Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

DISEÑO DE INVESTIGACIÓN PARA LA IMPLEMENTACIÓN DE UNA RUTINA AUTOMATIZADA DE *HEALTH CHECK* EN EQUIPOS DE LA RED IP DE ACCESO POR RADIO (IP-RAN) DE UN PROVEEDOR DE SERVICIOS DE INTERNET EN GUATEMALA

Marvin Saúl Arredondo Torres
Asesorado por el MSc. Ing. Christian Antonio Orellana López

Guatemala, marzo de 2022

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

DISEÑO DE INVESTIGACIÓN PARA LA IMPLEMENTACIÓN DE UNA RUTINA AUTOMATIZADA DE *HEALTH CHECK* EN EQUIPOS DE LA RED IP DE ACCESO POR RADIO (IP-RAN) DE UN PROVEEDOR DE SERVICIOS DE INTERNET EN GUATEMALA

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

MARVIN SAÚL ARREDONDO TORRES
ASESORADO POR EL MSC. ING. CHRISTIAN ANTONIO ORELLANA LÓPEZ

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO ELECTRÓNICO

GUATEMALA, MARZO DE 2022

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANA	Inga. Aurelia Anabela Cordova Estrada
VOCAL I	Ing. José Francisco Gómez Rivera
VOCAL II	Ing. Mario Renato Escobedo Martínez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Br. Kevin Armando Cruz Lorente
VOCAL V	Br. Fernando José Paz González
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Pedro Antonio Aguilar Polanco
EXAMINADOR	Ing. Guillermo Antonio Puente Romero
EXAMINADOR	Ing. Helmunt Federico Chicol Cabrera
EXAMINADOR	Ing. José Aníbal Silva de los Angeles
SECRETARIO	Inga. Lesbia Magalí Herra López

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

DISEÑO DE INVESTIGACIÓN PARA LA IMPLEMENTACIÓN DE UNA RUTINA AUTOMATIZADA DE *HEALTH CHECK* EN EQUIPOS DE LA RED IP DE ACCESO POR RADIO (IP-RAN) DE UN PROVEEDOR DE SERVICIOS DE INTERNET EN GUATEMALA

Tema que me fuera asignado por la Dirección de Escuela de Estudios de Postgrado con fecha 02 de agosto de 2021.

Marvin Saúl Arredondo Torres

EEPFI-PP-0189-2022
Guatemala, 12 de enero de 2022

Director
Armando Alonso Rivera Carrillo
Escuela De Ingenieria Mecanica Electrica
Presente.

Estimado Ing. Rivera

Reciba un cordial saludo de la Escuela de Estudios de Postgrado de la Facultad de Ingeniería.

El propósito de la presente es para informarle que se ha revisado y aprobado el Diseño de Investigación titulado: **IMPLEMENTACIÓN DE UNA RUTINA AUTOMATIZADA DE HEALTH CHECK EN EQUIPOS DE LA RED IP DE ACCESO POR RADIO(IP RAN) DE UN PROVEEDOR DE SERVICIOS DE INTERNET EN GUATEMALA** , el cual se enmarca en la línea de investigación: **Infraestructura de red - Infraestructura de red**, presentado por el estudiante **Marvin Saúl Arredondo Torres** carné número **201114214**, quien optó por la modalidad del "PROCESO DE GRADUACIÓN DE LOS ESTUDIANTES DE LA FACULTAD DE INGENIERÍA OPCIÓN ESTUDIOS DE POSTGRADO". Previo a culminar sus estudios en la Maestría en ARTES en Ingeniería Para La Industria Con Especialidad En Telecomunicaciones.

Y habiendo cumplido y aprobado con los requisitos establecidos en el normativo de este Proceso de Graduación en el Punto 6.2, aprobado por la Junta Directiva de la Facultad de Ingeniería en el Punto Décimo, Inciso 10.2 del Acta 28-2011 de fecha 19 de septiembre de 2011, firmo y sello la presente para el trámite correspondiente de graduación de Pregrado.

Atentamente,

"Id y Enseñad a Todos"

Christian Antonio Orellana López
INGENIERO ELECTRÓNICO
COL. 11,939

Mtro. Christian Antonio Orellana López
Asesor(a)

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
ESCUELA DE POSTGRADO
FACULTAD DE INGENIERIA

Mtro. Mario Renato Escobedo Martinez
Coordinador(a) de Maestría

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERÍA
DIRECCIÓN
ESCUELA DE POSTGRADO

Mtro. Edgar Dario Alvaréz Cotí
Director
Escuela de Estudios de Postgrado
Facultad de Ingeniería

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA

EEP-EIME-0189-2022

El Director de la Escuela De Ingenieria Mecanica Electrica de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del Asesor, el visto bueno del Coordinador y Director de la Escuela de Estudios de Postgrado, del Diseño de Investigación en la modalidad Estudios de Pregrado y Postgrado titulado: **IMPLEMENTACIÓN DE UNA RUTINA AUTOMATIZADA DE HEALTH CHECK EN EQUIPOS DE LA RED IP DE ACCESO POR RADIO(IP RAN) DE UN PROVEEDOR DE SERVICIOS DE INTERNET EN GUATEMALA** , presentado por el estudiante universitario **Marvin Saúl Arredondo Torres**, procedo con el Aval del mismo, ya que cumple con los requisitos normados por la Facultad de Ingeniería en esta modalidad.

ID Y ENSEÑAD A TODOS

Ing. Armando Alonso Rivera Carrillo
Director
Escuela De Ingenieria Mecanica Electrica

Guatemala, enero de 2022

Decanato
Facultad de Ingeniería
24189101- 24189102
secretariadecanato@ingenieria.usac.edu.gt

LNG.DECANATO.OI.197.2022

La Decana de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica, al Trabajo de Graduación titulado: **DISEÑO DE INVESTIGACIÓN PARA LA IMPLEMENTACIÓN DE UNA RUTINA AUTOMATIZADA DE HEALTH CHECK EN EQUIPOS DE LA RED IP DE ACCESO POR RADIO (IP-RAN) DE UN PROVEEDOR DE SERVICIOS DE INTERNET EN GUATEMALA,** presentado por: **Marvin Saúl Arredondo Torres ,** después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANA
FACULTAD DE INGENIERÍA

Inga. Aurelia Anabela Cordova Estrada
Decana

Guatemala, marzo de 2022

AACE/gaoc

ACTO QUE DEDICO A:

Dios	Por ser el guía de mi camino siempre, darme sabiduría y entendimiento para alcanzar mis metas. Sin Él no soy nada ni nadie.
Mis padres	Aura Fidelia Torres y Edgar Arredondo Pocasangre, por darme la vida y ser mi apoyo constante hasta el día de hoy, brindarme su amor y enseñanzas día a día, sin ustedes este logro no fuese posible.
Mis hermanos	Karin Paola, Edgar Estuardo y Rony Oswaldo Arredondo, por ser inspiración y ejemplo para alcanzar la excelencia.
Mis amigos	Enrique Espinoza, Fernando Rodas, Ixim Morales, Humberto Sosa y Christopher Cisneros por ser apoyo incondicional y motivación para siempre cumplir el lema de Don Bosco *Ad Astra*.
Mi familia	Por sus enseñanzas, cariño y consejos a lo largo de toda mi vida.
Mi novia	Evelyn Regina Chacón por ser mi complemento, apoyo en todos mis proyectos e impulso para concluir esta etapa.

AGRADECIMIENTOS A:

Universidad de San Carlos de Guatemala	Por ser la *alma mater* que me abrió el camino hacia el conocimiento y el mundo del saber.
Facultad de Ingeniería	Por proporcionarme los conocimientos que me han permitido alcanzar esta meta.
Mis amigos y compañeros de carrera	Por su compañía y apoyo brindado durante esta etapa.
Mi mejor amiga	Mary Godoy, por motivarme y siempre estar en los momentos difíciles.
Mi asesor	MSc. Ing. Christian Orellana, por haberme guiado durante este trabajo de graduación.
Tigo Guatemala y compañeros de trabajo	Por abrirme las puertas de la empresa y ser pilar fundamental para mi desarrollo personal y profesional. Por las experiencias y conocimiento compartido.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE SÍMBOLOS

Símbolo	Significado
Q	Quetzal
%	Porcentaje

GLOSARIO

BBU *Baseband Unit*. Unidad que procesa la banda base en un sistema de telecomunicaciones.

CPU *Central Processing Unit*. Elemento central de una computadora, encargada del procesamiento de datos.

IBM *International Business Machines.* Corporación multinacional de tecnología informática y consultoría.

ICMP *Internet Control Message Protocol*. Protocolo utilizado para enviar mensajes de error e información operativa indicando si un host no es alcanzado o que un servicio solicitado no está disponible.

IoT *Internet of Things*. Describe la red de objetos físicos que incorporan sensores, software y otras tecnologías con el fin de conectar e intercambiar datos con otros dispositivos y sistemas a través de internet.

IP *Internet Protocol*. Es un protocolo no orientado a la conexión responsable del direccionamiento y la fragmentación de paquetes de datos.

IS-IS *Intermediate System to Intermediate System*. Es un protocolo de estado de enlace que básicamente

	maneja un mapa para enrutar paquetes mediante la convergencia de la red. Se conoce como un protocolo IGP.
ISO	*International Organization for Standardization*. Es una organización para la creación de estándares internacionales, está compuesta por diversas organizaciones nacionales de normalización.
IT	*Information Technology*. Término que se refiere a hardware, software, telecomunicaciones, redes y personas involucradas para crear, almacenar, intercambiar y utilizar información.
MPLS	*Multiprotocol Label Switching*. Mecanismo para transportar datos de forma estándar, diseñado para las redes basadas en circuitos y paquetes.
NMS	*Network Management System*. Es una aplicación o conjunto de aplicaciones que permite a los administradores de red administrar los componentes independientes de una red dentro de un marco de administración de red más grande.
OSPF	*Open Shortest Path First*. Es un protocolo de enrutamiento de tipo estado de enlace, desarrollado para las redes IP y basado en el algoritmo de primera vía más corta. Se conoce como un protocolo IGP.

