UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL

TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TEMA:

"SISTEMA ELECTRÓNICO PARA EL MONITOREO ACTIVO Y REINICIO REMOTO DEL NODO "OLT – CARANQUI" DE LA EMPRESA SAITEL, MATRIZ IBARRA"

AUTOR: IBUJÉS ESPINOSA ANDRÉS MARCELO

DIRECTOR: MSC. CARLOS ALBERTO VÁSQUEZ AYALA

IBARRA-ECUADOR

2022

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DEL CONTACTO			
CÉDULA DE IDENTIDAD:	1003561865		
APELLIDOS Y NOMBRES:	Andrés Marcelo Ibujés Espinosa		
DIRECCIÓN:	Ejido de Caranqui-Ibarra		
EMAIL:	ibujesmarcelo@gmail.com		
TELÉFONO FIJO:		**TELÉFONO MÓVIL:**	
DATOS DE LA OBRA			
TÍTULO:	"SISTEMA ELECTRÓNICO PARA EL MONITOREO ACTIVO Y REINICIO REMOTO DEL NODO "OLT – CARANQUI" DE LA EMPRESA SAITEL, MATRIZ IBARRA"		
AUTOR (ES):	Andrés Marcelo Ibujés Espinoza		
FECHA: DD/MM/AA	14/10/2022		
PROGRAMA:	■ **PREGRADO**	☐ **POSGRADO**	
TÍTULO POR EL QUE OPTA:	Ingeniero en Electrónica y Redes de Comunicación		
ASESOR / DIRECTOR	Msc. Carlos Alberto Vásquez Ayala		

2. CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros. Ibarra, 14 de octubre del 2022.

EL AUTOR:

Andrés Marcelo Ibujés Espinoza

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN

MAGÍSTER CARLOS ALBERTO VÁSQUEZ AYALA, DIRECTOR DEL PRESENTE TRABAJO DE TITULACIÓN CERTIFICA:

Que, el presente trabajo de titulación denominado: "SISTEMA ELECTRÓNICO PARA EL MONITOREO ACTIVO Y REINICIO REMOTO DEL NODO "OLT – CARANQUI" DE LA EMPRESA SAITEL, MATRIZ IBARRA", ha sido desarrollado por el señor Andrés Marcelo Ibujés Espinoza bajo mi supervisión.

Es todo en cuanto puedo certificar en honor a la verdad.

.....

Msc. Carlos Alberto Vásquez Ayala

DIRECTOR

Ibarra, 14 de octubre del 2022

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

AGRADECIMIENTO

Quiero agradecer a Dios por cada día de vida que me brinda; a mi madre por sacrificarse todos los día mientras tuvo vida, por el apoyo que me brindó para terminar mis estudios universitarios; a mis docentes que me enseñaron mucho más que la materia a tratar, sino que también a ser una mejor persona; a mi tutor quien me ayudó y guió cuando más lo necesité y supo encaminarme de manera paciente y dedicada para lograr este proyecto; finalmente a las personas especiales que siempre están apoyándome en tiempos difíciles, dándome ánimo.

Andrés Marcelo Ibujés Espinoza

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

DEDICATORIA

Este Proyecto se lo dedico a mi madre quien no se encuentra conmigo pero que gracias a ella pude culminar con este meta, ya que, fue quien siempre me brindó su apoyo y motivación para poder seguir y avanzar pese a las dificultades que se encuentren en la vida.

Andrés Marcelo Ibujés Espinosa

RESUMEN

La investigación detallada en el presente documento consiste en el desarrollo de un dispositivo electrónico denominado SCYNODE que permite el monitoreo activo del nodo "OLT - Caranqui", el cual, supervisa la temperatura interna del gabinete que contiene los equipos que conforman parte de la infraestructura de la red de fibra óptica de la empresa SAITEL en el sector Caranqui, así como también, la apertura del mismo por personal autorizado y no autorizado y el reinicio remoto de los dispositivos "OLT Inhibidos" que conforman al nodo.

El dispositivo en su etapa inicial realiza la adquisición de datos del nodo, para ello, se hace uso de sensores; el sensor DHT 11 se utiliza para monitorear la temperatura interna dentro del gabinete y el sensor electromagnético MC-38 que detecta el ingreso al nodo.

Como plataforma de lectura y unidad central de procesamiento de datos se usa el hardware y software libre Arduino, en este caso el Arduino Mega. Para el envío de datos se usa el módulo GSM/GPRS SIM 808L y para la visualización de resultados e interfaz de usuario se utiliza la infraestructura de la nube de Amazon Web Services para la implementación del sitio WEB, lo que permite a los administradores de red monitorear de forma remota las variables del nodo, también cuenta con un sistema actuador para el reinicio remoto de los elementos dentro del gabinete. Cuando el departamento de SOPORTE técnico de SAITEL detecte una falencia en las OLT, podrán ingresar a la interfaz gráfica de usuario y reiniciar el nodo para levantar el servicio dando continuidad en el mismo apenas se detecte el inconveniente.

Durante el desarrollo de la investigación se utiliza el modelo iterativo para el desarrollo del dispositivo realizando evaluaciones en cada etapa para la corrección respectiva, para finalmente realizar las pruebas finales implementado el sistema SCYNODE en el nodo "OLT-Caranqui" en la ciudad de Ibarra.

ABSTRACT

The detailed research in this document consists of the development of an electronic device denominated SCYNODE that allows the active monitoring of the "OLT - Caranqui" node, which supervises the internal temperature of the cabinet that contains the equipment that forms part of the infrastructure of the network optical fiber from SAITEL company in Caranqui, as well as its opening by authorized and unauthorized personnel and the remote restart of the “Inhibited OLT” devices that forms part of the node.

The device in its initial stage performs data acquisition of the node, for this, sensors are used; DHT 11 sensor is used to monitor the internal temperature inside the cabinet and the MC-38 electromagnetic sensor that detects entry to the node.

As a reading platform and central data processing unit, free Arduino hardware and software is used, in this case the Arduino Mega. For sending data, the GSM/GPRS SIM 808L module is used and for the visualization of results and user interface, Amazon Web Services cloud infrastructure is used for the implementation of the WEB site, which allows network administrators remotely monitor the variables of the node, it also has an actuator system for the remote restart of the elements inside the cabinet. When the technical SUPPORT department from SAITEL detects a failure in the OLT, they will be able to enter the graphical user interface and restart the node to restart the service, giving continuity to it as soon as the inconvenience is detected.

During the development of the investigation, iterative model is used for the development of the device, carrying out evaluations at each stage for the respective correction, to finally carry out the final tests, implementing the SCYNODE system in the "OLT-Caranqui" node in the city of Ibarra.

GLOSARIO DE ACRÓNIMOS

SAITEL: Soluciones Avanzadas Informáticas y Telecomunicaciones

WISP: Wireless Internet Service Provider / Proveedor de servicios de Internet inalámbrico

FTTH: Fiber To The Home / Fibra óptica hasta el hogar

EMELNORTE: Empresa Eléctrica Regional Norte

ODF: Distribuidores de fibra óptica

OLT: Terminales de línea óptica

UPS: Uninterruptable Power Supply / Sistema de alimentación ininterrumpida

BDD: Base de datos

Mbps: Megabites por segundo

TICs: Tecnologías de la Información y Comunicación

UIT: Unión Internacional de telecomunicaciones

DNS: Servidor de nombres de dominio

UART: Universal asynchronous receiver-transmitter / Receptor-transmisor asíncrono universal

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO I. ANTECEDENTES

1.1. Introducción

En el presente capítulo se muestra los datos preliminares para la realización del trabajo de titulación, mismo que contiene el tema, además se presenta la formulación del problema al cuál se desea brindar una solución, se planean los objetivos y con el alcance se delimita el proyecto, finalizando con la justificación en dónde se evidencia las razones por las cuales se va a realizar el proyecto.

1.2. Tema

"SISTEMA ELECTRÓNICO PARA EL MONITOREO ACTIVO Y REINICIO REMOTO DEL NODO "OLT – CARANQUI" DE LA EMPRESA SAITEL, MATRIZ IBARRA"

1.3. Problema

La empresa de Soluciones Avanzadas Informáticas y Telecomunicaciones (SAITEL), Proveedora de Servicios de Internet Inalámbrico (WISP) tanto en la Sierra Norte como en la Sierra Central; con la implementación de infraestructura de red óptica, mediante la tecnología de Fibra Óptica hasta el Hogar (FTTH), brinda el servicio de internet de alta velocidad para la cuidad de Ibarra, servicio de calidad y de gran demanda, red de datos diseñada para proveer la mejor experiencia a sus usuarios al navegar por Internet, priorizando la disponibilidad, continuidad y velocidad del servicio.

Los aspectos antes mencionados son de vital importancia en la actualidad, por cuanto, el continuo desarrollo y oferta de nuevas y variadas plataformas Web o Móvil de contenido (Multimedia, Educativo, Social, entre otros.) digital, y el aparecimiento de hardware moderno que para su correcto funcionamiento requiere de conexiones online, han hecho del Internet una necesidad fundamental en el cotidiano vivir (Universo, 2020), por lo que, la continuidad y disponibilidad del servicio son aspectos críticos para la empresa.

La Red Óptica Activa de comunicaciones de SAITEL actualmente está conformada por 9 Nodos Centrales ubicados estratégicamente en la ciudad, cada uno constituido por un Distribuidor de Fibra Óptica (ODF), dos Terminales de Línea Óptica (OLT), un Rúter, una batería de 12 V y una Fuente de Alimentación Ininterrumpida (UPS) que actúa como sistema de energía de respaldo, ubicados en el interior de gabinetes metálicos herméticos de montaje

superficial, instalados en la postería de EMELNORTE (Empresa Eléctrica Regional Norte) y que cumplen la función de 'Sala de Equipos' en un esquema de red de Fibra Óptica.

Actualmente se han venido suscitando eventos recurrentes que inciden en el desempeño y continuo funcionamiento de determinados dispositivos de los Nodos Centrales, que tienen relación directa o indirecta, debido a la elevada temperatura a la que están sometidos los elementos como los Transceptores Ópticos, como causa de estaciones veraniegas más intensas y prolongadas en la ciudad, temperatura que se incrementa drásticamente debido al espacio reducido de las Salas de Equipos (gabinetes metálicos herméticos), que no disponen de un sistema de ventilación o de rejillas para la circulación del aire, causando que la señal óptica sea percibida como incorrecta, lo que, degenera en el funcionamiento inestable de los dispositivos (Paucar., 2020).

Los inconvenientes antes mencionados, no solamente están relacionados con la temperatura, sino que, se han identificado algunos eventos, uno de ellos hacen referencia a la seguridad física en los Nodos, debido a que, se han venido suscitando de manera recurrente actos de robo en el Nodo "OLT – Caranqui", en dónde fueron violentadas las seguridades de la Sala de Equipos, y posterior la sustracción de todos los dispositivos, componentes y elementos que la constituyen, perjudicando de manera económica a la empresa, y con el inconveniente más crítico que es la de interrumpir por intervalos de tiempo muy extensos el servicio a un número considerable de familias que acceden a Internet a través del nodo situado en el sector Caranqui.

De igual manera, se han detectado e identificado problemas como consecuencia directa de la falta de interoperabilidad, ya sea en la capa física (potencia óptica, sensibilidad, entre otros), como la de enlace de datos (formatos de trama) (Kramer, 2017), entre las OLT ubicados en los Nodos Centrales y las ONT/ONU ubicadas en el domicilio de los abonados.

Debido a los acontecimientos descritos anteriormente, los ingenieros y técnicos de la empresa han establecido una solución provisional a los problemas que se han venido presentando en los Nodos, que han sido denominados por los técnicos de la institución "Inhibición de Equipos" , la cual consiste en realizar un reinicio de los dispositivos OLT, in situ, situación que conlleva a destinar recursos como personal técnico, vehículos y el tiempo, factor determinante , ya que, considerando el lapso de tiempo desde la detección del problema en determinado Nodo, el desplazamiento del personal y la puesta en ejecución del reinicio de los equipos OLT hasta el restablecimiento completo del servicio, hacen que todo el proceso sea

muy crítico para la empresa, considerando que, la percepción que los usuarios tienen de la calidad del servicio depende netamente de la continuidad, disponibilidad y velocidad del servicio que la empresa puede proveer.

Este proyecto propone el diseño de un sistema electrónico de monitoreo activo del nodo de fibra óptica "OLT – Caranqui" a través de una interfaz Web, que permita el seguimiento de la temperatura en la Sala de Equipos (Gabinete de equipamiento), la alerta automática de acceso al Gabinete de Equipamiento, encaminando a preservar la seguridad de los mismos y prevenir robos futuros en la infraestructura de telecomunicaciones de la empresa, finalmente el control de reinicio remoto de los dispositivos OLT, evitando el desplazamiento de técnicos hasta el nodo en conflicto para la realización de un reinicio de forma manual, lo que permitirá mejorar el tiempo de restitución del servicio y así brindar continuidad, disponibilidad y calidad en el acceso de internet a los abonados.

1.4.Objetivos

1.4.1. Objetivo general

Implementar un sistema electrónico para el monitoreo activo y reinicio remoto de equipos OLT del nodo "OLT - Caranqui" de la empresa SAITEL matriz Ibarra, que permita verificar la temperatura, accesos de intrusión y brindar continuidad en el servicio de internet a los usuarios en caso de presentarse algún evento.

1.4.2. Objetivos específicos

- Realizar una revisión bibliografía que permita definir y describir el marco referencial en torno a la temática, aportando la base científico-teórica necesaria para realizar un adecuado diseño del sistema.
- Realizar el levantamiento de información de las características, funciones y eventos más relevantes de los equipos, dispositivos y elementos que conforman la Infraestructura de Red de Fibra Óptica de SAITEL, que permitan describir a través de datos estadísticos, comportamientos anómalos o desperfectos en el Nodo en cuestión.
- Determinar los requerimientos de hardware y software, para diseñar e implementar tanto el dispositivo que permita el monitoreo activo, como la interfaz gráfica web con el fin de un correcto funcionamiento del sistema.

- Realizar pruebas de verificación del sistema, previa instalación del dispositivo "hardware" en el Nodo "OLT - Caranqui", para determinar el funcionamiento con el fin de realizar los respectivos ajustes para obtener el desempeño requerido.

1.5. Alcance

El presente proyecto se enfoca en el desarrollo de un sistema electrónico para el monitoreo activo y seguridad, el cual permitirá supervisar la temperatura, alertar accesos, y reiniciar equipos OLT en el Nodo "OLT – Caranqui", desde una interfaz web, lo que permitirá minimizar el tiempo de restitución del servicio de internet a los usuarios que se conectan desde el Nodo.

En base a la criticidad de la temática a investigar, se realizará un análisis bibliográfico que permita definir y desarrollar el marco teórico referencial, en base a información pertinente y sustentable.

Se recopilará información necesaria de la infraestructura de la red de Fibra Óptica de SAITEL en base a aspectos como el esquema de Red, características de los dispositivos y equipos, balance de eventos relacionados con los problemas recurrentes en la infraestructura que conforman los Nodos Centrales, para de esta manera describir y definir al nodo "OLT - Caranqui" como nodo de pruebas para la instalación del dispositivo central que constituye parte del sistema.

Debido a la necesidad imperante de un sistema funcional que provea de una solución de bajo costo, rápido despliegue y confiable, se observa la necesidad de verificar y seleccionar una metodología que se acople de la mejor manera al proyecto, que sirva como herramienta para el fácil desarrollo e implementación del sistema.

Se realizará un análisis que permita comparar y seleccionar el hardware, software, necesarios y adecuados, en base a requerimientos de funcionamiento previstos y de esta manera seleccionar elementos, dispositivos, plataformas de desarrollo de "Código Abierto", desde una perspectiva de eficiencia y optimización de recursos, las cuales conformarán el sistema electrónico en cuestión.

Dichos Aspectos que determinarán el diseño del sistema, el cual estará constituido por un Microcontrolador de Placa Reducida (Sistema Embebido) de plataforma de Código Abierto que hará de dispositivo central de tratamiento, procesamiento de señales y de enlace, mediante los siguientes elementos, un sensor de temperatura que estará ubicado en el interior del

Gabinete Metálico (Sala de Equipos), un sensor magnético de apertura que estará ubicado en la puerta de acceso al interior de la estructura metálica.

Además contará con un Módulo GSM/GPRS que aprovechando las infraestructuras de comunicaciones de proveedores de servicios móviles disponibles en el Ecuador, a través del protocolo TCP/IP, brindará la posibilidad de establecer una comunicación bidireccional con los servicios Web y de Base de Datos asistidos en "La Nube", servicios que serán provistos y alquilados a un proveedor de "Cloud Computing", que por medio de una interfaz gráfica web de telemetría y seguridad, permitirá monitorear la temperatura, recibir alertas cuando se abra la puerta del gabinete, y activar un circuito actuador que estará instalado en el interior del gabinete, el cual cortará el flujo continuo de alimentación a las OLT, y de esa manera poder reiniciarlos de manera remota.

El sistema estará conformado de dos partes, la primera que constituye la interfaz gráfica Web de usuario y todo el software necesario para su diseño e implementación, y la segunda parte constituida por todo el hardware para el despliegue de un dispositivo que estará dotado por toda la parte de electrónica necesaria en un solo dispositivo que contendrá los módulos, sensores, y actuadores, que por medio de un "botón" en la interfaz de telemetría y seguridad, permitirá realizar la función de "Actuador de Reinicio Remoto de las OLT", logrando interrumpir el flujo continuo de alimentación hacia las OLT disponibles en la Sala de equipos del Nodo "OLT - Caranqui".

