trabajar y dar soporte a una amplia gama de dispositivos, plataformas y sistemas operativos. Esta plataforma se basa en PHP y MySQL, ayudando a descubrir los dispositivos automáticamente. Se puede trabajar con diferentes tecnologías de hardware y software: Cisco, Windows, HP, FreeBSD, Juniper, Dell Brocade, Netscaler, Foundry, NetApp, entre otros. Observium fue desarrollada y mantenida por un grupo de ingenieros de redes y administradores de sistemas experimentados.

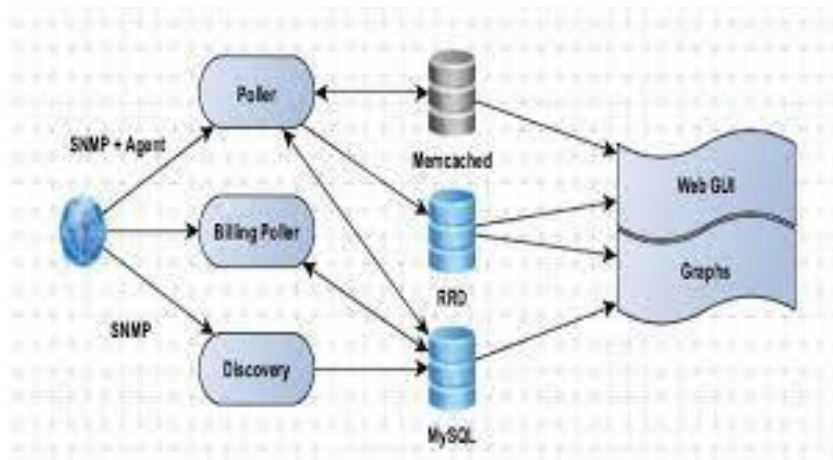


Ilustración 1.1.2 Arquitectura de Observium. [6].

### 1.1.3 PRTG

En [1] explica que es un software que permite monitorear las redes sin tener que instalar agentes en los equipos a monitorear; para esto, se emplea una interfaz muy intuitiva y fácil de utilizar, adicionalmente posee un motor de supervisión de última generación que posibilita monitorear redes de cualquier tamaño, sean pequeñas o grandes. Se combinan diferentes tecnologías que se usan para el monitoreo, por ejemplo: SNMP, NetFlow, Flow, WMI, entre otras. “PRTG permite tener disponibilidad de los componentes de red, medir su tráfico y su uso, y reduce costos evitando interrupciones, optimizando las conexiones, ahorrando tiempo y controlando los Acuerdos de Nivel de Servicio (SLAs)”.

### 1.1.4 NAGIOS

Nagios es un software para el monitoreo y análisis de tráfico en tiempo real. Este sistema provee un esquema sobre los recursos de un ISP, como potenciales amenazas a la

seguridad de la red; esta información es útil para los administradores de redes. En [7] se indica que Nagios expone toda la información de estados y alertas del sistema para detectar fallas en el servicio y soluciones posibles a los problemas que se presenten.

Su diseño se basa en una interfaz web intuitiva fácil de usar y muy ágil en cuanto a rendimiento. La herramienta de Nagios provee una vista centralizada de todo el tráfico en general y los recursos, con paneles interactivos, que permite visualizar: flujos de tráfico, actividad sospechosa en cuanto a seguridad, métricas del servidor del sistema y un sondeo del estado de la red.

### **1.1.5 ZABBIX**

En [8] se señala que Zabbix es otra herramienta open source muy popular que consiste en brindar soluciones a múltiples industrias en cuanto a los sistemas críticos de alto rendimiento se refiere. (Ej. Entidades bancarias, Educación, Salud, Agencias gubernamentales entre otras). El equipo de IT de Zabbix también ofrece soporte técnico 24/7, capacitación en el campo deseado, e integración con herramientas propias de una empresa en particular.

En cuanto al monitoreo de redes, Zabbix permite recopilar datos clave de las métricas, pero ofrece otros servicios y funciones como:

- Servicios en la nube (Cloud Computing)
- Actualmente desarrollando tecnologías en la parte de Docker y los contenedores.
- Trabajan con sensores en IoT.
- Consultas a la base de datos y logs
- Detección de fallas en tiempo real
- Análisis de posibles anomalías y comportamiento inusual
- Predicción de datos
- Envío de alertas al correo electrónico y SMS



## 1.2 LENGUAJES DE PROGRAMACIÓN PARA MODELOS MATEMÁTICOS

### 1.2.1 PYTHON

En [9] “se indica que Python es un lenguaje de programación de alto nivel utilizado para múltiples propósitos incluyendo el modelado matemático y algoritmos predictivos dentro del campo de la ciencia de datos y aprendizaje de máquina”. Es relativamente sencillo de aprender y aplicar las técnicas teniendo apoyo ya que actualmente existe una creciente comunidad de desarrolladores que brindan soporte, soluciones y documentación completa en todo ámbito.

Varios proyectos realizados en otros lenguajes de programación suelen ser de bajo nivel, ya que la sintaxis y ejecución es compleja puesto que, al momento de realizar pruebas en el código, requieren múltiples cambios y la recopilación repetitiva puede ralentizar una aplicación en producción. Python es un lenguaje de ágil ejecución. En Python, el código puede ejecutarse automáticamente, teniendo en cuenta que aparte de lograr ejecutar scripts de extensión .py, Python provee la opción de trabajar en ambientes para ejecutar líneas de código y comandos de manera individual.

Actualmente las versiones de Python estables son:

- Python 3.7
- Python 3.8

Python, además de ser un lenguaje robusto para el campo de las Ciencia de Datos y Machine Learning, tiene librerías que son útiles para modelados matemáticos, así como para gráficos, lectura de datos en archivos y extracción de estos para un propósito determinado. Algunas de las librerías y herramientas son las siguientes:

- **SciPy:** Proporciona algoritmos de optimización, integración e interpolación para tipos de problemas matemáticos relacionados y orientados a planteamiento de ecuaciones algebraicas. Contiene herramientas adicionales para computo de matrices y arreglos
- **Pandas:** Se utiliza mayormente en el manejo de datos, lectura de archivos (ya sean estos de .csv, SQLite y html) y al realizar operaciones entre columnas, en ordenamiento, agrupación u obtener totalizados de un conjunto de datos.

- **Numpy:** Esta herramienta es una de las más significativas de Python y sirve para el cálculo y operaciones numéricas, aritméticas e inicialización de datos aleatorios; trabaja en conjunto con la librería Pandas.
- **Matplotlib:** Es una librería que permite graficar funciones matemáticas, valores de una variable, crear figuras interactivas e incluso importar interfaces gráficas (GUIs) de Jupyter Lab.
- **Statsmodels:** Es un módulo que proporciona clases y funciones para aproximaciones y redondeo de varios modelos estadísticos, así como pruebas controladas y modelados de datos.
- **Flask:** Es un Microframework de Python que contiene herramientas, librerías adicionales y tecnologías que permiten construir una aplicación web.

### 1.2.2 MATLAB

En [10] MATLAB (Matrix Laboratory) se indica que es un programa muy requerido al momento de realizar cálculos numéricos con vectores y matrices, incluye un entorno sencillo de manejar con la capacidad de crear scripts.m, en el cual se puede programar funciones según los requerimientos de un problema matemático. Matlab también permite crear gráficas de varios tipos y es sumamente eficaz a la hora de trabajar con polinomios y funciones exponenciales y logarítmicas etc.

Una ventaja muy destacada de MATLAB es su constante evolución y mejoría. En cada versión se van agregando distintas funciones que son de gran ayuda para estudiantes de ingeniería, así como profesionales en general. La programación en este entorno es similar a la del lenguaje BASIC o C, pero no es considerado un lenguaje de programación sino más bien ofrece la facilidad de programar ciertos procesos con el fin de resolver problemas complejos.

### 1.2.3 JULIA

En [11] define a Julia como un lenguaje de programación multiplataforma que combina la robustez de C y C++ con la facilidad de uso de Python. Normalmente es utilizado en el campo de la computación científica, así como también en la química, biología y Machine Learning.

Julia es un lenguaje gratuito y de código abierto, es versátil en el sentido que tiene la capacidad de invocar directamente las funciones de C y las de Python mediante un paquete llamado PyCall. Algunos de los paquetes para el uso de análisis estadístico-similares a los de Python son:

- **DataFrames:** Utilizado para leer archivos .xls de Excel.
- **CSV:** Es útil para la lectura de archivos .csv
- **Time Series:** Empleado en el análisis de series temporales
- **ScikitLearn:** Es la implementación de esta API para el lenguaje Julia.

#### 1.2.4 R

En [12] se describe al lenguaje de programación R como un sistema diseñado para análisis estadísticos y creación de gráficos en base a datos proporcionados. Es útil “para modelos lineales y no lineales, pruebas de simulación, así como clasificación y segmentación de los datos”.

Este lenguaje fue muy utilizado hasta que Python tomó su lugar como exponente en el ámbito de manejo de datos, ciencia de datos y el aprendizaje no supervisado. Pero de igual manera, tiene sus ventajas:

- Es eficiente para el análisis de datos
- Es open source
- Multiplataforma
- Permite cargar librerías y paquetes para un propósito determinado.

#### 1.2.5 JAVA

“Java es un lenguaje de programación multiplataforma creado por Sun Microsystems” [13] en el cual se puede programar desde juegos y aplicaciones de escritorio hasta aplicaciones web. Es muy utilizado y de alta demanda en entidades bancarias ya que, al ser completo, permite conectar a cualquier entorno de base de datos. “Es un lenguaje de programación orientado a objetos, lo que permite almacenar datos en colecciones y ArrayLists para lograr obtener información en cuanto sea necesario”.

## 1.3 ARQUITECTURAS DE RED.

### 1.3.1 MODELO OSI

En [14] explica que el Modelo OSI es un concepto que describe el mundo de sistemas de las redes y telecomunicaciones como una estructura de siete capas, cada una con su propia función. Es un marco conceptual de cómo funciona cada capa y se comunica a través de una red. Este modelo de referencia ayuda a los ingenieros de redes, administradores e ingenieros de sistemas a entender cómo funciona el manejo e intercambio en las redes de datos desde un ordenador hacia otro, sin importar la localidad del dispositivo y bajo qué sistema operativo funciona cada uno.

Las capas del modelo OSI son las siguientes:

- L1-Capa física
- L2-Capa de Enlace de Datos
- L3-Capa de Red
- L4-Capa de Transporte
- L5-Capa de Sesión
- L6-Capa de Presentación
- L7-Capa de Aplicación.

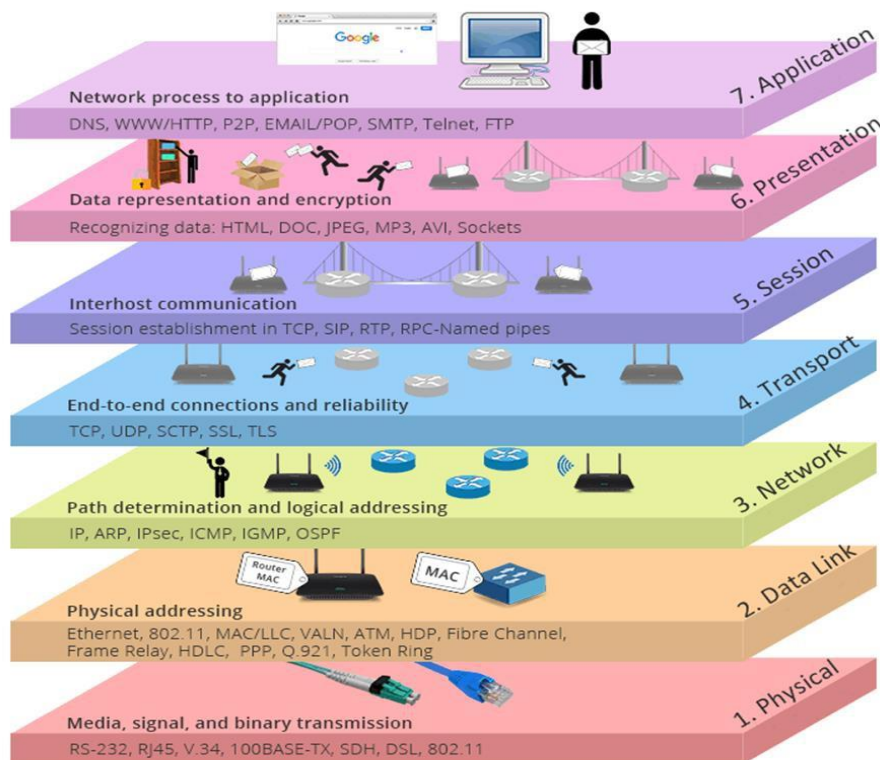


Ilustración 1.1.3 Capas del modelo OSI [15]

### **1.3.1.1 CAPAS**

El autor en [16] explica que estas capas se proporcionan mediante una combinación de controladores, protocolos de tarjetas de red, sistemas operativos, aplicaciones en conjunto con el hardware y dispositivos de red que facilitan la transmisión de datos sobre Ethernet, fibra óptica, Wifi u otros protocolos. Estas capas, como presenta la ilustración

1.5.1, sirven para visualizar y analizar las redes; son de gran ayuda para analistas e ingenieros al momento de detectar fallas en las redes como sería un daño físico. Programadores también aprovechan el modelo tal emplearlo como un apoyo para el desarrollo de y decidir en cuales de estas capas se procede a operar.

### **1.3.1.2 Capa de Aplicación**

En [16] explica que esta capa es la que interactúan la mayoría de los usuarios provee servicios de red hacia el cliente o usuario final. Son mayormente protocolos como HTTP, pero también se incluyen otros servicios y aplicaciones:

- Outlook
- Office
- Skype
- SMTP

Concretamente, son todos aquellos servicios que permiten a la capa de aplicación proveer y recibir datos hacia la capa de presentación. Ofrece el acceso a la red, proporcionando herramientas visibles con las cuales el usuario final interactúa, brindando acceso a servicios de red relacionados con las aplicaciones como mensajería, transferencia de archivos y consultas a la base de datos. En efecto se agrega un encabezado con datos de la capa de aplicación.

### **1.3.1.3 Capa de Presentación**

El autor en [16] dice que esta capa realiza las tareas de procesamiento de sintaxis, es decir el parsing o conversión de datos de distintos formatos. Organiza los datos y busca la manera de presentarlos hacia la capa aplicación. Esta capa crea un paquete de datos que se va a transportar por las capas subyacentes.

La capa superior se puede utilizar para la aplicación de usuario final y en efecto se puede comprimir, encriptar y desencriptar datos.

Un ejemplo de esto son las tiendas en línea o sitios E-Commerce. En cuanto se realiza una orden de compra, se genera una transacción que debe manejarse mediante una transmisión segura, lo que significa que los datos proporcionados desde esta tienda en línea se transmitirán de manera encriptada hacia la capa de presentación, que luego deben ser desencriptados y validados. Algunos de los tipos de contenidos que se encuentran en esta capa son: HTML, imágenes .jpg, archivos .mp3 entre otros.

#### **1.3.1.4 Capa de sesión**

En [16] los autores definen a la capa de sesión como una de las últimas capas superiores del Modelo OSI y su labor es controlar las conexiones entre dispositivos finales. Establece, gestiona y finaliza las conexiones entre aplicaciones locales y remotas. Esta capa también soporta múltiples tipos de conexiones y se responsabiliza de la autenticación y reconexión si ocurriese una interrupción en la red. Una vez establecida la sesión entre dos nodos, se coordina la secuencia de datos para verificar que se minimice el riesgo de fallas dentro de dicha sesión, es decir, si se llegara a suscitar una falla en la sesión, automáticamente se corta la comunicación entre los nodos. Una vez restablecida, se ubicará en un último punto de la comunicación previo al fallo. Los protocolos de la capa de sesión se ponen de acuerdo en cuanto a parámetros de establecimiento de conexión y cuando deben finalizar esta conexión.

#### **1.3.1.5 Capa de Transporte**

En [16] explica que una vez se establece la sesión, los datos se pasan desde y hacia la capa de Transporte, y se responsabiliza de coordinarla transferencia de datos entre dos puntos. Esto incluye: la cantidad de datos, la tasa de transferencia y su destino, etc.

“El ejemplo más sobresaliente de esta capa es el protocolo TCP, basado en el protocolo de Internet (IP). Los números de puertos de TCP y UDP funcionan en la capa 4 mientras que las direcciones IP funcionan en la capa 3 de red”.

### **1.3.1.6 Capa de Red**

El autor en [16] expone que los datos en la capa de red están compuestos de paquetes. En esta capa se identifica el enrutamiento entre las distintas redes conectadas; esta es la capa en la cual las direcciones IP se convierten en direcciones físicas del hardware destino. Los routers o enrutadores trabajan en esta capa utilizando los protocolos de enrutamiento para dirigir el flujo de los paquetes a ser transferidos.

Algunas de las funciones clave de esta capa son:

- **Direccionamiento:** Asegurando que las direcciones origen y destino sean colocadas encima de la trama, para ayudar a identificar los dispositivos en una red.
- **Interconexión:** Es decir el enlace lógico entre dispositivos.
- **Empaquetado de datos:** Como esta capa recibe tramas de las capas superiores, las convierte en paquetes.

### **1.3.1.7 Capa de Enlace de Datos**

En [16] se explica que esta capa se encarga de asegurar el transporte de datos por el medio físico, guiado o no guiado hacia el nodo receptor, identificando cada equipo incluido en la red con la dirección MAC única de estos dispositivos dentro de su tarjeta de red (NIC). Es muy similar al mecanismo de funcionamiento de la capa 3, sino que en este escenario se opera bajo la misma red, dispositivos dentro de la misma red.

Esta capa facilita el tránsito de la información a través de un enlace físico. De manera que lo más importante es el direccionamiento físico dentro de la topología de red, el acceso a la red, notificación de errores, entrega ordenada y el control de flujo.

### **1.3.1.8 Capa Física**

En [16] se indica que es la capa inferior del modelo OSI, y se encarga de todos los componentes físicos de la conexión. “En esta capa se realiza la gestión de los componentes electrónicos de la red. Se reciben las tramas procedentes de la capa de enlace de datos” y el resto superiores que luego serán convertidos en secuencias de bits

para poder viajar por el medio físico de la red; estos posibles medios son: cable coaxial, ADSL o enlaces de fibra.

### 1.3.2 TCP/IP

“El modelo TCP/IP fue definido como una iniciativa del Departamento de Defensa de los Estados Unidos” con ARPANET para interconectar varias redes de universidades y agencias gubernamentales utilizando las líneas telefónicas y no fue implementado como modelo sino hasta años después.

“TCP/IP toma su nombre de dos protocolos clave, TCP (Protocolo de Control de Transmisión) e IP (Internet Protocol)”, Es la pila de protocolos más utilizado en los sistemas de información de la actualidad. Es un modelo de coordinación dividiendo el software en capas, dando paso a una implementación sencilla, pruebas de código y la comunicación entre capas mediante interfaces determinadas.

Tabla 1.3.2 Capas del modelo TCP/IP.

CAPA	PROTOCOLOS Y COMPONENTES
Aplicación.....	Aplicaciones, Telnet,FTP.
Transporte.....	TCP, UDP
Internet.....	IP,ICMP, ARP/RARP
Interfaz de red y Hardware.....	Interfaces de red

#### 1.3.2.1 Capa Física

El autor en [16] explica que esta capa del conjunto de protocolos TCP/IP contienen todas las funciones para transportar los bits de información a través del medio físico. La parte física incluye cuatro partes importantes como la mecánica, eléctrica u óptica, funcional y de procedimiento.

En [16] se detalla el mecanismo específico de acceso al medio, detallando el tamaño y tipo de conectores dentro la conexión física y todos los medios que posibilitan la transferencia de bits de datos que van a ser procesados en las capas superiores. La parte eléctrica especifica y determina el valor de voltaje o las condiciones favorables para la conexión verificando los pines activos representados con 1 y 0. La parte funcional



determina la función de cada pin (pin de envío de datos, otro de recepción entre otros). La parte de procedimiento es básicamente un proceso que trabaja con Ethernet en cuanto a los cables de par trenzado y se agrega un preámbulo y delimitador de trama de inicio.

Otras características significativas de la capa física son:

- Tasa de Transferencia de datos: Indica el número de bits por segundo que pueden enviarse.
- Sincronización de bits: El emisor y receptor están sincronizados de tal manera que la información enviada pueda ser reconstruida de manera oportuna del flujo de datos recibido.
- Configuración: Los tipos de conexiones no se reducen a Punto-a-Punto únicamente. En conexiones Punto-a-Multipunto, el enlace conecta a dos o más dispositivos, de tal manera que el sistema debe estar configurado para realizar un broadcast en caso de ser necesario.
- Topología: Esta parte se puede implementar de distintas maneras. En topología tipo malla, todos los dispositivos están conectados entre todos y mayormente utilizada en redes inalámbricas. En topología estrella, la conexión es centralizada, es escalable y la detección de fallos es más simple. La topología anillo, es una conexión en forma circular y el envío de información pasa a través de todos los nodos conectados.

### **1.3.2.2 Capa de Enlace de Datos**

La capa de enlace de datos según [16] realiza la tarea de armado de trama, el “direccionamiento físico, detección de errores y el procedimiento a seguir en caso de que se detecten”. También se lleva cabo el control de acceso, de tal manera que se identifica el protocolo de red de un paquete específico. En general incluye los siguientes elementos:

- Datos: Del paquete que llega desde la capa de red e incluye contenidos de un mensaje encapsulado.
- Encabezado: Este incluye los datos de control de direccionamiento y se coloca al inicio de la trama.

Al transmitir datos, esta capa añade la cabecera que contiene la dirección MAC de host emisor y destinatario al paquete que llega desde la capa de red. Cada host en una red tiene una dirección MAC. Las laptops por lo menos tienen dos direcciones MAC, una para la LAN cableada y otra para internet.

### **1.3.2.3 Capa de Red/Internet**

La capa de red en TCP/IP se responsabiliza de la tarea de direccionamiento, empaquetado y direccionamiento a través de varios enlaces no necesariamente adyacentes. En [17] se destacan tres protocolos importantes de esta capa son: “El Protocolo de Internet (IP), protocolo de resolución de direcciones (ARP) y el protocolo de mensajes de control en Internet (ICMP)”.

- Direcciones IP se asocian directamente con el protocolo del mismo nombre, y adicionalmente para identificación de host a host del sistema receptor.
- Formato de paquetes agrupándolos en unidades conocidas como datagramas y estos son al encabezado IP de la trama de datos con su respectivo tamaño y orden de secuencia.
- El protocolo ARP normalmente se encuentra en el borde de las dos capas, red y enlace de datos, este proporciona mecanismos para el redireccionamiento de los datagramas a un sistema receptor determinado, asociando MAC y direcciones IP.
- El protocolo ICMP es útil para detección de errores de red. como paquetes descartados o no enviados. Adicionalmente, a modo herramienta, el comando ping sirve para realizar un envío de paquetes de datos y notifica cualquier anomalía o correcto envío y entrega de los paquetes de datos.

### **1.3.2.4 Capa de Transporte**

Según [16], el proceso de correcta entrega de los paquetes es una tarea de la capa de transporte. Para que se garantice la entrega, se divide el contenido del mensaje en paquetes en un proceso de segmentación. La capa de red reenvía cada uno de los paquetes de manera independiente, y no reconoce la relación entre estos, es decir, si es un paquete de correo electrónico o cualquier otro contenido, la capa de red hace caso omiso. La capa de transporte a diferencia de la capa de red asegura que cada mensaje llegue a su

destinatario en orden. Esto implica que esta capa contiene mecanismos de control de flujos y errores.

El protocolo TCP facilita las funciones de control, formando paquetes IP en unidades conocidas como datagramas. Protocolos significativos de esta capa son:

- TCP: Es un protocolo orientado a conexión; es un servicio confiable que proporciona una entrega ordenada de paquetes.
- UDP: Protocolo no orientado a conexión; es un servicio poco confiable; es decir se envían los paquetes, pero se hace caso omiso si su entrega fue exitosa.

#### **1.6.2.5 Capa de Aplicación**

“La capa de aplicación es el nivel más alto del modelo TCP/IP que proporciona al usuario con las interfaces y protocolos necesarios. Adjunta las funciones de la capa de sesión, de presentación”. Algunas de estas funciones son:

- Facilitar al usuario el uso de los servicios de red.
- Algunos de los servicios incluyen: inicio de sesión (login), formateo de mensajes, correos electrónicos y transferencia de archivos.
- Protocolos que operan dentro de esta capa del modelo TCP/IP son: HTTP, para acceder a datos en la web como texto, audio y video. SNMP, para la gestión de dispositivos dentro de un sistema de monitoreo.

#### **1.3.3 INTERNET**

Internet como tal es un sistema global de redes de computadoras interconectadas entre sí. Según [14] es una interconexión global de redes pertenecientes a varias compañías, gobiernos o cualquier individuo en particular, permitiendo que todos estos dispositivos que estén conectados a dichas redes se enlacen entre sí desde cualquier lugar en el mundo.

Para facilitar esta comunicación, los dispositivos que van a vincularse deben utilizar el mismo lenguaje o protocolo, es decir, el protocolo de internet IP). El envío de información sobre IP es similar al envío de mensajes por correspondencia. Bajo esta

modalidad, los contenidos se manejan sujetos a convenciones y protocolos para cada tipo de comunicación. Ejemplos de estos protocolos son los siguientes:

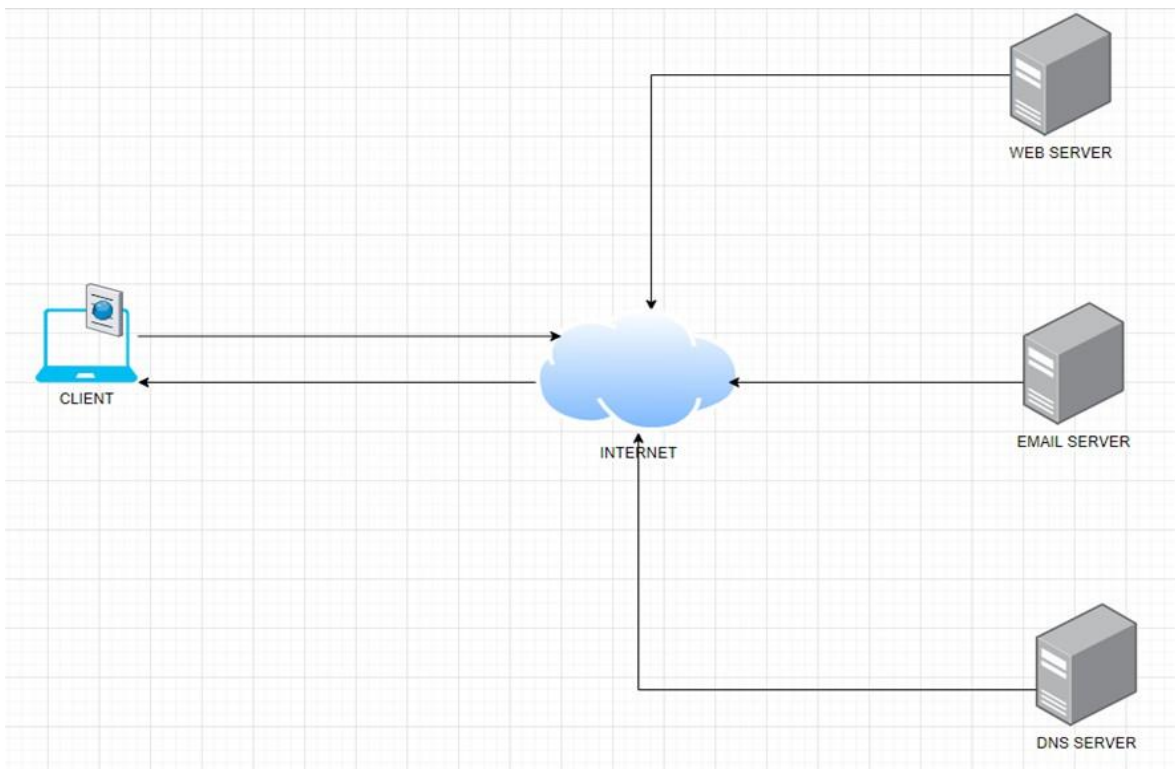
- SMTP para envío de correo electrónico
- HTTP para acceso a sitios web.