OSI	*Open System Interconnection*. Es el modelo de referencia que describe las actividades de red basado en una estructura de siete capas.
Pseudowire	Es una emulación de una conexión punto a punto a través de una red de conmutación de paquetes.
QoS	*Quality of Service*. En telecomunicaciones es el rendimiento promedio de una red de telefonía o datos, particularmente percibido por los usuarios de red.
RRH	*Remote Radio Head*. También conocido como *Remote radio unit* (RRU) son los radios que se colocan en las torres y van conectados hacia la BBU, se encargan de ejecutar toda la funcionalidad de RF como transmitir y recibir, filtrar y amplificar.
Syslogs	Es un estándar para el envío de mensajes de registro en una red IP.
TCP	*Transmission Control Protocol.* Es un protocolo de red que permite que dos *hosts* se establezcan una conexión e intercambian flujos de datos.
TDM	*Time Division Multiplexing*. Es un método de multiplexación en el que el ancho de banda total del medio de transmisión es asignado a cada canal durante una fracción del tiempo total.

Trap	Son los mensajes que le permiten a un agente SNMP reportar los cambios de estado al administrador SNMP cuando ocurre un evento.
UDP	*User Datagram Protocol*. Es el protocolo que permite el envío de datagramas a través de la red sin haber establecido una conexión previamente con el destino.
VPLS	*Virtual Private LAN Service*. Es un método para crear túneles capa dos, multipunto a multipunto, basado en MPLS.
VPN	*Virtual Private Network*. Es un método utilizado para transportar varios tipos de tráfico de red utilizando como base MPLS, con el fin de segmentar las tablas de ruteo para cada cliente.

RESUMEN

El presente trabajo plantea el diseño de investigación de una propuesta de implementación de una rutina automatizada de *health check* en equipos de la red IP de acceso por radio (IP-RAN) de un proveedor de servicios de internet.

Para abordar la problemática se trabajarán varias fases que comprenden la revisión documental de la información estándar que debe estar incluída en un *health check* para equipos de telecomunicaciones, definición de los parámetros físicos y lógicos necesarios para conocer el estado físico del *hardware* y el correcto funcionamiento de las configuraciones lógicas en los equipos de la red IP-RAN del proveedor de servicios de internet, el proceso de desarrollo de un software que permita interpretar toda la información recolectada en cada uno de los equipos para presentarla en un reporte final el cual podrá ser utilizado por un usuario para su respectivo análisis.

La implementación de una rutina automatizada de *health check* en equipos de telecomunicaciones es de gran ayuda para un proveedor de servicios de internet o para toda empresa que cuente con una red amplia, ya que aporta información fundamental para la detección de fallas antes de que sucedan, disminuyendo de esta manera las actividades correctivas que muchas veces se realizan en escenarios de afectación de servicios y aumentando las actividades preventivas que se realizan en escenarios controlados sin afectación.

1. INTRODUCCIÓN

En los inicios de las telecomunicaciones era impensable que las redes de acceso fueran tan robustas y de gran escala como lo son hoy en día, el teléfono móvil es cada vez más una herramienta de trabajo y un dispositivo de entretenimiento para muchos, por lo que los usuarios necesitan mayor conectividad y velocidades de descarga considerables para soportar la variedad de servicios que existen, como las aplicaciones de *streaming* (transmisión) de video, contenido en la web, aplicaciones de *cloud* (nube), videollamadas, entre otros, es tal la variedad de servicios que deben ofrecer los proveedores de servicios, que es necesario tener una red con equipos que soporten las altas cantidades de tráfico sin incurrir en fallas.

Para todo proveedor de servicios de internet es de suma importancia contar con una red estable y saludable, y así poder brindar servicios sin que se vea afectada la calidad y la experiencia del cliente. Para alcanzar este objetivo, una actividad fundamental es ejecutar rutinas de *health check* (control de salud) en cada uno de los equipos que conforman la red, un *health check* no es más que una serie de evaluaciones que se realizan a los equipos de una red con el fin de diagnosticar fallas en ciertos componentes de *hardware* o parámetros de configuración para poder brindar recomendaciones y aplicar acciones correctivas o preventivas.

La empresa de estudio en el presente trabajo es uno de los grandes proveedores de servicios de internet de Guatemala, cuenta con una red lo suficientemente robusta para brindar una gran cantidad de servicios a sus usuarios. El control y monitoreo de la red es eficiente pero no cuentan con algún

procedimiento o software que realice constantes rutinas de *health check* en los equipos de la red IP-RAN (*IP-Radio Access Network*), esta es una actividad que le cuesta dinero a la empresa ya que es solicitada a los proveedores de los equipos y toma algún tiempo obtener los resultados, por ello este trabajo tiene como objetivo implementar un software que de forma automatizada ejecute estas rutinas en los diferentes equipos y genere reportes del estado de los diferentes parámetros de entorno físico y lógico.

El trabajo se llevará a cabo mediante un análisis de los parámetros de entorno físico y lógico de cada equipo que conforma la red IP-RAN del proveedor de servicios de internet, identificando los más críticas y que pueden traducirse en una falla en el equipo si no son controladas a tiempo, luego utilizando el protocolo SNMP (*Simple Network Management Protocol*) se identificarán las OIDs (*Object Identifier*) necesarias utilizando el archivo de MIBs (*Management Information Base*) que nos brindarán la información de cada parámetro seleccionado y por último, mediante el desarrollo de un *software* que permitirá consultar esta información e interpretarla, se generarán reportes con la información actual del equipo, listos para ser analizados y ejecutar las acciones necesarias para prevenir fallas que afecten la calidad de los servicios brindados.

Se presenta una serie de conceptos que es necesario comprender antes de iniciar en el análisis de información por el protocolo SNMP y el manejo de archivo de MIBs y OIDs (*Object Identifier*).

Se da a conocer los diferentes parámetros de entorno para conocer el estado físico y lógico de un equipo de una red de acceso por radio IP, parámetros que ayudarán a identificar fallas o evitar antes de que sucedan.

2. ANTECEDENTES

González (2014), en su estudio hace referencia a los modelos y estándares de gestión y manejo de redes, explica una forma ordenada y estructurada de la correcta gestión de información basándose en un esquema que utiliza la base de información de gestión (MIB), para determinar qué identificador de objeto (OID) es el correcto para capturar un parámetro en específico de un equipo de red. Este trabajo se relaciona con la investigación planteada ya que muestra la documentación de entidades internacionales que dan los fundamentos para gestionar una red, obtener información vía SNMP y cómo estructurar la relación entre una comunidad SNMP.

Cuchala (2016), en su estudio hace referencia a la relación administrador - gestor de eventos, como debe ser la arquitectura utilizada y la comunicación para interpretar los datos obtenidos vía SNMP. Esto se relaciona con el trabajo planteado de forma que es necesario seguir una arquitectura, basada en los estándares, de correcta comunicación entre los agentes administrador-gestor de eventos, para poder interpretar la información que se recolectó vía SNMP de cada uno de los equipos de la red IP de acceso por radio.

Jukic, Hedi y Speh (2017), en su estudio realizan un análisis y comparativa de la información recolectada utilizando agentes SNMP de varios proveedores de hardware, observando la forma en que cada proveedor estructura la información de sus agentes SNMP.basado en sus MIB propietarias. Para el estudio propuesto es de importancia esta investigación ya que la empresa donde se desarrollará posee una red IP de acceso por radio conformada por varios proveedores de

hardware, por lo que es de apoyo para saber analizar de forma correcta las MIBs de cada uno.

Junco y Rabelo (2018), en su investigación proponen un tipo de alarmas basadas en patrones de comportamiento, los cuales son definidos con anterioridad utilizando valores máximos y mínimos conocidos como umbrales. Referente al estudio propuesto esta clasificación de alarmas es de utilidad ya que en la red IP de acceso por radio algunos equipos son más exigidos que otros, por lo que se pueden configurar valores umbrales para escenarios diferentes en la red.

Quispe (2019), realizó un prototipo de monitoreo de dispositivos utilizando el protocolo SNMP basado en un software libre para una empresa e-Commerce, en su estudio plantea una clasificación de siete tipos de alarmas que pueden presentar los equipos, en relación al trabajo que se está planteando, esta clasificación es de ayuda para dividir los datos que se desean colocar en los reportes de *health check* según su criticidad y así proponer acciones según la cantidad de alarmas que pertenezca a cada grupo.

3. PLANTEAMIENTO DEL PROBLEMA

3.1. Descripción general

Cada día las redes de telecomunicaciones deben ser más robustas, el teléfono móvil cada vez es más exigido y utilizado más como una computadora portátil, con la aparición de nuevas plataformas de contenido y la necesidad de estar más conectados, los anchos de banda necesarios van incrementándose aceleradamente mientras las redes de acceso por radio deben responder rápidamente, es por ello que para un proveedor de servicios de internet es fundamental contar con una red saludable y funcionando correctamente para no afectar la calidad de servicio y experiencia de los usuarios finales.

La empresa objeto de este estudio es uno de los grandes proveedores de servicios de internet de Guatemala, cuenta con una amplia gama de servicios como lo es telefonía móvil, servicios residenciales de cable, internet y telefonía, servicios corporativos y algunos más. La cobertura de la empresa es en todo el país por lo que cuentan con una red IP de acceso por radio bastante amplia.