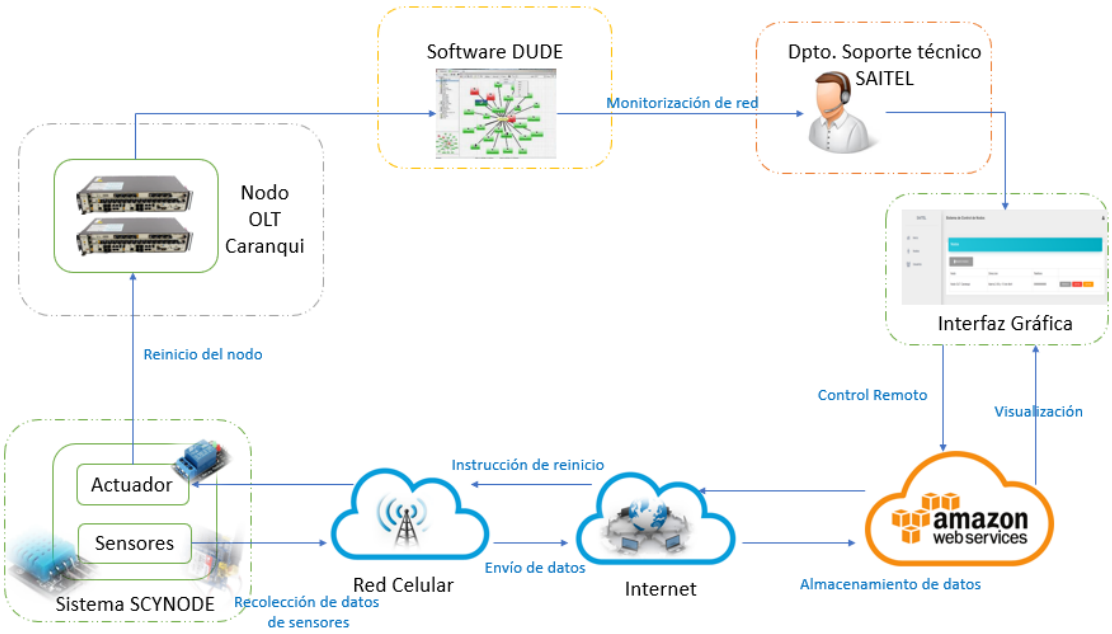
El dispositivo será ensamblado y dispuesto, considerando las características físicas y la morfología del gabinete metálico, teniendo en cuenta el espacio reducido, distribución de los dispositivos y cables, las fuentes de alimentación disponibles y las altas temperaturas dentro del gabinete, de tal manera que facilite su instalación y adaptación en el habitáculo.

Las pruebas de funcionamiento se realizarán cuando el sistema completo esté en producción, y el dispositivo esté instalado en el Nodo "OLT - Caranqui", que por medio de la interfaz web, permitirá verificar la presentación de la información (temperatura), la rapidez de alertas de apertura (puerta del gabinete) y el tiempo que el circuito actuador de reinicio remoto es activado desde la interfaz web de usuario. En la etapa de pruebas de funcionamiento se valorará la información captada y almacenada en la base de datos del sistema, lo cual servirá para un posterior análisis que cumplan con las metas planteadas para llevar una estadística de seguridad, temperatura en el interior del gabinete y un conteo de reinicios de las OLT, de esta manera verificar el funcionamiento integral de la solución para la problemática planteada. En

la Figura 1 se observa la arquitectura del sistema en donde se muestra una visión general del funcionamiento del sistema.

Figura 1

Arquitectura del sistema



Fuente: *Autoría*

1.6. Justificación-Detalle del impacto

El presente proyecto se realiza con la finalidad de proveer a la empresa SAITEL de un sistema electrónico de monitoreo activo y reinicio remoto de equipos OLT para el nodo “OLT - Caranqui”, que por medio de una interfaz web, alerte el acceso, monitoreé la temperatura interna y permita el reinicio remoto de las OLT.

La necesidad de desarrollar el sistema, es con el objetivo de aminorar la cargar laboral, agilitar el tiempo de respuesta en la restitución del servicio para las aproximadamente trescientas familias que acceden al servicio de internet desde el nodo “OLT – Caranqui”, reservar los recursos materiales, humanos y económicos, en lo que conlleva desplazarse y efectuar el reinicio de los dispositivos del Nodo manualmente, además, uno de los objetivos que persigue la empresa es la de proveer de disponibilidad y continuidad en el servicio, de costo asequible, permitiendo de esta manera la reducción de la brecha digital social y que el uso y acceso a las Tecnologías de la Información y las Comunicaciones (TIC) sea universal Fuente especificada no válida..

Hasta el momento SAITEL no cuenta con un sistema que permita realizar el monitoreo activo de ciertos aspectos como la temperatura, alertas de acceso y el reinicio de equipos OLT remotamente. Si el Nodo "OLT- Caranqui" empieza a presentar complicaciones, causa dificultades o en la mayoría de los casos la interrupción completa en la conexión a un número muy considerable de familias que acceden al servicio de internet a través del nodo en cuestión, hasta que el personal técnico sea designado y despachado, se desplacen al Nodo, y realice el reinicio manual de los dispositivos OLT, se ha estimado en promedio que el proceso lleva treinta y siete minutos, no obstante, en el caso de que todos los técnicos se encuentren atendiendo órdenes de trabajo, se dará prioridad a las mismas, situación que incrementará el tiempo de solución al evento. Con la implementación de un control remoto a través de interfaz Web del Nodo "OLT-Caranqui", se mejorará el rendimiento de trabajo de la empresa, minimizando la movilización de contingente humano, acelerando drásticamente la restitución del servicio, lo que garantiza: disponibilidad y continuidad del mismo, en beneficio de sus abonados y, por ende, a la empresa.

Con la implementación del proyecto se podrá aplicar, adquirir conocimientos y destrezas en el campo de la electrónica aplicada, implementación de Servicios de Computación en la Nube, software para desarrollo y las redes de datos para aplicaciones de servicios, brindando la posibilidad de manejar e integrar diferentes plataformas y arquitecturas OpenSource, además de cumplir con uno de los requisitos necesarios como parte del proceso de titulación profesional.

CAPÍTULO 2. FUNDAMENTO TEÓRICO

En este capítulo se sintetiza la revisión bibliográfica de conceptos relacionados con la seguridad en la infraestructura de telecomunicaciones, desde un análisis general hasta las claves para garantizar la integridad de la misma, además se establecen mecanismos de seguridad en la actualidad, metodologías para el diseño de proyectos entre otros.

2.1. Seguridad de la infraestructura de telecomunicaciones

Años atrás la seguridad de la infraestructura de telecomunicaciones y de las TICs se aplicaba a sectores bancarios o aplicaciones de investigación espacial y militares. En la actualidad con el continuo crecimiento de las comunicaciones de datos, especialmente debido al internet, la seguridad se ha transformado en una prioridad para todos (ITU, 2015).

Es de vital importancia para la industria de las telecomunicaciones contar con mecanismos de seguridad para las infraestructuras de red, con la finalidad de satisfacer los requerimientos del entorno actual.

La importancia del sector de las telecomunicaciones para la seguridad, economía y bienestar social origina la implementación de sistemas robustos de seguridad en su infraestructura, ya que, ésta puede experimentar ataques, incidentes físicos que ponen en peligro la información, instalaciones, dispositivos, la integridad del personal técnico y de terceros, así como también la disponibilidad y continuidad de un servicio en específico.

2.2. Arquitectura de seguridad para sistemas de telecomunicaciones

La arquitectura de seguridad de redes de telecomunicaciones se fundó para tratar retos de seguridad global de los proveedores de servicios, empresas y usuarios, y es aplicable a los nuevos servicios de las redes de nueva generación como son: datos, voz, servicios ópticos, inalámbricos, por cable y redes convergentes (Criollo Ortiz & Aguirre Carvajar, 2017). Esta arquitectura aborda cuestiones de seguridad para la administración, control, uso de la infraestructura, los servicios y las aplicaciones de la red.

El diseño divide lógicamente un conjunto complejo de redes de extremo a extremo relacionadas con la seguridad, características en componentes arquitectónicos separados, esta separación permite un enfoque sistemático para seguridad de un extremo a otro que se puede utilizar para planificar nuevas soluciones de seguridad, así como para evaluar la seguridad de las redes existentes.

2.2.1. Dimensiones de seguridad

Una dimensión de seguridad es un conjunto de medidas de seguridad diseñadas para abordar un aspecto particular de seguridad de la red (Horcajo, 2020).

Se establece ocho indicadores que preservan la integridad de la infraestructura contra las principales amenazas de seguridad que son: control de acceso, autenticación, no repudio, confidencialidad de los datos, seguridad de las comunicaciones, integridad de los datos, disponibilidad, privacidad.

Los indicadores de seguridad correctamente diseñados e implementados respaldan la política de seguridad de una empresa de telecomunicaciones.

- **Dimensión de seguridad de control de acceso**

Protege contra el uso no autorizado de los recursos de la infraestructura de red. El control de acceso garantiza que solo el personal o los dispositivos autorizados tengan acceso a la red, elementos, información almacenada, flujos de información, servicios y aplicaciones.

- **Dimensión de seguridad de autenticación**

Sirve para confirmar las identidades de las entidades que solicitan el acceso. La autenticación asegura la validez de las identidades reclamadas de las entidades que participan en comunicación, por ejemplo: persona, dispositivo, servicio o aplicación y proporciona seguridad de que una entidad está intentando una reproducción no autorizada de una comunicación anterior.

- **Dimensión de seguridad de no repudio**

Proporciona medios para evitar que un individuo o entidad niegue la ejecución de acciones específicas en relación con los datos, poniendo a disposición pruebas de la acción (UNIR, 2021) asegura la disponibilidad de evidencia que puede ser presentada a un tercero y utilizada para probar que se ha producido algún tipo de evento, como tipo de evidencias se tiene: prueba de origen de datos, prueba de propiedad, prueba de uso de recursos, entre otros.

- **Dimensión de seguridad de confidencialidad de datos**

La dimensión de seguridad de la confidencialidad de los datos protege los datos de la divulgación no autorizada.

El cifrado, las listas de control de acceso y los permisos de archivos son estrategias usadas con frecuencia para proporcionar la confidencialidad de los datos.

- **Dimensión de seguridad de las comunicaciones**

La dimensión de seguridad de las comunicaciones garantiza el flujo de información entre los flujos terminales, la información no se desvía ni intercepta en el tránsito hacia los extremos finales.

- **Dimensión de seguridad de la disponibilidad**

La dimensión de seguridad de disponibilidad asegura que el acceso con autorización a la red no sea negado, debido a eventos que perturben la red. Los medios de recuperación ante desastres están incluidos en esta categoría.

- **Dimensión de confidencialidad de la privacidad**

Presta la protección de la información que pueda proceder, a partir del análisis de las acciones de la red (Mantelero, 2017).

Ejemplos de esta información incluyen los nombres de los servidores de dominio de los dispositivos en la red del proveedor de servicios, direcciones IP, geo ubicación del usuario, visitas en sitios web, entre otros.

2.2.2. Capas de seguridad

Para proveer de una solución de seguridad de un extremo a otro, las dimensiones descritas en el apartado 2.2.1, debe aplicarse a una jerarquía de equipos de red y agrupaciones de instalaciones, denominadas capas de seguridad.

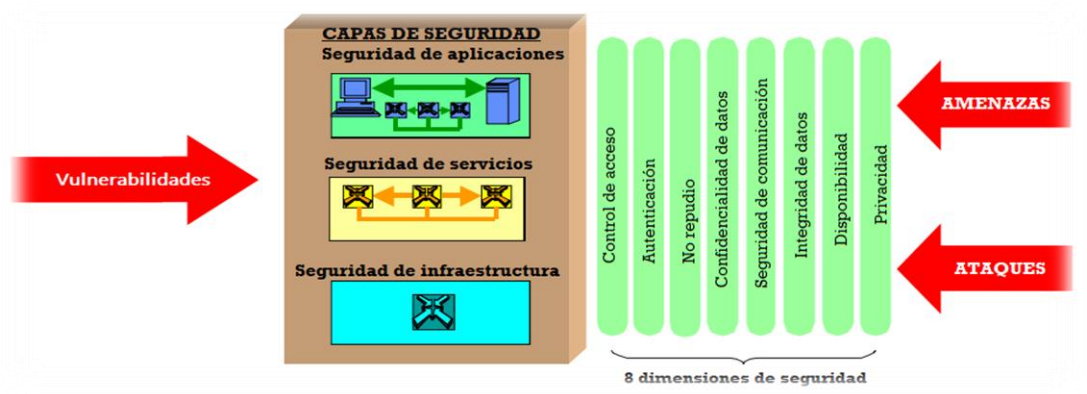
Se definen las siguientes capas de seguridad: capa de seguridad de la infraestructura, capa de seguridad de servicios y capa de seguridad de aplicaciones.

Las capas de seguridad identifican dónde se debe abordar la seguridad en los productos y soluciones proporcionando una perspectiva secuencial de la seguridad de la red, por ejemplo, las primeras vulnerabilidades de seguridad se abordan en la capa de infraestructura, luego para la capa de servicios y finalmente la seguridad en la capa de aplicación.

La Figura 2 muestra cómo las dimensiones de seguridad se aplican a las distintas capas para disminuir las vulnerabilidades que existen en cada capa.

Figura 2

Aplicación de las dimensiones de seguridad a las capas de seguridad



Fuente: *(Ahmad, Namal, Ylianttila, & Gurtov, 2016)*

- **Capa de seguridad de infraestructura**

La capa de seguridad de infraestructura consta de las instalaciones de transmisión de la red, así como de los elementos y dispositivos de red. La capa de infraestructura representa la base de construcción fundamentales de las redes, sus servicios y aplicaciones.

Ejemplos de elementos pertenecientes a la capa de infraestructura son los: enrutadores, conmutadores, servidores virtuales, así como los enlaces de comunicación entre enrutadores, nodos, OLTs, conmutadores, entre otros (Ahmad, Namal, Ylianttila, & Gurtov, 2016).

La seguridad de la capa de infraestructura tiene que ver con asegurar la operación, administración, mantenimiento y aprovisionamiento de la red y sus elementos, enlaces de comunicación y plataformas de servidores que componen la red. Se considera la configuración de dispositivos y los enlaces de red dentro del plano de gestión de seguridad.

Un ejemplo de gestión de infraestructura que debe protegerse es la configuración de un enrutador y de equipos ubicados en los nodos. En la Tabla 1 se describe los objetivos aplicando las dimensiones de seguridad a la capa de infraestructura.

Tabla 1

Objetivos de seguridad en la capa de infraestructura

Dimensión de seguridad	Objetivos de seguridad
Control de acceso	Asegurar que solo el personal o dispositivos autorizados están acreditados a realizar actividades administrativas o de gestión en los dispositivos de red o enlace de comunicaciones. Esto se aplica tanto a la gestión directa del

	dispositivo a través de un puerto y la gestión remota.
Autenticación	Verificar la identidad de la persona o dispositivo que realiza la gestión administrativa o actividad en el dispositivo de red o enlace de comunicaciones. Las técnicas de autenticación pueden ser requeridas como parte del control de acceso.
No-repudio	Proporcionar un registro que identifique a la persona o dispositivo que realizó cada administración o actividad de gestión en el dispositivo de red o enlace de comunicaciones y la acción que se ha realizado. Este registro puede utilizar como prueba del autor del documento administrativo o actividad de gestión.
Confidencialidad de datos	Proteger el dispositivo de red o la información de configuración del enlace de comunicaciones acceso o visualización no autorizados. Esto se aplica a la información de configuración residente en el dispositivo de red o enlace de comunicaciones, así como la información de configuración de respaldo almacenada. Proteger la información de autenticación administrativa, por ejemplo: identificaciones de administrador y contraseñas, del acceso o visualización no autorizados. Las técnicas utilizadas para abordar el control de acceso pueden contribuir a brindar confidencialidad a los datos.
Seguridad de comunicación	En el caso de la gestión remota de un dispositivo de red o enlace de comunicaciones, hay que asegurarse de que la información de gestión solo fluye entre las estaciones de gestión remota, el dispositivo y el personal autorizados para su gestión.
Integridad de datos	Proteger la información de configuración de los dispositivos de red y enlaces de comunicaciones contra: modificación, eliminación, creación y replicación no autorizadas. Esta protección se aplica a la información de configuración residente en el dispositivo de red o enlace de comunicaciones, así como información de configuración que está en tránsito o almacenada en sistemas fuera de línea. El mismo tipo de consideración se aplica a la información de autenticación administrativa.
Disponibilidad	Asegurar que la capacidad de administrar el dispositivo de red o el enlace de comunicaciones por personal o dispositivos no se pueden negar. Esto incluye protección contra ataques activos, denegación de servicio, así como protección contra ataques pasivos como la modificación o eliminación de la información de autenticación administrativa (por ejemplo, administrador de identificaciones y contraseñas).
Privacidad	Asegurar que la información pueda usarse para identificar el dispositivo de red o las comunicaciones. El enlace no está disponible para personal o dispositivos no autorizados. Ejemplos de este tipo de información incluye: la dirección IP de un dispositivo de red o el nombre de dominio. Se debe tener la capacidad de identificar si el dispositivo de red proporciona información de orientación a los

atacantes.