Las convenciones pueden ser desarrolladas por cualquier individuo o entidad, pero siempre deben trabajar bajo normas del protocolo IP, aclarando que los dispositivos responsables del transporte de datos de internet son los routers. En el Core o parte central de la red, internet ofrece un servicio: obtener datos de un usuario o dispositivo final, sin importar la ubicación desde donde esté conectado este usuario y haciendo caso omiso del contenido de este mensaje.

### **1.3.4 ARQUITECTURA CLIENTE-SERVIDOR**

En [17] dice que es una arquitectura cliente-servidor, siempre existirá un equipo permanentemente encendido mejor conocido como servidor, el cual recibe las solicitudes y peticiones de los clientes. Un ejemplo claro de esto es una simple aplicación Web, la cual tiene su propio servidor encendido 24/7 y atiende peticiones de navegadores ejecutándose en los dispositivos cliente. Cuando un servidor Web recibe una petición para un objeto de un host cliente, el servidor responderá con el objeto solicitado. Se nota que según [18] esta arquitectura los clientes no se comunican directamente entre ellos, sino más bien, como en el ejemplo del servidor Web, dos navegadores no se comunican entre sí. Se puede verificar el estado del servidor simplemente enviando paquetes de datos a la IP del servidor mediante el comando ping. Algunas de las aplicaciones destacadas que se basan en esta arquitectura son: Web, FTP, Telnet, y correo electrónico.

En muchos casos, en una aplicación cliente-servidor existe la necesidad de optar por múltiples servidores para mantener un balance estable de excesivas solicitudes, especialmente tratándose de grandes compañías como Google y Facebook. Estos gigantes tecnológicos optan por soluciones mucho más avanzadas como la incorporación de centros de datos dentro de su infraestructura global, los cuales albergan múltiples equipos servidores de alto rendimiento y hardware de capacidad elevada. De acuerdo con [17] Google bajo su infraestructura posee entre 30 a 40 centros de datos distribuidos a nivel global para mantener el funcionamiento de varios servicios que ofrece esta empresa como Gmail, YouTube etc.



*Ilustración 1.3.4 Esquema general de la arquitectura Cliente-Servidor*

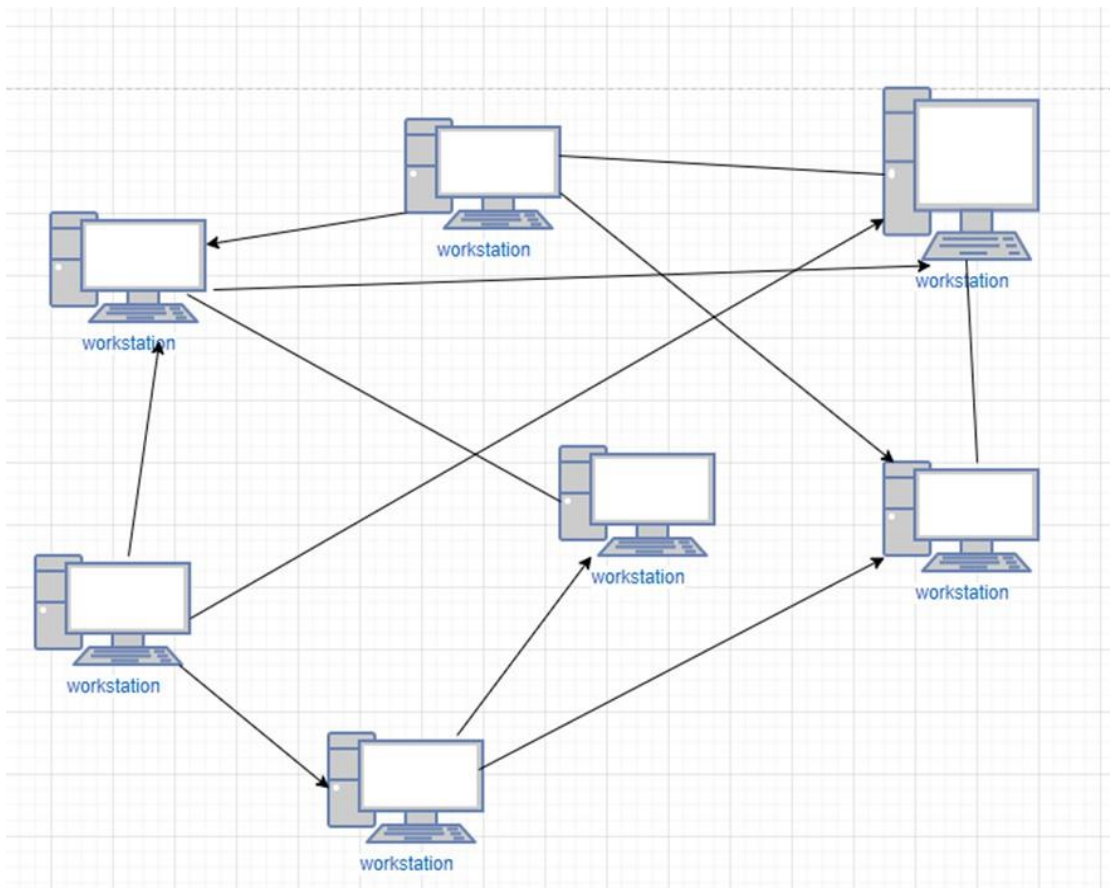
### **1.3.5 ARQUITECTURA PEER-TO-PEER**

En [17] se indica que en la arquitectura P2P existe poca dependencia de servidores de alto rendimiento en los centros de datos. Contrario al esquema cliente-servidor, P2P busca la comunicación directa entre varios hosts conectados llamados peers que en si son hosts interconectados. Estos peers, no pertenecen a algún proveedor de servicios, sino más bien son dispositivos finales, ordenadores, computadoras portátiles controlados por los mismos usuarios, y la mayoría conectados desde sus domicilios, campus universitarios y oficinas remotas; estos equipos que se comunican sin enviar mensajes ni solicitudes a un servidor específico, más bien todos los equipos o hosts de esta red tienen los mismos privilegios y comparten la responsabilidad del procesamiento de datos.

Características adicionales:

- Ideal para redes pequeñas de hasta 10 computadores.
- Permisos especiales son otorgados a cada ordenador por un esquema regulador.
- Propenso a fallar cuando un nodo con recursos pierde conectividad.
- El costo de implementación es bajo.

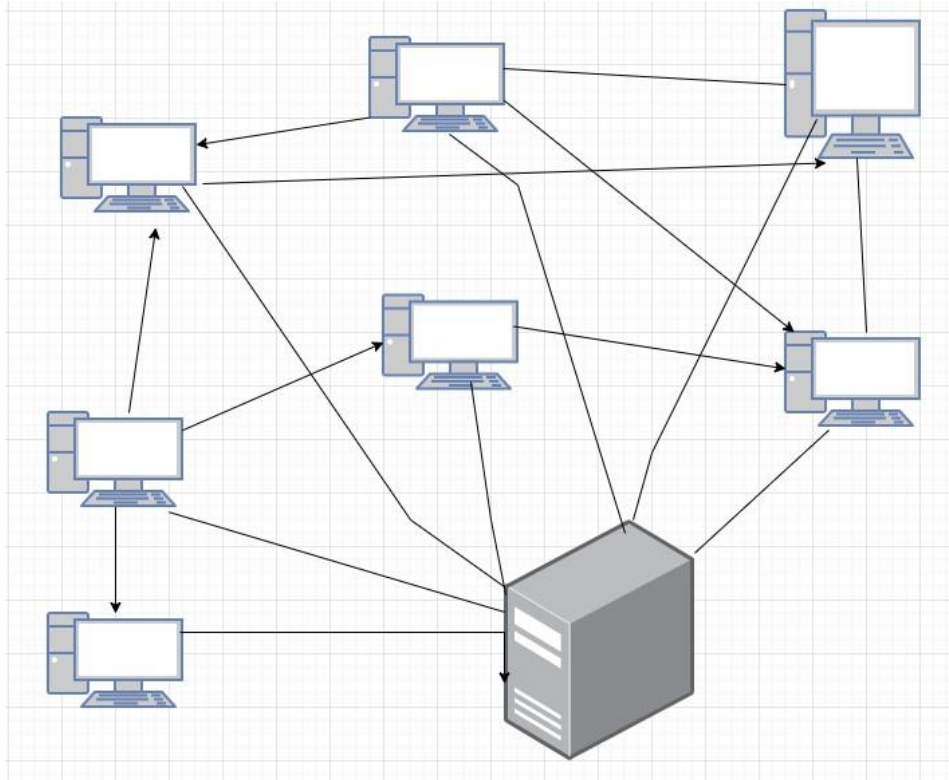
- En vista que carece de un sistema centralizado, el almacenamiento de datos no es igual en cada nodo.



*Ilustración 1.3.5.a Esquema general de la arquitectura P2P*

En la Ilustración 1.3.5.a, se tiene un ejemplo ilustrativo de una arquitectura P2P descentralizada; los nodos operan de manera equitativa en cuanto a “procesamiento y almacenamiento de la información”. En esta arquitectura los nodos intercambian información de los nodos vecinos y otra particularidad es el sistema jerárquico conformado por nodos ordinarios (ON) y nodos superiores (SN) en el cual se opera de la siguiente manera:

- Un nodo ordinario debe estar asociado a un nodo superior.
- Un nodo superior contiene la información de un conjunto de nodos asociados.
- La designación de super nodos es dinámica y el criterio principal es la capacidad de rendimiento, conectividad entre otras características.



*Ilustración 1.3.5.b Esquema general de una arquitectura P2P centralizada*

En la Ilustración 1.3.5.b se tiene una arquitectura híbrida, es decir un esquema P2P centralizado, en el cual todos los nodos individuales se comunican con un servidor que gestiona el almacenamiento, administración de recursos y seguridad dentro de una topología específica.

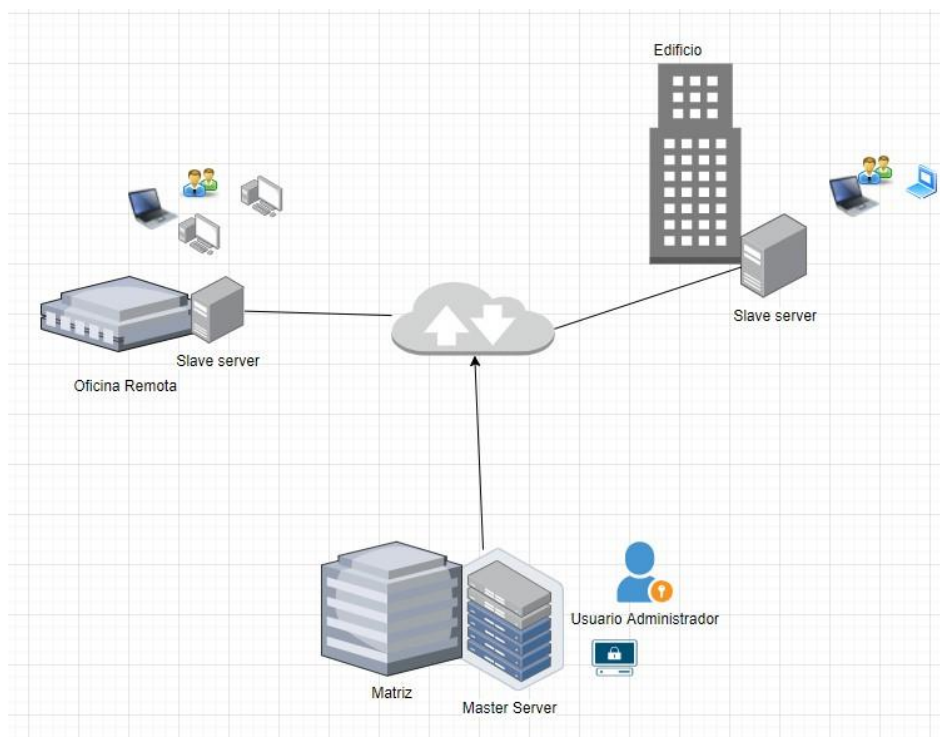
### **1.3.6 ARQUITECTURA DISTRIBUIDA**

De acuerdo con [6] se indica que el sistema distribuido es un conjunto o grupo de equipos que están ejecutando tareas de manera independiente, pero simulan operar como un solo equipo de manera descentralizada optimizando el procesamiento y/o el almacenamiento de información. Sus características principales son:

- **Concurrencia:** Se permite optimizar recursos disponibles habilitando la capacidad de utilizarlos simultáneamente por múltiples usuarios de la red.
- **Modularidad:** Característica que permite optar por más flexibilidad de partes o módulos del sistema posibilitando en sí su flexibilidad y escalabilidad al momento de integración de varios servicios.
- **Transparencia:** Tiene como objetivo principal, ocultar al usuario final y esa separación de los componentes es la que forma un sistema distribuido. En cuanto

al acceso, es decir el usuario percibe el acceso a objetos del sistema como si accediera tanto de manera local como remota. Transparencia de migración, se refiere al cambio hacia tecnologías más seguras y resilientes sin afectar a los usuarios.

- Independencia de componentes de hardware: Es importante ya que, caso contrario, si un componente fallara, en el sistema posiblemente se comprometerían totalmente las operaciones y transacciones. Sin embargo, de esta manera los procesos siguen ejecutándose y no se interrumpe ni se registran pérdidas de datos.
- Apertura: La apertura a migrar a nuevas tecnologías o adición de nuevos componentes y hardware de distintos vendedores.
- Interoperabilidad: Esta característica dicta que un sistema tenga la capacidad de operar en distintas plataformas y sistemas operativos mediante interfaces de comunicación específicas y middleware.



*Ilustración 1.3.6: Esquema general de una arquitectura distribuida.*



## **1.4 HARDWARE DE REDES.**

### **1.4.1 ROUTERS**

En [14] se define un “router o Enrutador es un dispositivo de hardware” que permite conectar varios dispositivos finales en una misma red u otras redes enviando paquetes de datos basándose en su dirección. Entre varias de sus aplicaciones, mayormente son utilizados para proporcionar acceso a internet enlazando distintas redes de área local o incluso interconectando múltiples sucursales de una misma empresa mediante el uso de VPN.

Los Routers operan en la capa tres del modelo OSI, utilizando un protocolo de enrutamiento permiten la comunicación con otros enrutadores para el intercambio de información de manera eficiente. En otras palabras, los routers conocen información específica como las direcciones IP y facilitan la comunicación entre distintas redes. Por ejemplo, si una empresa A tiene una IP de 10.0.1.x y empresa B tiene asignada la IP 192.168.2.x, un Router enviará paquetes desde A hacia B, lo que un switch es totalmente incapaz de realizar [14]. Un router habilita una LAN hacia el internet global; en otros términos, si se desea conectar a una LAN hacia Internet vía un proveedor de servicio entonces su router va a requerir de una dirección pública asignada a una de sus interfaces para llevar a cabo esta conexión.

Cuando un Router es utilizado para conectar una red hacia Internet, una de las tareas más importantes del Router es enrutar el tráfico desde todos los dispositivos finales de esta LAN hacia el “lado público” del Router. Para ejecutar esta función el router utiliza una traducción de direcciones o NAT (por sus siglas en inglés). Un ejemplo de este proceso sería cuando un equipo o un ordenador, desde la red de área local, envía paquetes de datos por el router hacia Internet, el router sustituye su propia dirección IP pública por la IP del remitente, y mantiene un registro del envío de dicho paquete de datos desde el ordenador en la red local [14]. Una vez que el destinatario recibe el paquete, verifica que el remitente es de hecho el Router, luego este envía una respuesta hacia el router remitente, el cual reemplaza la dirección del remitente original por la dirección del destinatario, en efecto entregando la información a la computadora dentro de la red privada.

El Router brindará el enlace de nuestra red privada hacia el Internet. Un router particular sirve para ejecutar esta tarea, no obstante, elegir un Router específico para ciertos propósitos puede ser un poco complicado ya que el avance de nuevas tecnologías requiere una actualización de los dispositivos de red. Por ejemplo, un Router TP-Link como el reflejado en la ilustración 1.6.1 tiene las siguientes especificaciones:

- Conexión WAN habilitada para enlazar los servicios del ISP.
- Cuatro puertos ethernet de 1 Gbps, con la capacidad de conectar hasta 4 ordenadores o Smart TV box.
- Un punto de Acceso el cual funciona con IEEE 802.11 y 802.11ac

Estos routers pueden ser utilizados en oficinas pequeñas y el rendimiento será óptimo. Sin embargo, existe un tipo de routers, como el TP-Link TL-940N es un modelo de equipo básico que se fue muy popular populares hace unos años atrás, pero con el alto requerimiento de ciertas aplicaciones como Zoom y videojuegos. Debido al incremento de reportes de intermitencias y cortes de servicio se evidenció que dichos equipos no cumplían con los estándares para un óptimo rendimiento debido a que solo soporta un número limitado de dispositivos conectados simultáneamente.

Los Routers del tipo doble banda modelos AC1200 o AC1900 tienen capacidades avanzadas de red y abastecen mayor ancho de banda en dispositivos finales modernos que ya soportan la conectividad 5G.



*Ilustración 1.4.1: Ejemplo de un Router Dual band de alta para mayor ancho de banda [19]*

Algunos de los beneficios de los routers incluyen el hecho de que se obtiene un gran nivel de seguridad de los datos transmitidos, es de alta confiabilidad e incrementa el rendimiento de redes dividiendo en dos subredes de distinta banda.

### 1.4.2 HUBS

Según [20], un Hub o concentrador divide una conexión de red en varios dispositivos. Un concentrador típico como el que se muestra en la ilustración 1.6.2, conecta a todos los equipos de la red vía cable ethernet. Cada ordenador envía una solicitud a la red a través del concentrador. Cuando el concentrador recibe una solicitud de una computadora en particular, envía mensajes de difusión de esta solicitud a través de la red a todos los dispositivos de red. Cada dispositivo de red verifica la solicitud para determinar si pertenece allí. De no ser así, la solicitud se descarta posteriormente. La desventaja de este proceso es el mayor consumo de ancho de banda y la comunicación es muy limitada, además es poco seguro ya que todos los integrantes pueden ver el tipo de tráfico que se transmite por medio del concentrador. En la actualidad, un concentrador es casi obsoleto debido al incremento de demanda en el mercado con enrutadores y conmutadores (switch).



*Ilustración 1.4.2: Un concentrador o Hub. [21]*

### 1.4.3 SWITCHES

En [18] se define un “Switch o conmutador de red que enlaza múltiples dispositivos en una red informática”. Este dispositivo de interconexión tiene funciones más avanzadas que la de un concentrador. Un switch tiene una actualización que determina el destino de los datos transmitidos. Este transmite un mensaje al destino deseado según la dirección

física de cada solicitud entrante. A diferencia del concentrador, un switch no transmite datos a todos los dispositivos a través de la red. Por lo tanto, hay mayores velocidades de transmisión de datos ya que cada computadora se comunica directamente con el switch. En la ilustración 1.4.3.a se muestra un switch o conmutador de red típico para pequeños hogares.



*Ilustración 1.4.3.a: Un switch simple para hogares o pequeños negocios. [22]*

Ahora bien, los conmutadores de red también se dividen en varias gamas dependiendo del propósito en el que se lo utilice. En domicilios y negocios pequeños basta con realizar el cableado estructurado utilizando switches para brindar conectividad a equipos finales, como ordenadores, televisores Smart, entre otros. Por otra parte, en medianas y grandes empresas en las cuales ya se requieren otro tipo de configuraciones de red adicionales; es necesario implementar QoS, reglas de firewall más avanzadas, entonces es recomendable un switch de múltiples puertos administrable o un Switch capa 3, en tal caso se requieren switches más avanzados como el que se muestra e la ilustración 1.4.3.b.



*Ilustración 1.4.3.b: Un switch más avanzado para empresas, medianos y grandes negocios [23]*

#### **1.4.4 Adaptadores de Red**

Los adaptadores de red o tarjetas de red (NICs por sus siglas en inglés), son componentes de hardware que enlazan una computadora con otra dentro de la misma red. Las tarjetas de red soportan tasas de transferencia desde 10 Mbps hasta 1000 Mbps.

#### **1.4.5 Servidor**

En [24] se define a un servidor “como un computador que cumple con una función específica dentro de una red. Los servidores, como su nombre lo indica, se utilizan para dar servicios a los demás equipos que se encuentran interconectados entre sí”. “Para seleccionar un Servidor es necesario conocer las necesidades reales y a futuro de la organización, ya que de esto va a depender el buen funcionamiento, la seguridad de operación y la tranquilidad de los usuarios al estar manejando los procesos diarios de automatización”. Sin embargo, existen otros factores claves para la correcta selección de este, como son:

- La cantidad de información y datos que se maneje y almacene.
- La cantidad de transacciones internas (las aplicaciones que se ejecutan en el servidor.)
- La cantidad de transacciones externas (la cantidad de usuarios que usan las aplicaciones y servicios.)
- La forma de integrar o la estructura de la red.
- La necesidad de velocidad y tiempo de acceso.

Las funciones principales del Servidor son:

- Centralizar y concentrar la información.
- Centralizar las aplicaciones (correo, archivos, Web, programas, etc.)
- Estandarizar las operaciones de la organización.

Básicamente, el siguiente esquema general es el denominado esquema cliente-servidor y es uno de los más aplicados.



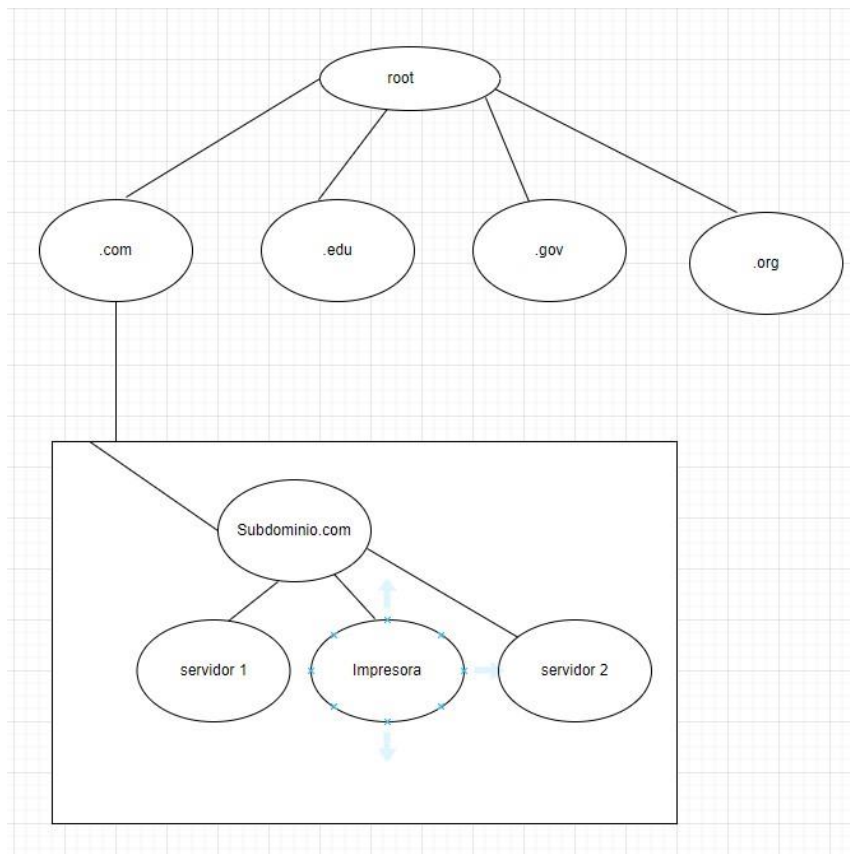
*Ilustración 1.4.5: Un ejemplo ilustrativo de servidores y su representación en diagramas de red.*

## **1.5 SERVICIOS Y PROTOCOLOS**

### **1.5.1 DNS**

En [14] se establece que las páginas web son básicamente números de direcciones específicas de red que se relacionan directamente con el servidor del origen de datos, los cuales son asociados por las computadoras y se proyectan en pantalla como, por ejemplo, una página web. En TCP/IP, DNS (Domain Name Service) permite utilizar nombres para denominar sitios web para referirse a estos hosts donde se alojan la páginas o sitios web, proporcionando un sistema estandarizado para nombrar hosts específicos en Internet.

Los nombres únicos se organizan de manera jerárquica bajo dominios, de hecho, como se puede observar en la ilustración 1.5.1, el árbol de dominios inicia con el dominio raíz, como punto de partida para todo dominio. Debajo de este, están los cuatro dominios de alto nivel como: edu, com, org y gov. En realidad, pueden existir más niveles superiores debajo del nodo root o raíz y estos a su vez pueden tener más nodos.



*Ilustración 1.5.1: Árbol jerárquico de dominios*

Dentro de un nombre de dominio, puede existir un subdominio personal para completar su identificación se puede complementar con su dominio padre. Dentro del subdominio, la parte dentro del rectángulo en la ilustración 1.5.1, se pueden tener 3 nodos adicionales como ejemplo de una red de hogar. La denominación de cada uno de estos hosts es la siguiente: `servidor1.subdominio.com`, `impresora.subdominio.com` y `servidor2.subdominio.com` [14].

Características adicionales de DNS:

- Los nombres dentro de DNS hacen caso omiso de letras mayúscula y minúsculas, es decir en la búsqueda de tal dominio, se puede escribir: `Subdominio.com`, `SUBdominio.com` o `SubDominio.com`
- Un nombre dentro de un nodo DNS puede ser compuesto de hasta 63 caracteres si incluir el punto.
- Un subdominio es un dominio que se encuentra debajo del dominio principal.
- Es un sistema con una estructura jerárquica similar al árbol de directorios de las carpetas del sistema operativo de Windows, la diferencia es el sentido de la

identificación, en DNS se inicia desde abajo hacia la raíz y e Windows se empieza en la raíz y termina en la carpeta final.

- Los sufijos de dominio único son asignados por IANA (Internet Assigned Number Authority).
- El administrador de dominio tiene control total sobre el dominio.

### **1.5.2 PPP**

Según [25], el protocolo PPP es un “protocolo de TCP/IP que se utiliza para conectar un sistema informático con otro”. Una conexión o enlace PPP existe cuando dos sistemas se conectan físicamente mediante una línea telefónica. PPP opera en la capa de enlace de datos del modelo OSI y su propósito principal es encapsular los protocolos de capa 3 con toda la información dentro de las tramas para lograr transmitirlos mediante enlace seriales de manera síncrona o asíncrona.

Previo al lanzamiento de PPP, existía HDLC (High-Level Data Control), cuyas limitaciones solo eran útiles en cuanto a detección de errores. Al descubrir un error se descartaba la trama en el proceso de FCS (Frame Check Sequence), pero bastaba con eso.

PPP establece una conexión directa entre dos nodos de una red. Proporciona autenticación, encriptación y compresión. Tres componentes clave de PPP son:

- Un componente de encapsulamiento que transmite datagramas sobre la capa física
- Un Protocolo de control de enlace (LCP) que establece, configura y prueba el enlace, así como revisa los ajustes, opciones y usos.
- Aplica uno o más Protocolos de Control de Red (NCP) para negociar los parámetros de configuración opcionales y funciones para la capa de red.

### **1.5.3 PPPoE**

El protocolo PPPoE es la evolución de PPP con encapsulamiento de las tramas PPP sobre Ethernet [26]. “Surgió en el año 1999 cuando DSL era popular aplicando principios de PPP para autenticación con un nombre de usuario y contraseña que proporciona el ISP”. [27]



Este protocolo se sigue implementando en la actualidad dentro de los dispositivos de red de usuarios aplicando el uso de perfiles que permitan conexión a una LAN de hogar. Además, dentro de PPPoE se incluyen la capacidad de acceder a recursos remotos de trabajo externos, utilizando VPN o cualquier mecanismo para configurar una conexión remota.