Actualmente la empresa cuenta con un monitoreo de la red muy completo, y la atención de las fallas es bastante eficiente, sin embargo, muchas de las fallas podrían prevenirse utilizando rutinas de health check en los equipos, con el objetivo de que la atención de fallas sea de forma preventiva y no correctiva cuando ya existe algún tipo de afectación o peligro de que ocurra.

3.2. Definición del problema

Es muy importante comprender el problema que motivó este trabajo de investigación para ello es necesario detallar el problema, delimitar el área que abarca el problema y responder a una serie de preguntas de investigación.

3.2.1. Especificación del problema

Para toda empresa de telecomunicaciones es importante reducir gastos de operación y maximizar la calidad del servicio que ofrecen a sus clientes, para ello es muy importante reducir las fallas que se puedan generar en los equipos, disminuyendo de esta manera el gasto en *hardware*, y cambiando las actividades correctivas, por actividades preventivas que no representan afectación a la operación y permitan alargar el tiempo de vida útil de los equipos.

Actualmente en la empresa las actividades de *health check* para los equipos de la red IP de acceso por radio son ejecutadas por los proveedores de los equipos, estas tareas no son parte del contrato de soporte que se tiene acordado, por lo que no son realizadas constantemente, de solicitar esto, tienen un costo adicional y requieren de un tiempo de espera para obtener los resultados de las pruebas, el presente trabajo pretende desarrollar una solución propia de la empresa para ejecutar estas tareas sin solicitar apoyo de los proveedores.

3.2.2. Delimitación del problema

El estudio se tiene planificado realizarlo en uno de los principales proveedores de servicios de internet de Guatemala, impactando a la red IP-RAN de todo el país, durante los meses de enero a agosto del año 2022.

3.2.3. Pregunta principal de investigación

¿Cómo se puede realizar una rutina de *health check* para equipos de una red IP de acceso por radio de un proveedor de servicios de internet en Guatemala?

3.2.4. Preguntas complementarias de investigación

- ¿Cuáles son los parámetros más críticos para conocer el estado físico y lógico de cada elemento de red?

- ¿Qué protocolo se puede utilizar para obtener la información necesaria de cada elemento de red?

- ¿Cómo se puede interpretar la información recolectada en cada equipo de red?

4. JUSTIFICACIÓN

La realización de la presente investigación se justifica en la línea de investigación de Gestión y monitoreo de redes de la Maestría en Ingeniería para la Industria con orientación en Telecomunicaciones, debido a que su desarrollo se utilizan sistemas de gestión a base de protocolos de administración de redes como SNMP, con la finalidad de lograr un óptimo desempeño y control de una red de IP-RAN.

Toda red de telecomunicaciones necesita un constante control y mantenimiento para garantizar su desempeño, aumentando la calidad de servicio y la experiencia del cliente, por ello, esta investigación se enfoca en la importancia de mantener una red saludable a base de ejecutar rutinas de *health check* constantemente en cada uno de los elementos de la red, con el fin de recabar información del estado físico y lógico de cada equipo y así poder ejecutar las respectivas tareas de mantenimiento correctivo o preventivo.

Para un proveedor de servicios de internet es de suma importancia tener el control de su red, conocer el estado de cada uno de los elementos que la conforman ya que de esto depende gran parte del funcionamiento de la red y la calidad de los servicios ofrecidos, por ello, esta investigación buscar dar a conocer los parámetros más críticos e importantes de cada elemento de red, necesarios para mantener un control, y cómo recabar esta información mediante un procedimiento automático.

En definitiva, el cliente final será el mayor beneficiado, ya que gozará de un servicio de alta calidad, libre de fallas y con un alto porcentaje de disponibilidad.

La empresa proveedora de servicios también se beneficiará ya que tendrá una mayor visibilidad del estado de la red, evitando que los equipos lleguen al punto de fallar repentinamente afectando los servicios e incurriendo en pérdidas económicas y quejas de los clientes.

5. OBJETIVOS

5.1. General

Implementar una rutina automatizada de *health check* en equipos de la red IP de acceso por radio (IP-RAN), de un proveedor de servicios de internet en Guatemala.

5.2. Específicos

- Identificar los parámetros más críticos de un elemento de red, de una red IP de acceso por radio, para conocer su estado físico y lógico.

- Aplicar el protocolo SNMP para obtener la información necesaria de cada equipo en la red.

- Desarrollar un *software* que permita interpretar la información recolectada de cada equipo en la red.

- Automatizar la generación de reportería con los datos del *health check* de cada elemento de red.

.

6. NECESIDADES POR CUBRIR Y ESQUEMA DE SOLUCIÓN

La automatización de tareas es fundamental en proyectos de IT, por ello esta investigación está centrada en implementar y automatizar rutinas de *health check* en los equipos de la red IP-RAN, para cubrir la necesidad de tener un mayor control y monitoreo del estado físico y lógico de los equipos de la red y así anticiparse a cualquier evento que afecte los servicios brindados.

También se busca satisfacer la necesidad de disminuir la cantidad de actividades correctivas y aumentar las actividades preventivas, con el objetivo de disminuir los tiempos de afectación de servicios y el deterioro del *hardware*, aumentando su tiempo de vida al atacar anticipadamente las fallas.

6.1. Esquema de la solución

Para la solución al problema de investigación se realizará una serie de pasos secuenciales ya que cada tarea depende de la conclusión de la tarea anterior, el trabajo a realizar se puede delimitar en seis puntos específicos descritos de la siguiente manera.

- Revisión documental, buscar bibliografías que sean de apoyo para determinar la información que debe incluir un reporte de *health check* para equipos de telecomunicaciones.

- Clasificar los equipos de la red IP-RAN del proveedor de servicios de internet y definir los parámetros físicos y lógicos para conocer el estado de estos equipos.

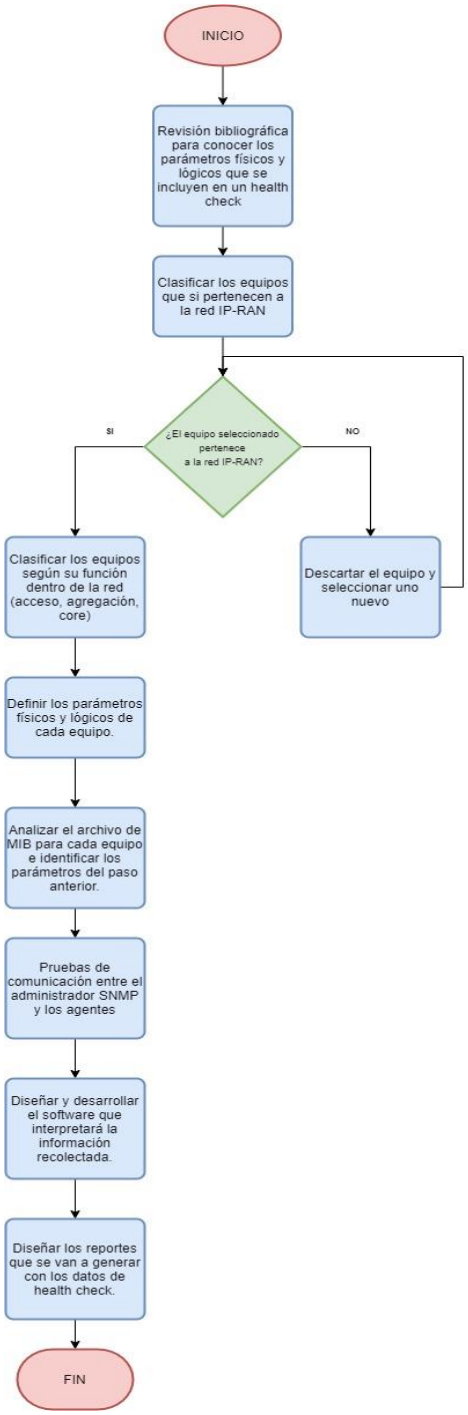
- Analizar el archivo de MIBs de cada equipo e identificar el OID de cada parámetro definido en el punto anterior.

- Realizar pruebas de comunicación entre el administrador SNMP y los agentes SNMP y validar la información recolectada con las OIDs identificadas anteriormente.

- Diseñar y desarrollar el *software* que permitirá interpretar la información recolectada por el administrador SNMP.

- Diseñar los reportes donde se presentará la información del *health check* para cada equipo.

Figura 1. **Esquema de la solución**



Fuente: elaboración propia, empleando Draw.io.

7. MARCO TEÓRICO

7.1. Redes IP-RAN

Según Marichal (2021) es el término utilizado para referirse a una red de acceso por radio (RAN) basada en IP/MPLS como capa de transporte, capaz de transportar múltiples servicios que requieren un alto ancho de banda, alta confiabilidad y baja latencia. Se utilizan para interconectar los nodos de acceso de telefonía móvil con los elementos que conforman el núcleo de la telefonía móvil.

Son la evolución de las redes tradicionales basadas en conmutación de circuitos que utilizaban la multiplexación por división de tiempo (TMD) como tecnología de transporte.