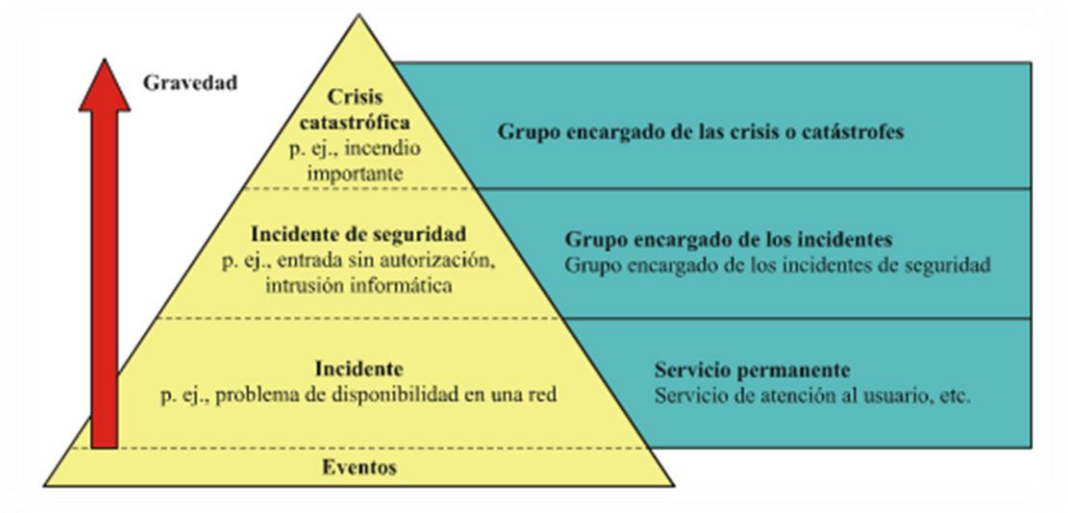
Fuente: (Saleh, 2019)

2.3. Clasificación y procesamiento de incidentes de seguridad en las empresas y compañías de telecomunicaciones

La expresión incidente de seguridad puede expresarse como "una violación de seguridad amenaza y vulneración de puntos débiles que repercuten sobre las medidas de seguridad de los equipos activos de una empresa u organización". En la Figura 3 se observa en una pirámide los eventos que tienen incidencia en la barrera de seguridad.

Figura 3

Pirámide de eventos que inciden en la barrera de seguridad de una empresa y/o compañía



Fuente: *(Romero Castro, Figueroa Morán, Vera Navarrete, & Álava Cruzatty, 2018)*

- Evento: Es un acontecimiento que se puede percibir, pero no es posible predecirlo o controlarlo por completo.
- Incidente: Es un evento en el cual los efectos no son de gravedad.
- Incidente de seguridad: Es cualquier evento aleatorio o premeditado dirigido u ocasionado en la barrera de seguridad.
- Incidente de seguridad en las TICs: Es un evento aleatorio o premeditado cuyo potencial afecta la seguridad de las TICs, por ejemplo: ingreso en servidores sin autorización, virus informáticos, robos de los equipos físicos, hackeo de claves, etc.
- Crisis: Estado originado por un evento, que puede tener resultados negativos en la operabilidad de las redes de comunicación. En general cada empresa proveedora de

servicios de TICs tiene un equipo que gestiona las crisis y dan soluciones a las situaciones presentadas (ITU, 2015).

2.4. Estrategias de seguridad para las infraestructuras de telecomunicaciones

Con la finalidad de brindar una protección a las infraestructuras críticas de telecomunicaciones es de suma importancia la implementación de algunas estrategias que permitirán la prevención de cualquier incidente. Las empresas de redes públicas o privadas de telecomunicaciones poseen internamente por norma y obligatoriedad un plan de acción para la prevención de interrupciones en los servicios y la adecuación servicios de emergencia en casos imprevistos o de fuerza mayor (Vaseashta, Susmann, & Braman, 2017), es por lo mencionado que las medidas de seguridad son esenciales para garantizar la continuidad de las operaciones.

A continuación, se detallan algunas de las principales medidas que es posible adoptar para evadir y aminorar los efectos de las amenazas en la infraestructura de telecomunicaciones.

2.4.1. Socializar con el personal de la empresa

Se debe integrar y conservar una cultura de seguridad en todo el personal que conforma la empresa, sin excluir a la planta directiva y administrativa.

2.4.2. Análisis de riesgos a través de una evaluación periódica

Una estrategia de seguridad para conservar la integridad de la infraestructura crítica de telecomunicaciones es la ejecución de evaluaciones periódicas de riesgos en las instalaciones. Con esto se podría ayudar al cálculo del porcentaje de probabilidad de que una amenaza se haga realidad dentro de las instalaciones, nodos de comunicaciones, gabinetes de equipos, sistemas informáticos, servidores, etc.

2.4.3. Contar con un espacio adecuado

Como una de las principales estrategias de seguridad se tiene el aprovisionamiento de un espacio idóneo en donde se encuentra concentrada la infraestructura tecnológica. Este espacio deberá estar adecuadamente separado y establecido es aquí en donde se ubicarán los dispositivos y elementos de telecomunicaciones como: equipamiento eléctrico, telefonía, routers, cableado, servidores, Entre otros. (Silva Ponce de León, 2018). En este espacio deberá estar diseñado de tal manera que permita la integración de otros sistemas y dispositivos de importancia como lo son: circuitos cerrados, alarmas, audio, entre otros.

2.4.4. Instalar gabinetes industriales especializados

Los gabinetes industriales son un elemento indispensable para asegurar la seguridad de la infraestructura crítica de telecomunicaciones, estos pueden ser de características estándar o especializadas, el objetivo es que sean compatibles con el equipamiento existente en las instalaciones.

2.4.5. Contar con una solución de climatización

Es necesario tener presente que cada infraestructura de telecomunicaciones puede manejar diferencias en cuanto a los tamaños y disposición de los gabinetes de equipos. Por tal motivo, se precisan soluciones de climatización que se adapten acorde a los requisitos, con ello se estabilizará la carga de temperatura y se garantizará el desempeño adecuado de los mismos.

2.4.6. Estricto control de acceso de personas y materiales

Al momento de implementar medidas de seguridad en las infraestructuras críticas de telecomunicaciones se debe contar siempre con un estricto control, tanto del personal que accede a las instalaciones, como de los materiales que ingresan o salen para mantenimiento. Personas ajenas al equipo técnico o maleantes pueden ocasionar daños en los lugares donde se encuentran ubicados los dispositivos como en: oficinas, nodos, antenas, gabinetes de equipos, etc. (Angulano, 2019). Además, se puede integrar: sistemas de cerraduras electrónicas en las áreas críticas antes mencionadas, equipos de detección de acceso y alarmas conectados a una central o servidor externo y remoto esto como centro de monitoreo propio de la empresa, softwares analíticos que sirvan de apoyo en la detección temprana de irregularidades en los protocolos de seguridad establecidos por la empresa, contar con un centro de monitoreo propio que valide de forma continua la ejecución de protocolos de seguridad de todas las personas que ingresan a las instalaciones y además genere alarmas en casos emergentes.

2.5. Monitoreo de red

Es el método mediante el cual los administradores de red obtienen información en tiempo real sobre el estado de la red, es decir, si los dispositivos están funcionando de manera óptima con herramientas como software que ayudan a identificar falencias con la finalidad de resolver un evento mejorando la eficiencia de la red (CISCO, 2022).

Los sistemas de monitoreo de red están conformados por software y hardware que permiten realizar un seguimiento a la misma y su funcionamiento como el tráfico, ancho de banda, tiempo de actividad además de mostrar actualizaciones de estado con la finalidad de

detectar oportunamente fallas en los dispositivos conectados a la red; cuando se presenta una actividad inusual los administradores pueden identificar los problemas más rápido.

2.5.1. Monitoreo activo de redes

Para este tipo de monitorización se introduce paquetes de pruebas en la red, o se envía paquetes a los elementos de la red y se evalúa tiempos de respuesta. El monitoreo activo tiene puede agregar tráfico en la red y es usado para evaluar el rendimiento de esta. Este monitoreo se basa en los protocolos ICMP, RTT, TCP, UDP, permitiéndose: diagnosticar problemas de red, detectar retardo, pérdida de paquetes, disponibilidad de dispositivos, tasa de transferencia, detectar fallas a nivel de capa aplicación y pérdida de paquetes.

2.5.2. Monitoreo pasivo de redes

Mediante la obtención de datos recolectados, se analiza el tráfico que circula por la red mediante software que registra la información que envían los dispositivos de red que cuentan con software de análisis de tráfico con soporte para SNMP,1 RMON y software para monitorización de ancho banda como Netflow. El monitoreo pasivo no agrega tráfico a la red.

2.6. Software para el monitoreo de redes

El monitoreo de red es muy importante para garantizar un correcto funcionamiento de la infraestructura y sistemas y también ayuda a solucionar fallas en la red además ayuda a optimizar el servicio ya que presenta información detallada de los recursos disponibles; otro aspecto importante es la seguridad determinando las áreas específicas que necesitan mantenimiento y tomar decisiones de manera oportuna en caso de presentarse eventualidades, para ello existe software encargado de detectar falencias de manera efectiva, algunos programas de software son: PRTG, NAGIOS, Zennos, The DUDE, entre otros.

2.6.1. The DUDE

Es una aplicación de MikroTik gratuita, que puede mejorar la forma de administración del entorno de la red. Permite el escaneo automático de todos los dispositivos dentro de subredes específicas, con esta herramienta se puede dibujar y diseñar un mapa de la topología, monitorear los servicios y los dispositivos generando alertas en caso de que algún servicio tenga problemas. (Mikrotik, 2022).

The Dude cuenta con las siguientes características:

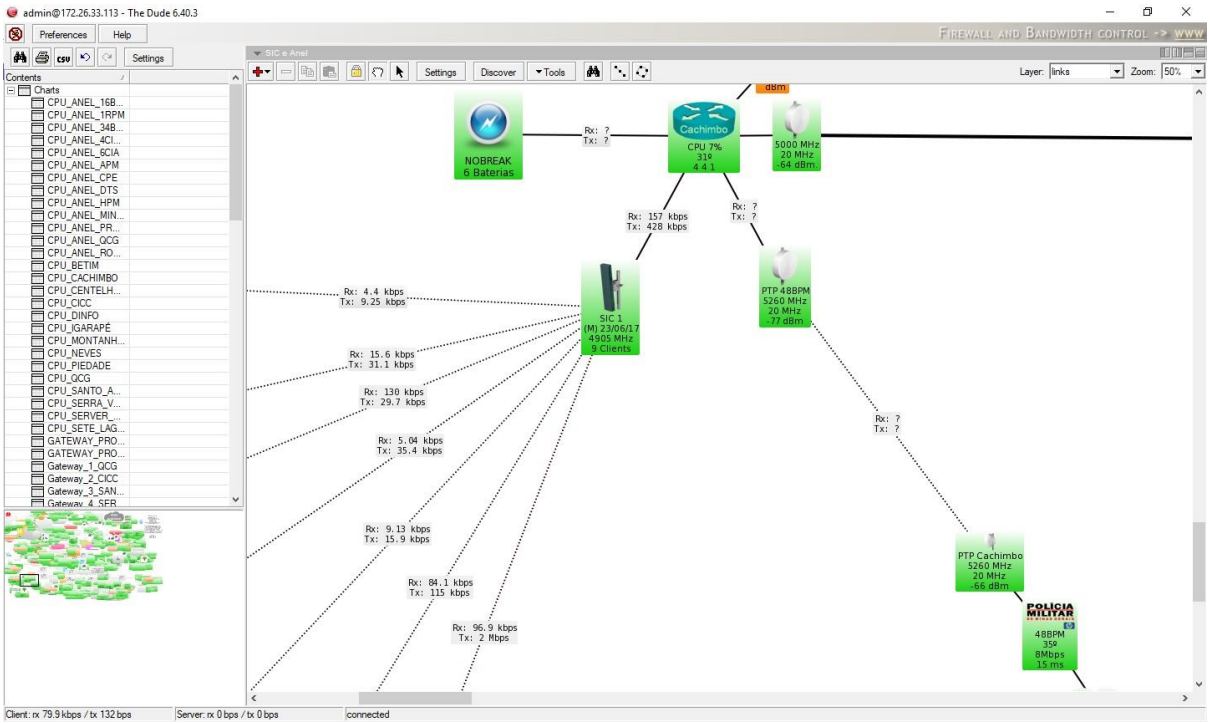
- Descubrimiento automático de redes (Cualquier marca o dispositivo).
- Monitoreo de enlaces y notificaciones.
- Permite dibujar mapas y agregar dispositivos personalizados.

- Admite monitoreo de SNMP, ICMP, DNS y TCP.
- Acceso directo a herramientas de control remoto para la gestión de dispositivos
- Admite servidor Dude remoto y cliente local
- Se ejecuta en el entorno Linux Wine, MacOS Darwine y Windows

En la Figura 4 se muestra la interfaz gráfica de The DUDE, donde se aprecia un mapa de red, cuando el dispositivo está en estado down, se tornará de color rojo, caso contrario estará en color verde lo que indica que el equipo está en estado up.

Figura 4

Interfaz Gráfica de THE DUDE



Fuente: *(Mikrotik, 2022)*

Mediante este software, el administrador de red es capaz de dibujar diagramas completos de la estructura total de la red, puede añadir dispositivos a la topología con la finalidad de controlar las funciones que realizan los diferentes equipos de red y el estado de los mismos mediante ping, traceroute, conexión remota, test de ancho de banda, telnet, ftp entre otros. El software genera estadísticas para alertar a los administradores sobre las eventualidades presentadas.

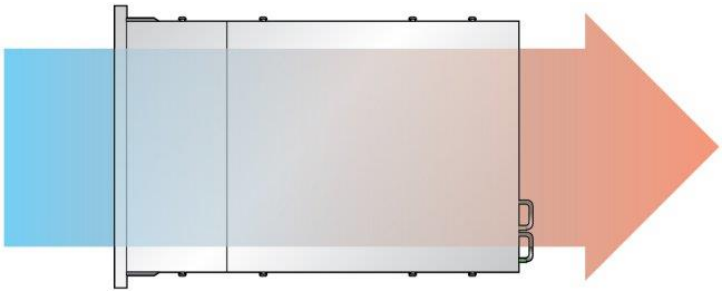
2.7.Necesidades de refrigeración de equipos de telecomunicaciones

Un sistema de enfriamiento garantiza el buen funcionamiento del equipo activo y se previenen posibles pérdidas de información o desconexiones que afectan inmediatamente en procesos importantes de la empresa de telecomunicaciones. La ventilación adecuada es un factor importante a la hora de montar infraestructura IT a prueba de fallos, debido a que los sistemas se recalientan en muy poco tiempo si no disponen de una ventilación adecuada.

La temperatura interior dentro de un gabinete va aumentando debido a los dispositivos activos que se encuentran funcionando (servidores, SAI, switches, routers, firewalls, olts, entre otros) y puede ocasionar fallos de rendimiento en los equipos y también pueden afectar la vida útil de los equipos. El aumento de la temperatura reduce significativamente la vida útil del hardware hasta un 45% en determinadas circunstancias. Por tal razón se debe equipar con elementos de ventilación a las instalaciones de infraestructuras IT (gtlan, 2022). Los armarios rack están equipados con una estructura exterior perforada que facilita la ventilación natural, pero esto no es suficiente para mantener el interior a una temperatura óptima. Por ello es recomendable el uso de sistemas de ventilación (gtlan, 2022). Los ventiladores expulsan el aire caliente del interior del rack, se colocan en la parte superior del armario para aprovechar el flujo natural ascendente del aire caliente o en la parte posterior o laterales del gabinete, estos sistemas son controlados por sensores y actuadores para establecer su activación y desactivación dentro de rangos de temperatura establecidos. En la Figura 5 se observan los requisitos de circulación de aire con la finalidad de mantener el interior del gabinete de los nodos con una temperatura estable.

Figura 5

Requisitos de circulación de aire



Fuente: *(Oracle, 2022)*

2.8. Red PON

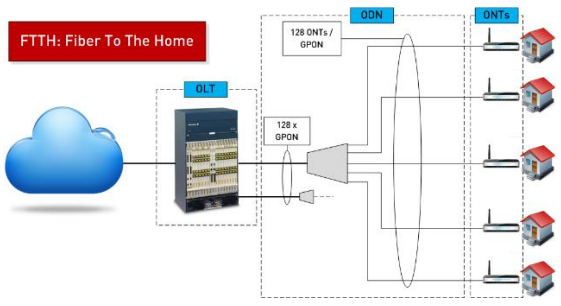
Una red óptica pasiva es una red de fibra óptica que usa una topología de punto a multipunto y splitters ópticos para la transmisión de datos de un punto único de transmisión a varios puntos finales de usuario; la ventaja que conlleva una red PON, es el uso de equipos activos en el envío y recepción de la información, por lo que estas redes PON ofrecen grandes ventajas desde el punto de vista energético. Las redes PON se usan para transmitir y recibir información hacia y desde los usuarios finales. Actualmente existen nuevas tecnologías lo que ha dado paso a las redes como son la GPON, EPON o XGPON (Mikaeil, Hu, Ye, & Hussain, 2017).

2.9. Arquitectura de red de fibra óptica FTTH

La arquitectura FTTH como: Fibra Óptica Al Hogar y es una tecnología de telecomunicaciones que consiste en la utilización de cableado de fibra óptica y sistemas de distribución ópticos para la provisión de servicios de Internet (banda ancha), Telefonía IP y Televisión (IPTV) a hogares, negocios y empresas. Los componentes principales y la arquitectura general de la red FTTH en cualquier operador de telecomunicaciones consta de: el terminal de línea óptica (OLT), el marco de distribución óptica (ODF), el divisor óptico pasivo (POS), el terminal de distribución de fibra (FDT), el terminal de acceso de fibra (FAT), Unidad/terminal de red óptica (ONU/ONT) así como se muestra en la Figura 6. Todos estos elementos son los que conforman una red FTTH.

Figura 6

Arquitectura de red FTTH



(Telequismo, 2022)

2.9.1. OLT

Es un dispositivo de central, el cual se puede conectar al Switch principal mediante un cable de red y convertirlo en una señal óptica. La fibra óptica única está interconectada con el

divisor óptico en el extremo del usuario. Se implementan el control, la gestión y el alcance desde la ONU del equipo de usuario. En la Figura 7 se muestra el OLT CXR GP2500.

Figura 7

OLT CXR GP2500

Fuente: *(CXR, 2022)*

2.9.2. ONU y ONT.

Son dispositivos del lado del usuario. No hay diferencia en función, pero si son diferentes en ubicación, por ejemplo, una celda, la ONT es un dispositivo ubicado directamente en la casa del usuario, y la ONU puede colocarse en el corredor, y cada usuario está conectado a la ONU a través de un dispositivo como un Switch. En la Figura 8 se muestra un dispositivo ONU.