#### 1.5.4 ETHERNET

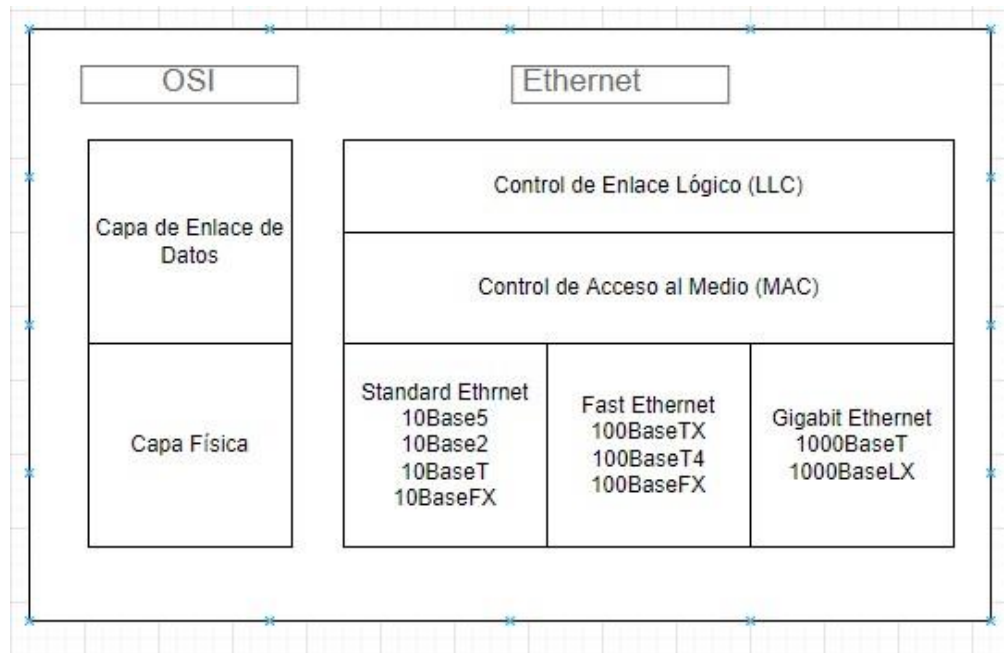
El protocolo Ethernet trabaja en las primeras dos capas del modelo OSI: la física y enlace de datos. Este standard apareció en la década de los 70 y fue la base para el Ethernet definido en IEEE 802.3 [4], “La versión actual de Ethernet opera con varias tasas de transferencia.<sup>1</sup> Sin embargo, todas las versiones de Ethernet son compatibles la una con la otra, de manera que pueden interconectarse dispositivos, Switches, puentes y hubs enlazando segmentos de red que utilicen distintos tipos de medios para conexión”.

Las velocidades actuales de Ethernet se miden en millones de bits por segundo (Mbps), o en billones de bits por segundo (Gbps). Estas versiones varían en sus velocidades:

- **Standard Ethernet:** Velocidades de 10 Mbps, es muy poco popular en tecnologías emergentes.
- **Fast Ethernet:** Velocidades de 100 Mbps, se sigue utilizando para los dispositivos donde la velocidad es un factor importante, como, por ejemplo, en impresoras.
- **Gigabit Ethernet:** Velocidades de 1000 Mbps y más, es la velocidad de internet más avanzada en cuanto a tecnologías de alto rendimiento. Velocidades más altas llegan desde 10 Gbps hasta 100 Gbps en redes de altas prestaciones.

---

<sup>1</sup> La tasa de transferencia en redes se refiere a la velocidad máxima que puede llegar a medirse sobre la red en óptimas condiciones. En cuanto a la velocidad real de transporte de datos en redes, este término se conoce como throughput.



*Ilustración 1.5.4: Ethernet y el modelo OSI.*

Gigabit Ethernet es el standard más actualizado por que soporta tasas de transferencia más avanzadas que utilizan la mayoría de las laptops y ordenadores modernos. Los centros de datos proporcionan servicios críticos a nivel empresarial tales como servicios en la nube y de respaldo en caso de caídas del sistema y desastres de tal manera se requiere tecnologías de red robustas; entornos en los cuales los administradores de red tengan la capacidad de enlazar servidores con switches y concentradores de red dentro de un rack de telecomunicaciones.

## CAPÍTULO 2 ANÁLISIS, REQUERIMIENTOS

### 2.1 ELICITACIÓN DE REQUERIMIENTOS

En los proyectos de software y aplicaciones o de escritorio, la toma de requerimientos es crucial para el producto final y productos entregables con los resultados deseados.

Para la implementación de este proyecto se hace uso de la metodología scrum, que trata de buenas prácticas para desarrollar el proyecto de forma ágil, trabajando de una forma colaborativa entre los integrantes del grupo, implementando buenas prácticas, lo que ayuda a obtener el resultado esperado en el proyecto. Además, se debe realizar entregables en cada fase del proyecto lo que permite que el cliente se vaya familiarizando con el proyecto, ya que va viendo el avance paso a paso.

La metodología scrum utiliza iteraciones o Sprint para el desarrollo del proyecto, donde cada sprint sirve validar la fase anterior. Para realizar esta metodología se debe realizar tres pasos que son:

- **El punto de partida es un conjunto de objetivos que deben priorizarse:** Esta fase es crucial, ya que según los objetivos priorizados se crearán las iteraciones necesarias y los entregables que se realizarán al cliente en cada sprint.
- **Sprint:** La metodología scrum se ejecuta en lapsos de tiempo periódicos y cortos que se denominan sprint, que es la esencia del método scrum. Los Sprints tienen una duración de 2 a 4 semanas donde se hará un resultado completo. Los Sprints tendrán el mismo formato de presentación y debe existir una comunicación continuada entre ellos.
- **Feedback y reflexión:** Al finalizar cada iteración se presenta el resultado para ser o no aprobado, los integrantes del grupo conversan sobre los aspectos positivos y negativos de software.

### **2.4.1 REQUERIMIENTOS**

Un requerimiento de Software, como definición de acuerdo con [28] “es una necesidad o limitación que se desea resolver. Es un proceso que requiere una elicitación, análisis y especificación y validación mediante pruebas de funcionamiento de software, así como el seguimiento cíclico para una evaluación del cumplimiento de las necesidades de un producto final”.

### **2.4.2 REQUERIMIENTOS FUNCIONALES**

- Diseñar e implementar un módulo en la aplicación para que los usuarios sean capaces de visualizar los diferentes tipos de fallos.
- Tener la capacidad de consultar las gráficas de consumo del ancho de banda en general.

### **2.4.3 REQUERIMIENTOS NO FUNCIONALES**

- Implementar métodos y algoritmos para la categorización de fallos.
- Definir un modelo matemático para predecir la proyección futura del ancho de banda.

## **2.2 HERRAMIENTAS**

Mediante una investigación realizada para designar las herramientas adecuadas que se requieren utilizar para la implementación de la arquitectura, se utilizó software recomendado open source con el fin de recopilar la información requerida dentro del desarrollo de la aplicación móvil propuesta

y se resolvieron los problemas planteados en el proyecto.

### **2.2.1 NEDI**

Para el monitoreo de las redes se usará NeDi; esta herramienta va a permitir obtener información sobre las redes, y mediante la base de datos poder usar esa información “para el desarrollo de la aplicación en Python. NeDi es una aplicación LAMP que permite recorrer la dirección MAC y las tablas ARP para encontrar dispositivos y ver los nodos finales conectados, y los almacena en una base de datos local”. Para ello usa características adicionales que posee como:

- Conciencia de topología inteligente.
- Mapeo/seguimiento de direcciones MAC.
- Gráficos de tráfico, error, descarte y transmisión con alertas basadas en umbrales.
- Monitoreo del estado de la interfaz y los pares BGP.
- Correlación de mensajes de syslog y trampas con eventos de descubrimiento.
- Mapas de red para documentación y paneles de control.
- Detectar puntos de acceso y encontrar dispositivos mediante el descubrimiento.
- Informes extensos que van desde dispositivos, módulos, interfaces hasta activos y nodos [2].

Se “puede iniciar sesión en la GUI de NeDi y realizar búsquedas para determinar el conmutador, puerto de conmutador o AP inalámbrico de cualquier dispositivo por dirección MAC, dirección IP o nombre DNS”. Según la documentación [2] “NeDi recopila la mayor cantidad de información posible de cada dispositivo de red que encuentra, extraer números de serie, versiones de firmware y software, temperaturas actuales y configuraciones de módulos, etc”.

“La arquitectura modular de NeDi permite una integración sencilla con otras herramientas. Por ejemplo, se pueden crear gráficos de cactus basados en la información descubierta”. La arquitectura de NeDi se puede dividir en los siguientes componentes:

Descubrimiento de red (nedi.pl) en azul claro arriba como se puede apreciar en la ilustración 1.3.1.

- Supervisión (moni.pl, trap.pl y syslog.pl) en azul.
- Daemon maestro y lista de agentes para centralizar instancias NeDi distribuidas, en violeta. (Véase ilustración 1.1.1)
- Descubrimiento de nodos para detalles de activos (recopilados por nedi.pl mediante WMI y SSH) en azul.
- Interfaz web modular escrita en PHP y algunos JavaScript en amarillo.
- Interfaz de API Restful escrita en PHP en amarillo oscuro.
- Archivo de configuración maestro (nedi.conf) en azul oscuro.
- Las dependencias también se indican arriba (por ejemplo, API solo habla con la base de datos y flow.pl usa Trafficdata para generar gráficos).

- NFDUMP se puede integrar opcionalmente, ya que la interfaz puede acceder y mostrar datos de Netflow.

### 2.2.2 SNMP

El protocolo que permitirá la comunicación entre NeDi y los dispositivos a monitorear será el “protocolo simple de gestión de redes (SNMP)” [29]. Es un protocolo de diagnóstico de la red que proporciona información del rendimiento actual de la misma. La información normalmente es requerida por el administrador de la red quien es el responsable de otorgar permisos, habilitar puertos de servicio, controlar flujos de tráfico, así como reglas de cortafuegos o firewall.

Las consultas típicas incluyen: la información clave como, el uso de CPU de servidores, picos de anchos de banda, estado de discos y unidades de almacenamiento. Todas estas variables y parámetros clave envían mensajes de confirmación a alguna plataforma que tiene SNMP habilitado. Los Traps son mensajes de notificación de eventos significativos, incluyendo fallas de energía eléctrica y temperatura de equipos críticos, entre otros.

Según el libro [29] se detalla que los dispositivos son monitoreados por el software designado, que a su vez interpreta las solicitudes y Traps (así como también protocolos) de tal manera que sirva para obtener reportes e información del estado de servidores, Routers, Switches, así como métricas de ancho de banda, ping con carga y tiempos de respuesta.

Según la publicación [29], se menciona que SNMP surge como una necesidad para la gestión centralizada de recursos y dispositivos desde una consola única para facilitar las tareas de un administrador, sin embargo, la irrupción de distintos vendedores y organizaciones con múltiples soluciones se situaron muy lejos de un standard, simplemente que abarque las funcionalidades de gestión de redes. Es por esta razón que SNMP tiene cierto nivel de complejidad y hay que tener claro que SNMP no es más que un protocolo que trabaja sobre ambos servidores y hardware de redes, compatible con Unix, Linux y Windows. En sí, no es una herramienta para visualización de datos, sino más bien genera datos que otras herramientas extraen para generar tablas, reportes y gráficos amigables al usuario administrador.

### **2.2.2.1 COMPONENTES DE SNMP**

SNMP utiliza el modelo Cliente-Servidor en conjunto con otros elementos que facilitan las conexiones y los parámetros requeridos para establecerla. Además, incluye los mensajes de alertas y notificaciones de eventos requeridos por ingenieros y administradores de red [29].

El gestor de SNMP es el software de cliente que habilita y envía las solicitudes SNMP. Se le conoce como gestor debido a que su función principal es extraer información de gestión relevante de distintos dispositivos mediante comandos ejecutados [29] .

Un agente SNMP se llama al servidor se ejecuta en un dispositivo como un Router, un servidor o cualquier estación de trabajo. Un agente SNMP es un poco más dinámico que muchos programas de un servidor; se le atribuye funciones como consultas al sistema local y proporcionar información hacia el gestor, e incluso es capaz de reconfigurar el Host esté o no configurado correctamente. Un agente SNMP opera de manera similar mediante comandos, pero en una máquina externa y en teoría puede lograr de manera exitosa múltiples tareas orientadas a la gestión de red.

Los sistemas NMS (Sistema Gestor de Red por sus siglas en inglés), son sistemas gestores diseñados con el objetivo de recolectar datos y enviar instrucciones a los agentes mediante comandos. Son capaces también de ejecutar herramientas de gestión vía múltiples protocolos. Estos incluyen programas que transforman datos SNMP en gráficos comprensibles para la toma de decisiones. En pocas palabras, un sistema con SNMP incorporado se denomina a un programa o software que ejecuta las búsquedas basadas en este protocolo transformándolas en información legible y concisa.

### **2.2.3 REDES PRIVADAS VIRTUALES (VPN)**

Según [30] “una red privada virtual o VPN es un mecanismo para establecer una conexión de acceso remoto entre redes intermediarias”, en muchos casos sobre internet. Las VPN permiten conexiones de larga distancia entre dos nodos extremos, túneles y protocolos de encapsulamiento crean una conexión segura de punto a punto. Estos “túneles” seguros redirigen el tráfico ocultando la dirección IP y encriptando datos del usuario.

Al momento de navegar por Internet, siempre existe la posibilidad de estar expuesto ante atacantes, usuarios mal intencionados y ciberdelincuentes. Las VPN justamente se encargan de proteger al usuario final ya que, al redirigir el tráfico, como se especifica en el documento [30] el usuario es capaz de esquivar ciertas restricciones y conectarse a muchos servidores de alto rendimiento en otras partes del mundo, permitiendo así acceder a determinada información, tales como plataformas de entretenimiento de otros países.

En el ámbito empresarial, se puede evidenciar el uso de VPN empleando métodos de encriptación, y autenticación para facilitar la integridad, confidencialidad y privacidad en la comunicación; muy útil para los siguientes casos:

- Transferencia de correos electrónicos de una o varias compañías, crítico para el envío de archivos confidenciales.
- Conexiones remotas desde un nodo confiable para resolución de posibles problemas en la red empresarial.
- Acceso a cuentas bancarias desde localidades lejanas, ya que, por razones de seguridad, varias instituciones restringen la conexión desde el extranjero, esto se evita accediendo mediante una VPN al conectarse a servidores locales del país de origen.
- Se evita la recolección de datos sin consentimiento basado en historial de compras y sitios web visitados.

Algunas de la VPN más populares en el mercado son: Express VPN, Surfshark, Nord VPN; VPN de acceso libre se incluyen Open VPN y Open Connect en Linux entre otras.

En este proyecto fue fundamental el uso de una VPN, ya que permite conectar directamente al router de borde empresarial. Open VPN es una buena opción, con una sencilla configuración de claves y perfiles para conexiones remotas y gratuita.

#### **2.2.4 FIREWALL**

Antes de abordar el tema de firewall, se debe tomar en cuenta ciertos niveles o zonas de riesgo; una red, subred o redes segmentadas pueden considerarse zonas de riesgo. A mayor riesgo, mayor seguridad es requerida para mitigarlo [31]. La zona opuesta o seguras le considera zonas de confianza y estas requieren menos seguridad.



La mayoría de las redes contienen dos o cuatro zonas de riesgo. Esas zonas incluyen la red privada (LAN), DMZ, extranet e Internet [30]. La zona de red privada tiene el menor nivel de riesgo y mayor nivel de confianza. Internet, por otra parte, tiene el nivel más alto de riesgo y menor confianza. Una DMZ tiene un nivel de riesgo un poco menor al de Internet, pero no un alto nivel de confianza como la red privada, es un nivel intermedio, medio-alto de riesgo y medio-bajo de confianza, respectivamente. Extranet también tiene un mayor nivel de riesgo que la red privada y más confianza que Internet, medio-bajo de riesgo y medio-alto de confianza.

Establecer los niveles de riesgo en una red es importante para las compañías y organizaciones ya que sirve para dictar las políticas y requerimientos de seguridad para cada zona. Dichos requerimientos incluirían la gestión del tráfico, uso de firewalls, uso de VPNs para acceder entre zonas, mejoramiento de seguridad de sistemas, escaneo de código malicioso o programa maligno, etc. Es altamente probable que se encuentre firewalls entre división de cada zona de riesgo como contramedida de seguridad.

Un firewall o cortafuegos es un componente clave de la infraestructura de una organización. Sirve como barrera que cumple ciertas tareas de seguridad. Es un dispositivo de filtrado que verifica que se cumplan las políticas de red para proteger la red de ataques externos, imponiendo restricciones que se aplican al comparar cada paquete entrante a un conjunto de reglas establecidas. Estas reglas especifican si un paquete es o bien permitido o denegado. Si es denegado, se lo descarta. Además, esta regla dicta que, si un paquete es denegado, se impide que llegue al destinatario.

#### **2.2.4 Node.js**

Es un entorno de ejecución versátil con la característica de funcionar en distintos sistemas operativos. Se caracteriza por su sintaxis simple y sencilla de entender. Esto hace que Node.js sea considerado un lenguaje para tener en cuenta por los desarrolladores al crear aplicaciones que se desempeñen en diferentes ámbitos como sistemas embebidos, Web, IA, redes, temas relacionados al Big Data, entre otros.

### **2.2.5 FLUTTER**

Es un SDK para desarrollo que incluye un gran número de librerías para el diseño de interfaz gráfica en aplicaciones. Estas aplicaciones podrán ser ejecutadas en varias plataformas, entre las que se incluyen Linux, Windows, MacOS, WEB, pero con un enfoque centrado principalmente en Android y iOS. Debido a que su rendimiento en estas plataformas es nativo; es similar a una aplicación desarrollada con Java o Kotlin para el caso de Android y Objective C o Swift para el caso de iOS. La primera versión estable de Flutter salió a la luz a finales del año 2018 de la mano de Google y desde entonces ha encontrado un nicho en el mercado de desarrollo de aplicaciones móviles.

### **2.2.6 HERRAMIENTAS DE MONITOREO COMUNES**

En cuanto a monitoreo de redes, se ha mencionado ejemplos de varios programas o software que utilizan SNMP para la gestión de redes. Sin embargo, existen varios comandos y métodos para diagnóstico y recopilación de información útil en los sistemas operativos para verificar conectividad. Conforme con cada propósito se tienen dos niveles de monitoreo como: a nivel de LAN ya nivel de WAN.

A nivel de LAN se trata de tener una idea de localizar fallas causantes de una conexión latente y se recomienda empezar revisando el tráfico local a través de la red de área local. Las ventajas más destacadas del monitoreo de tráfico local son:

- Detección de fallas más simple. Los virus y elementos no deseados son detectados y eliminados.
- Usuarios malintencionados son detectados en base a sus actividades mientras están conectados a la red.
- Equipos de red generan repostes de uso de recursos mediante estadísticas reales.

En cuanto al monitoreo de una WAN, se desea demostrar que el ancho de banda que se está consumiendo refleja el ancho de banda. Esto se puede revisar monitoreando el tráfico externo y esto incluye los siguientes beneficios:

- Costos justificados demostrando el uso actual que el proveedor de servicios está entregando.
- Proyecciones a futuro se pueden evidenciar en base a una media de consumo y tendencias actuales en continua evolución digital.

La detección de caídas del servicio de Internet es constatada o bien por el usuario o desde el ISP aplicando la función de gestión remota del mismo Router proporcionado al cliente. El ancho de banda debe coincidir con el del plan ofertado por el ISP; es este proceso incluso se puede obtener el consumo real que llega al cliente.

En la ilustración 2.2.6, se observa como un ejemplo la manera de verificar conectividad mediante el comando ping a una dirección web específica; se tienen paquetes enviados exitosamente el 100%, caso contrario, resultado sería tiempo de espera agotado o simplemente paquetes agotados. En la ilustración 2.2.7, se tiene el comando **tracert** el cual indica el número de saltos realizados hasta llegar una dirección destino en particular, traza todas las direcciones IP por las que recorrió el paquete hasta llegar a dicha IP, y adicionalmente se proyecta la métrica de latencia en ms que se tardó en realizar cada operación.

```
Microsoft Windows [Versión 10.0.19043.1526]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\alejo>ping www.google.com

Haciendo ping a www.google.com [172.217.28.100] con 32 bytes de datos:
Respuesta desde 172.217.28.100: bytes=32 tiempo=63ms TTL=116
Respuesta desde 172.217.28.100: bytes=32 tiempo=62ms TTL=116
Respuesta desde 172.217.28.100: bytes=32 tiempo=61ms TTL=116
Respuesta desde 172.217.28.100: bytes=32 tiempo=62ms TTL=116

Estadísticas de ping para 172.217.28.100:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 61ms, Máximo = 63ms, Media = 62ms
```

Ilustración 2.2.6: El comando ping que sirve para enviar paquetes a un host determinado.

```
C:\Users\alejo>tracert 8.8.8.8

Traza a la dirección dns.google [8.8.8.8]
sobre un máximo de 30 saltos:

  1    3 ms    2 ms    2 ms  192.168.0.1
  2    3 ms    3 ms    2 ms  192.168.100.1
  3    5 ms    7 ms    6 ms  10.180.0.38
  4   77 ms   67 ms   76 ms  84.16.10.101
  5   74 ms   67 ms   77 ms  94.142.97.159
  6   79 ms   71 ms   70 ms  190.98.141.27
  7   68 ms   69 ms   68 ms  108.170.229.40
  8   68 ms   66 ms   69 ms  172.253.69.129
  9   67 ms   66 ms   66 ms  dns.google [8.8.8.8]

Traza completa.
```

Ilustración 2.2.7: Comando tracert que muestra el número de hops o saltos hacia un destinatario.

### **2.3 TRABAJOS RELACIONADOS**

Los Proveedores de servicios de telecomunicaciones hoy en día son grandes empresas con una infraestructura de red diseñadas para soportar cierta cantidad de clientes para la continua mejora en cuanto a requerimiento y abastecimiento se refiere.

En una investigación [32] pertinente al monitoreo de redes, utilizando métodos paramétricos que permitan generar información relevante y picos de datos de entrenamiento, se realizaron varias estimaciones y aproximaciones en tiempos casi precisos con el fin de determinar excedentes de consumo de ancho de banda en una red de área local. En el presente proyecto se emplea un método similar en cuanto a picos de datos para verificar evidencias de consumo excedidas o debajo del límite de ancho de banda contratado. Luego con estos datos se obtienen ciertas conclusiones para realizar mejoras en el servicio o alguna recomendación.

Un proyecto con características similares [33] trata de un estudio de los principios de monitoreo de redes informáticas basándose en flujos de tráfico analizados con herramientas como Wireshark y NetFlow Analyzer. Luego utilizó los datos generados para implementación de un módulo; que mediante algoritmos bayesianos y arboles de decisión; en el cual realizó una clasificación de dispositivos y asociación de flujos de tráfico a un servicio en particular.

# CAPÍTULO 3 DISEÑO DE LA ARQUITECTURA

## 3.1 Diagrama de hilos de la empresa FINETIC.

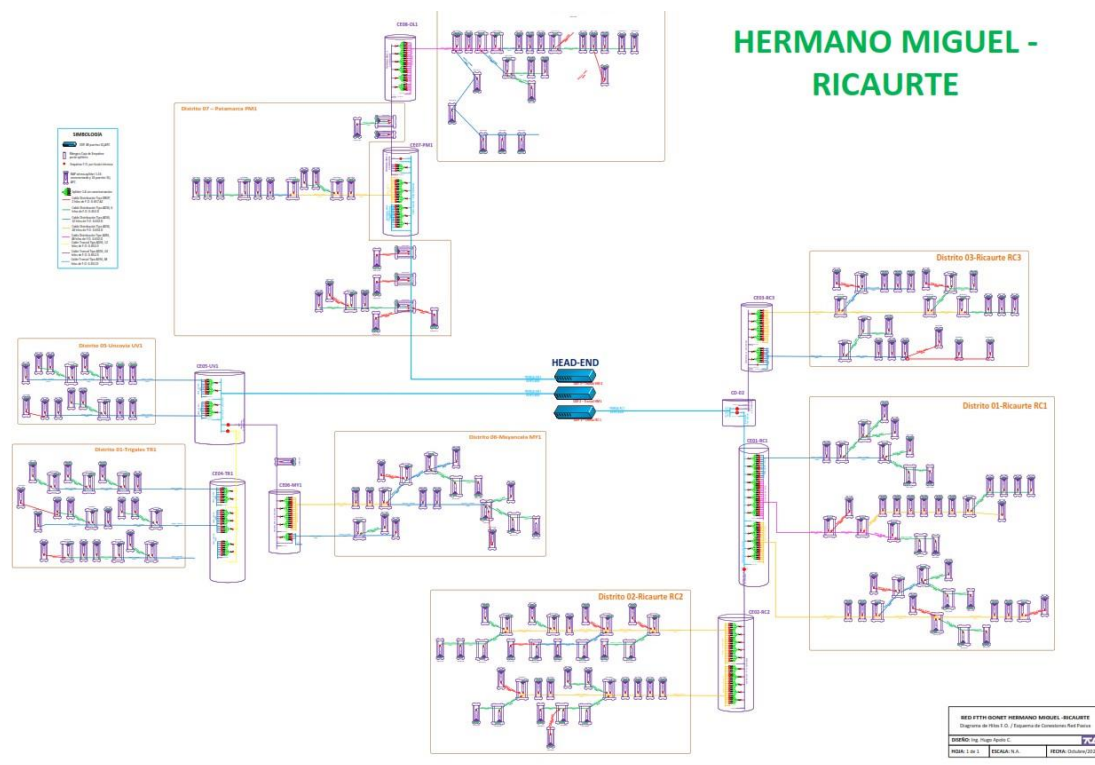


Ilustración 3.1 Diagrama de hilos de la red troncal del ISP.

En la ilustración 3.1, diagrama de hilos de la red troncal de la empresa FINETIC, presenta una troncal de 48 hilos, donde el hilo 1 que está saliendo del splitter 1 le corresponde la OL1A01, aquí se hace una derivación de los hilos del 17 al 23, se hace siete fusiones, conecta de la 17 al 23 área 48, y va conectado del 1 al 7 al correspondiente en la derivación del hilo número doce.

## 3.2 DEFINICIÓN DE LA ARQUITECTURA

Actualmente muchas de las empresas que brindan el servicio de Internet, esperan a que el usuario notifique sobre algún inconveniente en el servicio y luego proceden a brindar la solución a este problema, en cambio usando el monitoreo y la aplicación realizada en Node.js se podría detectar los fallos en tiempo real y sin necesidad que el usuario se comunique cada que vez que existan fallos de conectividad.

Esta plataforma se trata de un sistema distribuido que a través de sus múltiples capas hace uso de diferentes tecnologías y lenguajes de programación. En la interacción entre estas diferentes capas, se tiene la lógica de negocio que permite procesar los datos para luego entregar al usuario la información requerida. Aplicando los conocimientos de redes y los modelos de referencia en conjunto con el sistema distribuido, se construyó una plataforma capaz de monitorear la red utilizando herramientas específicas de Node.js y esto a la final realiza la comunicación con el servidor de monitoreo con el fin de obtener datos relevantes para la empresa.

También se hace uso de un teléfono inteligente donde se instalará la aplicación y se podrá visualizar los resultados de los diferentes fallos con sus posibles soluciones y así puedan resolver sin necesidad que el usuario este llamando a la empresa.

### 3.1.1 ANÁLISIS DE DATOS RELEVANTES

Dentro de la empresa se ha llevado a cabo un registro de sondeo de los soportes registrados mensualmente cuyos hallazgos revelan algunas pautas a tomar en cuenta en el desarrollo de la aplicación. Se almacenaron en una base de datos la información de los clientes quienes han reportado fallas en el servicio como antecedentes. En la ilustración 3.1.1 a continuación se graficaron los distintos tipos de fallos reportados por parte de los clientes.