7.1.1. Beneficios de una red IP-RAN

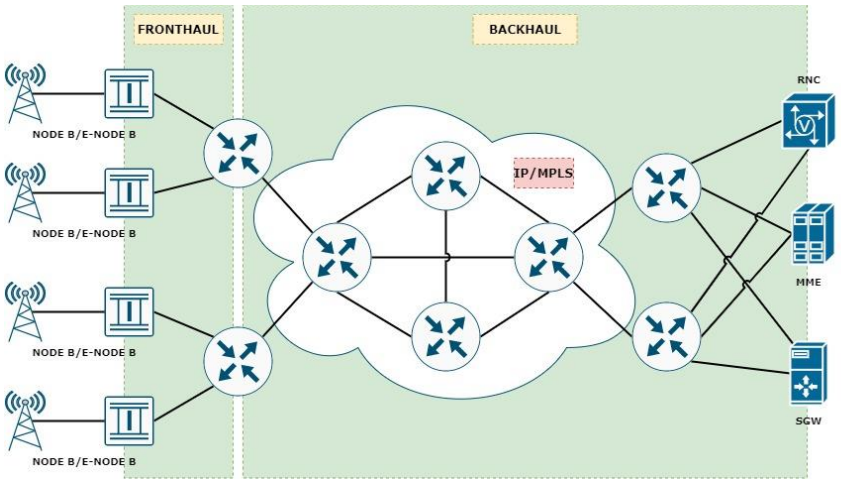
Son varios los beneficios de contar con una red IP-RAN, los principales son los siguientes:

- Cubrir la demanda de tráfico de forma eficiente
- Aplicación de calidad de servicio (QoS)
- Costos de implementación más bajos
- Optimización de recursos, principalmente el ancho de banda y el *hardware* de los equipos
- Latencia muy baja
- Alta disponibilidad de servicio

7.1.2. Arquitectura

Una red IP-RAN se puede estructurar en dos partes, se tiene una capa de acceso conocida como el *fronthaul mobile* y una capa media utilizada como transporte para enlazar el núcleo de la red con el acceso, conocida como *backhaul mobile*.

Figura 2. **Arquitectura de una red IP-RAN**



Fuente: elaboración propia, empleando Draw.io.

7.1.2.1. *Fronthaul mobile*

Consiste en la conexión que se establece desde la cabeza de radio remoto (RRH) pasando por la unidad de banda base (BBU), hasta el nodo de acceso de red IP/MPLS. Su función es transportar el tráfico desde la celda hasta la red IP/MPLS. Se pueden utilizar varias tecnologías de enlaces físicos como el cobre, microondas y fibra óptica.

Según VIAVI (2021) este término ha evolucionado desde su aparición en las redes LTE, donde se estableció para complementar la conexión de *backhaul* entre el núcleo de la red móvil hasta la BBU. El *fronthaul* se ha convertido en una parte fundamental para compensar la demanda de capacidad, disminución de latencia y confiabilidad de los servicios.

7.1.2.2. *Backhaul mobile*

Es la parte encargada del transporte de servicios de la red móvil, comprende el enlace entre el núcleo y el acceso. Su función es unificar todo el tráfico y converger sobre un mismo transporte, el cual puede ser transmitido sobre cualquier medio, hoy en día por lo general se utiliza la fibra óptica.

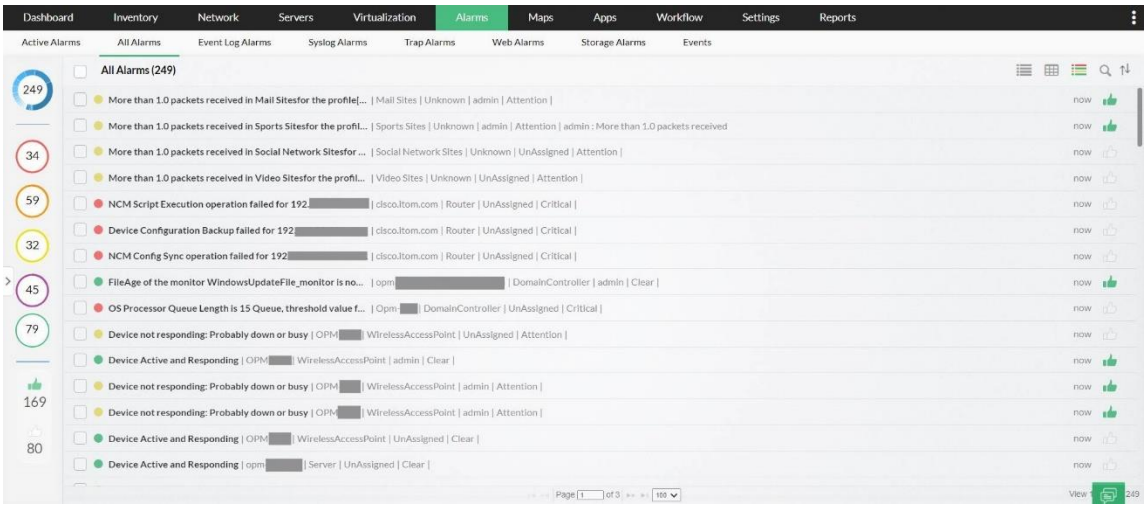
Utilizando VPN's configuradas sobre MPLS es posible diferenciar los diferentes tipos de tráfico que está siendo transportado sobre la red IP/MPLS, es decir, que el tráfico no se está mezclando entre sí, a pesar de que comparten el mismo transporte y ancho de banda. Basados en el tipo de servicio que se está transportando se pueden utilizar VPN's punto a punto (*pseudowires*) o multipunto en capa 2 (VPLS) o en capa 3 (IP VPN's).

7.2. Sistema de gestión de eventos

Es el componente de un gestor de redes que se encarga de la detección, identificación y resolución de problemas en una red. También es conocido por sus siglas en inglés como *Fault Management System* (FMS). La importancia de contar con un eficiente sistema de gestión de eventos radica en disminuir el tiempo de inactividad de la red y las fallas en los equipos, así como apoyar en la recuperación cuando estos eventos suceden.

Según Siggins (2020), el modelo propuesto por ISO para la gestión de redes plantea el monitoreo de eventos como una de las cinco claves fundamentales en el manejo y gestión de redes, definiéndolo como la habilidad de detectar, identificar, notificar y corregir eventos ocurridos.

Figura 3. **Ejemplo de sistema de gestión de eventos**



Fuente: ManageEngine (2021). *Fault Monitoring System.* Consultado el 10 de octubre de 2021. Recuperado de https://www.manageengine.com/network-monitoring/fault-monitoring.html

7.2.1. Funciones principales

Los sistemas de gestión de eventos son de gran apoyo para la gestión de redes, las funciones más importantes que desempeña son:

- Monitoreo en tiempo real
- Gestión de eventos
- Control, implementación y monitoreo de los recursos de la red
- Gestión de configuraciones
- Gestión de seguridad

- Análisis de causa-raíz

7.2.2. Ciclo de funcionamiento

El flujo de trabajo de un gestor de eventos es cíclico y continuo, inicia con la detección de la falla, sigue un determinado procedimiento hasta la resolución de la falla y termina donde empezó, en la detección de la falla. Todo gestor de eventos implementa un específico proceso siguiendo ciertos pasos básicos que se enlistan a continuación:

- Detección de un evento: se mantiene en constante monitoreo, con el fin de detectar alguna interrupción o bajo desempeño en los equipos o servicios monitoreados.

- Diagnóstico e identificación del evento: determina el origen del evento y su localización en la topología de red.

- Correlación y agrupación de eventos: busca si es un evento aislado o está relacionado con algún otro, la correlación es importante para realizar un análisis de causa-raíz.

- Restauración del servicio: al detectarse un evento y producirse la alarma en el gestor, este debería poder aplicar una solución automática mediante alguna aplicación o la ejecución de un script para restablecer el servicio lo más pronto posible. Existen eventos en los que el gestor no es capaz de brindar una solución, por lo ya es necesaria la intervención de personal.

- Resolución del evento: según la complejidad del evento, una restauración automática no siempre es factible, en estos casos, es necesaria la intervención manual de algún técnico de campo.

7.2.3. Tipos de sistemas de gestión de eventos

Existen dos tipos de sistemas de gestión de eventos, ambos se diferencian en su forma de operación y detección de eventos.

- Activos: son los que constantemente están monitoreando la red, y permiten de forma proactiva detectar un evento basado en los umbrales de monitoreo configurados. Utilizan protocolos como el ICMP, estatus de puertos TCP y UDP y contadores de desempeño.

- Pasivos: son los que esperan a que ocurra un evento para mostrar una alerta, se encuentran en modo de escucha hasta recibir la alerta por parte de algún equipo. Se apoyan de Syslogs, SNMP traps, logs de eventos.

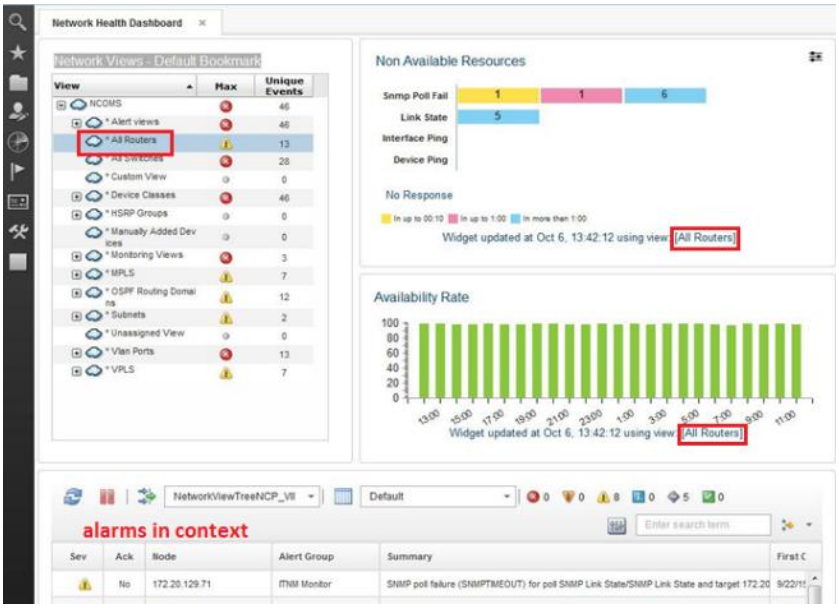
7.2.4. Gestor de gestores

El gestor de gestores es un sistema de gestión de eventos, que tiene la capacidad de agrupar los eventos de todos los gestores de monitoreo que se utilizan en la red, en un entorno de diferentes fabricantes.