Figura 8

Equipo ONU

Fuente: *(Bt-PON, 2022)*

2.9.3. Módulo transceptor SFP

Un SFP básicamente es un equipo transceptor insertable en caliente cuyo fin es que sirve como interfaz entre dos equipos de comunicaciones los cuales pueden ser un Switch, Router u OLT, entre otros y la red de fibra óptica, además están diseñados para soportar

diferentes estándares de comunicaciones (Amazon, 2022). En la Figura 9 se observa un tranceptor SFP.

Figura 9

Tranceptor SFP

Fuente: *(Intellinet, 2022)*

2.9.4. ODF.

El marco de distribución óptica (ODF) es el dispositivo de red donde las fibras de los cables exteriores se terminan y están disponibles para interactuar con los equipos activos. El ODF ofrece una conexión flexible entre los puertos o divisores de equipos activos y la terminación del cable exterior. Las fibras se identifican y almacenan en carcasas o estantes separados físicamente para simplificar el mantenimiento de la fibra y para proteger o evitar interferencias accidentales en los circuitos de fibra, así como se muestra en el Figura 10.

Figura 10

ODF de 48 hilos

Fuente: *(MatrixTelcom, 2022)*

2.10. IOT en el control de dispositivos

Un dispositivo IoT es un elemento que cuenta con conexión a Internet y programado mediante software para realizar una actividad específica, en donde se pueden medir físicas o controlar remotamente dispositivos generando una experiencia en el usuario final, midiendo datos y analizándolos mediante técnicas de inteligencia artificial; existen diversas aplicaciones del IOT por ejemplo: obtención de parámetros físicos, control de máquinas, toma de datos para

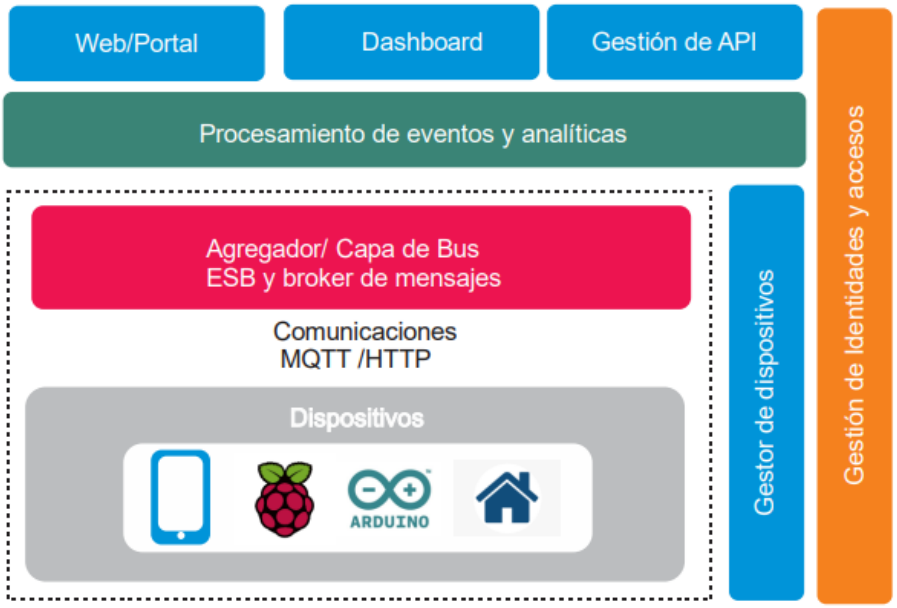
mantenimiento predictivo, monitorización de activos, automatización de procesos manuales, entre otros.

2.11. Arquitectura del IOT para sistemas de control

Según la ISO 30141 la arquitectura IoT se define "como una infraestructura de entidades físicas, sistemas e información, interconectados junto con los servicios inteligentes que pueden procesas y reaccionar información tanto en el mundo físico y el mundo virtual y pueden influir en las actividades en el mundo físico." En la Figura 11 se aprecia una arquitectura del IOT.

Figura 11

Arquitectura IOT



Fuente: *(Suárez, 2021)*

2.11.1. La capa del dispositivo

En esta etapa se detalla todo el Hardware de la arquitectura IoT, esta capa está asociada a los dispositivos IoT que están conectados a internet mediante comunicación directa o indirecta, algunas placas de desarrollo que encontramos en esta capa son: Arduino con conexión Ethernet, Arduino Yun con conexión wifi, Raspberry Pi conectado vía Ethernet o Wi-fi, dispositivos ZigBee conectados mediante Gateway de ZigBee, dispositivos conectados a teléfonos móviles con Bluetooth, entre otros.

2.11.2. La capa de comunicaciones

Se encarga de enviar y recibir la información de los dispositivos, cumpliendo la funcionalidad de conectar entre los diferentes equipos. Los protocolos más reconocidos para este fin son: HTTP/HTTPS, MQTT, protocolo de aplicación restringida (CoAp), entre otros.

2.11.3. La capa de agregación de bus

Son los agregadores o Brokers de comunicación que soportan un servidor HTPP y/o Broker MQTT para comunicarse con los dispositivos, esta capa permite agregar y combinar comunicaciones de diferentes dispositivos, además de enrutar las comunicaciones a dispositivos específicos y tienen la posibilidad de actuar como un Gateway.

2.11.4. La capa analítica y procesamiento de los eventos

En esta capa se realiza la gestión y revisión de los datos enviados, teniendo presente la capacidad para almacenar datos de los dispositivos conectados a la arquitectura. escalabilidad que puedan tener y las acciones que deben realizar los dispositivos con el mundo real.

2.11.5. La capa de comunicación cliente/externo.

La arquitectura de referencia se necesita dar una manera para que los estos dispositivos puedan comunicarse fuera de sistema orientado al propio dispositivo, esto permite conectar sistemas pensados en la web.

2.11.6. La capa de gestión de comunicación

La gestión de dispositivos está controlada por dos componentes. Un sistema en el servidor que se comunica con los dispositivos mediante varios protocolos y posibilita el control en masa e individual de los dispositivos. Una particularidad importante es poder gestionar el software y las aplicaciones de manera remota. Dependiendo de las características algunos dispositivos pueden no tener capa de gestión de comunicación por las limitaciones del hardware, en esta categoría se incluyen los dispositivos de 8-bits.

2.11.7. Gestión de accesos e identidades

La capa de gestión de acceso y entidades ofrece la validación del acceso de los dispositivos mediante Tokens, Soporte para “OpenID Connect”, esta hace relación a la capacidad de identificar el dispositivo que realiza las peticiones entrantes de la capa web, Directorio de los usuario y gestión de políticas para la gestión de control de acceso (Chakray, 2015).

2.12. Supervisión remota

La supervisión remota es usada para la transmisión de datos de dispositivos de IoT o para determinar la validez de los datos. Mediante la supervisión remota de dispositivos IoT se captura los datos de los dispositivos en tiempo real para evaluar el estado de cada dispositivo IoT y enviarle notificaciones si hay problemas de transmisión de datos o datos fuera de alcance. Supervisión remota de dispositivos IoT también proporciona un marco para la recopilación de información de diagnóstico que permite obtener información orientada a los resultados sobre el estado de los activos (AWS, 2022).

2.13. Plataformas de computación en la nube

La plataforma como servicio o PaaS es un conjunto de servicios basados en la nube que permite a los desarrolladores y usuarios empresariales crear aplicaciones a una velocidad que las soluciones en las instalaciones de la empresa no se pueden alcanzar. Al tratarse de un servicio basado en la nube, no hay necesidad de preocuparse por la configuración y el mantenimiento de servidores, parches, actualizaciones y autenticaciones, entre muchas otras tareas: los usuarios pueden centrarse en crear la mejor experiencia de usuario posible.

2.13.1. AWS

AWS (Amazon Web Services) es una plataforma de servicios en la nube del gigante mundial del comercio electrónico Amazon. Se encuentra entre las ofertas de infraestructura como servicio preferidas disponibles en la actualidad. La plataforma también proporciona ofertas de PaaS y SaaS para satisfacer las necesidades de las empresas en una gran cantidad de dominios de la industria. AWS cuenta con varias funciones convenientes que aprovechan el poder del aprendizaje automático, la inteligencia artificial y el análisis, facilita el funcionamiento sin esfuerzo de servidores y aplicaciones y viene con características convenientes como CDN, base de datos administrada y almacenamiento de archivos.

Cuenta con un conjunto de herramientas y servicios que permiten la computación en la nube, además tiene infraestructura escalable y de bajo costo que presta algunos servicios dependiendo de los requerimientos de los usuarios, como por ejemplo: potencia de cómputo, opciones de almacenamiento, redes, bases de datos entre otros; proporciona una infraestructura global en la nube, permitiendo adaptabilidad y escalabilidad, además es independiente del sistema operativo que se utilice lo que es importante cuando se requiere de opciones de innovación para empresas o negocios.

Las principales ventajas de esta plataforma son:

- Seguridad ya que cuenta con certificaciones y autorías tales como: PCI DSS nivel 1, FISMA Moderate, HIPAA Y SOC 1, ISO 27001 y auditoria SOC 2, lo que la hace confiable.
- Bases de datos mediante gestión y almacenamiento de información, permite el acceso a bases de datos como: MySQL, Oracle, Aurora, PostgreSQL, SQL Server, MongoDB, entre otros.
- Bajo costo ya que, los negocios no necesitan realizar una fuerte inversión en infraestructura, solo utilizar los recursos que ofrece la plataforma.
- Accesibilidad absorbiendo la carga de trabajo.
- Resilencia permitiendo el trabajo en contingencias con un 99.99999% de tiempo en línea.

2.14. Metodologías para el desarrollo de proyectos tecnológicos

Muchas áreas de la actividad humana y profesional, como la ingeniería de máquinas, la industria aeroespacial, la exploración espacial, control climático, protección del medio ambiente, seguridad nacional, finanzas y economía, cuidado de la salud, etc., están basados en la creación y desarrollo de proyectos de tecnología, cada uno de estos proyectos partió de una idea y para llegar a su fin de manera exitosa tuvo que pasar por una serie de procesos sistemáticos, para que este conjunto de procesos se lo realice de manera organizada se aplican a los proyectos metodologías y/o modelos que permitirán guiar el transcurso de su desarrollo paso a paso (Pasian, 2015).

Sin importar la metodología que se aplique a los proyectos estos en su mayoría tienen etapas básicas que van desde: la planificación y análisis de requerimientos, diseño de la arquitectura del proyecto, desarrollo y programación, pruebas, y concluye en el despliegue que es la etapa en la cual el proyecto se implanta en un ambiente real ya sea controlado o no.

Con el transcurso del tiempo y la evolución tecnológica se han diseñado una amplia gama de metodologías para el desarrollo de proyectos tecnológicos ya que estos responden a requerimientos de las empresas, entidades que los patrocinan, tamaño y alcance de los proyectos, tiempo de vida y ejecución, etc. (Guévin, 2019). Entre las metodologías más conocidas están las siguientes: modelo en cascada, scrum, Prince2, PERT, Extreme Programming, modelo iterativo, Kanban.

2.14.1. Modelo iterativo

La gestión de proyectos con este modelo se basa en la preparación de iteraciones a lo largo del ciclo de vida del proyecto.

Las iteraciones son pasos incrementales hacia la finalización de un proyecto. Los enfoques iterativos se utilizan en proyectos de desarrollo de software y proyectos tecnológicos que implican software y hardware, estos enfoques promueven la velocidad y la adaptabilidad, ya que el beneficio de la iteración es que puede ajustarse a medida que avanza en lugar de seguir una ruta lineal (Zumba Gamboa & León Arreaga, 2018). Una de las orientaciones del modelo iterativo es liberar beneficios durante todo el proceso y no solo al final. En esencia, los proyectos iterativos deben exhibir valores y comportamientos centrales de confianza y flexibilidad.

2.14.2. Modelo en cascada

La gestión de proyectos en cascada traza un proyecto en distintas etapas secuenciales, y cada nueva fase comienza solo cuando se completa la anterior. La metodología en cascada es el modelo más tradicional para administrar un proyecto, en este sistema no se espera que cambie ninguna de las fases o metas (Haworth, 2021).

2.14.3. Scrum

Scrum es un método probado y ampliamente adoptado para lograr la agilidad del software. Al trabajar en sprints cortos, este ciclo se puede repetir hasta que se hayan completad suficientes elementos de trabajo, se haya agotado el presupuesto o llegue una fecha límite.

2.14.4. Prince 2

Prince 2 es un acrónimo de Proyectos en ambientes controlados. Es un método basado en procesos para administrar un proyecto. La característica clave de PRINCE2 se centra en la defensa de la estructura organizativa y utiliza un enfoque basado en productos. Se hace hincapié en dividir el proyecto en etapas manejables y controlables, proporciona un gran control sobre los recursos del proyecto y se destaca en la gestión del riesgo empresarial y del proyecto de forma más eficaz (PRINCE2, 2021).

2.14.5. Xtream Programing

En la década de 1990, el auge de Internet requirió un cambio en el desarrollo de software. Si el éxito de una empresa dependía de la velocidad a la que la empresa pudiera crecer y llevar productos al mercado, las empresas debían reducir drásticamente el ciclo de vida del desarrollo de software. Fue en este entono que Kent Beck creó la programación extrema XP,

una metodología de gestión de proyectos ágil que admite lanzamientos frecuentes en los ciclos de desarrollo cortos para mejorar la calidad del software y permitir a los desarrolladores responder a los requisitos cambiantes de los clientes (Altexsoft, 2018).

2.14.6. Kanban

El proceso Kanban se basa en extraer el trabajo de una etapa de proyecto pendiente y completar cada uno solo según sea necesario. Esta metodología elimina los sprints y los hitos atribuidos a los métodos de gestión de proyectos de Scrum y tradicionales. Se centra en un enfoque más visual de la gestión del tiempo, las dimensiones del proyecto y el presupuesto, para esta metodología estos son los tres factores que determinarán el éxito o fracaso de todo proyecto.

CAPÍTULO 3. DISEÑO E IMPLEMENTACIÓN DEL SISTEMA

Para el desarrollo del dispositivo electrónico para el monitoreo activo y reinicio remoto de la OLT Caranqui, se aplica la metodología del modelo iterativo; en la primera etapa se realiza un análisis de información recopilada de entrevistas y encuestas aplicadas a los involucrados directos e indirectos con la finalidad de establecer los requerimientos del sistema para luego diseñar la arquitectura de este, la cual será sintetizada y presentada en forma de diagrama de bloques.

En la segunda etapa, se diseña el sistema de acuerdo con los resultados obtenidos en la primera etapa, en el diseño se realiza el esquema del circuito, conexiones entre los elementos necesarios para el correcto funcionamiento del dispositivo.

En la tercera etapa de la metodología se realizan las pruebas necesarias de cada subsistema que conforma el dispositivo para luego integrar todos los bloques y obtener un resultado final de funcionamiento para luego en la cuarta etapa proceder a la evaluación de rendimiento del sistema.

3.1. Metodología

Para la selección de la metodología, inicialmente se parte de los requerimientos del proyecto, de igual forma, del conocimiento del investigador; puesto que, se necesita verificar cada fase del proyecto, se aplica la metodología iterativa con la finalidad de tener un dispositivo que cumpla con los requerimientos propuestos y así cumplir con los objetivos planteados.

Se realizará una recolección de datos de los niveles de temperatura ambiente a los cuales se ven sometidos los gabinetes de equipos, esto permitirá realizar una comparación entre la temperatura de trabajo actual y la temperatura de trabajo recomendada para los dispositivos ubicados dentro del gabinete de equipos del nodo OLT-Caranqui. Se culminará con la implementación del prototipo dentro de un ambiente controlado.

Para futuras menciones del sistema prototipo de monitoreo activo y reinicio remoto de dispositivos OLT mediante una interfaz web, se utilizará la siguiente nomenclatura SCYNODE, que parte de las siglas en inglés de SECURITY y NODE, entendiéndose como “Nodo Seguro”

Para iniciar el diseño del sistema propuesto, se realiza un análisis y esquema de los procesos a realizar en cada iteración, a criterio del autor, se ha demostrado que el sistema está completo al final de la tercera iteración, pero según el modelo de diseño de proyecto de tecnología en el que se trabaja, se pueden agregar iteraciones según sea necesario. La Tabla 2 presenta de manera simple y breve el contenido de cada iteración, así como las métricas

evaluadas al final de cada iteración. Cabe señalar que los procesos e indicadores a evaluar se enuncian de manera macro, dentro de cada uno de estos existen subprocesos que pueden ser considerados para definir un parámetro de evaluación. El contenido completo y detallado está dentro de cada una de las iteraciones propuestas.

Tabla 2

Contenido de los procesos a realizar en cada una de las iteraciones propuestas para el diseño del SCYNODE

Iteración	Procesos	Indicadores	Cumplimiento
Primera	-Análisis del escenario actual -Delimitación de los requerimientos -Requerimientos de Stakeholders -Requerimientos de arquitectura -Requerimientos del sistema -Recursos -Definición de los módulos -Selección de dispositivos	-Conceptualización del componente teórico -Dispositivos necesarios para el ensamblaje -Plataforma AWS disponible y activa	35%
Segunda	-Delimitación de los casos en los cuales es necesario el reinicio remoto de la OLT ubicada en el nodo OLT-Caranqui -Diseño del sistema-segunda iteración -Ensamblaje del dispositivo -Envío de datos -Diseño interfaz WEB	-Comunicación exitosa entre los módulos -Instancias cargadas en la plataforma AWS -Toma de los datos registrados en el gabinete de equipos de la OLT-Caranqui -Envío y recepción de datos Acceso mediante dirección -IP a la base de datos y al servidor web -Resultados de las mediciones de temperatura dentro del gabinete de equipos -Envío y recepción de la información -Almacenamiento en la base de datos en las tablas asignadas a cada dato -Acceso a la página web con la dirección IP y acceso a la cuenta de usuario con	35%

		verificación de credenciales -Publicación de la información en el servidor web -Integración de un dispositivo de refrigeración	
Tercera	-Pruebas en escenario a escala de laboratorio -Diseño del sistema-tercera iteración -Diseño de carcasa -Pruebas en el nodo	-Integración del dispositivo en el gabinete de equipos del nodo OLT-Caranqui -Envío y recepción de la información -Reinicio remoto de la OLT en un entorno controlado -Almacenamiento y publicación de la información	20%
Cuarta	-Evaluación de rendimiento -Establecimiento de conclusiones y recomendaciones	-Soporte técnico de SAITEL, da una opinión y evaluación del rendimiento sobre el dispositivo SCYNODE	10%

Fuente: *Autoría*

3.2. Técnicas de investigación

Mediante las técnicas de investigación se busca recopilar información para poder determinar la situación actual y sustentar el desarrollo del proyecto, por lo cual la información respectiva se la obtiene a partir del departamento de soporte técnico de la empresa SAITEL. En la Tabla 3 se detallan los métodos a utilizar y las fuentes de información respectivas.