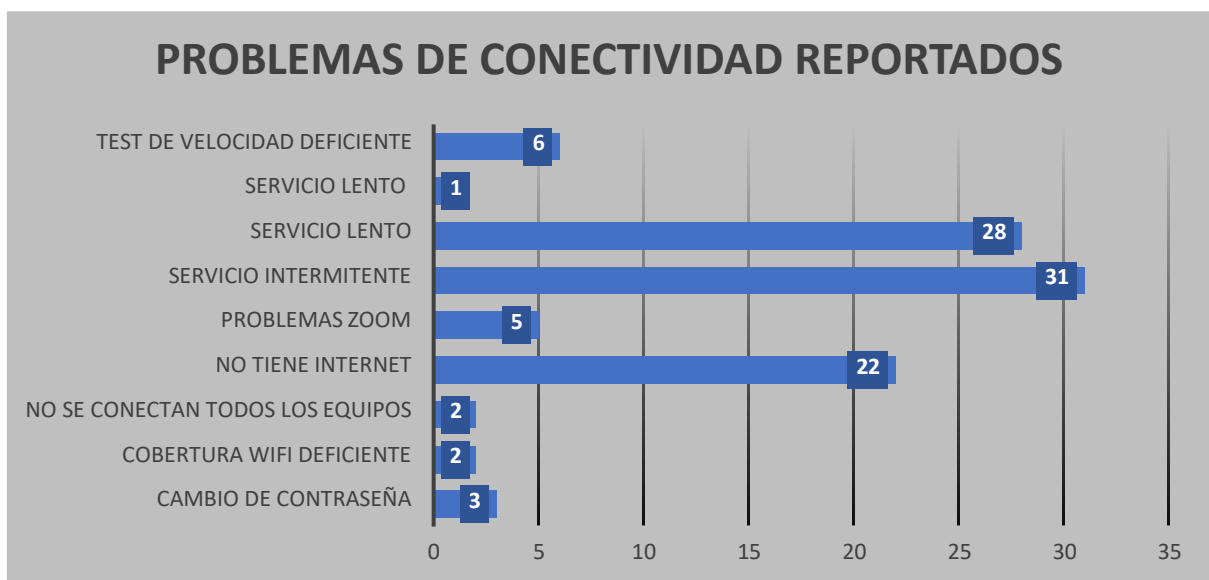


Ilustración 3.1.1: Reporte de problemas de conectividad.

Como se puede observar en la gráfica, el 60% de los fallos recaen en servicio lento e intermitente. La mayor causa probable de este fallo es por equipos deficientes, router u ONU, normalmente se confirma mediante un reinicio y reconfiguración para verificar si reincide el problema, con lo cual se procede a un cambio de equipo.

En la ilustración 3.1.2 en cambio, se realizó el seguimiento de la misma muestra de 100 clientes que reportaron problemas en el grafico anterior. Se determinaron varios problemas, de los cuales según el grafico (ilustración 3.1.2) casi el 50 % indican fallos de equipos. Con esta particularidad, el fallo repetitivo de equipos se tomó en cuenta al desarrollar la aplicación de recomendación.



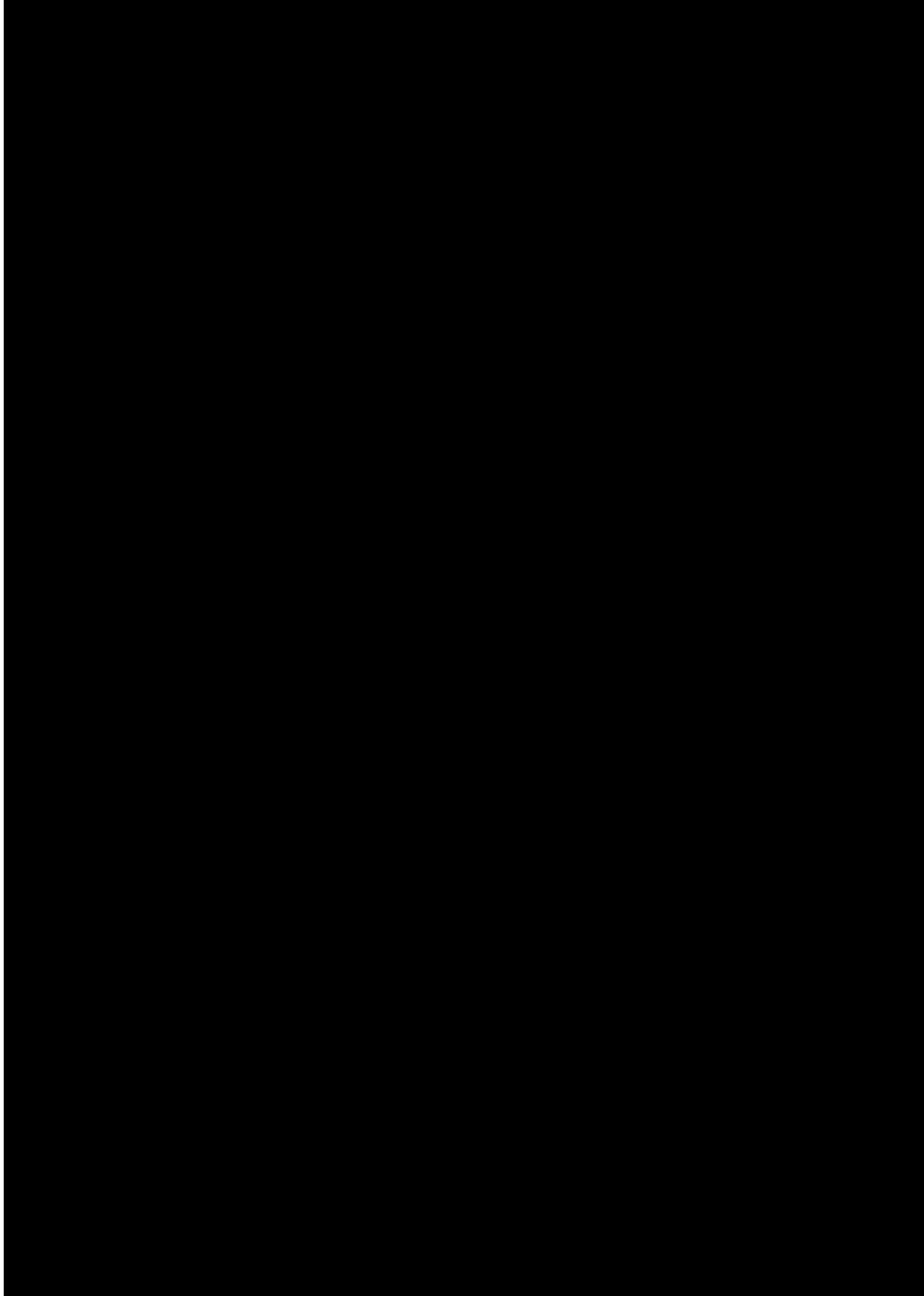
Ilustración 3.1.2: Reporte de problemas determinados por parte de la empresa.

### 3.3 ARQUITECTURA Y COMPONENTES

Previo al análisis de la arquitectura con un enfoque más amplio y el detalle de cada uno de los componentes, de antemano se debe destacar que NeDi; es una pieza clave que juega un papel principal dentro del sistema, puesto que es el encargado de recopilar toda la información necesaria para generar los reportes de fallos que se producen en la red.

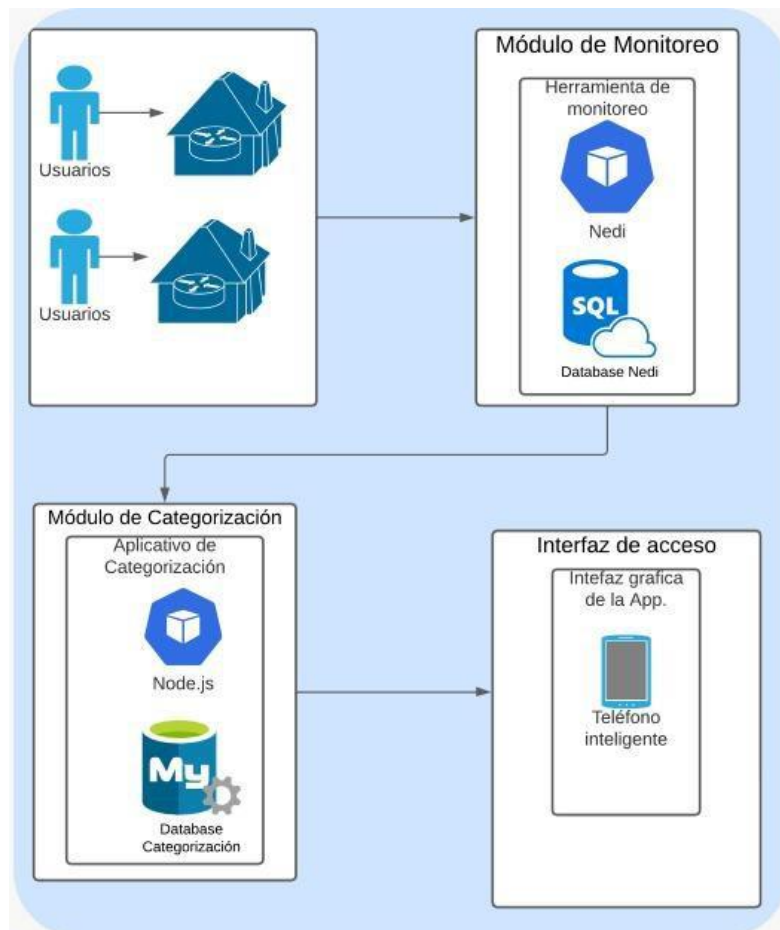
En esta arquitectura logrará que en la aplicación móvil se logre visualizar los distintos fallos que existen en las redes de última milla, para esto se instalará un servidor con NeDi ejecutándose de modo back-end, se realizará el monitoreo y se podrá obtener información que se requiere para poder categorizar los fallos. Con esa información se categoriza los

fallos y a continuación esa información se guardará en la base de datos. Con esos datos se hace un API Rest en Node.js para poder consumir desde la aplicación móvil que está realizada en Flutter, que permitirá visualizar los fallos de forma categorizada.



*Ilustración 3.3.1: 1 Diagrama de flujo de los módulos en la arquitectura del proyecto.*





*Ilustración 3.3.2 2 Arquitectura propuesta para el proyecto.*

Cada componente de la aplicación cumple un papel muy importante dentro de la arquitectura, mediante el funcionamiento correcto de cada componente se logrará exitosamente un funcionamiento óptimo de la aplicación. En la ilustración 3.3.1, se tiene el diagrama de flujo de la arquitectura y cada componente destacado de cada módulo. Por otra parte, en la ilustración 3.3.2 se muestra la arquitectura entre módulos y como interactúan entre sí. A continuación, se detalla cada componente:

### **3.2.1 Modulo de monitoreo**

NeDi mediante SNMP permite el monitoreo, mediante el cual se tiene un control de todos los puertos de un Switch, por ejemplo, realizando un barrido de todos los nodos y dispositivos interconectados física y lógicamente mediante VLANS creando un mapeado de la red aplicando un componente de su arquitectura conocido como Spanning Tree.

NeDi realiza descubrimiento de dispositivos de red conectados a nodos finales. Incluye dentro de su arquitectura características adicionales para gestionar redes empresariales segmentando en una topología inteligente que obtenga las direcciones MAC para el seguimiento, tráfico entrante y saliente, mensajes de error, paquetes descartados y una visualización del umbral basado en alertas y reportes del tiempo de actividad; verificación de estado de enlaces BGP y monitoreo de interfaces conectadas a nodos vecinos. NeDi también correlaciona los mensajes syslog y eventos específicos. Adicionalmente se tiene la capacidad del mapeado de redes para mayor documentación relevante como reportes y tableros de gestión, detección de puntos de acceso poco confiables, así como ubicar dispositivos basados en su IP.

La arquitectura modular de NeDi permite una integración de tecnologías híbridas con varias herramientas, así como creación de gráficos a partir de la información recuperada. En la siguiente tabla se tienen los componentes principales de NeDi con la información detallada de cada uno de ellos.

Tabla 3.2.1: Componentes principales de NeDi y sus funciones.

Objetivo	Componente	Descripción
Descubrir dispositivos de red utilizando SNMP y SSH/Telnet	nedi.pl	Ejecuta nedi.pl vía consola, System-NeDi en la interfaz Web o utilizar crontab para verificar intervalos fijos. Esto también sirve para rastreo de MAC e IP para recolección de datos de la interfaz de comunicación.
Monitoreo de dispositivos de red descubiertos	moni.pl	Ejecuta moni.pl vía consola, web o que se inicie mediante scripts init.d. Agrega dispositivos deseados y controla la frecuencia de monitoreo.
Recibir mensajes Syslog	sysloog.pl	Se ejecuta vía consola, web o auto arranque mediante init.d.
Recibir los mensajes trap SNMP	trap.pl	Configura trap.pl para el manejo de traps en snmpttrapd
Monitoreo de equipos NeDi remotos	master.pl	Agrega réplicas de Nedi remotas en su lista de agentes. Ejecutado del mismo modo que los anteriores, se pueden configurar métodos de como los agentes remotos proporcionan la conexión de APIs (ej.: https y ruta raíz).
Descubrir activos	nodl.pl	Ejecución similar a anteriores, se recomienda utilizar una base de datos distinta si nedi.pl se está ejecutando en otro proceso.
Monitoreo de Tráfico	nfdump, flowi.pl	Ejecuta nfcpad para netflow, sfcapd para sflow o nfcapd para capturar tráfico en una interfaz. Se debe especificar la ruta hacia los datos de netflow en fichero nedi.conf. En el mismo archivo se ajusta el atributo nfdpath y puertos IP para graficar.

Los siguientes son los componentes relevantes de NeDi dentro de su interfaz de administración [2]:

- Dispositivos
  - Equipos con SNMP habilitado, o bien un servidor o impresora.
  - Cliente o servidor con WMI habilitado.
  - Cliente o servidor UNIX con SSH habilitado.
- Módulos
  - Fuentes de alimentación o transceivers ópticos dentro de los dispositivos conectados.
  - Máquinas Virtuales en hipervisores.
  - Suministros en impresoras.
  - CPU, RAM, HDD, software instalado en WMI o dispositivos mediante SSH.
- Nodos
  - Direcciones MAC desde la bridge-forward table en un switch.
  - Direcciones IP de tablas ARP en routers o switches capa 3.
  - Resolución de DNS obtenidos del reverse lookup de IPs.
- Enlaces
  - Conexiones entre dispositivos almacenados en una tabla de enlaces
  - Son creados mediante CDP, LLDP.
- Activos
  - Objetos con un numero serial en la tabla de inventarios.
  - Gestión mediante apartado de Gestión de Activos, así como importación de archivos CSV con información relevante.
- Políticas
  - Reglas definidas en el apartado de System Policies para crear alertas o acciones.
  - Evaluadas en distintos puntos durante etapa de descubrimiento.
  - Paquetes, flujos de bytes son evaluados por flowi.pl.

El sistema de gestión de base de datos desempeña un papel importante en la arquitectura de este sistema; permite almacenar toda información referente a la red de la empresa, como, por ejemplo: la información de los contratos de clientes, información referente a la propia red y su estado de funcionamiento. Al mantener toda esta información almacenada es posible recuperarla mediante consultas para luego procesarla y posteriormente realizar un análisis.

### **3.2.2 Modulo de Categorización**

Es un entorno de ejecución basado en el motor v8 de Google. Permite ejecutar código Javascript desde el lado del servidor; aunque esto puede resultar un tanto paradójico si se tiene en cuenta el hecho de Javascript nació como lenguaje de programación para front-end y actualmente este se ejecuta en la mayoría de los navegadores permitiendo crear sitios web interactivos con animaciones y demás. Con Node.js es posible sacar un mayor

provecho a Javascript, y hace posible el tener una gran aplicación distribuida escrita en su totalidad en este lenguaje de programación, es decir, que tanto el front-end como el back-end utilizaran Javascript para funcionar; esto facilita el mantenimiento e integración entre módulos.

Para el análisis se requiere de la información almacenada de sobre la red y aplicar determinados algoritmos para generar los reportes requeridos para detectar problemas presentes en las redes GPON. Luego de detectar los fallos se realiza una categorización de los fallos y se asigna una prioridad. Se obtienen el estado de la red, nombre del cliente y fallo encontrado.

La categorización es el proceso de clasificar cada fallo empleando diferentes técnicas y herramientas que están incorporadas en la aplicación. Se asigna identificadores exclusivos (nombre/ID/valor). Este proceso se realiza luego del análisis y permite categorizar los fallos en diferentes niveles o jerarquías. Según estos niveles o jerarquías se recomienda una solución específica para cada fallo.

Los API permiten el intercambio de datos entre clientes y aplicaciones. También pone a disposición funciones adicionales que los desarrolladores pueden invocar y pasarles argumentos para recibir retroalimentación desde el servidor a través del protocolo HTTP. Los API Rest utilizan este protocolo como un medio para transmitir información y comunicar el servidor con los clientes.

Permite entablar un canal de comunicación entre la aplicación móvil y el servidor back-end encargado de obtener los datos almacenados en el sistema gestor de base de datos. Luego de procesar estos datos los transmite a la aplicación y permite al técnico a cargo obtener la información necesaria para corregir el problema.

### **3.2.3 Interfaz de Acceso**

El acceso a los servicios se realiza mediante un dispositivo que abstrae las funciones de un teléfono móvil y de un ordenador al mismo tiempo, lo que convierte a este dispositivo en un “ordenador de bolsillo”. Los teléfonos inteligentes incluyen funciones que permiten navegar por internet, instalar aplicaciones y por su puesto comunicar personas con GUI o interfaces gráficas. Dadas estas características y debido a su portabilidad

resulta particularmente conveniente generar un aplicativo que funcione sobre el dispositivo y facilite el acceso a la información y reportes de fallos presentes en el ISP.

#### **3.2.4 Administrador**

Es el recurso humano de la empresa responsable de gestionar, administrar y brindar soluciones en caso de ser necesario. Es el encargado de asignar visitas técnicas o supervisión de fallos o posibles anomalías de la red además de llevar una bitácora y un histórico de los diferentes tipos de fallos que se pueden suscitar. Al acceder al aplicativo móvil, el administrador recibirá reportes de estado de conectividad de ciertos usuarios que presenten fallas con el fin de proceder a realizar el soporte técnico adecuado.

## CAPÍTULO 4 IMPLEMENTACIÓN DE LA ARQUITECTURA

### 4.1 Diferentes fallos de red existentes

**Potencia baja:** Los valores de atenuación (dBm) obtenidos en la fibra del cliente exceden los -27dBm; lo que ocasiona intermitencias en la señal y en efecto, deficiencias en el servicio de internet. Con una potencia muy baja, la ONU es incapaz de procesar las señales de luz dispersa para la conversión a bits dentro del router lo que ocasiona una falla total del servicio. El rango de tolerancia de pérdida de potencia en redes GPON es hasta -27 dBm, en la ilustración 4.1.4 se presenta un diagrama de bloques que destacan los puntos de pérdida de señal establecidos.

**ONT defectuosa:** Como consecuencia de fallas en la tarjeta de la ONU u ONT, al conectar el cable drop de fibra hacia el hogar, armado con su respectivo conector SC/APC como los presentados en la ilustración 4.1.1. La ONU no reflejará potencia de señal alguna, esto se comprueba utilizando un OPM enganchado al conector, si detecta valores mayores a -27 dBm, se logra constatar el fallo de equipo, en este caso la ONU. Adicionalmente se debe comprobar el estado del puerto ethernet de la ONU con un router, si enciende el led correspondiente de la ONU, indica que el puerto es funcional.

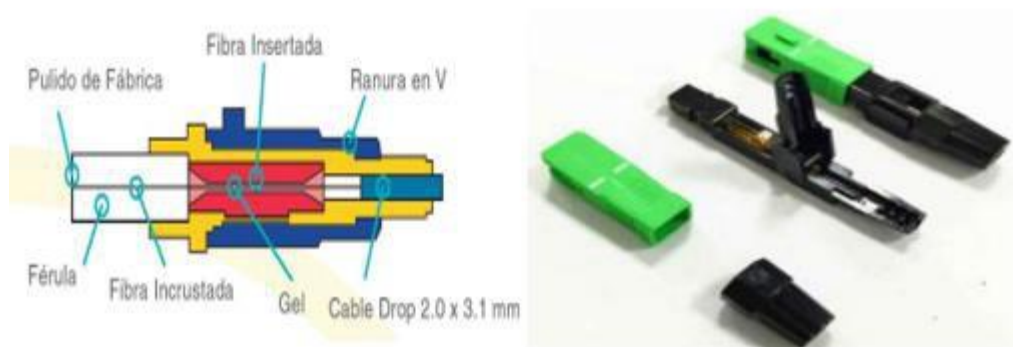


Ilustración 4.1.1:3 Conector SC/APC y sus partes. [34]

**Wifi no certificado:** Al momento de realizar la prueba de velocidad el resultado es poco eficiente y al momento de navegar por internet se nota que la velocidad del servicio está lenta, muy por debajo del ancho de banda contratado. La posible solución será la reconfiguración del Router o un reemplazo del equipo.



*Ilustración 4.1.2:4 Una fibra enganchada al OPM reflejando el estado LOS.*

**Saturación:** El servicio se ralentiza, posiblemente por excesiva cantidad de hosts conectados a la red, lo que indica que el ancho de banda actual no abastece a la cantidad de usuarios o el equipo designado es poco eficiente y una posible solución es el cambio de router. Se refleja en que el servicio se vuelve más lento y una posible solución sería el cambio de clave frecuentemente para que personas desconocidas no pueden acceder a la red.

**LOS (Pérdida de Señal):** El estado de la ONU reflejado en la ilustración 4.1.3 indica que la ONU no refleja potencia hacia OLT y el origen del fallo es desconocido, por lo tanto, una de las posibles soluciones es delegar un soporte presencial al cliente. Al realizar una medición de potencia, el resultado es similar al obtenido en la ilustración 4.1.2.

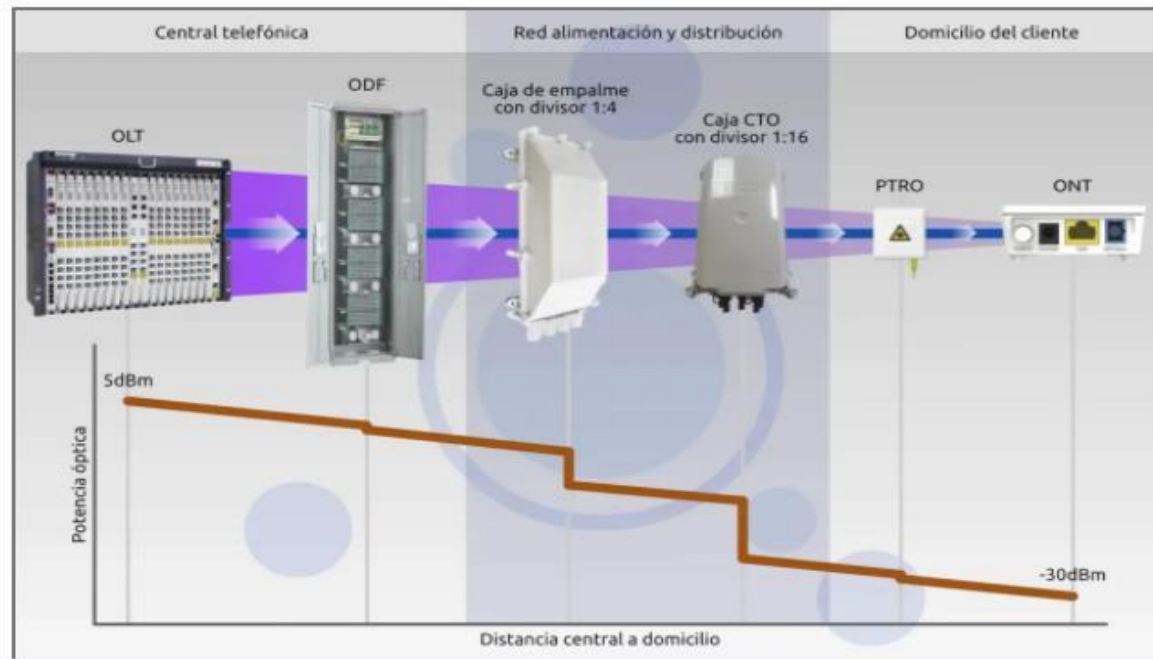




*Ilustración 4.1.3:5 ONU reflejando un estado en LOS.*

**PowerFail:** Las conexiones eléctricas defectuosas de un domicilio frecuentemente ocasionan este tipo de fallos. En ciertos casos el adaptador eléctrico del propio equipo no funciona. Sin embargo, si la falla proviene desde el medidor eléctrico puede incluso quemar los equipos como el router y la ONU. Esto se reflejará como un estado de PWR Fail dentro de la aplicación. Este tipo de fallo indica que existe una falla eléctrica en el domicilio o posiblemente la placa de la ONT se quemó.

**PPPOE:** Este es un fallo de autenticación para la conexión PPPoE. El usuario y contraseña deben ser los correspondientes que el ISP proporciona al cliente. Otra posibilidad es un error inesperado en la página o interfaz de configuración del router, el procedimiento a seguir para la corrección de este error es el reinicio de equipos, constatando de esta manera si reincide el problema, se requiere una reconfiguración. El fallo también puede suscitarse por un fallo de asignación de IP y esto se resuelve al apagar y encender los equipos.



*Ilustración 4.1.4:6 Diagrama de segmentación por bloques de una red GPON. [35]*

En la ilustración 4.1.4 se tiene un rango de valores de pérdida de potencia(dBm) en cada tramo de la red GPON a través de la oficina central, en sentido de descarga hacia la red de distribución y como punto destinatario la red de última milla en el domicilio del cliente. La OLT es el punto de partida de toda red GPON, luego en la parte del ODF o distribuidor de fibra óptica es donde pasan todas las fibras para realizar empalmes, interconexiones, adaptadores y los conectores deben ser armados acorde con las especificaciones detalladas en [31]. En el tramo de la red también se incluyen splitters y divisores ópticos en las cajas de distribución que reflejan pérdidas adicionales dentro de un rango de tolerancia hasta -27dBm en el punto del usuario.

Los fallos de las ONU ocurren, según la propuesta del artículo [36] indica que existen ciertas vulnerabilidades que afectan la seguridad y el correcto funcionamiento de estos dispositivos. Se trata de ataques de degradación que inciden en el algoritmo de control de colisiones dentro del protocolo TCP, lo cual es posible que afecte que el ancho de banda de los usuarios perjudicados. La propuesta de solución detallada en este artículo es un mecanismo DBA mejorado para combatir esta amenaza. Dentro de varias simulaciones realizadas en Python, se implementó una fase de detección para monitorear y mitigar cualquier anomalía que se presente según el comportamiento de las ONU probadas. Los resultados de estas pruebas demostraron que la seguridad mejoro en un 63% [36] de acuerdo con las comparaciones los distintos contenedores de tráfico.

Las tecnologías de fibra óptica ofrecen múltiples ventajas para un ISP ya que son económicas y eficientes en cuanto a rendimiento de la red desde la OLT en la oficina central hasta las ONU/T en los domicilios del usuario.

En [37] se señala que, a pesar de los beneficios ya mencionados, las redes FTTH tienden a presentar varios problemas mayormente desde la NAP de distribución hacia la ONU. El tendido del cable drop normalmente se encuentra en un ambiente áspero con áreas de vegetación elevada y alta densidad de tráfico que ponen en riesgo a cada enlace óptico de la zona. Es fundamental la necesidad de implementar un sistema centralizado y automatizado [37] en una red de sensores punto-a-multipunto capaz de recopilar eventos de degradación y anomalías en la red GPON, para que posteriormente el NMS logre localizar y proporcionar el debido mantenimiento a las fallas que se presenten.

La confiabilidad en una red GPON es importante ya que cualquier falla en la infraestructura conlleva a costos operativos elevados y posibles inconvenientes con los usuarios.

Se realizaron pruebas para constatar la factibilidad de la categorización fallos mediante el monitoreo con NeDi y se obtuvo que los fallos de potencia baja, ONT con problemas, wifi no certificado, saturación, exceso de clientes en routers obtuvieron porcentajes de efectividad de menos de 50% de efectividad dichas pruebas, en cambio las de: LOS (Pérdida de Señal), PowerFail (Pérdida de energía), PPPOE obtuvieron un porcentaje de más de 70% de efectividad al realizar las pruebas, por lo que se procedió a implementar las tres últimas en la aplicación donde se realiza la categorización de esos fallos.