Es de gran apoyo para todo operador de monitoreo de red ya que en una misma pantalla se pueden gestionar los eventos de varias redes de telecomunicaciones sin importar la tecnología (redes móviles, redes de transporte, redes inalámbricas, redes IP/MPLS, entre otros).

Un ejemplo de un gestor de gestores es el *Netcool Operations Insight* (NOI), esta es una herramienta fabricada por IBM que utiliza el análisis de alarmas y alertas en tiempo real que se combinan con análisis de datos históricos más amplios. Consiste en una solución para analizar y administrar entornos de monitoreo de aplicaciones, su alcance puede llegar a incluir opción de descubrimiento de red, visualización, correlación de eventos, análisis de causa-raíz basados en topología y configuración.

Figura 4. **Vista gráfica del *netcool operations insight***



Fuente: Ebookreading (2021). *IBM Netcool Operations Insight.* Consultado el 10 de octubre del 2021. Recuperado de: https://ebookreading.net/view/book/EB9780738441856_7.html.

7.2.5. Protocolo SNMP

El protocolo simple de gestión de red, conocido por sus siglas en inglés como *simple network management protocol*, es un protocolo perteneciente al grupo de protocolos de TCP/IP, se emplea para monitorear y administrar

dispositivos dentro de una red. Basado en el modelo OSI, este protocolo opera en la capa de aplicación utilizando los puertos UDP 161 y 162. Tiene compatibilidad con una gran variedad de dispositivos convencionales de red como *routers, switches*, puntos de acceso, entre otros. Así como dispositivos finales tales como impresoras, computadoras, cámaras de seguridad y hasta dispositivos de IoT. Este protocolo no se utiliza únicamente para *hardware*, también se puede aplicar para monitorear servicios.

En la actualidad existen tres versiones de SNMP:

- SNMPv1: es la primera versión de este protocolo, actualmente aún se sigue utilizando debido a la simplicidad en su esquema de autenticación, a pesar de que esta versión no cuenta con mucha seguridad. La prioridad con esta primera versión era cubrir la supervisión de equipos debido al rápido crecimiento de la red, por lo que los temas de seguridad no fueron debidamente atendidos.

- SNMPv2: esta versión incluye varias mejoras con respecto a la anterior, seguridad es la más destacada junto con rendimiento, confidencialidad y comunicación entre estaciones de gestión. Inicialmente no fue bien aceptada debido a la poca compatibilidad con la primera versión y complejidad para su despliegue, sin embargo, con actualizaciones posteriores se logró mejorar en estos temas, hoy en día ambas versiones son completamente compatibles. El nuevo sistema de seguridad de esta versión no fue bien recibido por los usuarios por su alta complejidad, lo que obligó a crear una nueva variante de esta versión del protocolo, dando paso a SNMPv2c el cual incluye todas las bondades de la versión dos cambiando al sistema de seguridad de la versión uno mejorado.

- SNMPv3: incorpora todas las funcionalidades de SNMPv2c e importantes cambios en aspectos de seguridad, desempeño y configuración remota, también revisiones de integridad, técnicas de cifrado al momento de la autenticación y cuentas de usuario. Esta versión a pesar de que se desarrolló desde 2002 no es la más utilizada en las organizaciones, sin embargo, si la seguridad es un aspecto importante a considerar, esta es la mejor versión a utilizar. Su configuración es un poco compleja, específicamente en la administración de usuarios, necesita mucho más procesamiento comparado con sus antecesores, concretamente en la supervisión en intervalos cortos de tiempo por la alta cantidad de mensajes SNMP que se generan. Esta versión maneja tres diferentes tipos de seguridad que se describen a continuación:

    - *NoAuthNoPriv*: significa que no necesita autenticación, ni privacidad. Los mensajes no están encriptados, por ello se recomienda utilizarla en redes privadas y seguras.

    - *AuthNoPriv*: significa que utiliza autenticación, pero sin privacidad. Los mensajes no están encriptados, pero si necesitan una autenticación para poder ser utilizados.

    - *AuthPriv*: significa que utiliza autenticación y es privado. Es la versión más segura. Los mensajes deben pasar por un proceso de autenticación y son cifrados durante toda la transmisión.

7.2.6. Componentes básicos de SNMP y sus funciones

Son cuatro los componentes principales de una red administrada por SNMP, a continuación, se describen.

- Agente de SNMP: según ManageEngine (2021) es un *software* que se ejecuta en el *hardware* o servicio que se está monitoreando, el cual recopila los datos de diferentes parámetros o métricas importantes para el rendimiento del equipo. El agente es quien envía toda la información solicitada por el administrador SNMP al sistema de administración de red (*network management system*), no es necesario recibir una petición por parte del administrador para enviar información, el mismo agente lo puede realizar de forma proactiva al producirse algún error o evento en el equipo. La mayoría de los equipos ya vienen con un agente SNMP preinstalado de fábrica, ya sea estándar o uno propietario de cada fabricante, únicamente es necesario activarlo y configurarlo para poder operar.

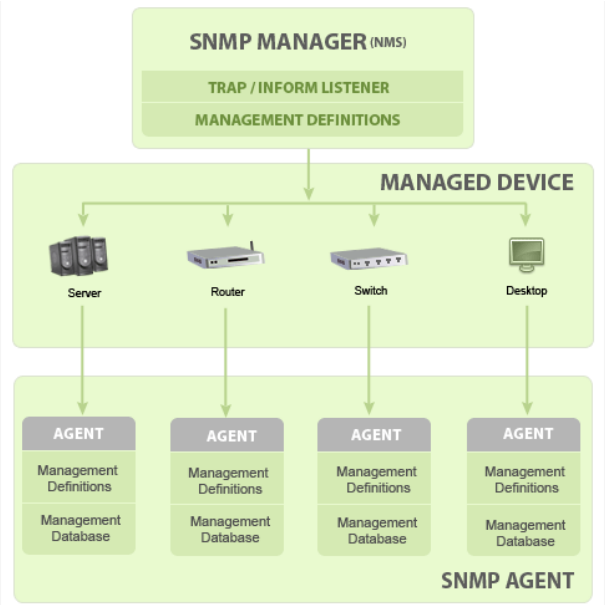
- Administrador de SNMP: también conocido como sistema de administración de red o por sus siglas en inglés como NMS, funciona como unidad central que recibe toda la información enviada por los agentes. El NMS realiza consultas cada cierto tiempo a cada uno de los agentes para que envíen actualizaciones de su información, este tiempo es configurable según el NMS que se esté utilizando. Existen administradores gratuitos los cuales por lo general vienen limitados en varias funciones comparados con uno de paga, los cuales pueden manejar una alta cantidad de información, redes bastante complejas y admiten una gran cantidad de nodos de red.

- Dispositivo administrado: es todo servicio o elemento de red que necesita ser monitoreado o algún tipo de administración, en ellos se ejecutan los agentes SNMP, estos equipos pueden ser *routers, switches*, servidores, estaciones de trabajo, impresoras, dispositivos IoT, entre otros.

- Base de Información de Administración (MIB): esta es una base de datos que todo agente SNMP cuenta con información que describe los

parámetros de los dispositivos administrados. El NMS utiliza esta base de datos para solicitar información específica al agente, puede traducirla e interpretarla según la función que se desea darle. Por lo general esta base de datos es un archivo de texto plano, contiene un conjunto estándar de valores específicos para cada elemento de red. SNMP también permite utilizar estos valores para un agente en particular mediante el uso de MIB privadas.

Figura 5. **Componentes básicos del protocolo SNMP**



Fuente: Manage Engine (2021). *Tutorial de SNMP.* Consultado el 12 de septiembre de 2021. Recuperado de: https://www.manageengine.com/es/network-monitoring/what-is-snmp.html.

7.2.7. Funcionamiento

El funcionamiento del protocolo SNMP se puede comparar con la comunicación cliente-servidor, ofreciendo comunicación por los métodos de monitorización por poleo (*polling*) y por trampas (*traps*).

7.2.7.1. Monitorización por *polling*

Este método funciona realizando un chequeo constante hacia una dirección IP en específico, requiere de un parámetro especial, la comunidad SNMP, la cual consiste en una cadena alfanumérica con la que se autoriza la operación, agregando de esta forma un poco de seguridad.

Al dirigir un chequeo hacia uno de los dispositivos se obtiene como resultado bastante información que para los humanos es difícil de interpretar, esta información corresponde a los valores de código de OID para un parámetro en específico del dispositivo monitoreado, para poder entender de mejor forma esta información, es necesario instalar el archivo de MIB del fabricante del equipo en el NMS. Según el NMS que se esté utilizando, es posible configurar alertas que ejecutarán acciones proactivas basado en los umbrales configurados.

7.2.7.2. Monitorización por *traps*

En este método es necesario configurar los elementos de red para que puedan enviar las alertas o *traps* cuando se cumplan ciertas circunstancias específicas, al mismo tiempo, se requiere de una herramienta que pueda recibir y analizar los *traps* SNMP, esta puede ser algún hardware que ejecute los servicios necesarios o un *software* de monitorización. La configuración SNMP para el envío de traps varía según el fabricante, por lo general cuentan con una interfaz de gestión a la que se puede acceder local o remotamente.

Para poder realizar una correcta monitorización de *traps* SNMP se deben tomar en cuenta varios factores.

- Es necesario contar con el archivo de MIB del fabricante para realizar la conversión de OID que envían los traps y así tener una descripción detallada del elemento de red que está fallando.

- Se debe tener conocimiento de los valores o límites normales para ciertos OID y así poder configurar alertas al llegar a cierto valor.