Tabla 3

Métodos de investigación

Método	Propósito	Fuente de Información
Encuesta	Conocer ideas, opiniones y datos fundamentales	Personal técnico SAITEL
Entrevista	Conocer estado actual de la red, nodos e infraestructura	Ing. Miguel Cuasapaz, jefe técnico SAITEL

Fuente: *Autoría*

3.2.1. Análisis de resultados

Luego de haber realizado la encuesta a 10 técnicos y luego de realizar la entrevista, se presentan los resultados que permiten desarrollar el proyecto, a continuación, se presenta la información obtenida y se establecen los antecedentes y análisis de la red GPON de SAITEL.

El sistema SCYNODE debe ser de tamaño reducido e instalado en el gabinete del nodo OLT Caranqui y no debe inferir en el estado del nodo UP/DOWN de los equipos de infraestructura que se encuentran en él.

El sistema SCYNODE debe contar con un sistema de refrigeración y ventilación para controlar la temperatura interna del nodo y debe estar conectado al respaldo de energía en caso de fallas de la red eléctrica. Los datos del sistema SCYNODE deben ser interpretados de forma clara en un servidor WEB en una interfaz gráfica amigable para el usuario, de igual forma el botón de reinicio debe activar un actuador que permitirá reestablecer los equipos dentro del nodo.

3.3. Análisis de la situación actual

3.3.1. SAITEL antecedentes

Soluciones Avanzadas Informáticas y Telecomunicaciones SAITEL, es una empresa que fue creada con el fin principal de brindar a la colectividad el servicio de Internet mediante enlaces inalámbricos y por medio de fibra óptica. Inicialmente sus operaciones las realizaba en la ciudad de Ibarra, posteriormente con la implementación de nuevas tecnologías y equipamiento la cobertura se amplío hacia las provincias y cantones aledaños, lo que permitió además el montaje de sucursales en Cayambe, Joya de los Sachas, Tulcán y agencias en Esmeraldas, Latacunga, Chone, Quito Norte, Quito Sur, El Coca, Shushufindi, Lago Agrio. (SAITEL, 2022).

3.3.2. Situación actual en la red GPON ciudad de Ibarra.

La Red Óptica Activa de comunicaciones de SAITEL actualmente está conformada por 9 Nodos Centrales ubicados estratégicamente en la ciudad, cada uno constituido por un Distribuidor de Fibra Óptica (ODF), dos Terminales de Línea Óptica (OLT), un Router, una batería de 12 V y una Fuente de Alimentación Ininterrumpida (UPS) que actúa como sistema de energía de respaldo, ubicados en el interior de gabinetes metálicos herméticos de montaje superficial, instalados en la postería de EMELNORTE (Empresa Eléctrica Regional Norte) y que cumplen la función de ‘Sala de Equipos’ en un esquema de red de Fibra Óptica.

Actualmente se han venido suscitando eventos recurrentes que inciden en el desempeño y continuo funcionamiento de determinados dispositivos de los Nodos Centrales, que tienen relación directa o indirecta, debido a la elevada temperatura a la que están sometidos los elementos como los Transceptores Ópticos, como causa de estaciones veraniegas más intensas y prolongadas en la ciudad, temperatura que se incrementa drásticamente debido al espacio reducido de las Salas de Equipos (gabinetes metálicos herméticos), que no disponen de un sistema de ventilación o de rejillas para la circulación del aire, causando que la señal óptica sea percibida como incorrecta.

Al tratarse de proyecto como plan piloto de la empresa SAITEL destinado en su primera etapa al supervisión remota de nodos y control de acceso a los mismos, el nodo OLT-Caranqui fue escogido estratégicamente por los directivos y personal técnico de la empresa ya que en el año 2021 fue uno de los gabinetes con mayor vulnerabilidad ante delincuentes, así también debido a que las altas temperaturas concentradas dentro de este gabinete de equipos puede producir fallas de funcionamiento ocasionando cortes en el servicio.

La red de infraestructura de SAITEL es monitoreada por el departamento técnico mediante el software The DUDE, el cual muestra alertas en color rojo en caso de que un dispositivo de res se encuentre en estado down y en color verde indicando su estado up, una vez que soporte detecta un nodo “caido” o en estado down, el personal técnico respectivo tiene que dirigirse al sitio en donde se encuentra ubicado el nodo y realizar un reinicio manual interrumpiendo el flujo normal de corriente eléctrica, una vez realizado esto se levanta el servicio. En la Figura 12 se muestra el estado de un equipo en UP/DOWN.

Figura 12

OLT Caranqui en software DUDE

Fuente: *SAITEL*

Debido a los acontecimientos descritos anteriormente, los ingenieros y técnicos de la empresa han establecido una solución provisional a los problemas que se han venido presentando en los Nodos, que han sido denominados por los técnicos de la institución "Inhibición de Equipos" , la cual consiste en realizar un reinicio de los dispositivos OLT, in situ, situación que conlleva a destinar recursos como personal técnico, vehículos y el tiempo, factor determinante , ya que, considerando el lapso de tiempo desde la detección del problema en determinado Nodo, el desplazamiento del personal y la puesta en ejecución del reinicio de los equipos OLT hasta el restablecimiento completo del servicio, hacen que todo el proceso sea muy crítico para la empresa, considerando que, la percepción que los usuarios tienen de la calidad del servicio depende netamente de la continuidad, disponibilidad y velocidad del servicio que la empresa puede proveer.

Al existir la necesidad de reiniciar la OLT el personal técnico se ve obligado a acudir personalmente al nodo para realizarlo, constituyendo para la empresa en una actividad generadora de gastos de movilización y asignación de personal que puede estar realizando otro trabajo. En los usuarios ocasiona un mayor tiempo de corte en el servicio generando molestias y una apreciación negativa de la calidad de este.

Este proyecto propone el diseño de un sistema electrónico de monitoreo activo del nodo de fibra óptica "OLT – Caranqui" a través de una interfaz Web, que permita el seguimiento de la temperatura en la Sala de Equipos (Gabinete de equipamiento), la alerta automática de acceso al Gabinete de Equipamiento, encaminando a preservar la seguridad de los mismos y prevenir robos futuros en la infraestructura de telecomunicaciones de la empresa, finalmente el control de reinicio remoto de los dispositivos OLT, evitando el desplazamiento de técnicos hasta el nodo en conflicto para la realización de un reinicio de forma manual, lo que permitirá mejorar el tiempo de restitución del servicio y así brindar continuidad, disponibilidad y calidad en el acceso de internet a los abonados.

3.4. Propósito del sistema

La investigación consiste en el desarrollo de un sistema electrónico que permita monitorear la temperatura del interior del nodo OLT Caranqui de la empresa SAITEL y el acceso no permitido al mismo a través de un servidor WEB como interfaz de usuario, el administrador de la red será capaz de reiniciar remotamente el nodo mediante una instrucción que será enviada desde el servidor en la nube, está acción estará a cargo del personal de soporte técnico de la empresa el cual monitoreará es estado del equipo (up/down) y lo reiniciará cuando esté "caído".

3.5. Ámbito del sistema

El dispositivo permitirá ahorrar recursos a la empresa SAITEL, es decir, tiempo en la movilización del personal técnico encargado hacia el sitio donde se detecta el error, con el ello se asegura de brindar continuidad en el servicio mejorando la apreciación del cliente, además de contar con un sistema de ventilación automático en base a la temperatura medida en el interior del gabinete del nodo, a su vez monitorear el acceso no permitido al mismo.

3.6. Descripción general del sistema

El sistema electrónico SCYNODE consta de sensores para la recopilación de datos mediante; el dispositivo consta de un sensor magnético, mismo que, sirve para monitorear el ingreso no deseado al nodo, un sensor de temperatura, el cual sirve para medir la temperatura dentro del gabinete y dependiendo de parámetros establecidos en un microcontrolador accionar un sistema de enfriamiento.

Consta también de un módulo GSM/GPRS, el cual sirve para establecer la conexión con el internet y así poder enviar información a servidores de bases de datos en la nube, consta también de un servidor WEB para la visualización de resultados, mismo que, tiene un botón de reinicio del nodo el cual a través del protocolo HTTP permite accionar un relé remotamente para interrumpir el flujo de corriente hacia los equipos OLT.

3.7. Determinación de Stakeholders

Este apartado hace referencia a los involucrados directa o indirectamente del proyecto, es decir, aquellas personas a las que les interesa el desarrollo de este, mediante los Stakeholders se puede obtener requerimientos específicos necesarios que el prototipo debe cumplir siendo así una solución óptima sustentando el trabajo de titulación.

Lo que se pretende es establecer los requerimientos necesarios de los usuarios para diseñar un sistema electrónico que permita ser parte de una solución, facilitando así el desarrollo de procesos dentro de la empresa SAITEL al momento de presentarse un evento y también en la toma de decisiones pertinentes. En la Tabla 4 se describe los Stakeholders involucrados en la presente investigación.

Tabla 4

Listado de Stakeholders para el diseño del SCYNODE

Rol General	Stakeholders
Usuarios directos	Personal técnico de la empresa SAITEL Administrador/a del SCYNODE

Usuarios indirectos	Abonados de la empresa SAITEL
Administradores	Ibujés Espinosa Andrés Marcelo
Director y fiscalizadores del proyecto	MSc. Carlos Vásquez MSc. MSc.

Fuente: *Autoría*

3.8.Requerimientos del sistema SCYNODE

De acuerdo con la revisión bibliográfica respecto al modelo iterativo para el desarrollo de un prototipo tecnológico, se establece a la definición de los requerimientos del sistema como primer paso para el inicio del proceso de diseño e implementación del SCYNODE.

Para determinar los requisitos del sistema, es fundamental evaluar los escenarios relacionados al diseño con el fin de obtener un dispositivo ideal para la implementación en un entorno de trabajo específico. En este contexto, se tienen en cuenta los siguientes escenarios y sus respectivos requisitos:

- Requerimientos de stakeholders
- Requerimientos de arquitectura
- Requerimientos del sistema

Para un manejo oportuno de la terminología que se utiliza en la definición de los requisitos se utilizará como nomenclatura las siguientes abreviaturas mostradas en la Tabla 5.

Tabla 5

Nomenclatura a usar para los requerimientos de diseño del sistema

Requerimiento	Abreviatura
RSH	Requerimientos de Stakeholders
RS	Requerimientos del sistema
RAS	Requerimientos de arquitectura

Fuente: *Autoría*

3.8.1. Requerimientos de Stakeholders

Estos requerimientos son aquellos que conciernen a las personas que tienen una participación directa o indirecta dentro del desarrollo e implementación del sistema, una

característica esencial de los stakeholders es una amplia trayectoria en la instalación, manejo y/o administración de OLTs en la empresa SAITEL.

La Tabla 6 enlista los procesos necesarios para identificar los requerimientos de stakeholders en relación al conocimiento y experticias del equipo técnico de la empresa SAITEL, se determinan dichos requerimientos en base a la encuesta realizada al personal técnico de la empresa SAITEL y la entrevista realizada al jefe técnico.

Tabla 6

Requerimientos de Stakeholders para el diseño del sistema prototipo de telemetría y reinicio remoto

RSH				
Orden	**Requerimiento**	**Prioridad**		
		Alta	**Media**	**Baja**
Requerimientos operacionales				
RSH1	Medir los niveles de temperatura dentro del gabinete de equipos	X		
RSH2	Almacenar los datos de los niveles de temperatura en una BDD	X		
RSH3	Acceso a la información almacenada, para los administradores del SCYNODE	X		
RSH4	Supervisión remota por parte del administrador y personal técnico autorizado, del estado de temperatura del gabinete de equipos a través de una página web		X	
RSH5	Acceso total y continuo por parte de los administradores de soporte técnico a la programación del dispositivo			X

RSH6	Las credenciales de acceso deben ser cambiadas continuamente			X
	Requerimientos de usuario			
RSH7	El servidor web siempre tiene que estar disponible para el administrador del sistema y personal técnico	X		
RSH8	Reinicio remoto de la OLT de ser necesario, en caso del aumento en los niveles de temperatura, mismos que sobrepasen los umbrales recomendados para el funcionamiento del dispositivo	X		
RSH9	El sistema debe generar una alerta para el administrador, cuando los niveles de temperatura en el gabinete de equipos inquieran en un estado de emergencia	X		
RSH 10	El sistema debe generar una alerta para el administrador, cuando exista un acceso no autorizado al gabinete de equipos	X		
RSH 11	La conexión del dispositivo hacia el internet debe ser de gran disponibilidad	X		
RSH 12	La visualización de resultados mediante la interfaz gráfica debe ser amigable con el usuario			X
RSH 13	La temperatura medida debe ser mostrada en tablas a través de la interfaz gráfica de usuario			X
RSH 14	El sistema debe ser de bajo costo			X

Fuente: *Autoría*

3.8.2. Requerimientos del sistema

Los requisitos del sistema originados a partir de la observación directa de los contratiempos ocurridos en los gabinetes de equipos y OLT de la empresa SAITEL, además de la investigación previa acerca de seguridad en la infraestructura de telecomunicaciones. Para este propósito, se realiza una encuesta con el personal técnico y administrativo de la empresa, las evidencias se encuentran al final del documento en la sección de anexos. En la Tabla 7 se detallan los requerimientos del sistema.

Tabla 7

Requerimientos del SCYNODE

RS				
Orden	**Requerimiento**	**Prioridad**		
		Alta	**Media**	**Baja**
Requerimientos de uso				
RS1	Ingreso a la página web mediante una cuenta de usuario, esto permitirá limitar el acceso a la información solo para personal autorizado	X		
RS2	Presentación en la página web, de la información acerca de los niveles de temperatura dentro del gabinetes de equipos	X		
RS3	Los niveles de temperatura deben ser mostrados de tal manera que el administrados comprenda el estado de los resultados, con etiqueta y/o colores		X	
RS4	Los datos deben ser apreciados en tiempo real por el personal autorizado			X
RS5	El sistema no debe saturarse	X		
RS6	El usuario debe acceder mediante credenciales de acceso designadas por el departamento de seguridad		X	
Requerimientos de interfaz				
RS7	Comunicación serial entre el dispositivo de medición de temperatura y la placa de	X		

	desarrollo			
RS8	Conexión a internet	X		
RS9	Almacenamiento interno de datos de forma temporal			X
RS10	La base de datos debe presentar la información en forma adecuada mediante registros			X
	Requerimientos físicos			
RS11	Tamaño del prototipo pequeño para que pueda ajustarse dentro del gabinete de equipos	X		
RS12	En caso de avería del sistema, este no debe inferir en el correcto funcionamiento de la OLT	X		
	Requerimientos de performance			
RS13	La plataforma Web no debe saturarse y debe tener Alta disponibilidad	X		
RS14	El dispositivo debe tomar datos y mostrarlos en tiempo real.	X		
RS15	El dispositivo debe funcionar las 24 horas del día teniendo alta disponibilidad	X		
RS16	La comunicación inalámbrica no debe interrumpirse	X		
	Requerimientos de modo y estado			
RS17	La plataforma WEB debe indicar la temperatura dentro del gabinete de equipos			X
RS18	La plataforma WEB debe indicar el acceso al gabinete de equipos mediante la activación de un sensor magnético			X

Fuente: *Autoría*

3.8.3. Requerimientos de arquitectura

Estos requerimientos permiten que el prototipo sea utilizable, estable y atractivo para el administrador. Aquí se definen los componentes estructurales del sistema con características

de escalabilidad y minimización de la complejidad a medida que el desarrollo del dispositivo se vuelve más extenso. En la Tabla 8 se detallan los requerimientos de arquitectura del SCYNODE.