## 4.2 PRERREQUISITO DE INSTALACIÓN DE NEDI

*Tabla 4.1 Prerrequisitos para la instalación de NeDi.*

<b>Componente</b>	<b>Característica</b>
Procesador	2 GHz y 1 núcleo.
Memoria RAM requerida	1 GB
Unidad de Almacenamiento	100 GB

### 4.3 INSTALACIÓN Y CONFIGURACIÓN DE NEDI

```
Cristhian@Cristhian MINGW64 ~  
$ sudo apt-get install apache2 libapache2-mod-php5 mysql-server libnet-snmp-perl  
libcrypt-rijndael-perl libcrypt-hcesha-perl libcrypt-des-perl libdigest-hmac-pe  
rl libio-pty-perl libnet-telnet-perl
```

Ilustración 4.2.1. Instalación de paquetes para instalar la aplicación NeDi.

```
Cristhian@Cristhian MINGW64 ~  
$ sudo wget https://www.nedi.ch/pub/nedi-2.0C.npkg|
```

Ilustración 4.2.2 Descarga de la aplicación de NeDi.

```
Cristhian@Cristhian MINGW64 ~  
$ sudo chown -R www-data:www-data /opt/nedi
```

Ilustración 4.2.3 Permisos para acceder a NeDi.

```
Cristhian@Cristhian MINGW64 ~  
$ sudo ln -s /opt/nedi/html/ /var/www/
```

Ilustración 4.2.4 Enlace simbólico para acceder a la aplicación.

```
Cristhian@Cristhian MINGW64 ~  
$ sudo mysqladmin -u root -p password "dbpa55"
```

Ilustración 4.2.5 Permisos de la base de datos

### 4.4 CODIGO RELEVANTE DE LA APLICACIÓN EN NODE.JS.

En la figura 4.3.1 Se observa la conexión que se realiza con la base de datos usando la librería “MySQL”, se pone los datos de la base de datos como: host, port, user, password,

database, además se puede controlar si existe error al momento de conectar a la base de datos.

```
////////MySQL
var connection = mysql.createConnection({
  host: 'localhost',
  port: 3306,
  user: 'tesis',
  password: 'admin.12345',
  database: 'tesis',
});

/// Revisar coneccion
connection.connect(error => {
  if (error) throw error;
  console.log("Base de datos corriendo");
});
```

Ilustración 4.3.1 Conexión a la base de datos MySQL.

En la figura 4.3.2 Se realiza un servicio Rest usando la librería Express para la consulta de inserción de datos.

```
✓ datoslos.map(value => {
  ✓ const sql = 'INSERT INTO Los SET ?';
  ✓ const losObj ={
    contrato: value.contrato,
    ip:value.ip,
    direccion:value.direccion,
    problema:value.problema,
    solucion:value.solucion,
    estado:value.estado,
    fecha:value.fecha,    ///agregue esto
    tiempo:value.tiempo
  }
  ✓ connection.query(sql,losObj, error => {
    if(error) throw error;
    console.log("cliente agregado");
  });
})
```

Ilustración 4.3.2 Método para la inserción de datos de LOS en la base de datos.

En la figura 4.3.3 Se realiza un servicio Rest usando la librería “Express” para que liste desde la base de datos.

```
app.get('/listPwrFailFecha/:tiempo', function (req, res, next) {
  const tiempo = req.params.tiempo;
  let sql = '';

  console.log('tiempo services', tiempo);
  if (`${tiempo}` <= 30) {
    sql = `SELECT * FROM PwrFail WHERE tiempo BETWEEN 0 and 30`;
    connection.query(sql, function (error, result, fields) {
      if (error !== null) {
        res.send('error, no existe datos en la base', error);
      } else
        res.json(result)
    });
    console.log('ingresa 30');
  } else if (`${tiempo}` > 30 && `${tiempo}` <= 60) {
    sql = `SELECT * FROM PwrFail WHERE tiempo BETWEEN 31 and 60`;
    connection.query(sql, function (error, result, fields) {
      if (error !== null) {
        res.send('error, no existe datos en la base', error);
      }
    });
  }
});
```

Ilustración 4.3.3 Método para la inserción de datos de LOS en la base de datos.

#### 4.5 CODIGO RELEVANTE DE LA APLICACIÓN EN FLUTTER.

En la figura 4.4.1 se observa el código para consumir el servicio Rest del fallo LOS del back end que fue desarrollado en Node.js.

```
final list<LosModel> notificaciones1 = [];
// final respuesta = await _dio.get('http://1858-191-100-63-76.ngrok.io/ip');
// final respuesta = await _dio.get('${url_server}/listLosFecha/:tiempo');
final respuesta = await _dio.get('${url_server}/listLosFecha/${tiempo}');
final lista = respuesta.data as List;
print(lista);
lista.map((e) => {notificaciones1.add(LosModel.fromMap(e))}).toList();

return notificaciones1;
```

Ilustración 4.4.1 Código del servicio de LOS en flutter.

En la figura 4.4.2 se puede visualizar el código que permite consumir el servicio Rest del fallo conocido como PowerFail del back-end que está realizado con Node.js.

```

final List<PwrFailModel> notificaciones1 = [];
// final respuesta = await _dio.get('http://1858-191-100-63-76.ngrok.io/ip');
// final respuesta = await _dio.get('$url_server/listPwrFailFecha/:tiempo');
final respuesta = await _dio.get('$url_server/listPwrFailFecha/$tiempo');
final lista = respuesta.data as List;
print(lista);
lista.map((e) => {notificaciones1.add(PwrFailModel.fromMap(e))}).toList();

return notificaciones1;
}

```

Ilustración 4.4.2 Código del servicio de LOS en flutter.

En la figura 4.4.3, se puede ver la codificación de la vista del fallo LOS, utilizando un ComboBox donde se selecciona el rango de tiempo y se visualiza los usuarios que se encuentran en cada rango.

```

body: (isLoading)
? const Center(
  child: CircularProgressIndicator(),
) // Center
: (lista.isNotEmpty)
? ListView.builder(
  itemCount: lista.length,
  itemBuilder: (context, int index) {
    return ListTile(
      title: Text(lista[index].contrato),
      subtitle: Text(lista[index].ip),
      onTap: () {
        Navigator.pushReplacement(
          context,
          MaterialPageRoute(
            builder: (context) => losSolucionView(
              notificacion: lista[index],
            )); // losSolucionView // MaterialPageRoute
      },
    ); // ListTile
  }) // ListView.builder
: Center(
  child: Text("No hay informacion para $selectValue minutos"), // Center

```

Ilustración 4.4.3 Código de la página principal del fallo LOS.

En la figura 4.4.4 Se puede observar la parte del código relevante de la vista del fallo PowerFail, usando un ComboBox donde se puede seleccionar el rango de tiempo y visualizar a los usuarios que se encuentran en cada rango.

```

body: (isLoading)
  ? const Center(
    child: CircularProgressIndicator(),
  ) // Center
  : (lista.isNotEmpty)
    ? ListView.builder(
      itemCount: lista.length,
      itemBuilder: (context, int index) {
        return ListTile(
          title: Text(lista[index].contrato),
          subtitle: Text(lista[index].ip),
          trailing: const Icon(Icons.keyboard_arrow_right),
          onTap: () {
            Navigator.pushReplacement(
              context,
              MaterialPageRoute(
                builder: (context) => pwrFailsolucionView(
                  notificacion: lista[index],
                )), // pwrFailsolucionView // MaterialPageRoute
            );
          },
        ); // ListTile
      }) // ListView.builder
    : Center(
      child: Text("No hay informacion para $selectValue minutos"), // Center
    );

```

*Ilustración 4.4.4 Código de la página principal del fallo PowerFail.*

En la figura 4.4.5 se puede observar la codificación de la página donde se muestra al usuario con la posible solución según los rangos de tiempo en estado LOS.

```

body: Container(
  padding: const EdgeInsets.all(20),
  child: Column(
    children: [
      Table(
        children: [
          const TableRow(
            decoration: BoxDecoration(
              color: Colors.black26,
            ), // BoxDecoration
            children: [
              Text('Usuario', style: styleTotal),
            ],
          ), // TableRow
          TableRow(
            decoration: const BoxDecoration(
              color: Colors.black12,
            ), // BoxDecoration
            children: [
              Text(widget.notificacion.contrato, style: styleDetalle),
            ],
          ) // TableRow
        ],
      ), // Table
      const SizedBox(height: 20),
    ],
  );

```

*Ilustración 4.4.5 Código de la visualización del usuario con la solución correspondiente del fallo de LOS.*

En la figura 4.4.6 se puede observar la codificación de la página donde se muestra al usuario con la posible solución según los rangos de tiempo en PowerFail.



```

const SizedBox(height: 20),
Table(
  children: [
    const TableRow(
      decoration: BoxDecoration(
        color: Colors.black26,
      ), // BoxDecoration
      children: [
        Text('Problema', style: styleTotal),
      ],
    ), // TableRow
    TableRow(
      decoration: const BoxDecoration(
        color: Colors.black12,
      ), // BoxDecoration
      children: [
        Text(widget.notificacion.problema, style: styleDetalle),
      ],
    ) // TableRow
  ],
), // Table

```

Ilustración 4.4.6 Código de la visualización del usuario con la solución correspondiente del fallo de PowerFail.

## 4.6 RESULTADOS

Se puede visualizar las gráficas realizadas de los resultados de las pruebas que se ejecutaron de la aplicación móvil. Los diagramas de caja son un método gráfico para el despliegue de variación en un conjunto de datos. En la mayoría de los casos, se utiliza para obtener un resumen de datos de distintas fuentes y posteriormente mostrar la información extraída en una gráfica.

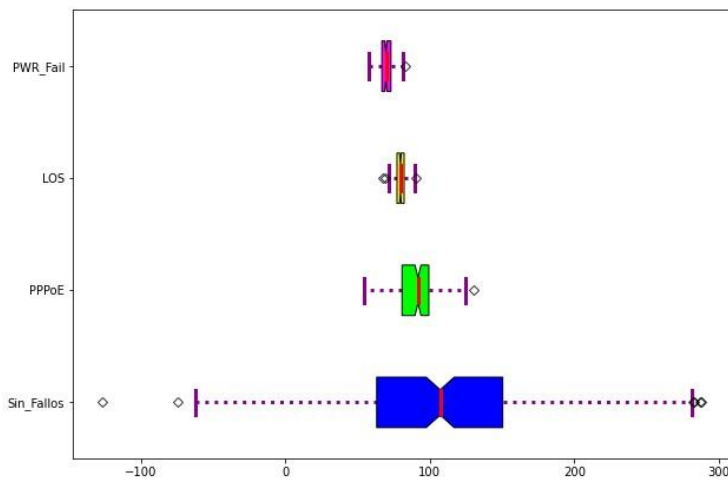


Ilustración 4.6.1 Gráfica de la prueba 1 de ejecución de la aplicación.

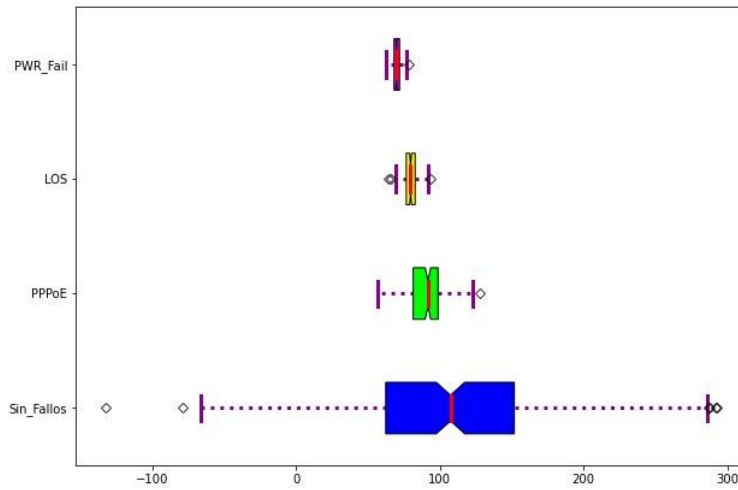


Ilustración 4.6.2 Grafica de la prueba 2 de ejecución de la aplicación.

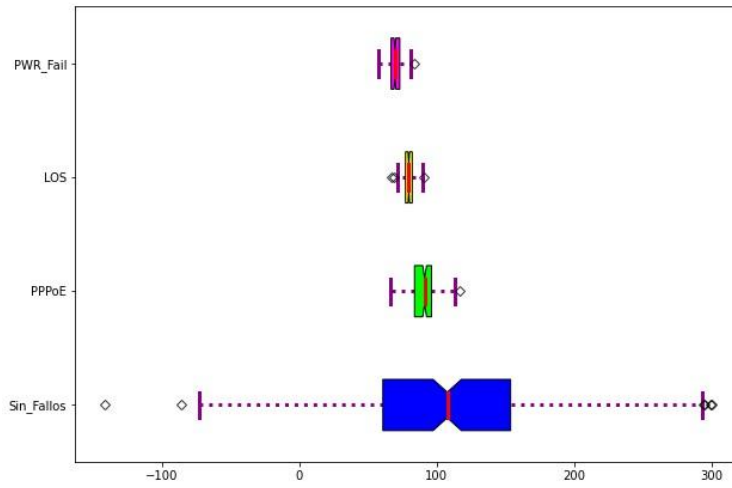


Ilustración 4.6.3 Grafica de la prueba 3 de ejecución de la aplicación.

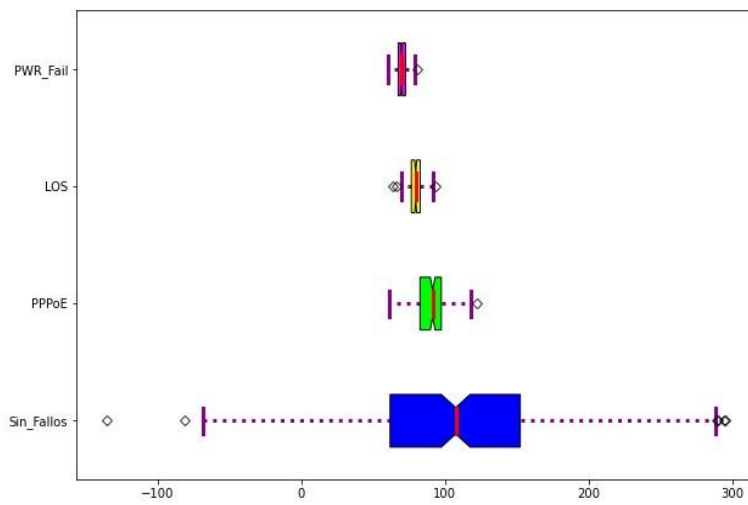


Ilustración 4.6.4 Grafica de la prueba 4 de ejecución de la aplicación.

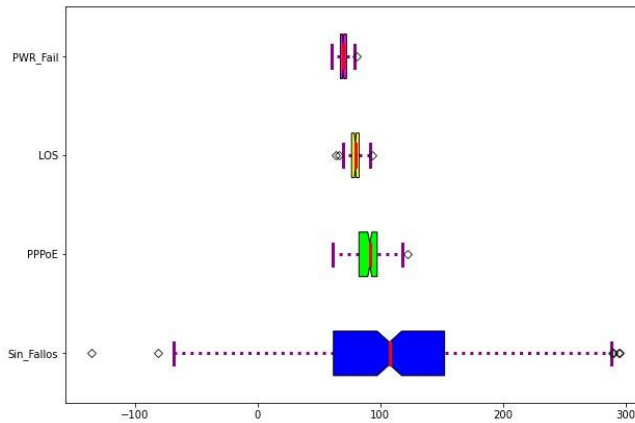


Ilustración 4.6.5 Grafica de la prueba 5 de ejecución de la aplicación.

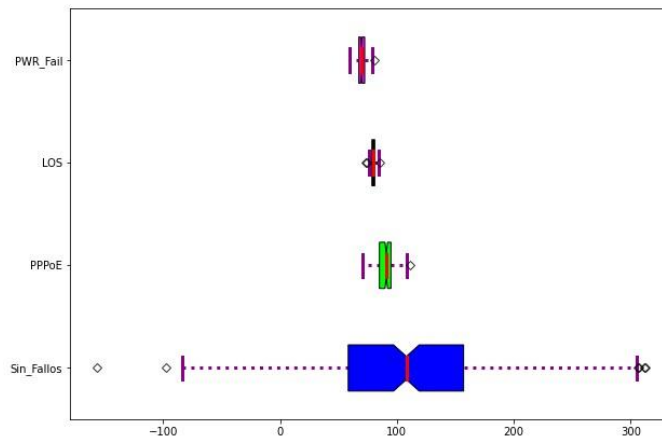


Ilustración 4.6.6 Grafica de la prueba 6 de ejecución de la aplicación.

En las ilustraciones 4.6.1 al 4.6.6 en el eje vertical se denotan los tipos de fallos y una opción adicional sin fallos; la variable horizontal es donde se encuentran los porcentajes de los resultados obtenidos, se puede observar que los resultados son parecidos en estas pruebas realizadas. Lo que se puede observar la baja cantidad de fallos en la red, la mayoría de los usuarios no presentan errores y un numero pequeño de usuarios presentan algún fallo, en LOS o eléctrico.

La distribución en PWR Fail y en LOS se mantuvo en un nivel bajo mientras que en PPPoE los valores obtenidos varían dependiendo de la hora en que se realizó la prueba y la variación de cada prueba tuvo un porcentaje de error de  $\pm 3\%$ .

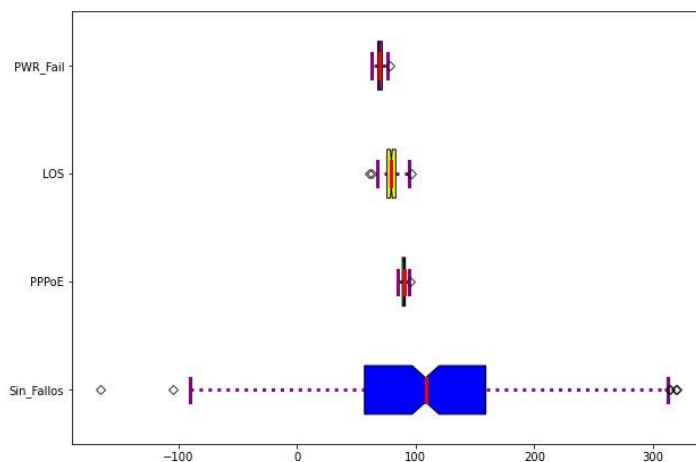


Ilustración 4.6.7 Grafica de la prueba 7 de ejecución de la aplicación.

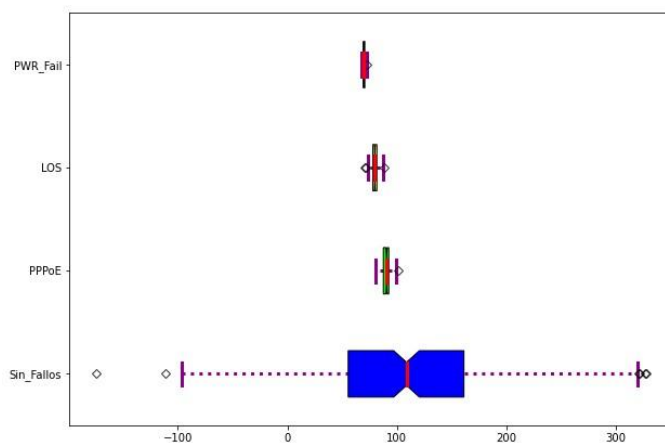


Ilustración 4.6.8 Grafica de la prueba 9 de ejecución de la aplicación.

En las ilustraciones 4.6.7 y 4.6.8 se puede observar que no se ha presentado usuarios con ninguno de los fallos como: LOS, PPPoE y PowerFail al momento de realizar estas pruebas.

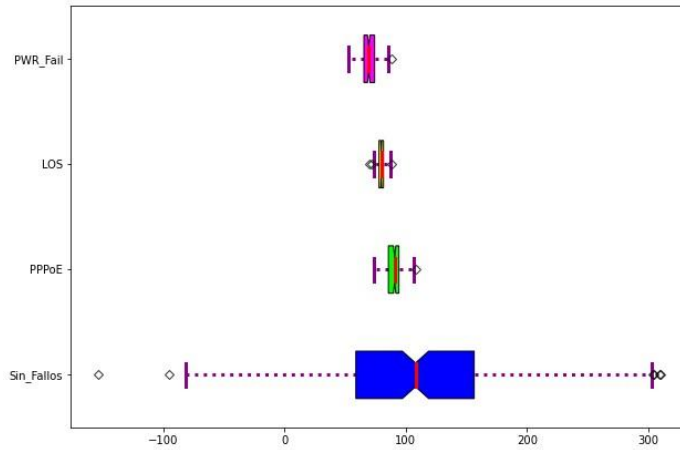


Ilustración 4.6.9 Grafica de la prueba 8 de ejecución de la aplicación.

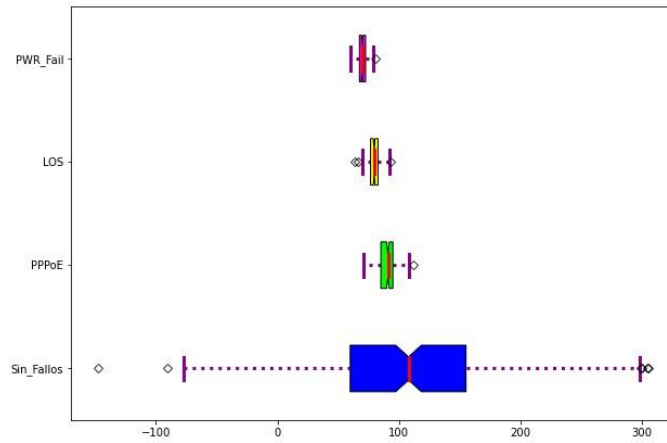


Ilustración 4.6.8 Grafica de la prueba 10 de ejecución de la aplicación.

En las ilustraciones 4.6.9 y 4.6.10 se tiene que se han presentados fallos de PPPoE y de LOS, pero muy pocos usuarios han presentado estos inconvenientes, la mayoría de los usuarios no presentan ningún tipo de fallo.

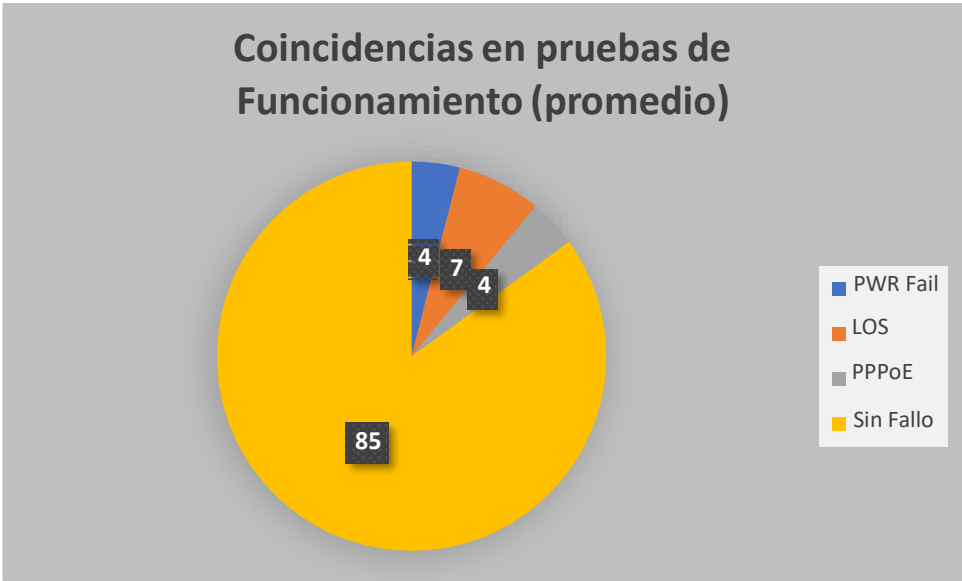


Ilustración 4.6.11 Grafica de la prueba 10 de ejecución de la aplicación.

En las ilustraciones 4.6.11 se puede observar que, de los 100 usuarios que formaron parte de las pruebas, como promedio, han existido 4 usuarios con PowerFail, 7 usuarios han presentado problemas de perdida de señal y 4 han presentado problemas de PPPOE, y el 85% de los usuarios no han presentado ningún tipo de fallo.

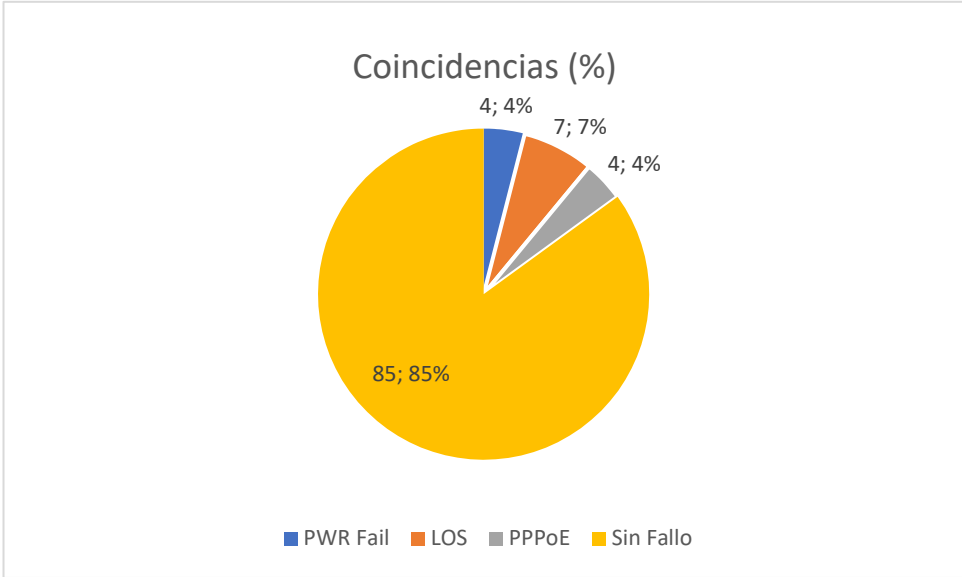


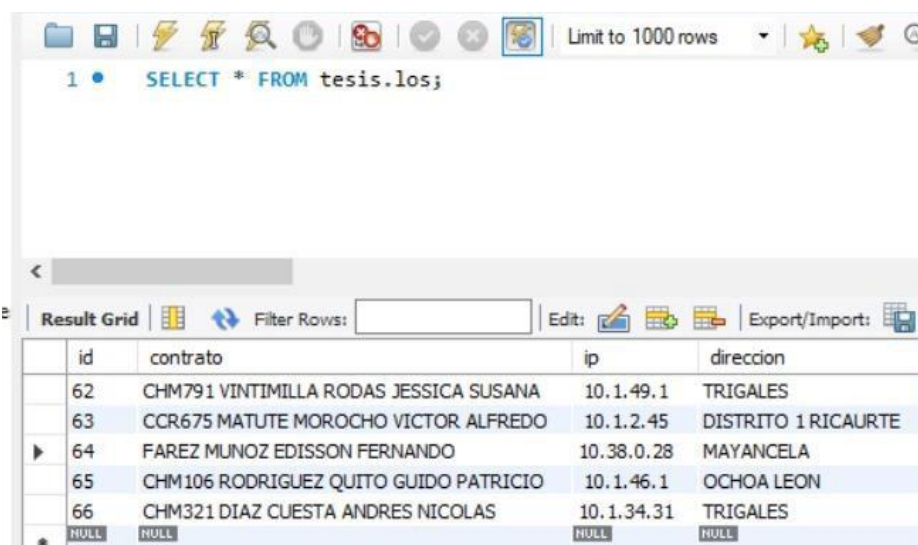
Ilustración 4.6.12: Porcentaje general obtenido del muestro de pruebas de la aplicación.

En la ilustración 4.6.12 se puede evidenciar que, de los 100 usuarios en la muestra, ha existido un 4% de usuarios con PowerFail, un 7% de usuarios han presentado problemas de perdida de señal y 4% han presentado problemas de PPPOE, y el 85% de los usuarios no han presentado ningún tipo de fallo.