- Conocer los valores críticos de falla de los equipos que se quieren monitorizar.

7.2.8. Tipos de mensajes SNMP

Existe una gran variedad de mensajes que se pueden utilizar para configurar la supervisión de una red por SNMP:

- *GetRequest*: mensaje enviado por el administrador SNMP para hacer una solicitud de datos, el dispositivo monitoreado devuelve el valor que le fue solicitado con un mensaje de respuesta.

- *GetNextRequest*: es un mensaje utilizado por el administrador SNMP para descubrir la información que tiene disponible un elemento de red. Iniciando desde el OID se puede continuar realizando solicitudes hasta que se haya recibido el último dato disponible, esto es útil para conocer toda la información disponible de un dispositivo del cual no se tiene conocimiento previo.

- *GetBulkRequest*: es una versión mejorada del mensaje *GetNextRequest*, en esencia permite realizar varios *GetNextRequest* al mismo tiempo, para

recopilar en una lista una cierta cantidad de información y parámetros disponibles. Apareció por primera vez en SNMPv2.

- *SetRequest*: comando de tipo administrador utilizado para establecer o modificar algún parámetro o configuración en el equipo administrado.

- *Response*: es el mensaje de respuesta que envía el agente SNMP al administrador.

- *Trap* (v2): es el mensaje (trampa) que envía el agente SNMP sin haber sido solicitado por parte del administrador. Se envían al momento de que el dispositivo administrado reporta un evento o al sobrepasar algún umbral configurado.

- *InformRequest*: este mensaje se agregó desde SNMPv2 y se utiliza para que el administrador confirme la captura de información enviada por un agente SNMP. Algunos agentes se configuran para que envíen traps hasta que reciban un mensaje de informe.

- *Report*: este mensaje se creó para SNMPv3, se utiliza para que el administrador pueda determinar el tipo de error que presentó el agente SNMP remoto. Dependiendo del tipo de error, el administrador puede enviar un mensaje nuevo corregido.

7.2.9. Identificador de objetos (OID)

Conocido en inglés como *object identifier*, son los parámetros utilizados para identificar los diferentes objetos de los dispositivos gestionados, se encuentran definidos en las MIB. Se representan como secuencias numéricas

que son asignadas de forma jerárquica. Cada proveedor define las OID para sus productos. A continuación, se presenta un ejemplo de OID para determinar el estado de una interfaz física en equipos CISCO:

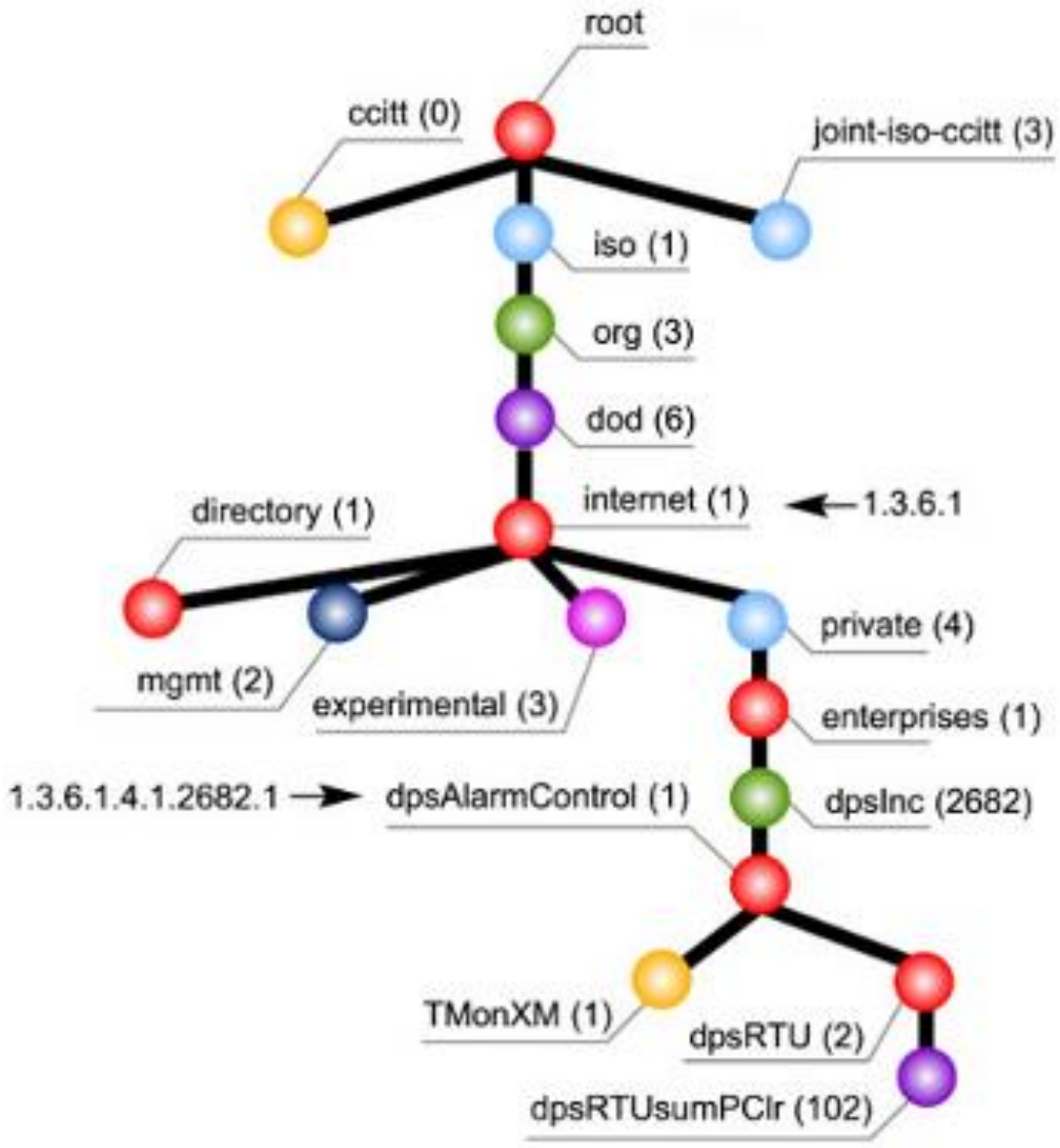
Figura 6. **Estructura de una OID**

Fuente: elaboración propia, empleando Word.

7.2.10. Base de información gestionada (MIB)

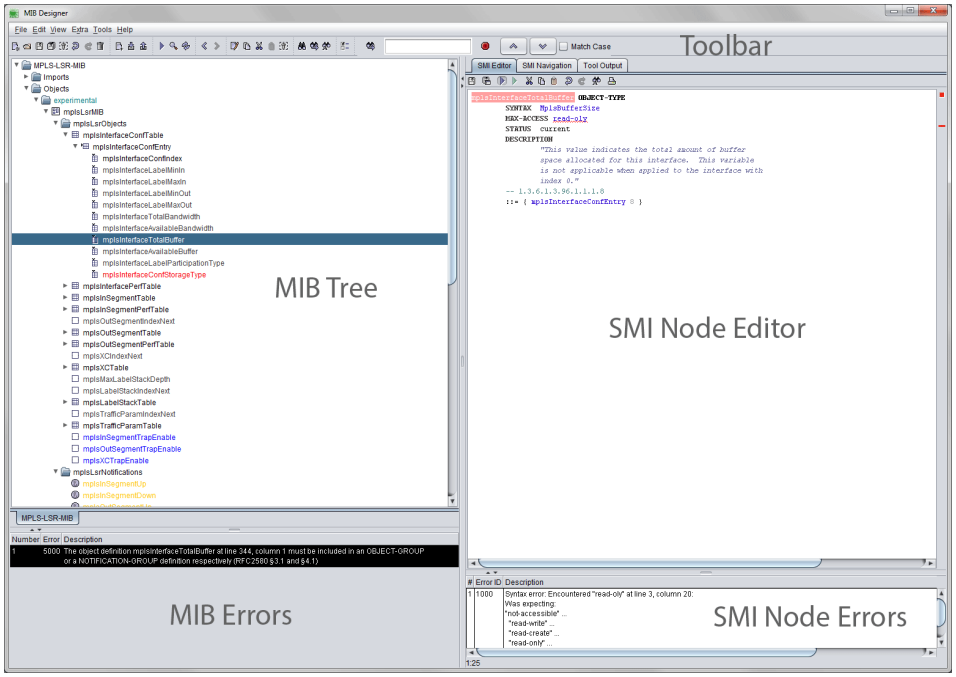
En inglés se conoce como *management information base*, es una colección de datos ordenados jerárquicamente en forma de árbol, con sus raíces y varios niveles. En resumen, una MIB se puede decir que está compuesta de varias OID.

Figura 7. **Estructura de una MIB**



Fuente: DenHartog (2021). *How to view, edit and read the management information base (MIB).* Consultado el 17 de septiembre de 2021. Recuperado de https://www.dpstele.com/snmp/mib/how-to-view-edit-read.php.

Figura 8. **Visualización de un archivo MIB en un *software***



Fuente: Agentpp (2021). *Using MIB designer*. Consultado el 17 de septiembre de 2021. Recuperado de https://agentpp.com/help/mds/4.2.0/index.htm#t=MIBDesigner2%2FMIBDesigner2%2FUsing_MIB_Designer.htm.

7.2.11. Necesidad de utilizar OIDs y MIBs

Cualquier información que se puede saber vía SNMP se trata individualmente por su OID, esta puede ser el porcentaje de utilización de memoria de un servidor, el tráfico en un *switch*, los archivos en cola de una impresora, entre otros. Por esta razón es que son necesarias las OID, ayudan a los administradores a identificar y supervisar los elementos de red. Para que exista una comunicación exitosa entre el dispositivo administrado y el administrador SNMP ambos necesitan conocer las OID disponibles.