Tabla 8

Requerimientos de arquitectura para el diseño del SCYNODE

RAS				
Orden	**Requerimiento**	**Prioridad**		
		Alta	**Media**	**Baja**
Requerimientos lógicos				
RAS1	Soporte de comunicación digital entre el sensor de temperatura y la placa de desarrollo			X
RAS2	Soporte de comunicación analógico entre el sensor magnético y la placa de desarrollo			X
RAS3	Acceso a la base de datos mediante un servidor WEB	X		
RAS4	Acceso al servidor WEB alojado en la nube	X		
RAS5	Comunicación entre la plataforma WEB y el dispositivo de dos vías	X		
Requerimientos de diseño				
RAS6	Soporte de protocolo HTTP para comunicación con el servidor web en la nube		X	
RAS7	Compatibilidad entre sensores y actuadores con la placa de desarrollo	X		
RAS8	Compatibilidad entre la placa de desarrollo y el módulo para la comunicación	X		
RAS9	Comunicación entre el dispositivo y la plataforma de almacenamiento en la nube		X	
RAS10	Los datos deben ser almacenados en la base de datos alojada en la nube	X		
Requerimientos de Software				
RAS11	Lenguaje de programación compatible con hardware	X		

RAS12	Entorno de programación de código abierto		X	
RAS13	Envío de alertas destinadas a los administradores de la plataforma web, en caso de existir una situación de emergencia		X	
RAS14	El sistema operativo debe ser Open Source	X		
RAS15	La plataforma de almacenamiento en la nube debe ser de alta disponibilidad	X		
	Requerimientos de Hardware			
RAS16	La placa de desarrollo debe tener un tamaño pequeño para que pueda ser integrado dentro de un gabinete de dispositivos como o similar al que se encuentra ubicado en el nodo OLT-Caranqui			X
RAS17	La placa de desarrollo debe ser de bajo costo			X
RAS18	Capacidad de almacenamiento en la base de datos, para el registro de las mediciones de temperatura		X	
RAS19	El dispositivo debe contar con un sensor de temperatura en el rango de 25 a 65 grados centígrados			X
RAS20	El sensor de temperatura debe ser de alta precisión	X		
RAS21	El tiempo de respuesta del sensor de temperatura debe ser alto	X		
RAS22	La fiabilidad y escalabilidad del sensor de temperatura debe ser alto			X
RAS23	El dispositivo debe contar con un sensor magnético para detectar el ingreso al nodo			X
RAS24	El módulo para la comunicación debe ser de	X		

	gran cobertura			
RAS25	El sistema debe contar con un relé como actuador para el reinicio remoto	X		
RAS26	El dispositivo debe contar con un sistema de enfriamiento	X		
	Requerimientos Eléctricos			
RAS27	Alimentación a través de una fuente de 5v DC	X		
RAS28	Voltaje de operación del sensor de temperatura de 5VDC		X	
RAS29	Voltaje de operación del sensor magnético de 5VDC		X	
RAS30	Alimentación conectada a sistema de respaldo de energía en caso de cortes eléctricos	X		

Fuente: Autoría

3.9. Alcance de la investigación

El sistema SCYNODE es un sistema de monitoreo y reinicio remoto de la OLT-Caranqui de la Empresa SAITEL, tiene la finalidad de acortar tiempos en el restablecimiento del servicio ante la aparición de eventos repentinos de infraestructura detectados por el departamento de soporte técnico de la empresa.

3.9.1. Restricciones

a) Únicamente está diseñado para el monitoreo del nodo OLT-Caranqui únicamente.
b) El desarrollador es el único que puede configurar y dar mantenimiento al sistema.
c) La comunicación del sistema de ser inalámbrica.
d) La comunicación no debe estar sujeta a la red del nodo, debe estar en otra red.
e) El sistema debe estar conectado a un respaldo de energía eléctrica en caso de fallas por parte de la empresa eléctrica.

3.9.2. Riesgos

a) Pérdida de conexión para el envío de información.
b) Caducidad de licencia de servidores de computación en la nube.

3.10. Elección del hardware y software

Para la elección del hardware y software se hará un análisis comparativo entre diferentes elementos con la finalidad de seleccionar los óptimos para la consecución de los objetivos planteados en el proyecto, por ende, un funcionamiento óptimo del sistema. Se tomará en cuenta las características técnicas según los datasheets de los diferentes sensores y placas de desarrollo integrando también los requerimientos de usuario, del sistema y de arquitectura con la finalidad de evaluar cada uno de ellos, así se usará los dispositivos y plataformas adecuadas.

Se colocará la valoración respectiva en base a los requerimientos tomando el valor de "1" para señalar que, si se cumple con el requerimiento y "0" para indicar que no cumple, así como se muestra en la Tabla 9.

Tabla 9

Asignación de valores de cumplimiento

Descripción	Valor
Si cumple	1
No cumple	0

Fuente: *Autoría*

3.10.1. Elección del Hardware de procesamiento

Se detalla un listado de placas de desarrollo a usar: Raspberry Pi, Arduino UNO, NodeMCU, además se muestra los requerimientos de hardware que forman parte de los requerimientos de arquitectura, de sistema y usuario, a su vez, los criterios de evaluación de rendimiento y procesamiento, se analizan los requerimientos luego se asigna los valores de cero y uno según corresponda para así obtener la mejor opción, así como se muestra en la Tabla 10.

Tabla 10.

Selección de la placa de desarrollo

Placa	Requerimiento							Total
	RSH 14	RAS 1	RAS 2	RAS 6	RAS 16	RAS 17	RAS 27	
Arduino UNO	1	1	1	1	1	1	1	7
NodeMcu	1	1	1	1	1	1	0	6
Raspberry PI	0	1	1	1	0	0	0	3
1 cumple								

0 no cumple
Elección Arduino UNO

Fuente: *Autoría*

De acuerdo a la Tabla 10 y en base a los requerimientos se selecciona Arduino UNO por su compatibilidad con los sensores, es de código abierto, es pequeño y pese a que no tiene un módulo de comunicación inalámbrica integrado, se puede adaptar un dispositivo para la comunicación y el envío de información; en este caso se ha escogido integrar el módulo de Arduino Uno con un procesador Atmega328P, debido a los requerimientos del sistema, entre uno de los que se puso a consideración es su precio y tamaño, así como la capacidad de entrada de datos analógicos y digitales que serán enviados desde el sensor de temperatura y sensor magnético siendo la placa de desarrollo que más se ajusta con los requerimientos del proyecto.

3.10.2. Elección del sensor de temperatura

Para realizar el análisis entre sensores de temperatura, es necesario comparar dispositivos que tengan las mismas características, tomando en cuenta una el costo y tamaño de las carcasas, cumpliendo los requerimientos planteados.

Para efectos del caso, se realiza la comparativa entre sensores de la familia DHT: 11, 21 y 22; En la Tabla 11 se muestra los requerimientos de hardware analizados con las valoraciones de cumplimiento de cero y uno según corresponda.

Tabla 11

Selección del sensor de temperatura

Hardware	**Requerimiento**							**Total**
	RSH 1	RSH 14	RS 11	RAS 19	RAS 20	RAS 21	RAS 22	
DHT11	1	1	1	1	1	1	1	7
DHT21	1	0	1	1	1	1	1	6
DHT22	1	0	1	1	1	1	1	3

1 cumple
0 no cumple
Elección DHT11

Fuente: *Autoría*

Como dispositivo para la toma de la temperatura se utiliza el sensor DTH11, debido a que la precisión de lectura y el tiempo de respuesta tienen una gran fiabilidad y exactitud, por otro lado, trabaja en el rango de temperaturas encontradas en el gabinete, es de bajo costo,

tamaño reducido y cumple con los requerimientos de usuario, requerimientos de sistema y de hardware por lo que es idóneo para el prototipo.

3.10.3. Elección del sensor magnético

Para realizar el análisis entre sensores magnéticos, es necesario comparar dispositivos que tengan las mismas características, tomando en cuenta el costo y tamaño de las carcasas, cumpliendo los requerimientos de planteados. Para efectos del caso, se realiza la comparativa entre los sensores KY003 y MC38 así como se muestra en la Tabla 12.

Tabla 12

Selección del sensor de magnético

Hardware	**Requerimiento**							**Total**
	RSH 10	RSH 14	RS 7	RS 11	RS 18	RAS 23	RAS 29	
KY003	1	1	1	0	1	1	1	6
MC38	1	1	1	1	1	1	1	7

1 cumple
0 no cumple
Elección MC38

Fuente: *Autoría*

Como se aprecia en la Tabla 12 el sensor adecuado para la seguridad del gabinete es el MC38 ya que cuenta con una estructura de fácil montaje en el nodo, además es de espacio reducido, fácil montaje en la puerta de la estructura metálica y las aplicaciones típicas del sensor encajan con los objetivos del proyecto.

3.10.4. Módulo para la comunicación inalámbrica

Para elegir el módulo encargado de la conexión del dispositivo hacia la red de Internet, es necesario tomar en cuenta el requerimiento RS11 que especifica que debe ser un dispositivo pequeño, RSH14 que indica que los datos deben ser mostrados en tiempo real, el requerimiento RS8 que especifica que debe ser tecnología de alta disponibilidad para el envío de datos a través del internet, de igual forma el rango de cobertura debe ser considerable, garantizando que el envío de datos se realice de manera correcta, además el dispositivo a escoger debe ser de código abierto y la disponibilidad de conexión y alcance de la misma, se elabora la Tabla 13 que describe los requerimientos mencionados y la valoración respectiva de si cumple o no con el criterio establecido.

Tabla 13

Selección de la tecnología para la comunicación inalámbrica

Tecnología	Requerimiento						Total
	RSH 11	RSH 14	RS 4	RS 8	RS 16	RAS 27	
Wifi	0	1	1	1	0	1	4
Ethernet	0	1	1	1	0	1	4
GPRS	1	1	1	1	1	1	6
1 cumple							
0 no cumple							
Elección GPRS							

Fuente: *Autoría*

Como se observa en la Tabla 13, se selecciona la tecnología GPRS para la comunicación entre el dispositivo y el Internet, en vista que, cumple con los requerimientos de disponibilidad de acceso a la red celular por su amplia cobertura en la ciudad de Ibarra, esta red permitirá la conexión con diferentes plataformas y proporciona estabilidad al momento de enviar los datos a los servidores y de esa misma forma efectuar la activación de un actuador para lograr el reinicio remoto del nodo.

El dispositivo acoplado al módulo de transmisión de datos es el SIM808 de la empresa SIMCOM y se lo selecciona, ya que, es compatible con la placa de Arduino. Este dispositivo permite la conexión con la red móvil celular, ventaja enorme que permite tener alta disponibilidad de conexión del dispositivo con el Internet, con lo cual se puede realizar el envío de la información a la nube en tiempo real con el único requerimiento de que haya señal telefónica celular, además de enviar SMS, por ende, se lo selecciona como placa para la comunicación inalámbrica.

3.10.5. Elección del software gestor de base de datos

Luego de la toma de datos, es necesario enviar los mismos a una plataforma para luego poder acceder a la información de forma segura y rápida, por ende, los datos deben estar organizados, disponibles para la apreciación de resultados y deben ser precisos con la finalidad de la toma de decisiones, en este caso la activación del sistema de enfriamiento.

Para la selección del gestor de base de datos se toma en cuenta los requerimientos mostrados en la Tabla 14 que hacen referencia al almacenamiento de datos, se requiere que el

acceso a la información sea eficiente, los datos deben ser presentados de forma remota y la capacidad de almacenamiento.

En este módulo se va a proceder con el almacenamiento de la información que previamente fue procesada en el módulo central, en la base de datos se asignará etiquetas para la identificación de los valores almacenados, las etiquetas corresponderán a la siguiente información: horario de acceso a los gabinetes de equipos y temperatura.

Tabla 14

Selección del software para la base de datos

BDD	**Requerimiento**				**Total**
	RSH 2	RS 2	RS 4	RS 10	
MySQL	1	1	1	1	4
PostgreSQL	1	1	1	1	4
dBase	1	1	1	1	4
1 cumple					
0 no cumple					
Elección MySQL					

Fuente: *Autoría*

Como se observa en la Tabla 14, las tres plataformas analizadas cumplen con los requerimientos de usuario para la selección del software de base de datos dependiendo de la instancia donde se encuentren almacenadas, pero en este caso se selecciona MySQL para tener una interfaz gráfica mucho más personalizada según criterios de diseño del administrador, información que será almacenada en la nube en una plataforma de cloud computing con la finalidad de acceder a la información.

El sistema gestor de base de datos (SGBD) permitirá administrar y gestionar la información recibida desde el módulo central.

Como sistema gestor de base de datos se escoge MySQL de Oracle, una de las razones principales por la cual se escogió este sistema es porque brinda un entorno de trabajo de código abierto y desarrollo web, además que este gestor puede manejarse desde distintos sistemas operativos.

Al ser un software de desarrollo con código abierto es posible hacer cambios dentro del código fuente y ajustarlo de acuerdo a las necesidades que se vayan presentando. Las etiquetas

creadas se pueden archivar de manera separada en lugar de colocar todas en un solo lugar, permitiendo así tener velocidad y flexibilidad ya que las tablas se encuentran anexadas con etiquetas definidas, logrando una combinación de datos de diferentes etiquetas de acuerdo a los requerimientos.

3.10.6. Elección de la plataforma de almacenamiento en la nube (Virtualización)

La plataforma de almacenamiento en la nube debe cumplir ciertas características ya que es el elemento central de administración al momento de presentar la información al usuario la cual debe ser eficiente permitiendo tener una instancia de forma virtual con la finalidad que el administrador de red pueda acceder a los recursos almacenados de forma remota, para ello se realiza una comparativa entre diferentes opciones tomando en cuenta los requerimientos: el usuario debe tener acceso remoto a la información, el dispositivo debe permitir el reinicio remoto del nodo, la disponibilidad debe ser alta, el envío y recepción de datos mediante el protocolo HTTP y la información debe ser presentada en un servidor web, estos requerimientos son mostrados en la Tabla 15.

Tabla 15

Selección de la plataforma de virtualización en la nube

Plataforma	**Requerimiento**					**Total**
	RSH 4	RSH 5	RSH 7	RS 4	RS 13	
AWS	1	1	1	1	1	6
Azure	1	1	1	1	0	5
Linode	1	1	1	1	0	5

1 cumple
0 no cumple
Elección AWS

Fuente: *Autoría*

Tomando en cuenta las prestaciones de Amazon Web Services y por la facilidad de uso se escogió esta plataforma como alojamiento del servidor central. Este servicio combina una matriz de herramientas increíblemente diversa, esto incluye bases de datos, alojamiento de servicios más conocidos como instancias, dispositivos móviles y análisis de redes. Otro de los factores clave por los cuales se escogió AWS es su increíble seguridad y capacidad para mantener a salvo la información.

3.10.7. Elección del sistema operativo donde se instalará el servidor web

La plataforma para el servidor WEB debe ser de código abierto y debe presentar una interfaz gráfica interactiva para el usuario y de fácil manejo, además que debe ser personalizada según los requerimientos de la empresa SAITEL, en este caso, no se utilizará plataformas establecidas en el mercado si no que, se implementará un servidor central mismo que será cargado en una instancia de AWS para acceder a los recursos e información almacenados en este servidor, con ello se obtiene realizar una interfaz gráfica de usuario interactiva de acuerdo con siguientes requerimientos: disponibilidad que debe tener el servidor, las alertas que deben ser apreciadas en la interfaz gráfica, el reinicio remoto del nodo, las notificaciones que deben ser generadas desde el sistema y deben ser visualizadas en la plataforma web y la seguridad de acceso al sistema mediante credenciales de autenticación de usuario mostrados en la Tabla 16.

Tabla 16

Selección del sistema operativo para el servidor WEB

Sistema operative	**Requerimiento**					**Total**
	RSH	RSH	RS	RS	RAS	
	7	12	2	17	4	
Ubuntu	1	1	1	1	1	5
Centos	1	0	1	1	1	4
Fedora	1	0	1	1	1	4
1 cumple						
0 no cumple						
Elección Ubuntu						

Fuente: *Autoría*

Se selecciona el sistema operativo Ubuntu, ya que, como se observa en la Tabla 16 cumple con los requerimientos establecidos, además de presentar una interfaz gráfica para el usuario, requiere poco espacio de memoria y se puede cargar con facilidad a la plataforma de AWS generando una instancia de la cual se puede acceder a sus recursos para la visualización de información, generación de alertas y envío del mensaje de reinicio.

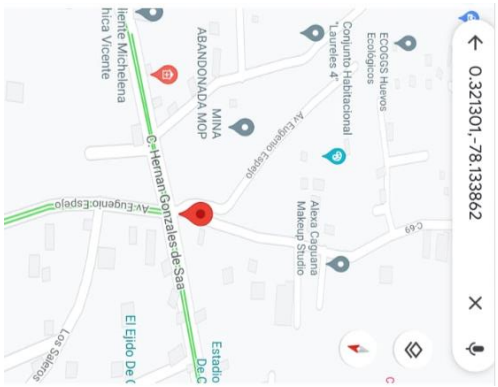
3.11. Diseño del sistema

De acuerdo con la adopción del modelo iterativo, se propone el desarrollo de este proyecto en fases con un proceso de retroalimentación a medida que asciende en cada nivel. Como primer paso de la primera iteración se realizó un análisis de los niveles de temperatura en el gabinete de instrumentos, el cual se realizó como procedimiento previo al diseño y pruebas del SCYNODE. La recolección de información se lo realiza tomando en cuenta las

estaciones climáticas del año, especialmente en aquellas épocas con mayores índices de radiación que de acuerdo a las recomendaciones de la investigación realizada por Varela y Ron (2020) en Ibarra específicamente, en el mes de julio hay los mayores índices de radiación solar, es por ello que se usa un período de tres semanas en el mes de abril de 2022, de esta manera se puede calcular una media aritmética en relación con los picos de temperatura a los cuales se encuentran sometidos los dispositivos ubicados dentro de las salas de equipos. La toma de muestras se realizó en el gabinete de equipos del nodo OLT-Caranqui perteneciente a la empresa SAITEL Matriz Ibarra ubicado en las calles Hernán Gonzáles de Saa y Avenida Eugenio Espejo. En la Figura 13 se puede observar la geolocalización del nodo.

Figura 13

Ubicación geográfica del nodo OLT Caranqui



Fuente: *Autoría*

El SCYNODE es un sistema orientado a incorporar seguridad a nivel físico para la infraestructura de red ubicada en el nodo OLT-Caranqui tomando en cuenta dos factores de vulnerabilidad tales como fallas en el funcionamiento de los equipos a altas temperaturas y violación de acceso a los gabinetes por parte de personas no autorizadas por la empresa, es por ello que, se pueden identificar dos etapas de acción en sistema propuesto que son: la identificación de la vulnerabilidad y la respuesta por parte del personal técnico de la empresa y de los elementos de seguridad integrados al dispositivo.

En la etapa de identificación de la vulnerabilidad, tomando en cuenta las variaciones en los índices de temperatura dentro de los gabinetes de equipos, se procederá con un monitoreo constante de los valores de temperatura, mientras que, para el caso de vulnerabilidad por acceso no autorizado, el sistema contará con un módulo de autorización de acceso. Esta información será enviada mediante UART al módulo de procesamiento de datos para después aplicar los

protocolos que se establezcan para cada tipo de vulnerabilidad. La información recopilada se almacenará en una base de datos ubicada en la nube.