## 4.7 RESULTADOS OBTENIDOS EN LAS PRUEBAS DE LA APLICACIÓN MÓVIL.

Al ejecutar la aplicación, esta realiza una consulta a la base de datos, se puede obtener los resultados de los fallos de clientes que aparecen en LOS o pérdida de señal. De acuerdo con los resultados obtenidos, la mayor cantidad de fallos son causados por fallas eléctricas dentro del fallo PWR Fail, esas desconexiones que se han detectado indican que un cliente se ha quedado momentáneamente sin servicio, se apagó la ONT o se reinició, pero el fallo también pudo ocasionarse por alguna actualización programada automáticamente dentro del Router y posterior reinicio de este. En cuanto a fallas de LOS, es importante destacar que son varios factores, como, por ejemplo, el conector SC/UPC dentro del equipo del cliente, potencia elevada a causa de puertos PON en la OLT del ISP, o simplemente daños ocasionados por agentes externos; estos fallos se registran muy frecuentemente.

A continuación, se detalla los usuarios con fallos de pérdida de señal o LOS, los cuales se encuentran almacenados en una base de datos, luego se podrá observar en la aplicación móvil los fallos y se podrá ver información más detallada del problema con su posible solución.



The screenshot shows a database query interface. At the top, there is a toolbar with various icons and a dropdown menu set to 'Limit to 1000 rows'. Below the toolbar, a SQL query is entered: '1 • SELECT \* FROM tesis.los;'. The results are displayed in a table with the following columns: 'id', 'contrato', 'ip', and 'direccion'. The table contains six rows of data, with the last row showing NULL values for the 'id', 'contrato', 'ip', and 'direccion' columns.

id	contrato	ip	direccion
62	CHM791 VINTIMILLA RODAS JESSICA SUSANA	10.1.49.1	TRIGALES
63	CCR675 MATUTE MOROCHO VICTOR ALFREDO	10.1.2.45	DISTRITO 1 RICAURTE
64	FAREZ MUNOZ EDISSON FERNANDO	10.38.0.28	MAYANCELA
65	CHM106 RODRIGUEZ QUITO GUIDO PATRICIO	10.1.46.1	OCHOA LEON
66	CHM321 DIAZ CUESTA ANDRES NICOLAS	10.1.34.31	TRIGALES
NULL	NULL	NULL	NULL

Ilustración 4.7.1 Muestra la base de datos, almacenados los datos de los fallos de LOS.

La figura 4.7.1 muestra algunos de los resultados mediante consultas a la base de datos en MySQL, de algunos fallos en el servicio en ciertos sectores de cobertura.

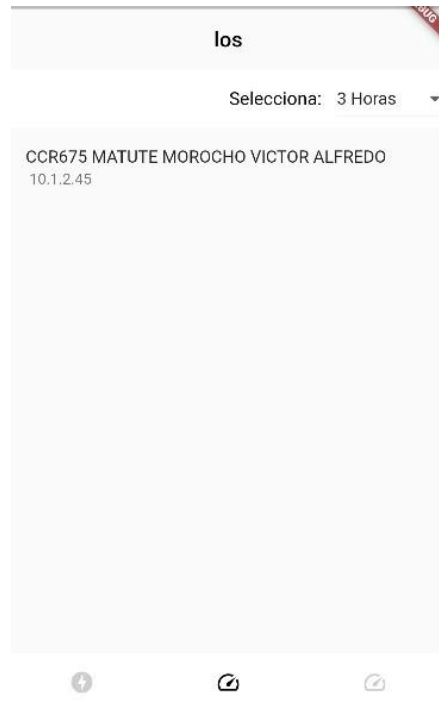


Ilustración 4.7.2 Muestra el resultado de los fallos LOS por rangos de tiempos al ejecutar la app móvil.

La figura 4.7.2, presenta un listado de todos los usuarios que presentan problemas de PowerFail y necesitan ser solucionados por parte del administrador.

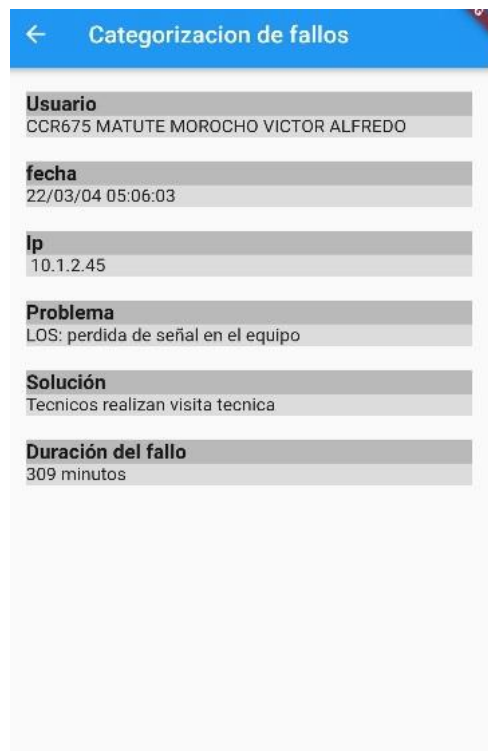


Ilustración 4.7.3 Esta página muestra al usuario con el problema y la posible solución en el fallo LOS.



La figura 4.7.3 ilustra una ventana que permite visualizar al usuario con su respectiva dirección IP, el problema y la propuesta de solución en fallos categorizados como LOS.

A continuación, se puede observar en la aplicación móvil los fallos junto con la información más detallada del problema y posible solución.



*Ilustración 4.7.4 Muestra el resultado de los fallos PowerFail por rangos de tiempos al ejecutar la aplicación móvil.*

La figura 4.7.4 presenta un listado de todos los usuarios que presentan problemas de PowerFail y necesitan ser solucionados por parte del administrador.

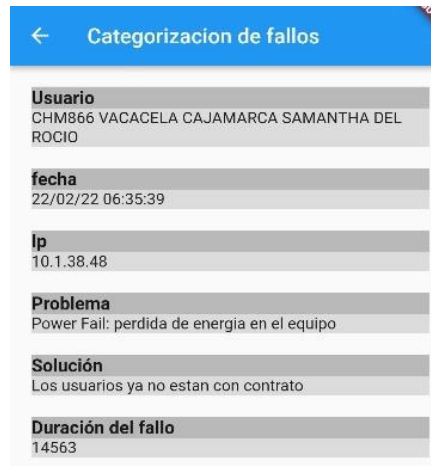


Ilustración 4.7.5 Esta página muestra al usuario con el problema y la posible solución en el fallo PowerFail.

La figura 4.7.5 es una ventana muestra al usuario con su respectiva dirección IP, el problema y la solución posible que se puede brindar en fallos categorizados como PowerFail.

A continuación, se puede observar en la aplicación móvil los fallos y se podrá observar la información más detallada del problema con su posible solución.

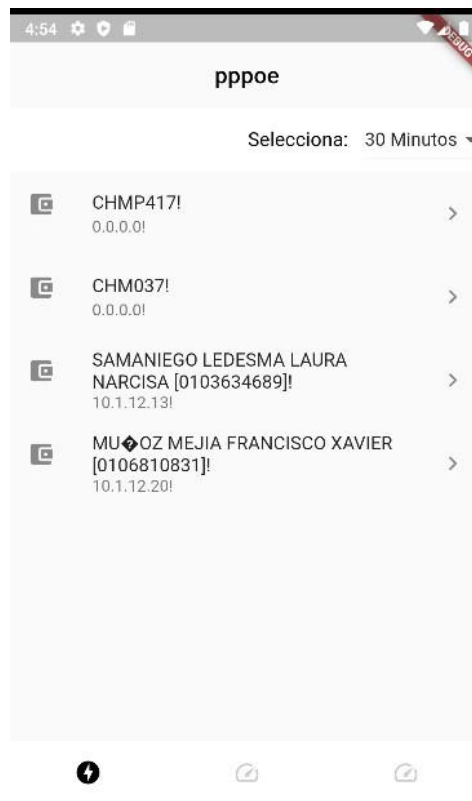
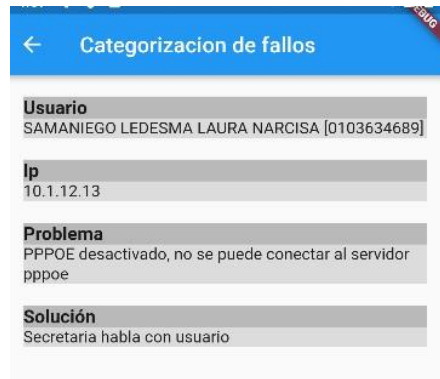


Ilustración 4.7.6 Aquí se muestra el resultado de los fallos PPPOE por rangos de tiempos.

La figura 4.7.6 presente un listado de todos los usuarios que presentan problemas de PPPOE y necesitan ser solucionados por parte del administrador como un soporte de usuario o cliente dependiendo la gravedad de la falla.



*Ilustración 4.7.7 Esta página muestra al usuario con el problema y la posible solución en el fallo PPPOE.*

La figura 4.7.7 es una ventana muestra al usuario con su respectiva IP, el problema y la solución posible que se puede brindar en fallos categorizados como PPPoE. Las soluciones varían y están relacionadas a los niveles de soporte que se puede brindar al usuario.

## 4.8 CRONOGRAMA DE ACTIVIDADES

<b>Análisis e implementación de la herramienta NEDI para la identificación y categorización de fallos en una red GPON; a nivel de red troncal, red de distribución y de última milla para optimización de recursos.</b>				
<b>Nº</b>	<b>Actividad Desarrollada</b>	<b>Recursos/Materiales/Conocimientos Requeridos-Adquiridos/Resultados</b>	<b>Fechas</b>	<b>Horas Requeridas</b>
<b>1</b>	Identificar fallos utilizando la herramienta NEDI opensource.	Libros, papers, páginas webs para la obtención de información sobre los fallos de la fibra óptica, utilización de la herramienta NeDi para revisión de los fallos.	06/04/21- 28/05/21	<b>120</b>
<b>2</b>	Categorizar los fallos según niveles o jerarquías existentes.	Empleando la herramienta Nodejs desarrollamos la aplicación que permita la implementación de una aplicación que permita la categorización de los fallos.	01/06/21 - 30/07/2021	<b>110</b>
<b>3</b>	Generar advertencias y posibles soluciones a las fallas por nivel o por jerarquías existentes.	En la aplicación anterior se debe agregar posibles soluciones a las fallas categorizadas por nivel o por jerarquías existentes.	01/08/2021 - 22/10/2021	<b>200</b>
<b>4</b>	Generar registros y almacenarlos en una base de datos.	En la base de datos MySQL almacenamos los registros de fallos y posibles soluciones.	25/10/2021- 03/12/22	<b>124</b>
<b>5</b>	Generar la proyección del consumo de ancho de banda según los registros obtenidos utilizando el lenguaje de programación Nodejs	Utilizando Nodejs, y mediante el celular para ejecutar la aplicación verificamos su correcto funcionamiento.	6/12/2021 - 25/02/2022	<b>156</b>
<b>Total, de horas de trabajo</b>				<b>800</b>

#### 4.9 PRESUPUESTO

<b>Recurso</b>	<b>Cantidad</b>	<b>Descripción</b>	<b>Precio Unitario (\$)</b>	<b>Costo Total(S) (\$)</b>
<b>Recurso Informático</b>	<b>2</b>	<b>Laptop</b>	<b>1350</b>	<b>2.700,00</b>
<b>Recurso Informático</b>	<b>1</b>	<b>Servidor</b>	<b>700</b>	<b>700</b>
<b>Transporte</b>	<b>100</b>	<b>trasladarse a empresa</b>	<b>0,30</b>	<b>30</b>
<b>Copias</b>	<b>200</b>	<b>Copias</b>	<b>0,05</b>	<b>10</b>
<b>Internet</b>	<b>1</b>	<b>Internet</b>	<b>120</b>	<b>120</b>
<b>Imprevistos</b>	<b>2</b>	<b>Gastos extras</b>	<b>400</b>	<b>400</b>
<b>Base de datos</b>	<b>1</b>	<b>Hojas de papel bond a-4</b>	<b>10</b>	<b>10</b>
<b>Recursos Humanos</b>	<b>2</b>	<b>Estudiantes investigadores</b>	<b>1800</b>	<b>3600</b>
<b>Recursos Humanos</b>	<b>1</b>	<b>Asesoría especializada</b>	<b>1000</b>	<b>1000</b>

## **CAPÍTULO 5 CONCLUSIONES, RECOMENDACIONES Y TRABAJOS FUTUROS**

### **5.1 CONCLUSIONES**

El monitoreo de redes de última milla es un tema complejo y abarca muchos factores por lo que se ha implementado una arquitectura que brinda soluciones con herramientas open source para el desarrollo de aplicaciones. Muchos NMS son orientados a propósitos específicos, como, por ejemplo, administración y gestión de servidores, otras se enfocan más en la parte de alertas, así como también orientados a tecnologías modernas como Cloud Computing.

La aplicación desarrollada, es capaz de adquirir información del estado de conectividad de los clientes del ISP. Además, se logró realizar mediante la programación en Flutter, extraer información útil de los clientes para verificar si un incremento de ancho de banda es necesario recomendar un incremento para solucionar problemas de intermitencia del servicio.

Esta aplicación en conjunto con todas las funciones definidas en el back-end incluyen beneficios tales como: registro de fallos, generación de reportes, categorización y clasificación de fallos y Utilizando la aplicación de recomendación se puede evitar que los usuarios perciban inconvenientes al momento de navegar, donde se puede realizar recomendaciones si se está utilizando más ancho de banda del contratado y poder decir al usuario que tiene la necesidad de aumentar el ancho de banda para satisfacer las necesidades del usuario.

Gracias a toda esta información previamente recopilada es posible generar y proponer varias soluciones además de alternativas a los fallos en función de su categoría y clasificación; por otra parte, permite optimizar los tiempos de respuesta de soporte técnico y solución de fallos, a su vez que incrementa la tolerancia a fallos implicando menos cortes de servicio e incrementando los beneficios para la empresa permitiendo ofrecer un servicio más confiable y robusto.

## **5.2 RECOMENDACIONES**

Es importante tener en cuenta la arquitectura con la que se va a trabajar, y al momento de realizar el despliegue se aconseja que se utilice herramientas que funcionen de manera local, por ejemplo, Python que es un lenguaje de programación que tiene como ventaja permitir la programación orientada a objetos, programación imperativa y en un grado menor la programación funcional.

Adicionalmente, para la constante mejora de sistemas de monitoreo y alertas a usuarios y administradores de red en grandes empresas, así como en ISP, se requiere una investigación de requerimientos específicos, enfocados a problemáticas comunes como cortes de servicio, mejoras en cuanto a soporte del cliente, concientización a los usuarios del servicio como tal, para evitar malentendidos sobre que obligaciones tiene la empresa y que tipo de servicios van más allá del alcance de un SLA. Se debe tener las bases sólidas en cuanto a proyecciones de mercado y que infraestructura es la adecuada para cumplir con estas necesidades de mercado en cualquier sector que se desea brindar un servicio.

Como solución adicional se recomienda la adquisición de equipos Cisco de la serie Meraki ya que con su infraestructura en la nube optimiza la gestión de todos los nodos conectados a la red. Además, ofrece soluciones específicas para cada cliente y constante monitoreo y alertas sobre estados y caídas del servicio.

## **5.3 TRABAJOS FUTUROS**

En el presente trabajo se propuso una arquitectura que permita la predicción de consumo de ancho de banda en el futuro y otra aplicación para detección y categorización de los fallos, pero existen varias otras propuestas que se pueden realizar como:

- Poder solventar problemas de configuración desde la aplicación móvil.

En futuras investigaciones, se pueden implementar algunos de los principios de detección de fallos empleando tecnologías actuales como SDN, lo cual implique delimitar el plano de control y el plano de datos para partir de una arquitectura básica de redes definidas por software. En un sistema robusto con estas capacidades, los ingenieros de redes estarán en capacidad de segmentar la parte física y lógica de la red creando de esta manera un NMS unificado, pero bien estructurado.

Una posible implementación que se puede realizar como trabajo es un sistema de alertas, es decir, junto con las notificaciones que se puede alertar desde el ERP como ODO; agregando un complemento que alerte a un grupo de técnicos mediante un servicio REST como en Postman. En dicho servicio implementado se indica a que numero de celular se procedería a enviar mensajes SMS o WhatsApp para posteriormente escanear el cliente del servicio REST con un código QR y desde este programa enviar un broadcast a todo el grupo o un técnico de turno en particular que se encargue de algún soporte emergente.

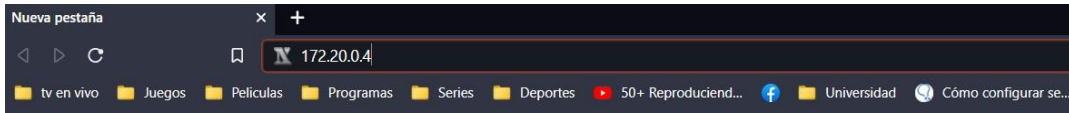
Otra posible implementación se puede realizar colocando un medidor de potencia conectado como un dispositivo de paso lo que va a permitir monitorear si ocurren fallos a lo largo de la red troncal y de distribución y así poder categorizar esos fallos y poder agregarlos en la aplicación móvil y lograr que los usuarios tengan el menor número de inconvenientes al momento de navegar. La implementación en fase de pruebas se realizaría colocando un Raspberry Pi en un Network Access Point (NAP), un sensor orientado a detectar señales ópticas que las convierta en digitales para luego obtener lecturas en un nodo receptor. Aplicando técnicas de programación y lógica, se delimitarían rangos de tolerancia de pérdida de potencia, esto con un sistema de alarmas y alertas incorporado para verificar el estado de la red troncal, esto en la parte física. En la red de distribución, nodo principal, de manera similar, mediante una red de sensores, en un Router de borde, inicialmente, en fase de prueba y error, verificar el estado de las VLAN que conectan a varios clientes, el estado de los enlaces conectados hacia los proveedores de salida a Internet como son NEDETEL y TELCONET entre otras redes de transporte y portadoras dentro del país. Con este proceso se puede descartar si el fallo se suscitó por caídas de los enlaces externos o bien si el fallo es interno del ISP.



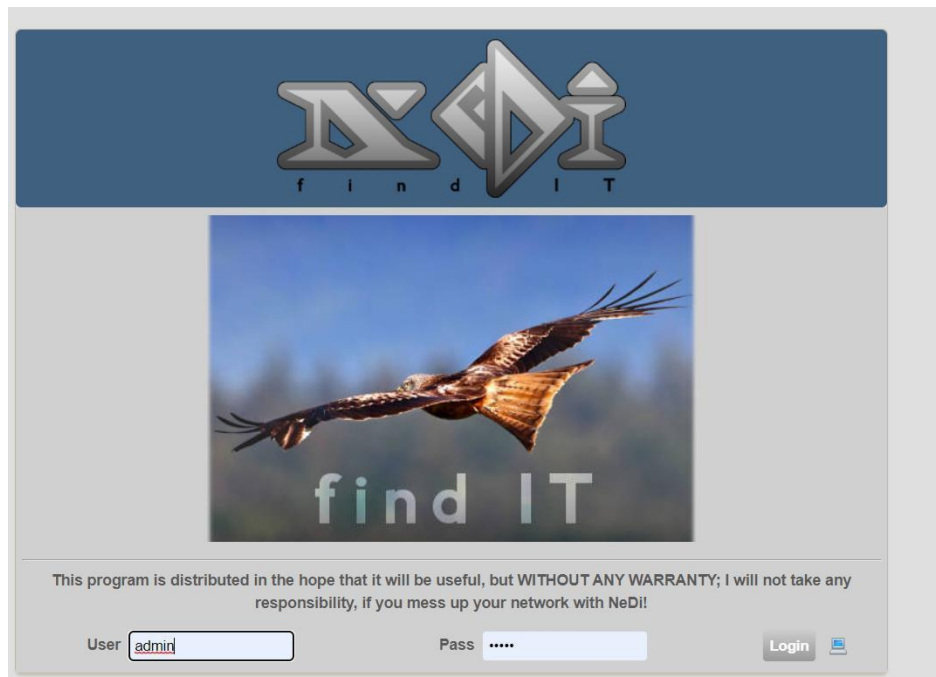
## ANEXOS

### Anexos 1 Configuración de Nedi

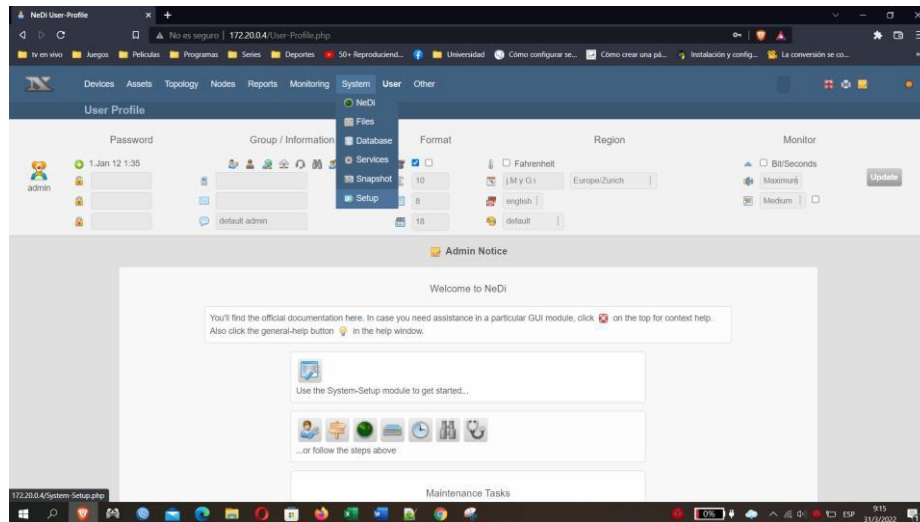
Para acceder a configurar el Nedi, se ingresa mediante la IP del servidor y con ello se empezará la configuración para inicializar el monitoreo.



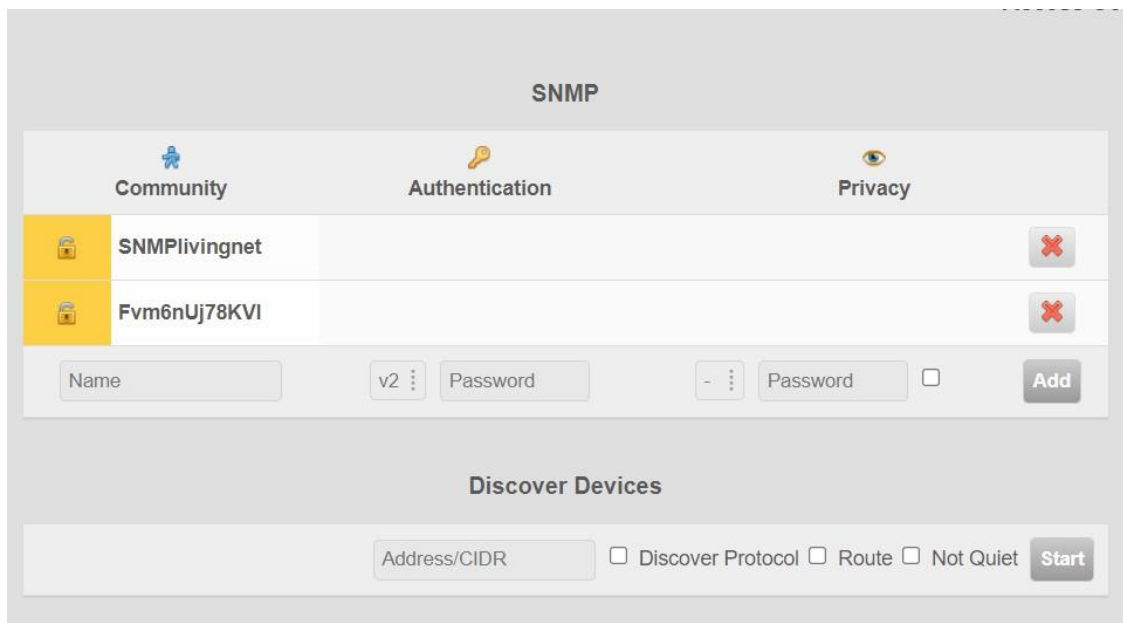
Luego se ingresan las credenciales especificadas durante la instalación de NeDi.



Una vez ingresado a la interfaz web de Nedi, se dirige a la pestaña System y luego se elige la opción setup y se abrirá una ventana donde se realizan configuraciones adicionales.



Ahora se procederá a configurar las comunidades SNMP que se encuentran en los routers de borde, con lo cual Nedi conseguirá acceder a los equipos pasivos para empezar con el monitoreo, además se agrega la IP del router, parámetro crítico para iniciar el monitoreo de la red del ISP.



Posteriormente, la aplicación empezará a monitorear. Se dirige a devices y luego a interfaces, dentro de este apartado están todas las interfaces físicas conectadas dentro del nodo principal.