Todos los objetos por supervisar de un dispositivo administrado deben conocer las MIB de dicho dispositivo, es por ello por lo que los administradores de la red deben verificar que las MIB estén almacenadas tanto en el administrador SNMP como en el agente SNMP.

7.3. *Health check*

Es una evaluación que se realiza en los elementos de una red para diagnosticar el estado de ciertos componentes de *hardware* y configuraciones lógicas para brindar una serie de recomendaciones basado en normativas o estándares.

Esta evaluación brinda una visión bastante clara del funcionamiento interno de cada elemento de red, es de gran ayuda para identificar problemas actuales y evitar problemas potenciales, con el fin de reducir las fallas en la red y los tiempos de inactividad.

En un *health check* de redes de telecomunicaciones se pueden diferenciar dos tipos de parámetros que son los que se desean evaluar.

- Parámetros de entorno o físicos: son todos los parámetros que tienen relación con algún componente de *hardware* del equipo, estos pueden ser temperatura de las tarjetas, utilización de CPU y memoria, estado de controladoras, estado de las interfaces, entre otros.

- Parámetros lógicos: son los parámetros de configuración que influyen en el correcto funcionamiento del equipo basado en el papel que desempeña dentro de la red. Algunos ejemplos podrían ser adyacencias de IS-IS y OSPF.

7.4. Automatización

Automatización es un conjunto de elementos mecánicos y electromecánicos que trabajan en conjunto con la más mínima intervención humana. Es aplicable en cualquier área donde se realicen tareas repetitivas, sin embargo, los sectores más comunes están relacionados a la fabricación, robótica y sector automotriz, el sector IT no está fuera de, ya que muchas tareas son automatizadas con el fin de reducir tiempos y costos.

7.4.1. Automatización en IT

El objetivo principal es el mismo, reducir o hasta reemplazar por completo la intervención humana, utilizando sistemas de *software* que generen instrucciones para resolver procesos repetitivos en los sistemas de IT.

Automatizar es clave para optimizar procesos de IT, los entornos más modernos y dinámicos de IT hoy en día necesitan tener la capacidad de adaptarse de forma constante y acelerada, por ello es fundamental la automatización.

7.4.2. ¿Cómo implementar la automatización de procesos?

Cualquier tarea de IT es apta para aplicar un cierto nivel de automatización, se puede aplicar a cualquier elemento, desde automatizar una red completa hasta su infraestructura, implementaciones realizadas en la nube, e incluso en la aplicación de configuraciones de equipos mediante la utilización de scripts de programación.

8. PROPUESTA DE ÍNDICE DE CONTENIDOS

9. METODOLOGÍA

9.1. Diseño de la investigación

Dado que el objetivo de estudio es implementar una rutina automatizada de *health check* en equipos de la red IP de acceso por radio de un proveedor de servicios de internet en Guatemala, se recurrirá a un diseño no experimental, el cual será aplicado de manera transversal de tipo descriptivo.

De acuerdo con Hernández, Fernández y Baptista (2015) la investigación no experimental son estudios realizados sin manipulación alguna de variables de forma deliberada, los fenómenos son analizados mediante la observación en su ambiente natural. Estos autores también señalan que los diseños transversales tienen como propósito describir variables y analizar su incidencia e interrelación en un momento dado. Un diseño transversal descriptivo consiste en ubicar una o más variables a un grupo de personas u otros seres vivos, objetos, situaciones, contextos, fenómenos y proporcionar su descripción.

9.2. Enfoque de la investigación

El presente trabajo de investigación será diseñado bajo el planteamiento metodológico del enfoque cualitativo, puesto que basado en las características y necesidades del trabajo es el que mejor se adapta, ya que no se realizará ninguna clase de medición numérica con el objetivo de responder a las interrogantes de la investigación.

Según Hernández, Fernández y Baptista (2015) el enfoque cualitativo utiliza la recolección y análisis de datos, sin hacer mediciones numéricas, para descubrir nuevas interrogantes o afinar las preguntas de investigación existentes.

Se utilizará la técnica de observación para recabar toda la información necesaria para el desarrollo del tema de investigación.

9.3. Población de estudio

Según Gómez (2006) la población se puede definir como el conjunto total de los objetos de estudio, que tienen en común ciertas características, funcionales a la investigación.

Para el presente trabajo la población de estudio está conformada por todos los equipos de la red IP de acceso por radio del proveedor de servicios de internet ubicado en Guatemala, en el que se desarrollará la investigación.

9.4. Muestra

De acuerdo con Gómez (2006) para un estudio con enfoque cualitativo la muestra es una unidad o un grupo de análisis, sobre el cual se recolectarán datos, sin que estos sean estadísticamente representativos de la población de estudio.

En el presente trabajo se utilizará el método de muestreo no probabilístico, en el cual, según Hernández, Fernández y Baptista (2015) los elementos no se seleccionan al azar, sino con base en las características del estudio o a juicio del investigador. La muestra para este estudio no está definida por un número exacto de equipos, se determinará según los diferentes modelos de equipos que se tienen en la red IP-RAN.

9.5. Técnicas de investigación

El presente trabajo de investigación se apoyará en dos técnicas de investigación, por el enfoque cualitativo del estudio, la primera de ellas será la observación, según Heinemann (2016) es la captación y el registro controlado de datos con una finalidad específica para la investigación, mediante la percepción visual o acústica de un fenómeno o situación.

La segunda será la investigación bibliográfica, que no es más que la revisión del material bibliográfico existente que trata el tema de estudio.

9.6. Instrumentos de recolección de datos

En el presente trabajo se utilizará la observación directa como principal instrumento de recolección de datos, ya que se tendrá contacto y acceso a los equipos de la red IP-RAN del proveedor de servicios de internet para poder obtener la información necesaria.

La entrevista se utilizará como un instrumento secundario, se seleccionará un grupo de expertos en la minupalación de los equipos de la red IP-RAN y se les consultará los parámetros físicos y lógicos que creen necesarios extraer de cada equipo para colocarlos en el *health check*.

9.7. Operacionalización de variables

En base al objetivo general: implementar una rutina automatizada de *health check* en equipos de la red IP de acceso por radio (IP-RAN) de un proveedor de servicios de internet.

Tabla I. **Operacionalización de variables**

OBJETIVO ESPECÍFICO	VARIABLE	TIPO DE VARIABLE	INDICADOR	TÉCNICA
Identificar los parámetros más críticos de un elemento de red, de una red IP de acceso por radio, para conocer su estado físico y lógico.	Información del estado físico y lógico de los equipos.	Independiente de tipo cualitativa.	• Parámetros físicos. • Parámetros lógicos	• Investigación documental. • Revisión vía CLI en cada equipo.
Aplicar el protocolo SNMP para obtener la información necesaria de cada equipo en la red.	Mensajes de SNMP.	Dependiente del tipo cualitativo.	• Archivo de MIB. • OIDs seleccionadas para identificar cada parámetro físico y lógico	• Análisis de MIB con algún software. • Análisis de traps SNMP.
Desarrollar un software que permita interpretar la información recolectada de cada equipo en la red.	Información colectada en el administrador SNMP	Dependiente del tipo cualitativo.	• Código de programación.	• Análisis de código de información. • Recopilación de información en una base de datos.
Automatizar la generación de reportería con los datos del health check de cada elemento de red.	Reporte de healthcheck.	Dependiente del tipo cualitativo.	• Lista de parámetros extraídos de cada equipo. • Procedimiento para generar un reporte.	• Pruebas de interacción entre el usuario y el desarrollo de software.

Fuente: elaboración propia.

10. TÉCNICAS DE ANÁLISIS DE LA INFORMACIÓN

Debido a que la investigación tiene un enfoque cualitativo, la principal técnica de análisis de información será el análisis de texto, ninguno de los objetivos de la investigación requiere hacer análisis numérico, por lo tanto, no será necesaria ninguna técnica estadística o matemática.

Inicialmente se realizará análisis de textos para determinar cuáles son los parámetros físicos y lógicos que deben estar presentes en un *health check* estándar para un equipo de telecomunicaciones. También se analizará la red IP-RAN del proveedor de servicios, apoyada con documentación de los proveedores de *hardware*, con el fin de determinar qué parámetros físicos y lógicos es necesario considerar para cada equipo, dependiendo la función que desempeña dentro de la red (equipo de acceso o núcleo).

Posteriormente se analizarán los archivos de MIBs para cada equipo considerado en el estudio, con el fin de seleccionar las OIDs que contienen el valor de los parámetros físicos y lógicos definidos previamente. Para esta tarea se requerirá el apoyo de un *software* analizador de MIBs.

Durante la fase de desarrollo del software se necesitará analizar toda la información recolectada por el administrador SNMP y así asignarle un formato adecuado para la presentación de los datos en cada reporte de *health check* generado.

11. CRONOGRAMA

En esta sección se presenta de manera resumida y cronológicamente el desarrollo del proceso de solución para este trabajo de investigación, el cual constará de siete fases y abarcará un total de veintinueve semanas desde el inicio hasta la presentación del informe final.

La primera fase es investigativa y tomará un tiempo de tres semanas, se realizará una búsqueda de los parámetros físicos y lógicos adecuados que deben estar presentes en un *health check* de equipos de telecomunicaciones.

La segunda fase será para definir y enlistar los parámetros físicos y lógicos necesarios para conocer el estado de los equipos de la red IP-RAN del proveedor de servicios de internet, tendrá una duración de tres semanas.

En la tercera fase se realizará un análisis de los archivos de MIBs de los diferentes modelos de equipos que se tienen en la red IP-RAN, identificando el OID de cada uno de los parámetros definidos en la fase anterior. Esta fase tendrá una duración de tres semanas.