Otra característica que debe cumplir el sistema SCYNODE es la capacidad de proporcionar reinicios remotos de los equipos de red por lo que se incorpora en su diseño un servidor web que permitirá el control y monitoreo del sistema en el que se incluye el registro de los valores de temperatura de los gabinetes de equipos y el número de accesos que se han realizado, a estos registros solamente se brindó acceso a personal autorizado por la empresa SAITEL.

3.11.1. Arquitectura del sistema

La arquitectura del sistema propuesto se desarrolla en base a un entorno modular que pueda adaptarse a la metodología iterativa y que brinde la facilidad necesaria para identificar características, necesidades y resolver futuros problemas de desarrollo e implementación. Con esta premisa se pueden identificar los siguientes módulos como componentes del sistema propuesto:

1. Módulo de toma de datos: Módulo dedicado al censado de apertura (contacto magnético) de puerta de gabinete y temperatura (DHT11) dentro del mismo, donde se encuentra la OLT. Datos que serán procesados por el módulo central de acuerdo con los parámetros establecidos en el diseño de SCYNODE.
2. Módulo central: Módulo principal dedicado a la recepción, almacenamiento y procesamiento de datos. El módulo central controlará actuadores en base al diseño definido. Esta parte del módulo también es la encargada de tener una comunicación bidireccional con el servidor WEB colocado en la plataforma AMAZON para que mediante esta pueda existir una interacción (apagado/encendido) con el módulo de alimentación del nodo a monitorear.
3. Módulo de base de datos: Módulo perteneciente a parte del software colocado en la plataforma AWS que permite mediante la comunicación HTTP con el módulo central almacenar datos que fueron ya recibidos y procesados.
4. Módulo de seguridad: Módulo que es parte del software AWS con procesamiento en la nube que notifica si los parámetros censados tienen alguna novedad como puede ser la temperatura o apertura de gabinete por algún concepto.
5. Módulo servidor web: Este módulo de servicio WEB que, para efectos del mismo, fue colocado en una instancia (Ubuntu 16.04) en la plataforma AMAZON AWS que es la

encargada de ser una interfaz que ayude a visualizar datos ya almacenados y también por la misma interfaz poder controlar (apagado/encendido) y poder evidenciar temperatura y apertura del gabinete con sus respectivas horas y fechas.

6. Módulo de alimentación (El funcionamiento integral de todos los módulos del SCYNODE está ligado al módulo eléctrico): Módulo de interacción que permite controlar el encendido/apagado de la OLT y otros equipos conectados al mismo en base al procesamiento y parámetros establecidos en el diseño.

En la Figura 14 se observa mediante un diagrama de bloques la arquitectura y proceso de funcionamiento del sistema propuesto.

Figura 14

Arquitectura del SCYNODE

Fuente: *Autoría*

La arquitectura del SCYNODE depende principalmente del censo y extracción de datos para que el módulo central pueda tratarlos y realizar procesos de actuación de elementos (ventilador interno del gabinete) según el diseño establecido. Con todo ello y posteriormente puedan ser almacenados en una base de datos colocada en la nube para un nuevo tratamiento, visualización de los mismos y si es el caso control del módulo eléctrico (apagado/encendido) para un eventual restablecimiento de equipos.

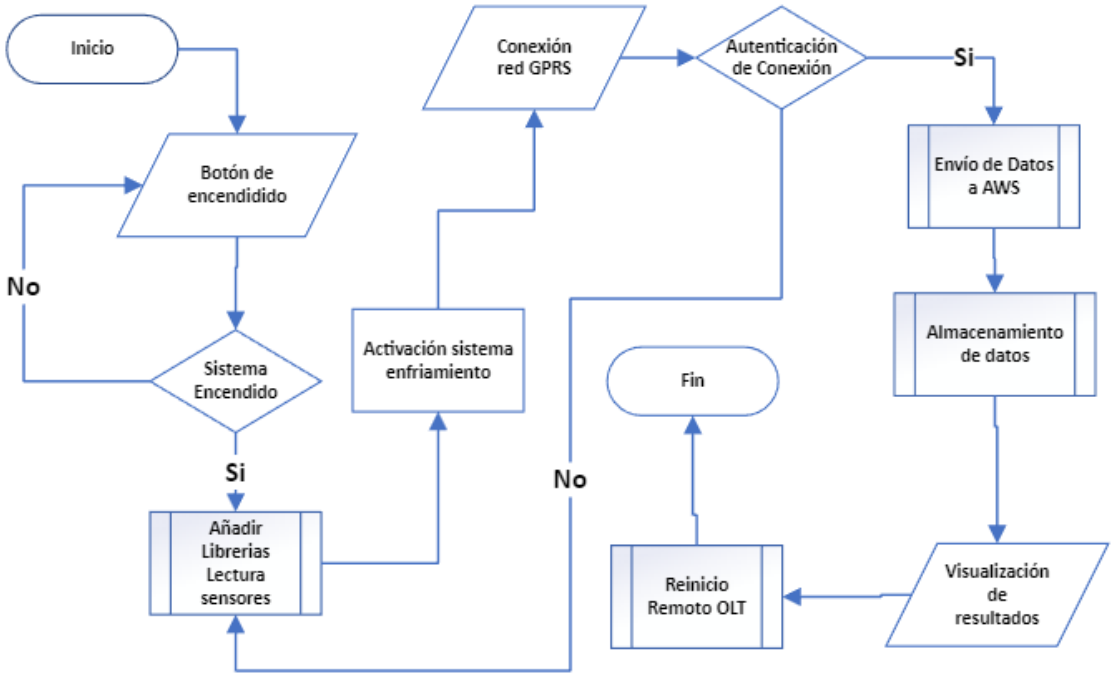
3.1.1. Diagrama de flujo del sistema

En la Figura 15 se muestra los procesos que el sistema debe seguir para lograr los objetivos planteados acorde con el funcionamiento de este, es decir, las acciones que el sistema SCYNODE presenta en determinados momentos durante su tiempo de operación. El sistema inicia con el botón de encendido, mismo que permite o impide el paso de corriente eléctrica

hacia los elementos; como primer paso se añaden las librerías de los sensores y del módulo GSM/GPRS, después de este proceso el sistema ya podrá conectarse a la red GPRS según se encuentre establecido en el criterio de programación del dispositivo, luego se envía información a la plataforma de AWS en donde se encuentra instalada la instancia del servidor web configurado para la presentación de información y base de datos, el usuario autorizado mediante peticiones accede a los recursos de red para visualizar datos y en base a criterios reiniciar remotamente el nodo principal.

Figura 15

Diagrama de flujo del sistema SCYNODE



Fuente: *Autoría*

Como se observa en la Figura 15, el dispositivo funciona siguiendo el diagrama de flujo en donde primero, es interruptor de encendido debe estar activado para que se permita el flujo de corriente eléctrica a los sensores y la placa de desarrollo.

Al haber flujo de corriente eléctrica, el sistema enciende, como siguiente paso la placa de desarrollo carga las librerías de los sensores para proceder a la interpretación de variables físicas, en este caso la temperatura y el ingreso al nodo mediante el sensor magnético, de igual forma se enciende el sistema de ventilación, luego se establece la conexión entre el dispositivo y el internet mediante la red GPRS. Luego los datos son enviados y almacenados en la base de datos; cada vez que el personal de soporte técnico tenga la necesidad de acceder información

referente al nodo con respecto a la temperatura, deberá hacer mediante el servidor WEB alojado en la nube, el personal observa los datos y toma la decisión de reiniciar o no el nodo, activando un actuador que interrumpirá la alimentación de los dispositivos OLT del Nodo en cuestión reiniciarlo o des inhibirlo.

3.2.Diseño por bloques

En este apartado se detallan de manera específica el funcionamiento de cada uno de los bloques que conforman el sistema SCYNODE, se muestra el diseño del bloque de adquisición de datos, la base de datos, el servidor Web para la visualización de resultados.

3.2.1. Módulo toma de datos

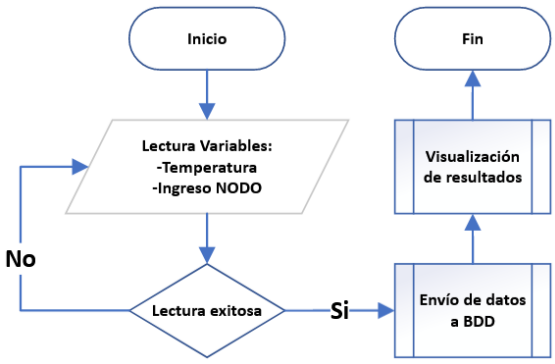
Los datos tomados en el primer módulo son enviados y recibidos en este módulo central, así como también se colecta y se registra la información de los ingresos o aperturas del gabinete de equipos. Esta información una vez tratada se enviará al módulo de base de datos. Los dispositivos involucrados en el módulo central son: una placa de Arduino encargada del tratamiento de la información y un módulo GSM/GPRS que permitirá la salida a internet.

La conexión entre el módulo de toma de datos y el módulo central es cableada ya que el sensor DHT11 es un componente de entrada analógica y necesita de un medio guiado para la entrega de información en forma de variaciones de voltaje. En primera instancia, el sistema mediante el sensor DHT 11 mide los parámetros de temperatura del gabinete donde se encuentran los equipos OLT del nodo en cuestión para formar una base de datos robusta y tener un registro de los mismos, así como también, mediante el sensor magnético, se tendrá un registro del acceso al nodo.

En la Figura 16 se muestra el diagrama de flujo del bloque de lectura de datos.

Figura 16

Diagrama de flujo boque de sensores



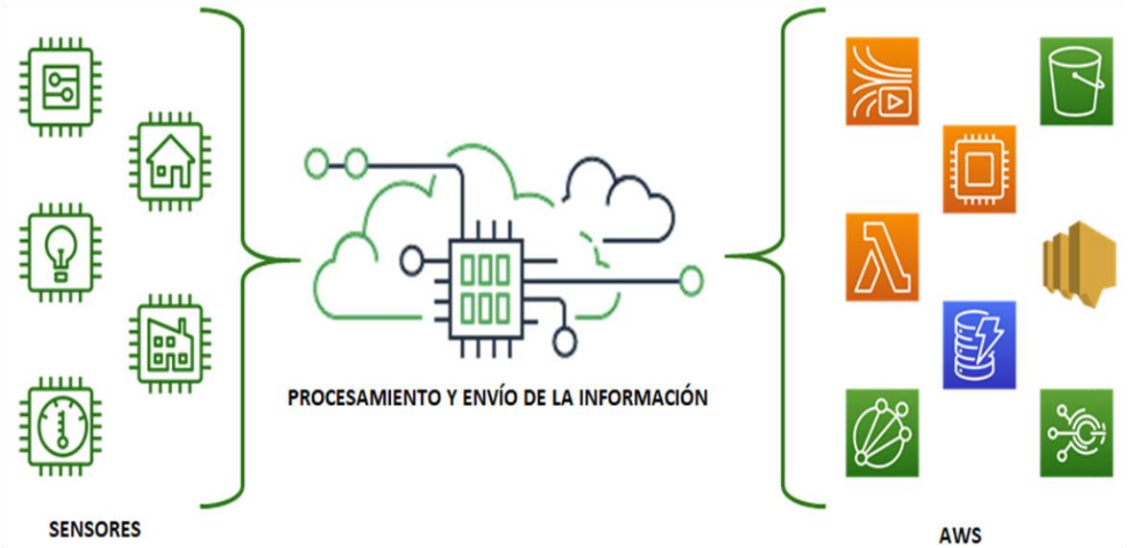
Fuente: *Autoría*

Una vez los datos tomados del sensor de temperatura y del control de acceso sean obtenidos y pasaron por el proceso de discriminación en Arduino son enviados al servidor de base de datos alojado como una instancia en AWS, la transmisión se la realiza utilizando el protocolo HTTP, esta conexión entre los sensores y el internet es posible gracias al módulo GSM/GPRS SIM808.

En la Figura 17 se observa el esquema de funcionamiento general de la transmisión de la información a AWS.

Figura 17

Esquema general de la transmisión de datos de sensores al Amazon Web Services



Fuente*: (AWS, 2021)*

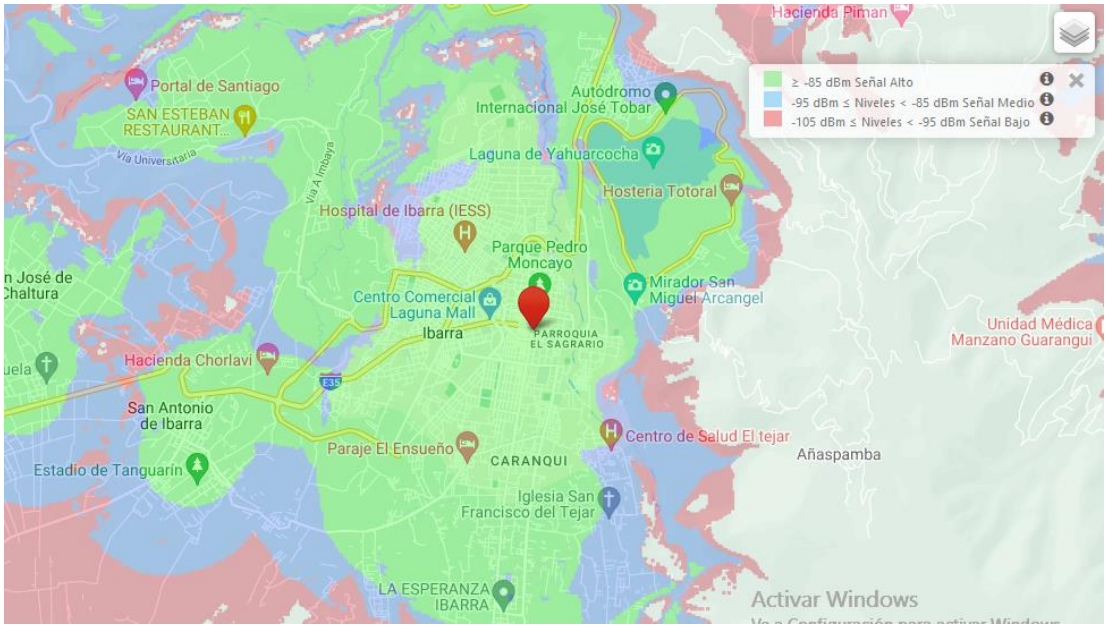
- **Selección de la operadora móvil**

Para que el módulo GSM, se conecte a la red, requiere de un chip, mismo que debe estar registrado en la operadora móvil que brinda el servicio a los usuarios; debido a que la empresa SAITEL, trabaja con la Operadora Claro a nivel nacional, se selecciona la misma como operadora móvil para el funcionamiento del proyecto. Claro trabaja usando las tecnologías de 2G, 3G y 4G en la ciudad de Ibarra.

En la Figura 18 se aprecia la cobertura 2 G que tiene claro en la ciudad de Ibarra para los sectores de Caranqui, La Esperanza, Yahuarcocha, Chaltura, San Antonio, La Esperanza, entre otros, en donde se aprecian tres colores: Verde en donde tiene un nivel de señal alto, celeste representa un nivel medio de señal y rojo un nivel bajo de cobertura.

Figura 18.

Mapa Cobertura 2G Claro

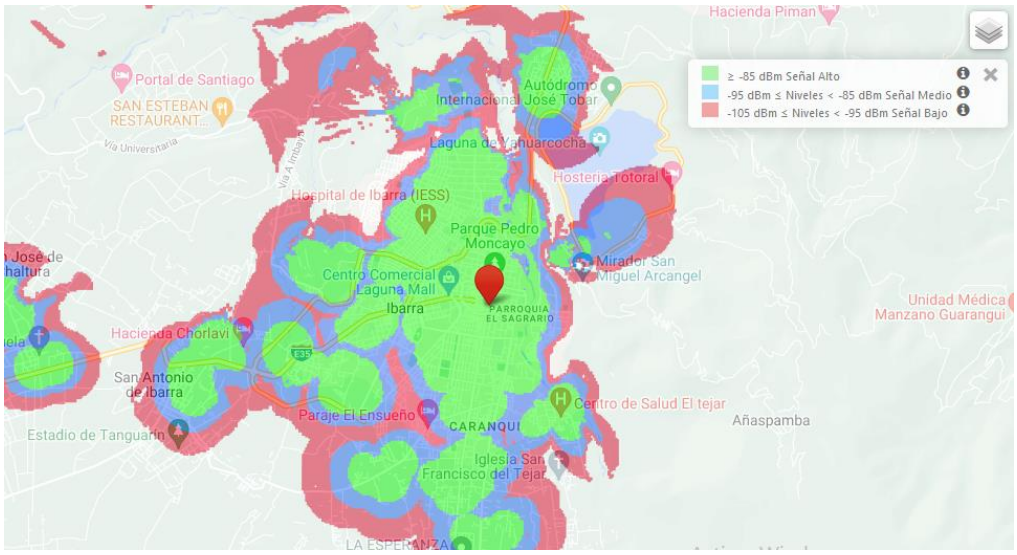


Fuente: *(Claro, 2022)*

En la Figura 19 se muestra el mapa de cobertura 3G de la operadora claro, en donde el color verde representa una intensidad alta de la señal específicamente en los sectores de Caranqui y Centro de Ibarra, color celeste con intensidad media de la señal en los alrededores de la ciudad y color rojo una intensidad baja de señal en los sectores más alejados.