NeDi Devices-Interfaces

172.20.0.4/Devices-Interfaces.php

Devices Assets Topology Nodes Reports Monitoring System User Other

List Modules Interfaces Vians Status Config Doctor Graph Write Add

Condition 1

250 Show

Image Port Name Index Devices Name Vendor Devices Type Group Location Contact First Discover Last Discover

Type Distribution

Type	Quantity
PPP	259
Layer 2 Virtual LAN	74
Other-250	64
Ethernet	43
Transparent bridge Interface	5
IEEE 802.3ad Link Aggregate	3
Virtual Interface	3
Other-1	1

Status Distribution

Status	Quantity
Active (3)	399
Inactive (1)	40
Disable (0)	13

3 Interfaces Status, Sort: Quantity

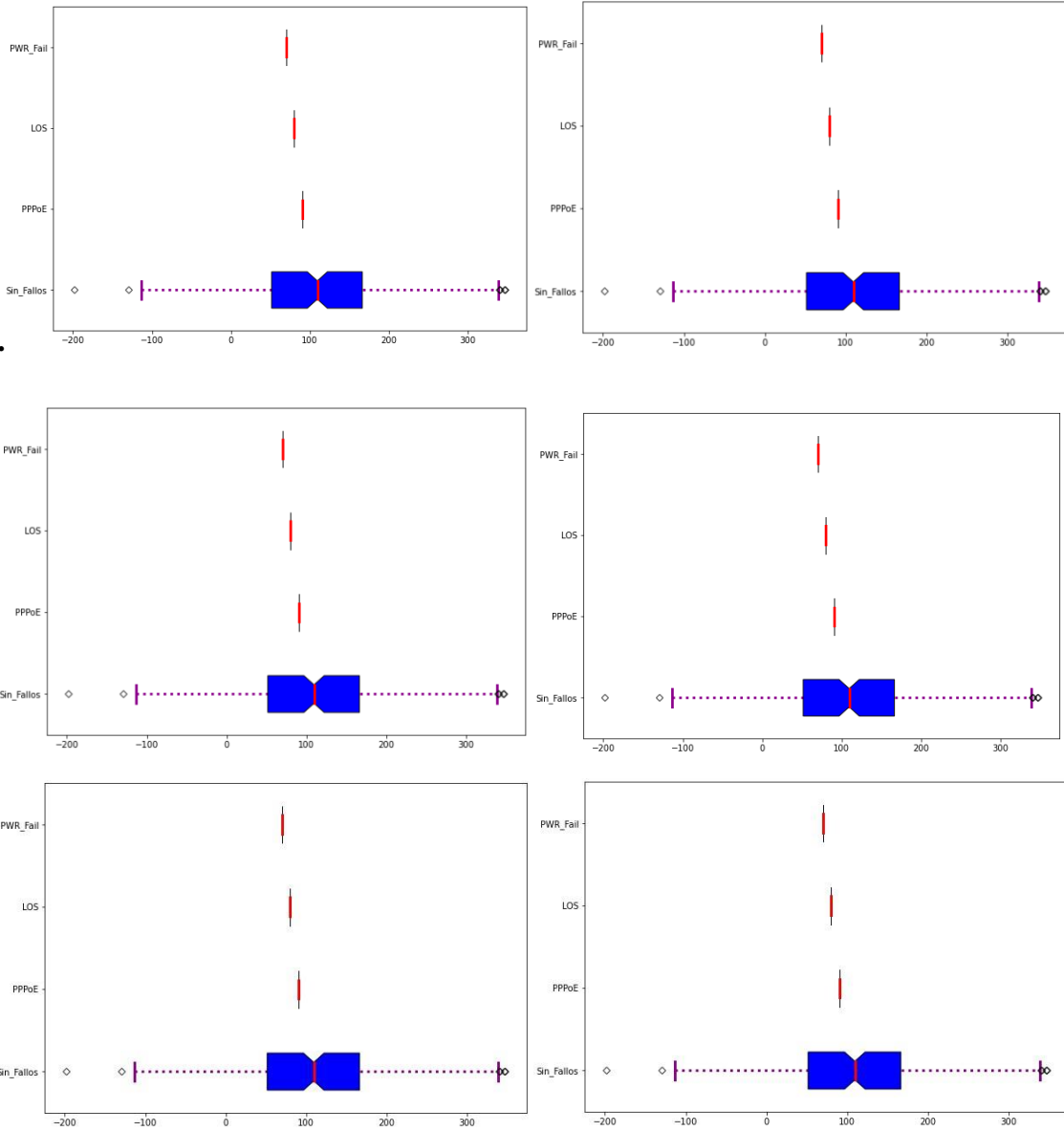
172.20.0.4/Devices-Interfaces.php

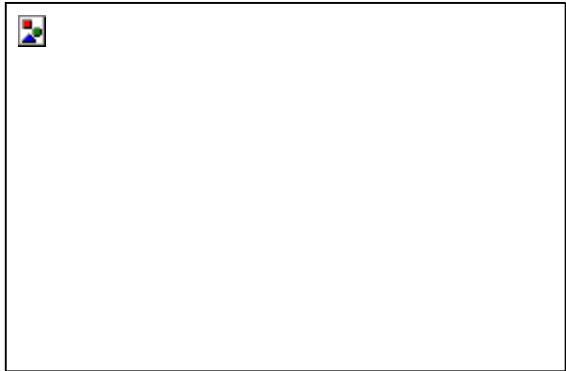
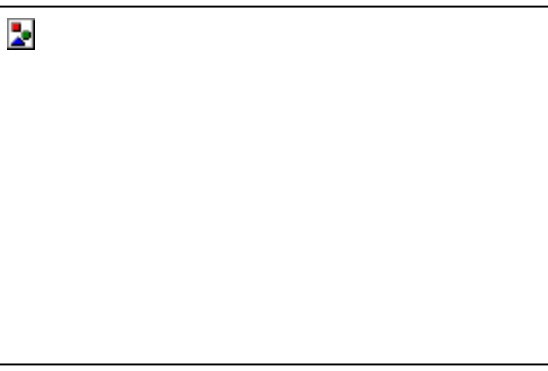
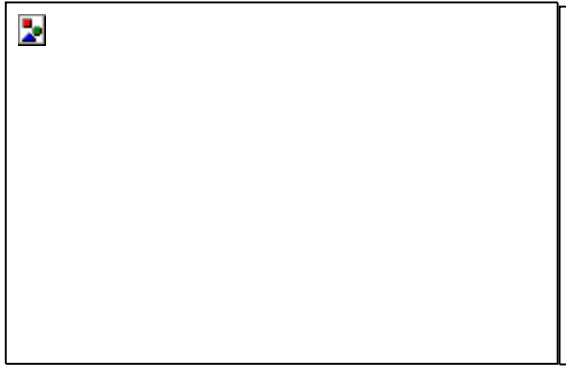
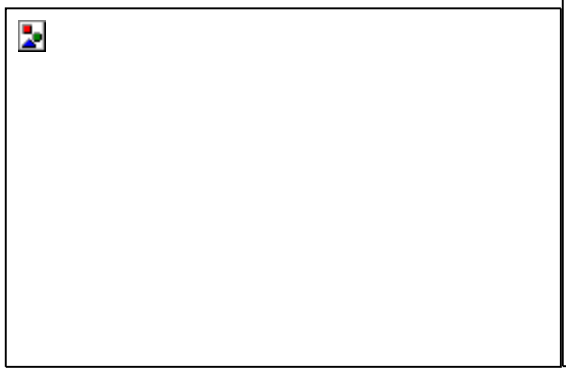
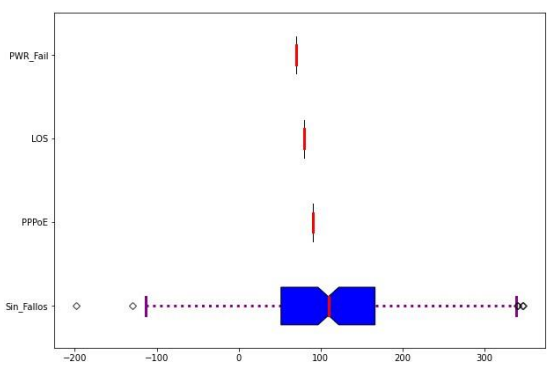
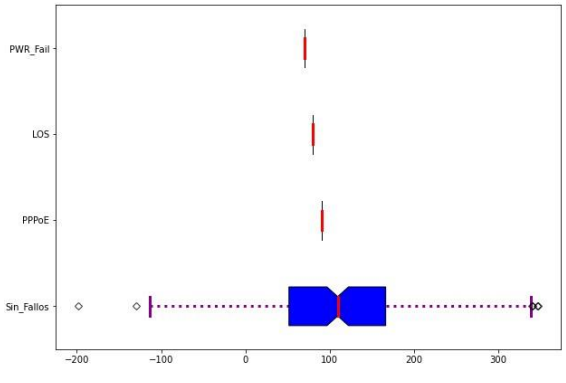
172.20.0.4/Devices-Interfaces.php

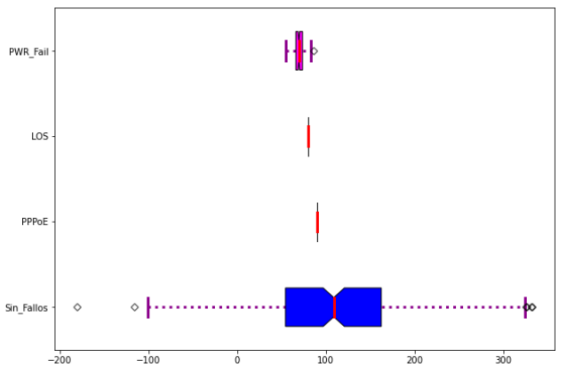
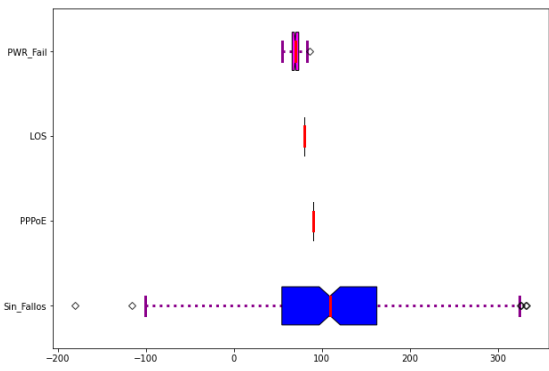
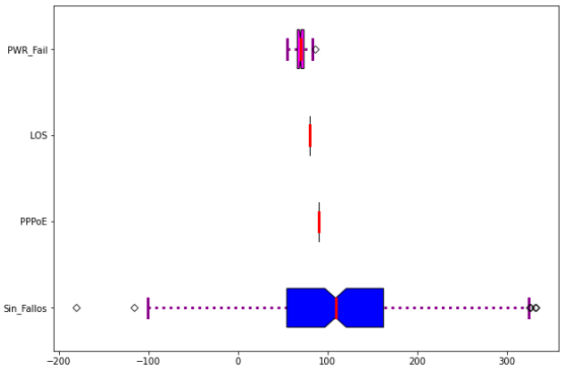
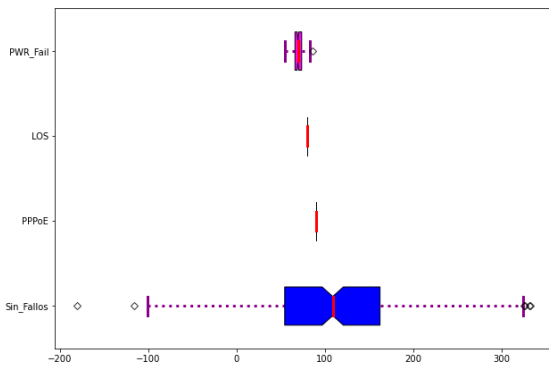
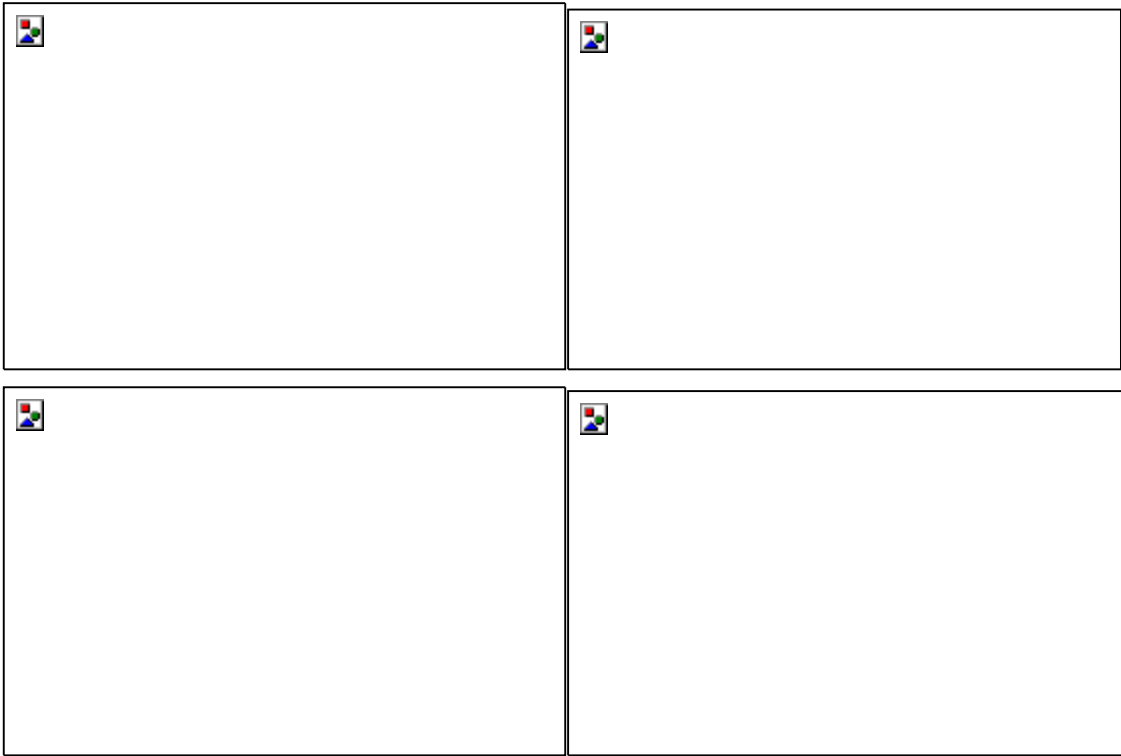
9:17 31/2/2022

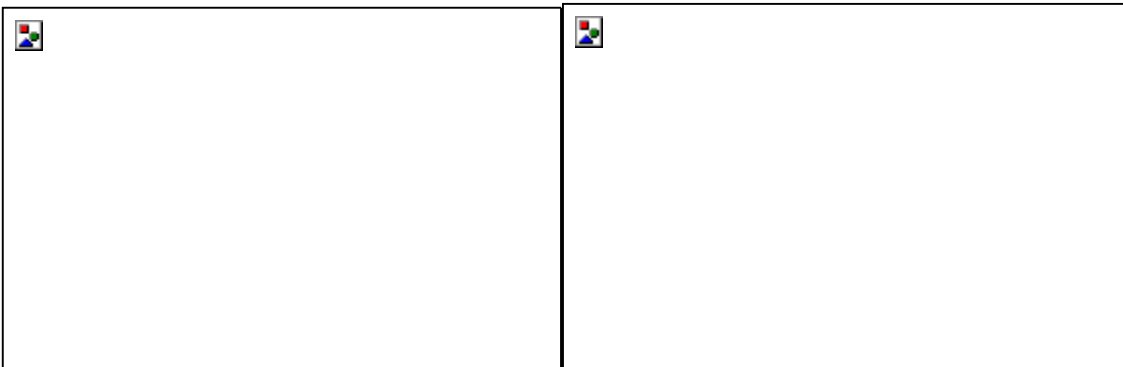
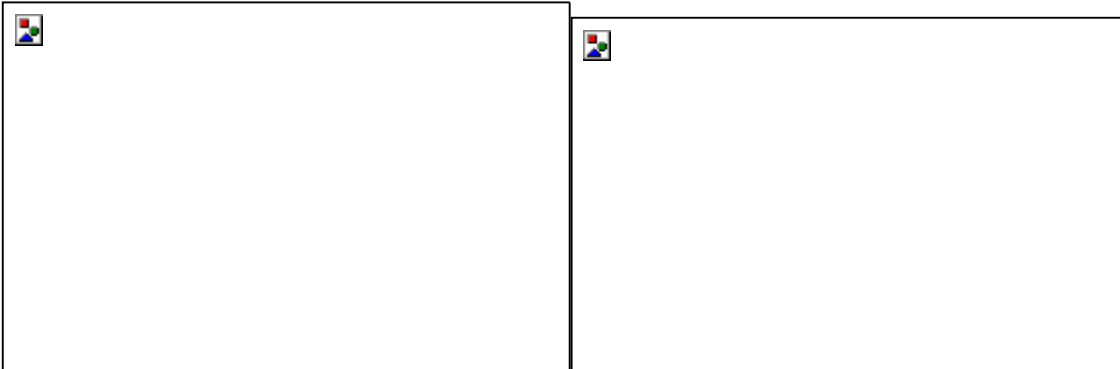
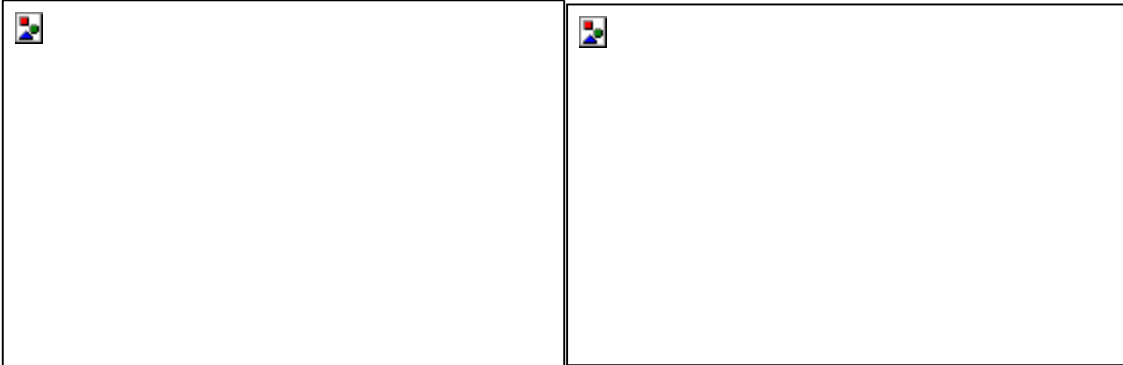
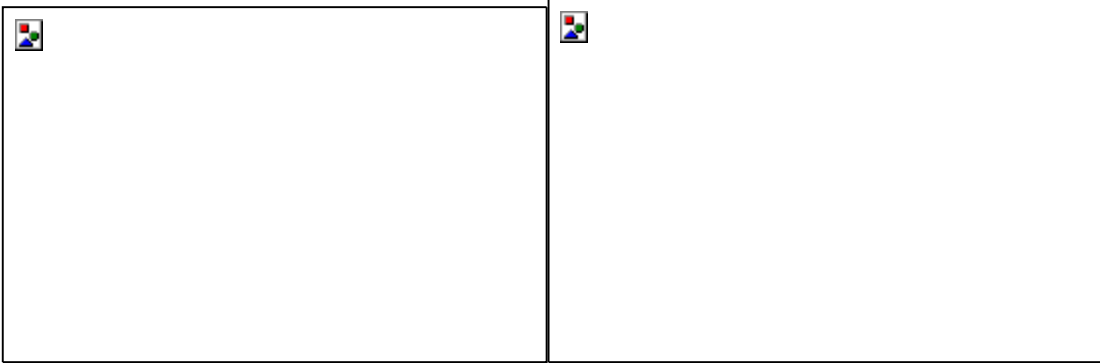
## Anexo 2 Graficas de pruebas realizadas.

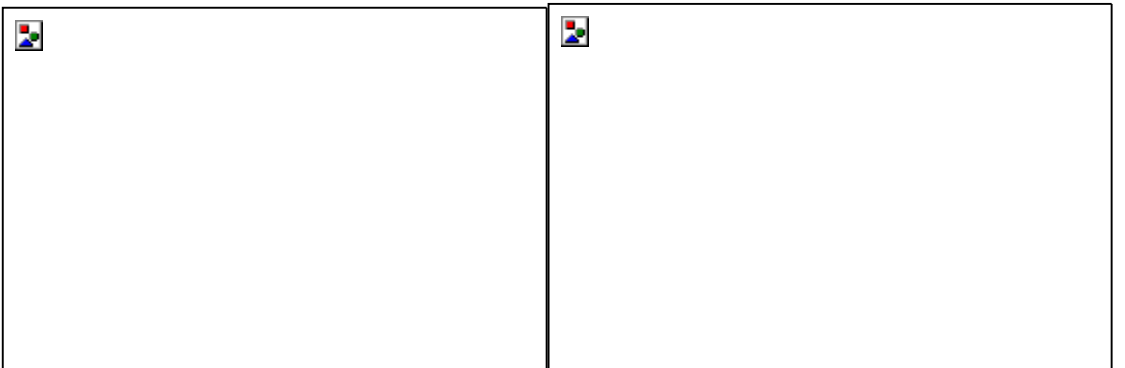
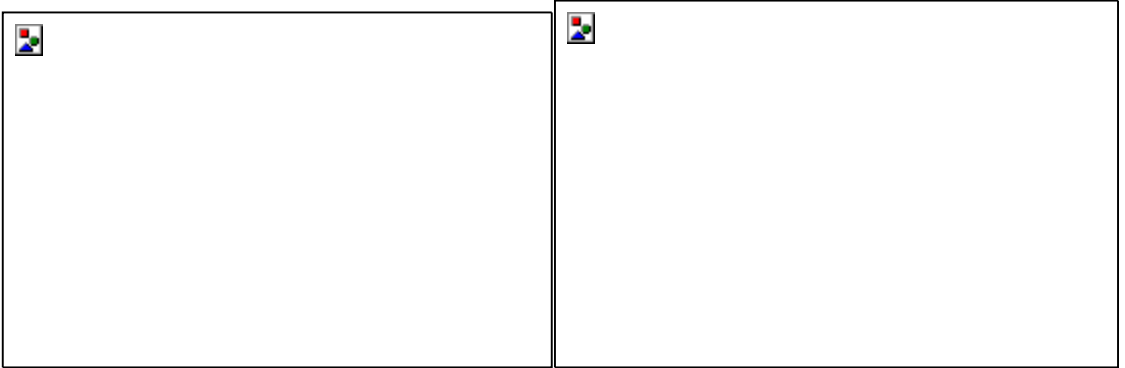
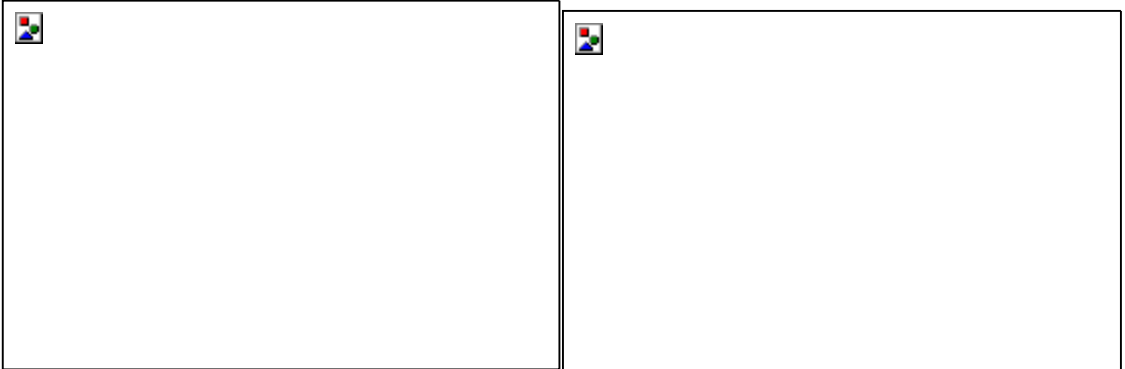
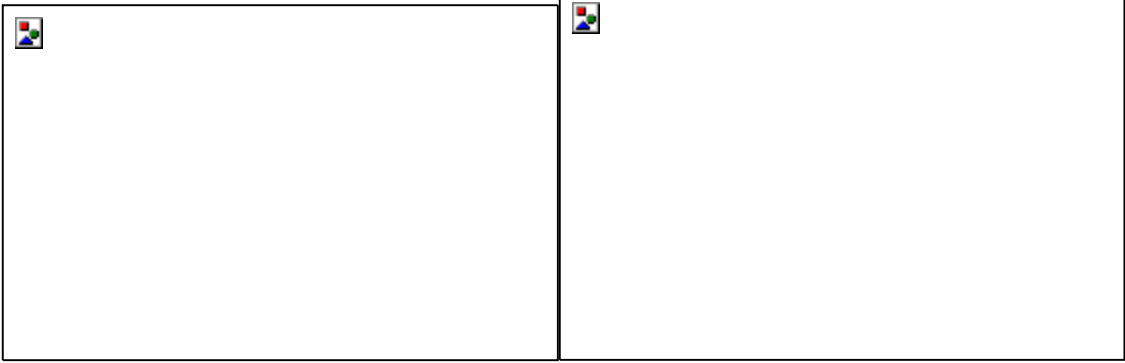
Para la validación del funcionamiento de la aplicación se realizaron 100 pruebas, en las cuales se puede afirmar que la mayoría de los clientes no presentan ningunos de los fallos en estudio y tal solo una minoría, específicamente en un 15% aproximadamente se detecta fallo alguno.



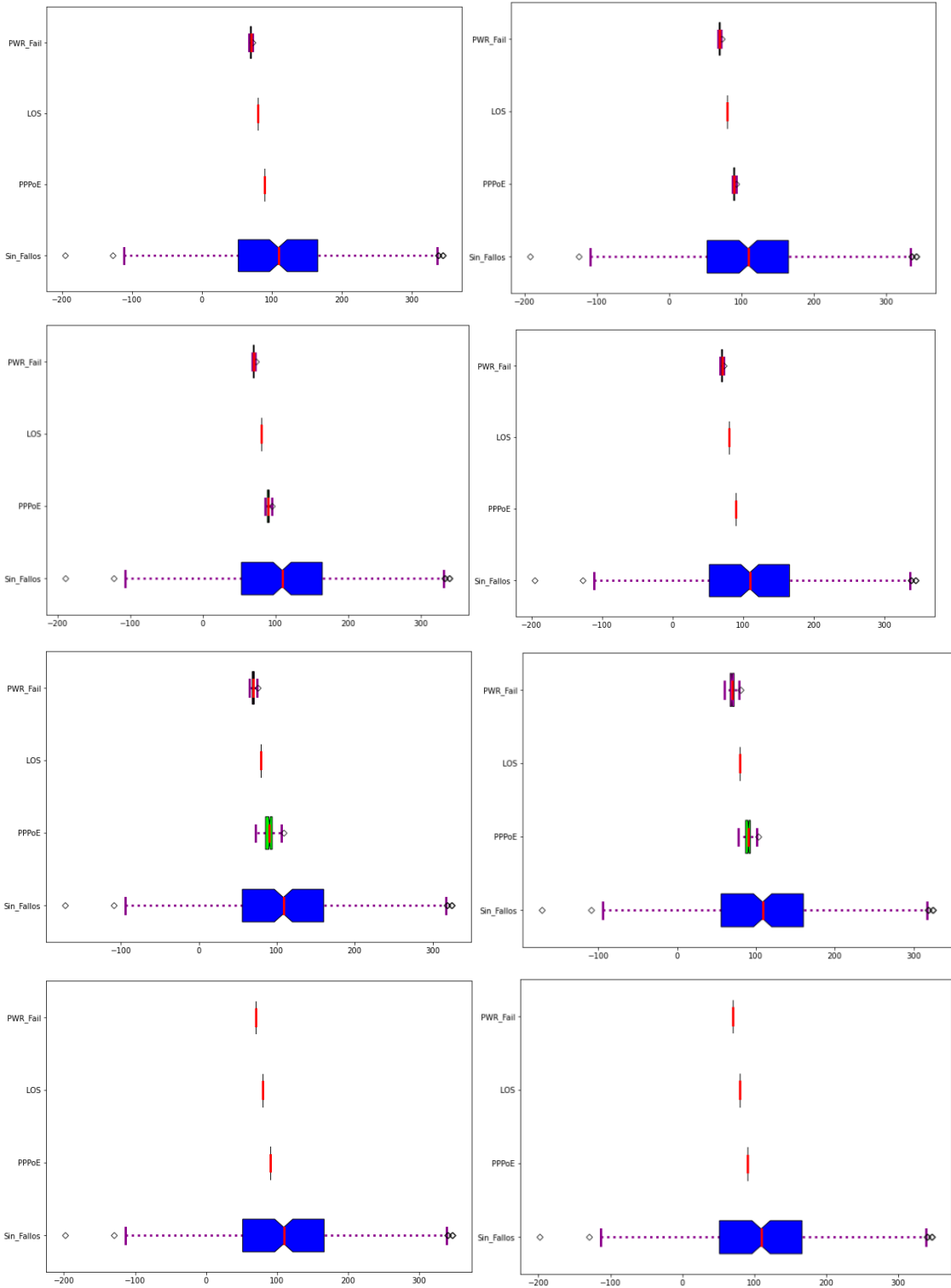


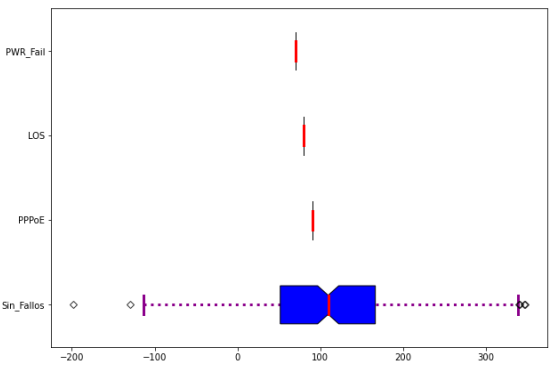
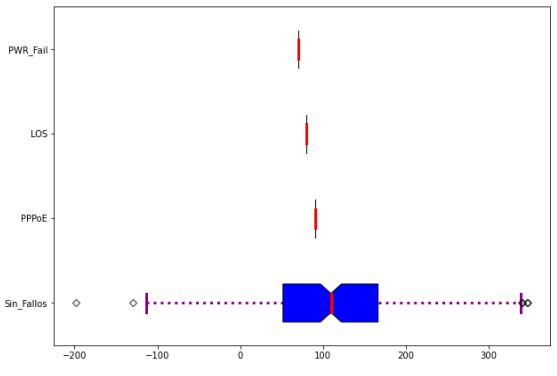
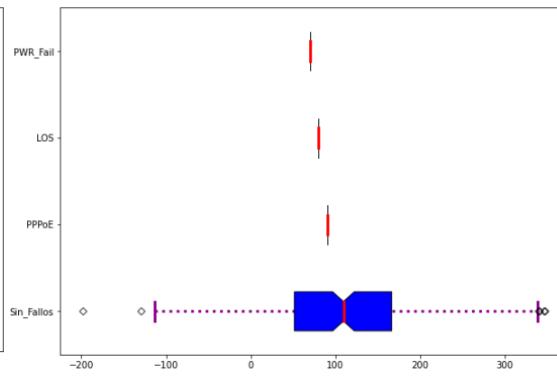
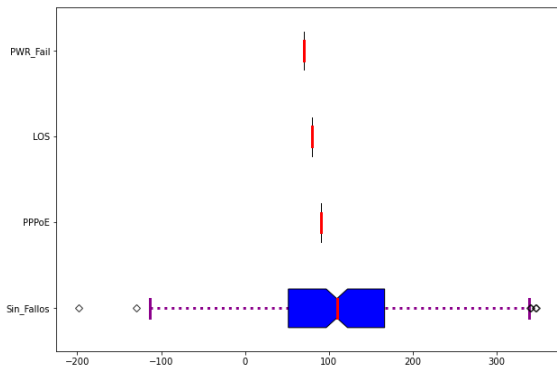
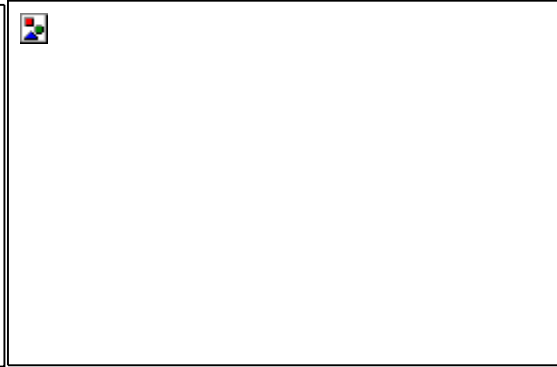
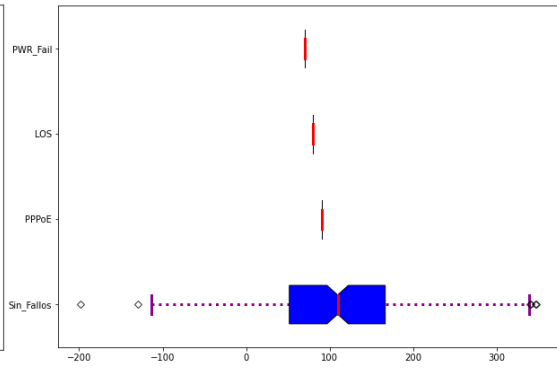
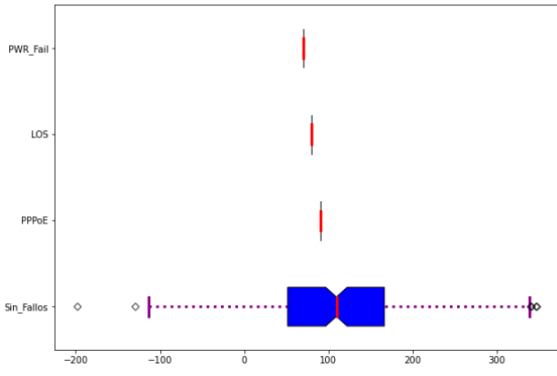