La cuarta fase será para realizar pruebas de comunicación utilizando el protocolo SNMP entre el administrador SNMP y los agentes SNMP en cada equipo, será necesario validar que la información enviada por cada equipo es la correcta. Esta fase tendrá una duración de cuatro semanas.

Luego de validar que se tiene una correcta comunicación entre el administrador y los agentes, inicia la quinta fase, en la cual se realizará el diseño

y desarrollo de *software*, el cuál será el encargado de enviar las instrucciones hacia el administrador para recopilar toda la información necesaria de cada uno de los equipos. Esta fase requiere del tiempo suficiente para realizar todas las pruebas necesarias y mitigar todo punto de falla en el *software*, por lo que se utilizarán ocho semanas para su ejecución.

En la sexta fase se realizará el diseño de los reportes que generará el software con los resultados del *health check* realizado a los equipos, se utilizarán dos semanas para ejecutar esta fase.

La séptima y última fase, será una fase de documentación, se realizará la presentación y discusión de resultados, redacción de las conclusiones y presentación de recomendaciones para futuros trabajos, esto tomará dos semanas de tiempo. Por último, se utilizarán las cuatro semanas restantes para realizar la redacción y corrección del informe final.

Tabla II. **Cronograma**

No.	Actividades / Semana	Enero		Febrero				Marzo				Abril				Mayo				Junio				Julio				Agosto		
		3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	Fase 1: Revisión de bibliografías																													
1	Investigar como se estructura un health check.																													
2	Investigar los parámetros físicos que se presentan en un health check.																													
3	Investigar los parámetros lógicos de que se presentan en un health check.																													
	Fase 2: Definir los parámetros físicos y lógicos de los equipos de la red IPRAN.																													
4	Clasificar los diferentes equipos que se tienen en la red IPRAN basado en su función (acceso, agregación y core).																													
5	Definir los parámetros físicos de cada elemento de red según su función dentro de la red.																													
6	Definir los parámetros lógicos de cada elemento de red según su función dentro de la red.																													
	Fase 3: Análisis de archivos de MIBs.																													
7	Buscar los archivos de MIBs para cada modelo de equipo de la red IPRAN.																													
8	Analizar los archivos de MIBs para identificar las OIDs de los parámetros definidos en la fase 2.																													
	Fase 4: Pruebas de comunicación con el protocolo SNMP																													
9	Validar el funcionamiento del administrador SNMP y los agentes SNMP.																													
10	Verificar que exista comunicación entre el administrador y cada agente.																													
11	Realizar pruebas de solicitud de información de las diferentes OIDs.																													
	Fase 5: Diseño y desarrollo del software																													
12	Definir el lenguaje de programación adecuado para desarrollar la aplicación.																													
13	Definir el diseño de la interfaz gráfica de la aplicación.																													
14	Identificar las variables a utilizar en el código de programación.																													
15	Desarrollo del código de programación.																													
16	Pruebas del código de programación.																													
17	Pruebas de validación de la información recolectada en cada equipo.																													
	Fase 6: Diseño de la reportería																													
18	Definir el diseño de los reportes generados por el desarrollo de software.																													
19	Pruebas de validación de información desplegada en los reportes.																													
	Fase 7: Documentación del informe final.																													
20	Presentación de resultados.																													
21	Discusión de resultados.																													
22	Redacción de las conclusiones.																													
23	Redacción de las recomendaciones.																													
24	Redacción del informe final.																													

Fuente: elaboración propia.

12. FACTIBILIDAD DEL ESTUDIO

Este trabajo de investigación contará con el apoyo de la empresa donde se desempeñará el estudio, los recursos físicos y materiales más importantes estarán a cargo de la empresa y el recurso humano junto con materiales secundarios estarán a cargo del investigador. Se tendrá la participación ad honorem de un asesor de investigación y el tiempo necesario del investigador para el desarrollo del trabajo. La empresa estará proporcionando el servidor que funcionará como administrador de SNMP y un espacio adecuado con servicios de energía eléctrica e internet para desarrollar la investigación. El investigador estará financiando los gastos de energía eléctrica y servicio de internet al trabajar fuera de la oficina de la empresa, así como el ordenador personal en el que se documentará toda la investigación.

Tabla III. **Costos del estudio**

	Materiales	**Presupuesto**
Recurso Humano	Investigador	Q. 0.00
	Asesor de investigación	Q. 0.00
Recurso Material	Oficina de trabajo	Q. 0.00
	Servidor como administrador SNMP	Q. 75,000.00
	Computadora personal	Q. 7,000.00
	Servicio de energía eléctrica e internet	Q. 3,500.00
	Gastos de papelería	Q. 1,000.00
	Gastos imprevistos	Q. 1,000.00
	TOTAL	**Q. 87,500.00**

Fuente: elaboración propia.

13. REFERENCIAS

1. AGENTPP (11 de enero, 2021). Using MIG designer. [Mensaje en un blog]. Recuperado de https://agentpp.com/help/mds/4.2.0/index.htm#t=MIBDesigner2%2FMIBDesigner2%2FUsing_MIB_Designer.htm.

2. Blumenthal, U. y Wijnen, B. (1998). *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)* (RFC 2264). Estados Unidos: Internet Engineering Task Force.

3. Blumenthal, U. y Wijnen, B. (2002). *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)* (RFC 3414). Estados Unidos: Internet Engineering Task Force.

4. Cuchala, S. (2016). *Gestión y Monitoreo de la red interna del gobierno provincial de Imbabura mediante el modelo de gestión ISO y software libre* (Tesis de licenciatura). Universidad Técnica del Norte. Ecuador, Ecuador.

5. DenHartog, M. (22 de febrero, 2021). How to view, edit, and read the management information base (MIB). [Mensaje en un blog]. Recuperado de https://www.dpstele.com/snmp/mib/how-to-view-edit-read.php.

6. Dordal, P. (2021). *An Introduction to Computer Networks*. Chicago: Estados Unidos: Autor. Recuperado de http://intronetworks.cs.luc.edu/current/ComputerNetworks.pdf.

7. Fernández, L. (30 de julio, 2021). Descubre para qué sirve el protocolo SNMP y cómo puede ser peligroso. [Mensaje en un blog]. Recuperado de https://www.redeszone.net/tutoriales/internet/protocolo-snmp-que-es/.

8. Gonzalez, V. (2014). *Diseño e implementación de un sistema de monitoreo basado en SNMP para la red Nacional Académica de Tecnología Avanzada* (Tesis de licenciatura). Universidad Santo Tomas, Colombia.

9. Hein, D. (12 de marzo, 2019). The Basics of Network Faul Management and Monitoring. [Mensaje en un blog]. Recuperado de https://solutionsreview.com/network-monitoring/the-basics-of-network-fault-management-and-monitoring/.

10. IBM (03 de marzo, 2021). IBM Netcool Operations Insigth. [Mensaje en un blog]. Recuperado de https://www.ibm.com/docs/en/cloud-private/3.2.0?topic=paks-netcool-operations-insight.

11. INCIBE (14 de septiembre, 2017). SNMP ¿Es tan simple como el nombre indica? [Mensaje en un blog]. Recuperado de https://www.incibe-cert.es/blog/snmp-tan-simple-el-nombre-indica.

12. Jukic, O., Hedi, I. y Speh, I. (mayo, 2017). Fault management and Management Information Base (MIB). *40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. Congreso llevado a cabo en Opatija, Croacia.

13. Junco, G. y Rabelo, S., (octubre, 2018). Los recursos de red y su monitoreo. *Revista Cubana de Informática Médica, 18*, 50-78.

14. Manage Engine (12 de enero, 2021). ¿Qué es un agente SNMP? [Mensaje en un blog]. Recuperado de https://www.manageengine.com/es/network-monitoring/what-is-snmp.html.

15. Manage Engine (02 de febrero, 2021). Network Faul Monitoring. [Mensaje en un blog]. Recuperado de https://www.manageengine.com/network-monitoring/fault-monitoring.html.

16. Marichal, X. (2021). *IP RAN*. Estados Unidos: Telecapp.

17. McCloghrie, K. (1991). *Management Information Base for Network Management of TCP/IP-based internets: MIB-II (RFC 1213)*. Estados Unidos: Internet Engineering Task Force.

18. Pandora FMS team (5 de noviembre,2019). Monitorización SNMP: claves para aprender a usar el Protocolo Simple de Administración de Red [Mensaje en un blog]. Recuperado de: https://pandorafms.com/blog/es/monitorizacion-snmp/.

19. Quispe, J. (2019). *Implementación de un prototipo de monitoreo de dispositivos de comunicación y usuarios finales utilizando el protocolo SNMP basada en software libre para una empresa e-Commerce* (Tesis de licenciatura). Universidad Nacional Mayor de San Marcos, Perú.

20. Red Hat (29 de enero, 2018). ¿Qué es la automatización? [Mensaje en un blog]. Recuperado de https://www.redhat.com/es/topics/automation/whats-it-automation.

21. Siggins, M. (20 de enero, 2020). What is Network Faul Management? [Mensaje en un blog]. Recuperado de https://www.dpstele.com/blog/what-is-network-fault-management.php.

22. VIAVI (4 de enero, 2021). Fronthaul. [Mensaje en un blog]. Recuperado de: https://www.viavisolutions.com/es-es/fronthaul.

23. XPLG (16 de febrero, 2021). What is fault management? A definition & introductory guide. [Mensaje en un blog]. Recuperado de: https://www.xplg.com/what-is-fault-management-2/.

24. Zeilenga, K. (2006). *COSINE LDAP/X.500 Schema (RFC 4524)*. Estados Unidos: Internet Engineering Task Force.