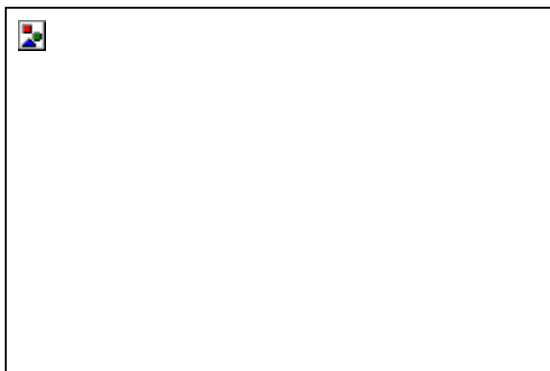
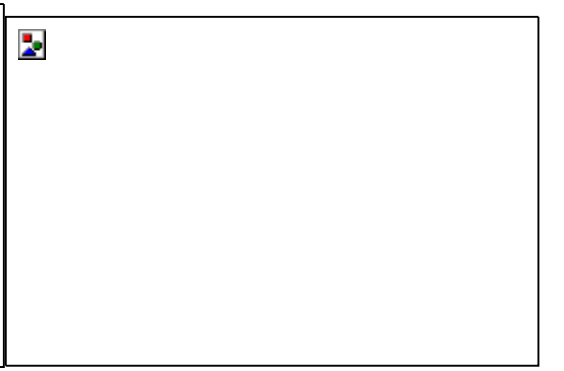
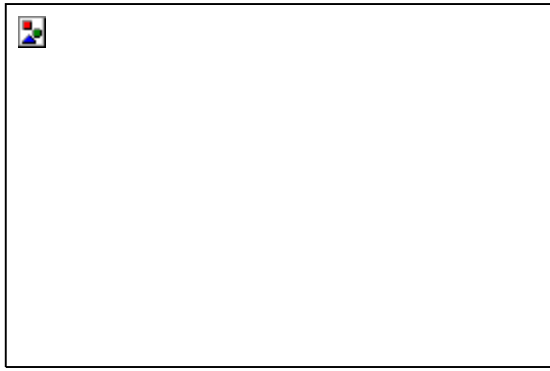
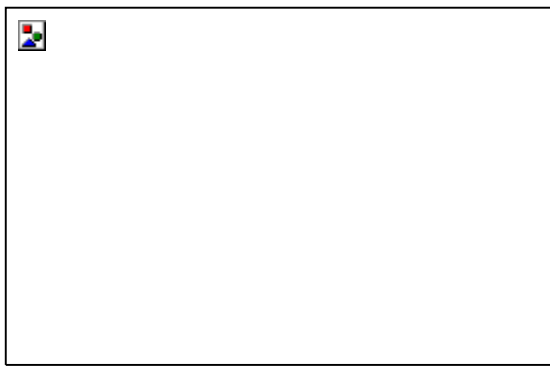
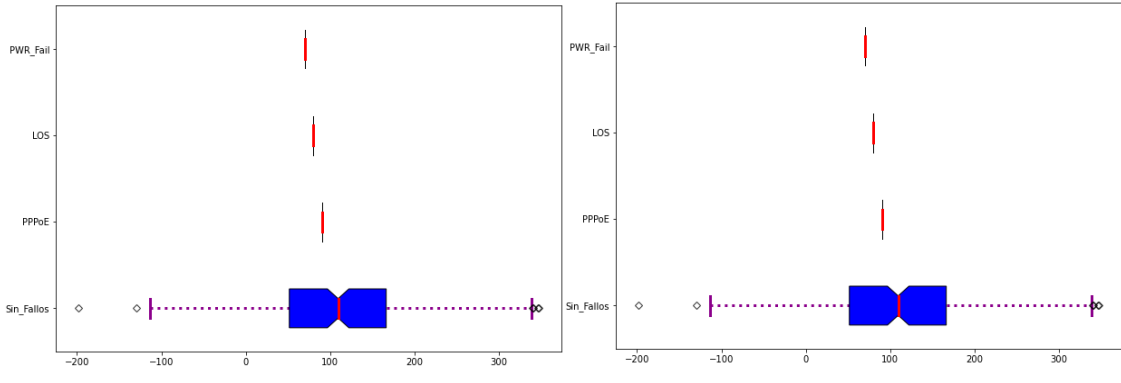


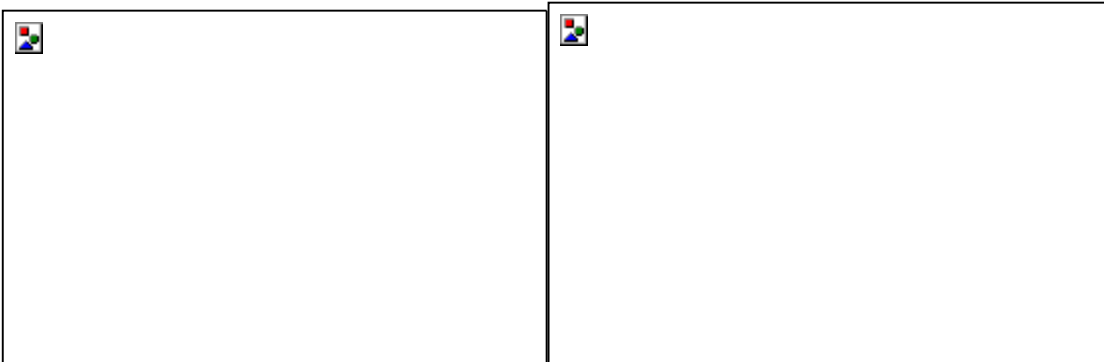
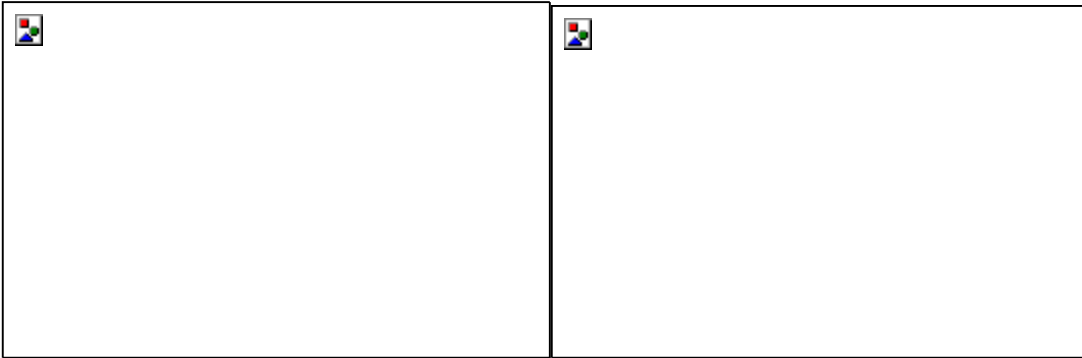
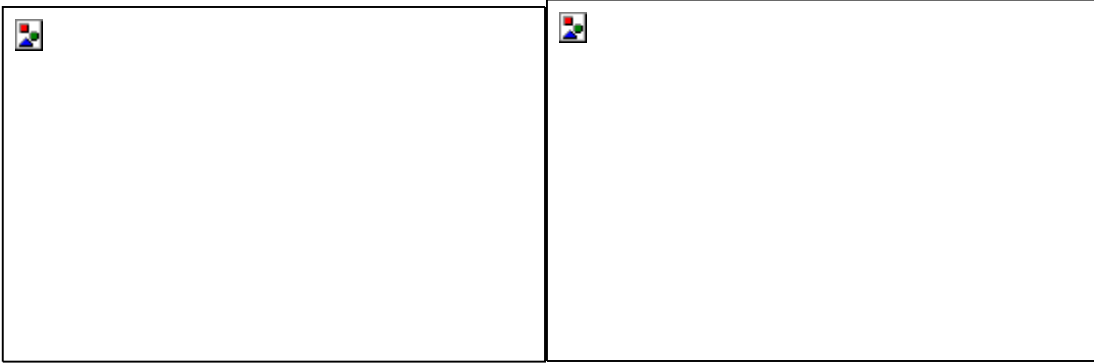
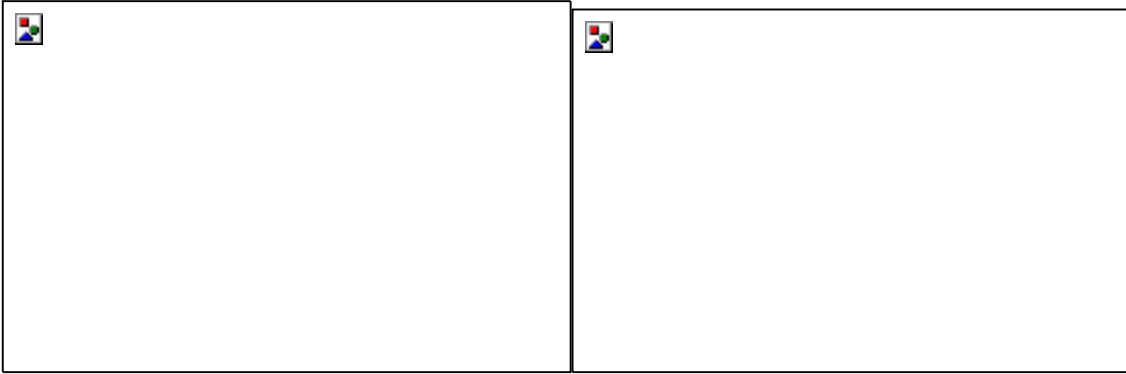


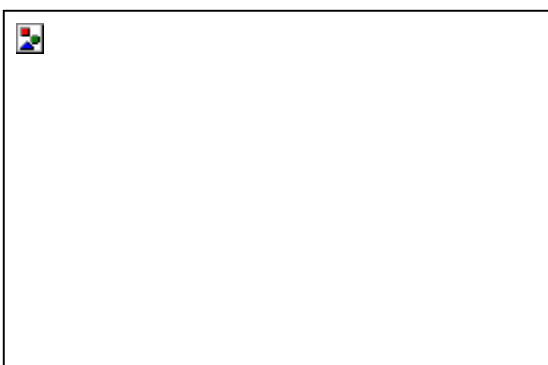
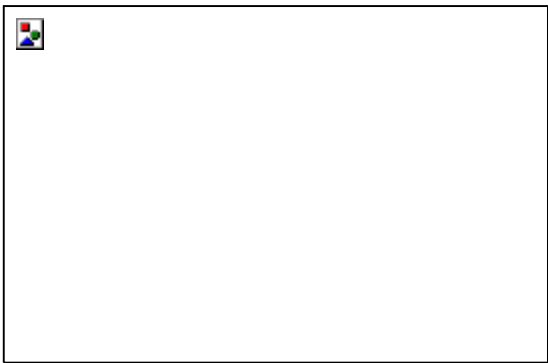
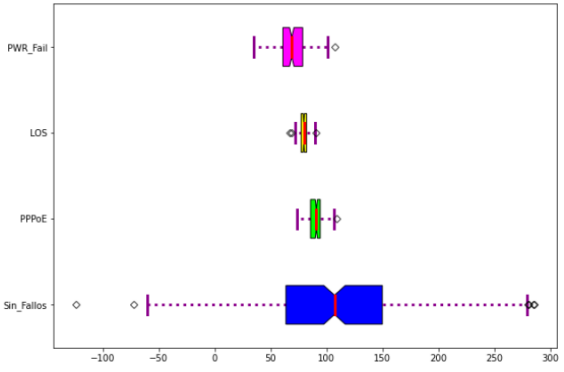
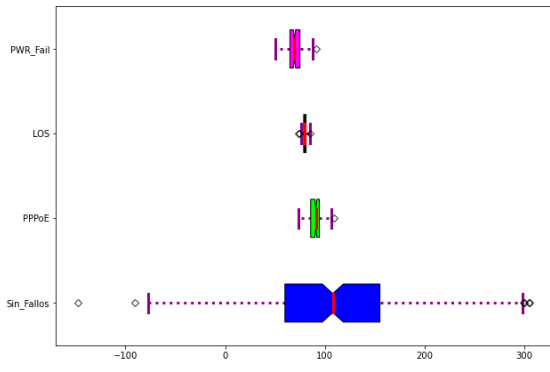


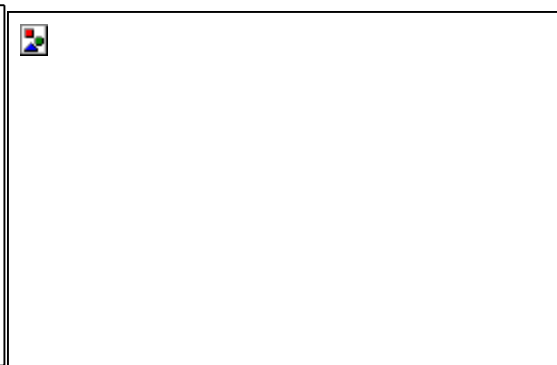
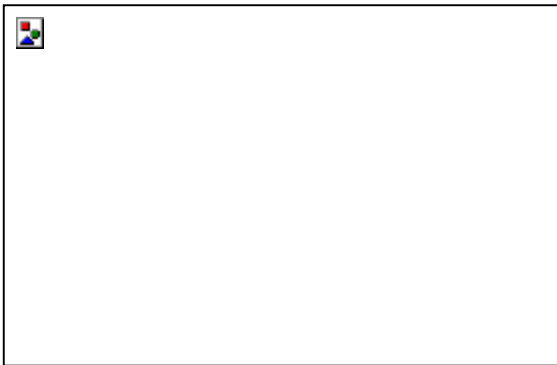
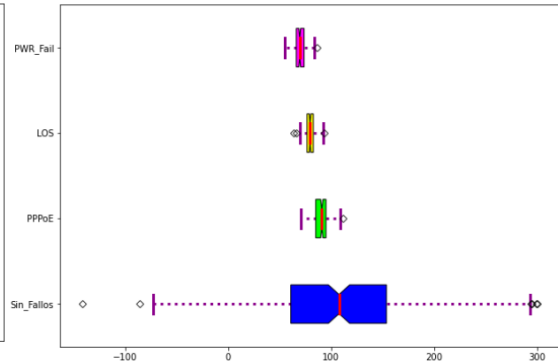
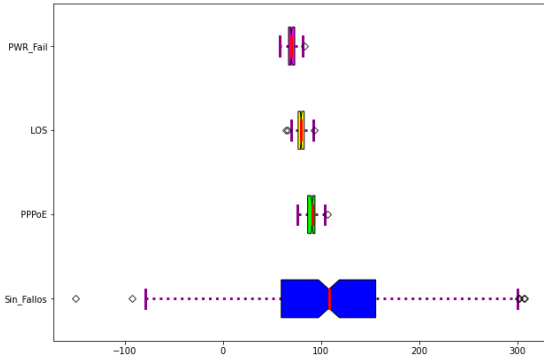
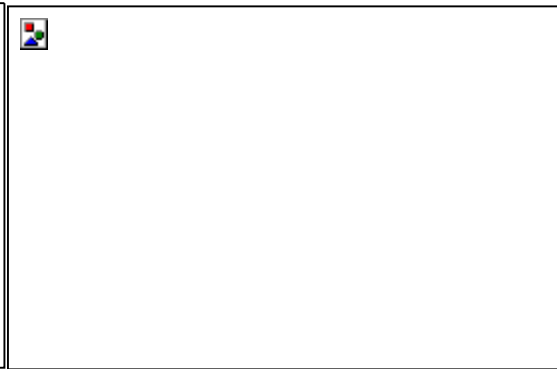


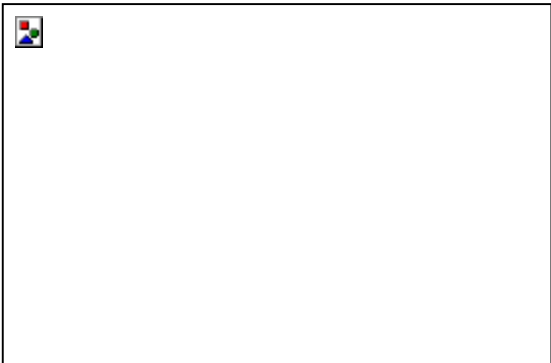
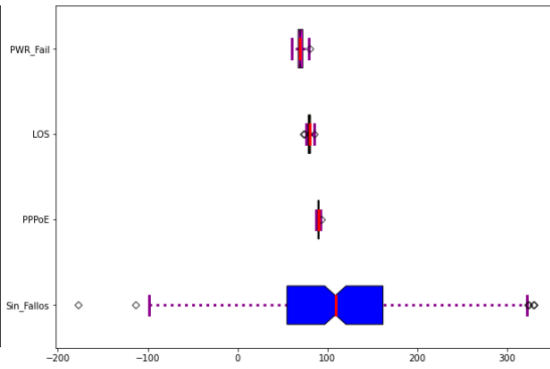
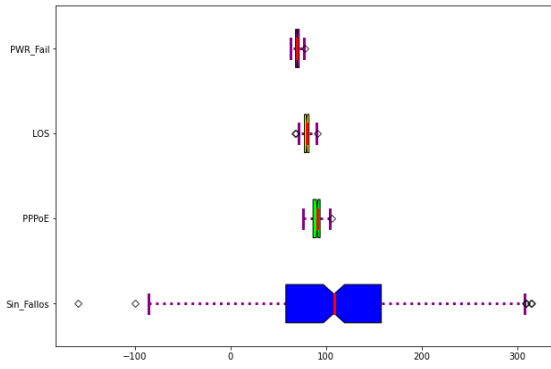












## Referencias

- [1] «PRTG,» 2021. [En línea]. Available: <https://www.setrys.com/prtg> . [Último acceso: 22 noviembre 2021].
- [2] NeDi, «The NetWorkers Guide to NEDI,» 2017.
- [3] A. G. M. Yépez, «PROPUESTA PARA MEJORAR LA COBERTURA DE LA RED INALÁMBRICA,» PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR, Quito, Ecuador, 2016.
- [4] Fluke Networks, «Fluke Networks,» 18 enero 2018. [En línea]. Available: <https://www.flukenetworks.com/blog/cabling-chronicles/previewing-our-bicisipresentation-passive-optical-network-pon-testing>.
- [5] «¿QUE ES NEDI?,» 2020. [En línea]. Available: <https://www.snagview.de/en/nedi-sv.html>. [Último acceso: 20 noviembre 2021].
- [6] «Observium, Gestión y Monitoreo de Redes,» 2021. [En línea]. Available: <https://www.observium.org/>. [Último acceso: 21 noviembre 2021].
- [7] «NAGIOS,» 2020. [En línea]. Available: <https://www.nagios.org/documentation/>. [Último acceso: 23 noviembre 2021].
- [8] «ZABBIX,» junio 2021. [En línea]. Available: <https://www.zabbix.com/documentation/5.4/en/manual/introduction/about>. [Último acceso: 23 noviembre 2021].
- [9] «Documenting Python,» 30 marzo 2021. [En línea]. Available: <https://devguide.python.org/documenting/>. [Último acceso: 02 octubre 2021].
- [10] MathWorks, «MathWorks,» 15 diciembre 2021. [En línea]. Available: [https://la.mathworks.com/help/matlab/language-fundamentals.html?s\\_tid=CRUX\\_lftnav](https://la.mathworks.com/help/matlab/language-fundamentals.html?s_tid=CRUX_lftnav).
- [11] «Julia 1.7 Documentation,» 05 mayo 2022. [En línea]. Available: <https://docs.julialang.org/en/v1/>. [Último acceso: 03 octubre 2021].
- [12] E. León, «Te contamos qué es el Lenguaje R,» 2 marzo 2021. [En línea]. Available: <https://www.baoss.es/te-contamos-que-es-el-lenguaje-r/>. [Último acceso: 2021 septiembre 2021].
- [13] M. S. P. C. A. M. Ortiz Ochoa, Programación orientada a objetos con Java y UML, Cuenca, Ecuador: Universidad Politécnica Salesiana , 2011.
- [14] D. Lowe, «Networking all in one for Dummies 9th Ed,» de *Networking all in one for Dummies 9th Ed*, Hoboken , New Jersey, Wiley & Sons, 2018, pp. 80-83.
- [15] Sheldon, «FS Community,» 21 septiembre 2021. [En línea]. Available: <https://community.fs.com/blog/tcpip-vs-osi-whats-the-difference-between-the-two-models.html>.
- [16] W. Goralski, «The Illustrated Network: How TCP/IP works in a Modern Network,» de *The Illustrated Network: How TCP/IP works in a Modern Network*, Cambridge, MA, USA, Morgan Kaufmann, 2017, pp. 30-43.
- [17] K. W. R. James W. Kurose, «Computer Networking: A Top-Down Approach 8th Ed,» de *Computer Networking: A Top-Down Approach 8th Ed*, MA, USA, Pearson , 2021, pp. 303-315.



- [18 R. Scott, «Networking for Beginners,» de *Networking for Beginners*,  
] Independently Published, 2019, pp. 15-22.
- [19 TP-LINK, «tplink.com,» 2021. [En línea]. Available: <https://www.tp-link.com/es/home-networking/wifi-router/archer-c60/>.
- [20 M. E. O’Kelly, «Network Hub Structure and Resilience,» *Springer Link*, vol. *Netw*  
] *Spat Econ*, nº 15, pp. 235-251, 2014.
- [21 Turbosquid, «turbosquid.com,» 2021. [En línea]. Available:  
] <https://www.turbosquid.com/es/3d-models/network-hub-3d-model-1544010>.
- [22 TP-link, «tplink.com,» 2021. [En línea]. Available: <https://www.tp-link.com/es/home-networking/soho-switch/tl-sf1008d/>.
- [23 TP-Link, «tp-link.com,» 2021. [En línea]. Available: <https://www.tp-link.com/ar/business-networking/unmanaged-switch/tl-sg1024/>.
- [24 L. Salazar, «Implementación de un servidor Linux,» UNIVERSIDAD NACIONAL  
] COLOMBIA , Unidad de Informatica, 2016.
- [25 IBM, «ibm.com,» IBM, 14 abril 2021. [En línea]. Available:  
] <https://www.ibm.com/docs/en/i/7.2?topic=concepts-what-is-ppp>. [Último acceso:  
11 abril 2022].
- [26 Juniper Networks, «www.juniper.net,» Juniper Networks, 18 septiembre 2021. [En  
] línea]. Available:  
[https://www.juniper.net/documentation/us/en/software/junos/interfaces-security-devices/topics/topic-map/security-interface-config-pppoe.html#:~:text=Protocol%20over%20Ethernet,Point%2Dto%2DPoint%20Protocol%20over%20Ethernet%20\(PPPoE\)%20combines,a%20bridg](https://www.juniper.net/documentation/us/en/software/junos/interfaces-security-devices/topics/topic-map/security-interface-config-pppoe.html#:~:text=Protocol%20over%20Ethernet,Point%2Dto%2DPoint%20Protocol%20over%20Ethernet%20(PPPoE)%20combines,a%20bridg). [Último acceso: 11 abril 2022].
- [27 K. F. Robert Sheldon, «Tech Target,» 01 09 2021. [En línea]. Available:  
] <https://www.techtarget.com/searchnetworking/definition/PPPoE>.
- [28 R. D. Pierre Bourque, «<http://www.cc.uah.es/drg/b/HispaSWEBOK.Borrador.pdf>,»  
] de *SWEBOK*, Los Alamitos, California, USA, IEEE Computer Society, 2004, pp. 31-36.
- [29 M. W. Lucas, *SNMP Mastery*, Tilted Windmill Press, 2018.  
]
- [30 D. K. J. Michael Stewart, «Network Security, Firewalls and VPNs,» de *Network*  
] *Security, Firewalls and VPNs*, Burlington, MA, Jones & Bartlett, 2021, pp. 536-540.
- [31 ITU-T, «UIT,» marzo 2020. [En línea]. Available: <https://www.itu.int/rec/T-REC-G.984.3-202003-!!Amd1/es>. [Último acceso: 11 abril 2022].
- [32 P. Tee, «The Role of Graph Entropy in Fault Localization and Network Evolution,»  
] Department of Informatics University of Sussex, Brighton, Sussex, UK, 2017.
- [33 Z. Kasner, «Flow-Based Classification of Devices in Computer Networks,»  
] Department of Theoretical Computer Science, Praga, Republica Checa, 2015.
- [34 Fibermax, «Conector Mecánico SC/APC,» enero 2019. [En línea]. Available:  
] <http://www.fibermax.pe/pdf/datasheets/DS%20-%20Conector%20Mec%3%A1nico%20FIC-SC-APC%20%2001-2019.pdf>.  
[Último acceso: 20 marzo 2022].

- [35 Josh, «Qué es la potencia óptica y cómo afecta al funcionamiento de tu conexión de fibra,» *bandaancha.eu*, 06 marzo 2022. [En línea]. Available: <https://bandaancha.eu/articulos/que-potencia-optica-como-afecta-10192>. [Último acceso: 2022 marzo 25].
- [36 N. Z. A. I. A. M. Z. A. R. N. M. Y. F. M. Atan, «Security enhanced dynamic bandwidth allocation,» *Journal of Optical Communications and Networking*, vol. 13, nº No. 12, pp. 301-311, 2021.
- [37 N. Z. ,. M. R. S. ,. K. K. Auwalu Usman, «Optical link monitoring in fibre-to-the-x passive optical network (FTTxPON): A comprehensive survey,» *ScienceDirect*, vol. Vol. 39, nº ELSEVIER, 2020.