Figura 19

Mapa Cobertura 3G Claro

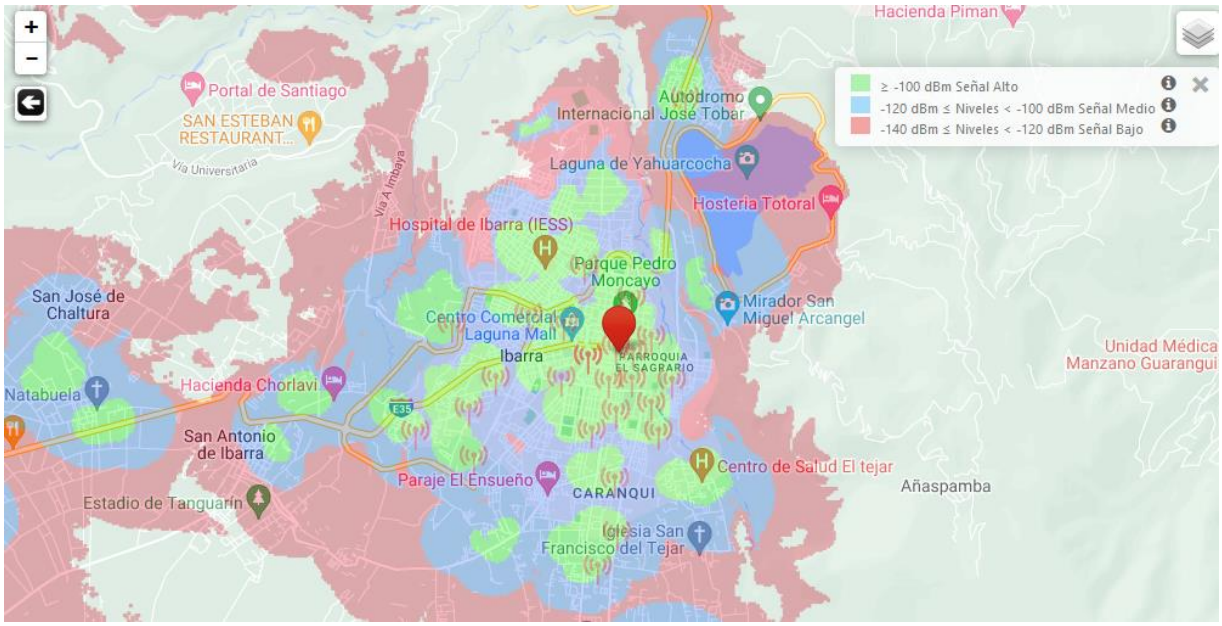


Fuente: *(Claro, 2022)*

En la Figura 20 se muestra el mapa de cobertura 4G de la operadora Claro en donde se aprecia de color verde los lugares con un nivel alto de señal en este caso sectores específicos del centro de la ciudad, color celeste con un nivel medio de intensidad de señal en este caso sectores Caranqui, Parque Pedro Moncayo y de color rojo los sectores con baja intensidad de señal en este caso alrededores de la ciudad.

Figura 20

Cobertura 4G Claro



Fuente: *(Claro, 2022)*

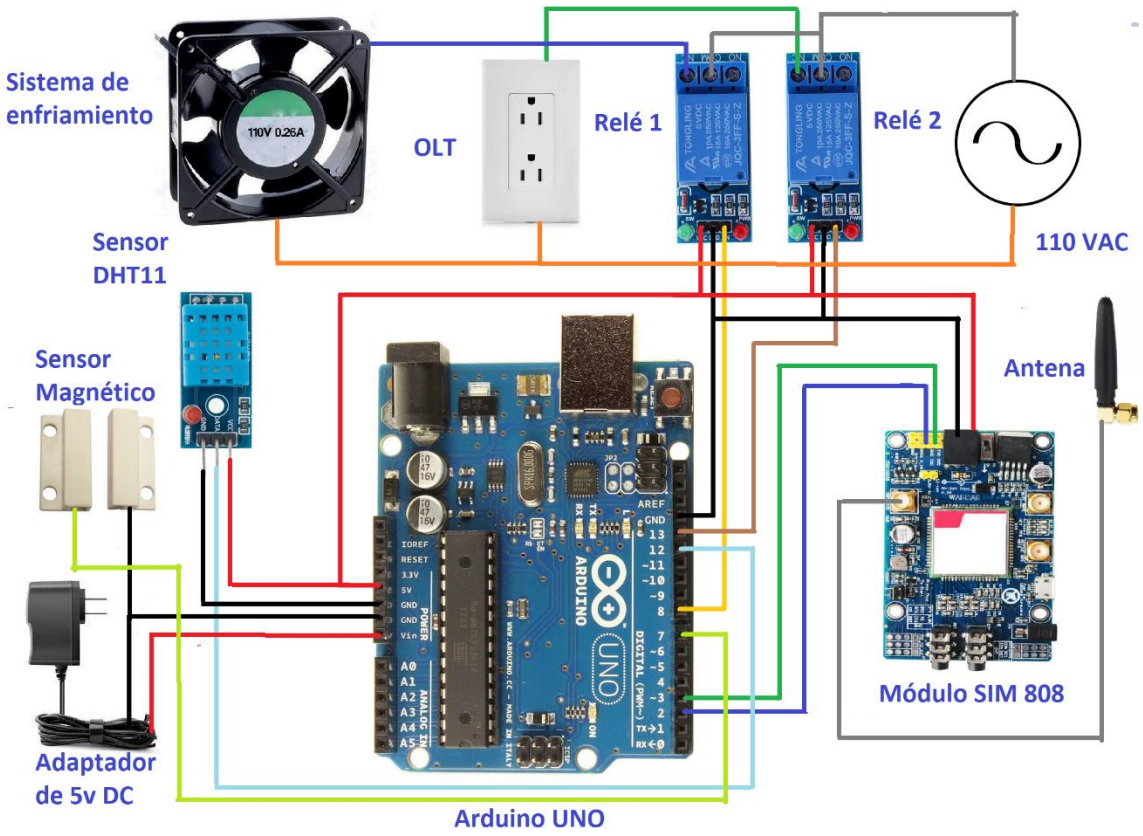
3.2.2. Módulo Central

En el diagrama de la Figura 21 se observa la interconexión de dispositivos que conforman el módulo central, ilustrando el intercambio de información entre ellos. El sensor de temperatura está conectado a los pines análogos de Arduino.

El módulo GSM/GPRS permitirá al SCYNODE tener una conexión a internet vía GPRS, este dispositivo se configura a través de los puertos UART utilizando instrucciones AT sencillas.

Figura 21

Diagrama de conexión de los dispositivos del módulo central del SCYNODE



Fuente: *Autoría*

3.2.3. Codificación placa de desarrollo

En este apartado se inicia con el proceso de programación de los módulos que integran el software, siendo estos: módulo central, base de datos, seguridad, servidor web.

El módulo central realizará el acoplamiento entre Arduino, el sensor de temperatura y el dispositivo de reinicio automático.

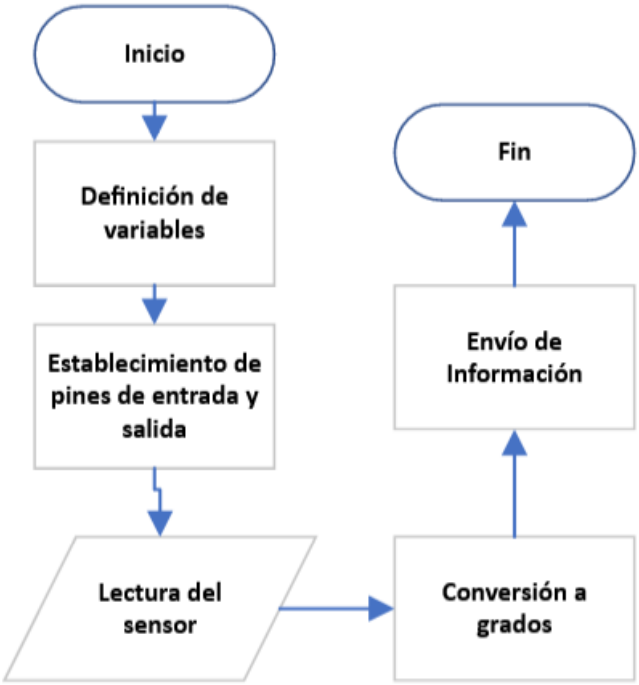
Cuando se lee un sensor analógico con Arduino se lo realiza utilizando el comando analogRead con lo que se obtiene como resultado un valor entre 0 y 1023, es decir cuando haya cero voltios devolverá 0 y si se obtiene un valor de 5 voltios Arduino devolverá un valor de 1023 (Hernández, 2019).

El diagrama de flujo de la Figura 22 ilustra el proceso a realizarse en el módulo central dentro de la primera iteración. Como parte de la primera iteración los datos obtenidos del sensor

de temperatura serán enviados para ser registrados en un archivo, con estos datos posteriormente se realizará un análisis e integrarán dispositivos o cambios.

Figura 22

Diagrama de flujo para el módulo central en la primera iteración para el SCYNODE



Fuente: *Autoría*

En la Figura 23 se puede observar parte del código de programación del módulo central, mientras que en el Anexo 3 se encuentra el código en su totalidad.

Figura 23

Líneas de código de la programación del módulo central-primera iteración, declaración de variables, inicialización de puertos

```
// Declaracion de variables globales
float tempC; // Variable para almacenar el valor obtenido del sensor (0 a 1023)
int pinLM35 = 0; // Variable del pin de entrada del sensor (A0)

void setup() {
  // Cambiamos referencia de las entradas analógicas
  analogReference(INTERNAL);

  // Configuramos el puerto serial a 9600 bps
  Serial.begin(9600);
}

void loop() {
  // Con analogRead leemos el sensor, recuerda que es un valor de 0 a 1023
  tempC = analogRead(pinLM35);

  // Calculamos la temperatura con la fórmula
  tempC = (1.1 * tempC * 100.0)/1024.0;

  // Envia el dato al puerto serial
  Serial.print(tempC);
  // Salto de linea
  Serial.print("\n");

  // Esperamos un tiempo para repetir el loop
  delay(1000);
}
```

Fuente*: Autoría obtenido de código de programación de Arduino para el SCYNODE*

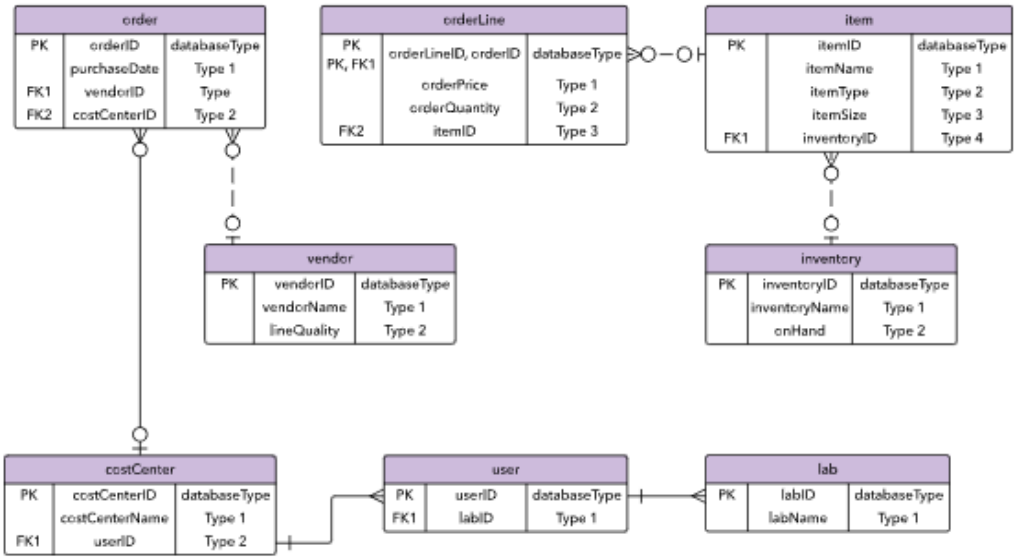
3.2.4. Módulo de base de datos

En esta sección se presenta el diseño y estructura de la base de datos del SCYNODE. Esta base de datos se diseña basándose en el modelo de BDD relacional en donde, en tablas compuestas de columnas y filas se ordenarán los datos, estos se identificarán mediante etiquetas como fecha, temperatura, acceso, entre otros.

Con este modelo es posible crear relaciones entre tablas, que pueden ser uno a uno o uno a muchos (Cánovas Izquierdo, Díaz , Puente, & García Molina, 2011). En la Figura 24 se observa la estructura general de una base de datos relacional.

Figura 24

Diagrama entidad-relación del modelo de base de datos relacional



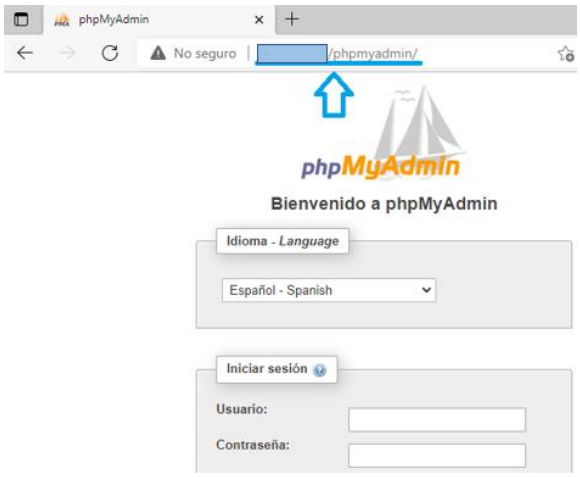
Fuente: *(Cánovas Izquierdo, Díaz , Puente, & García Molina, 2011)*

La base de datos se alojará como una instancia dentro de Amazon Web Services y para la programación de esta se utilizará MySQL en modo gráfico con la plataforma phpMyAdmin. En el Apéndice B se detalla la creación de una instancia en AWS.

La estructura de la base de datos tiene como inicio la dirección IP asignada para el ingreso siendo la siguiente: x.xx.xxx.xx/phpmyadmin, como se puede observar en la Figura 25.

Figura 25

Dirección IP otorgada por AWS para el acceso a la BDD

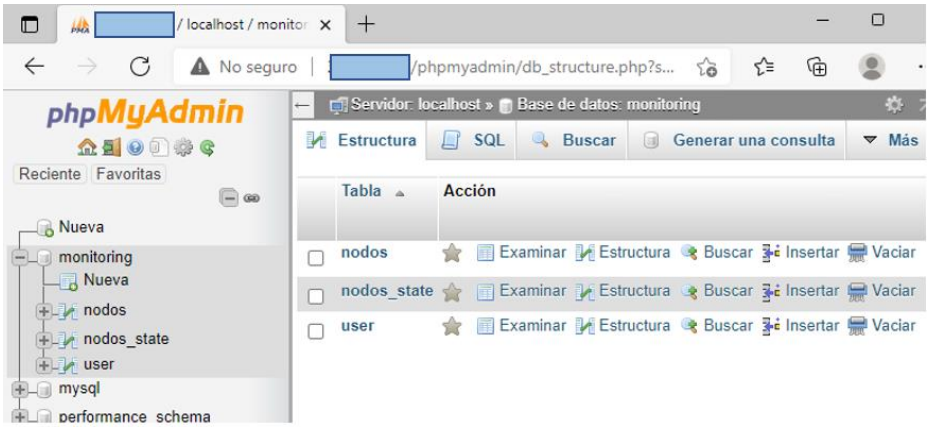


Fuente: *Autoría, Módulo BDD del SCYNODE*

A continuación, en la Figura 26 se presenta la estructura de la BDD, el nombre de la base de datos es monitoring, y cuenta con tres tablas que se detallarán secuencialmente.

Figura 26

BDD monitoring y tablas creadas en la base de datos del SCYNODE



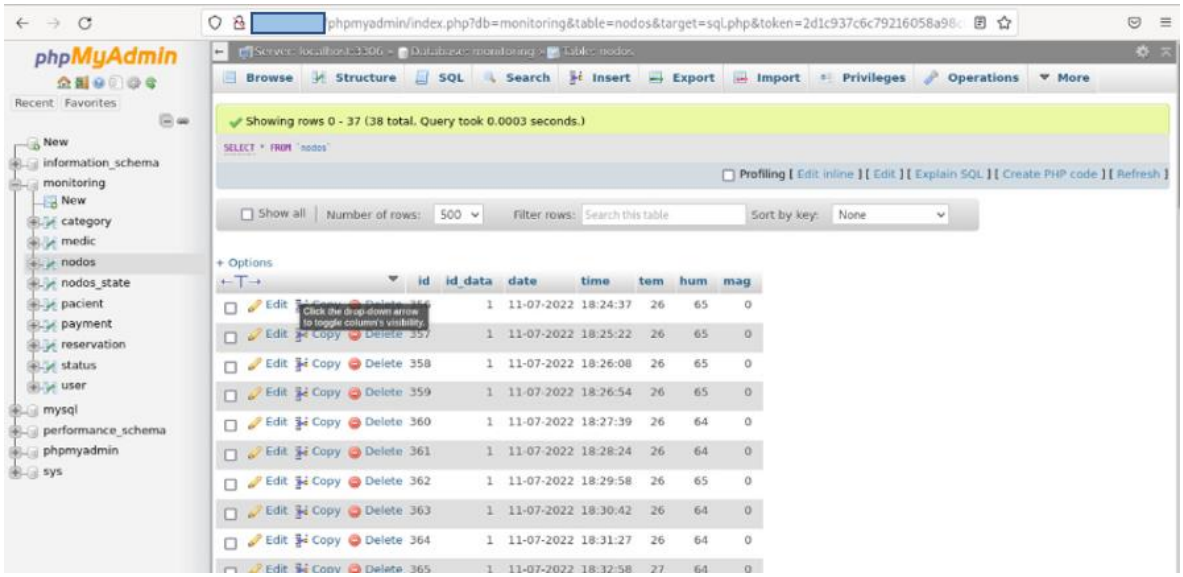
Fuente: *BDD del SCYNODE*

La Tabla “nodos” fue creada para el registro de los nodos que se van a monitorear, como plan piloto es el nodo OLT-Caranqui perteneciente a la empresa SAITEL. En esta tabla además de los nodos se verá ciertos indicadores del gabinete de equipos, como lo son la temperatura, fecha, hora y un número de identificación.

El indicador de humedad se integró a la BDD porque en un futuro fuera de este proyecto puede ser necesario medir ese parámetro, esta Tabla se ilustra en la Figura 27.

Figura 27

Tabla "nodos" de la BDD del SCYNODE



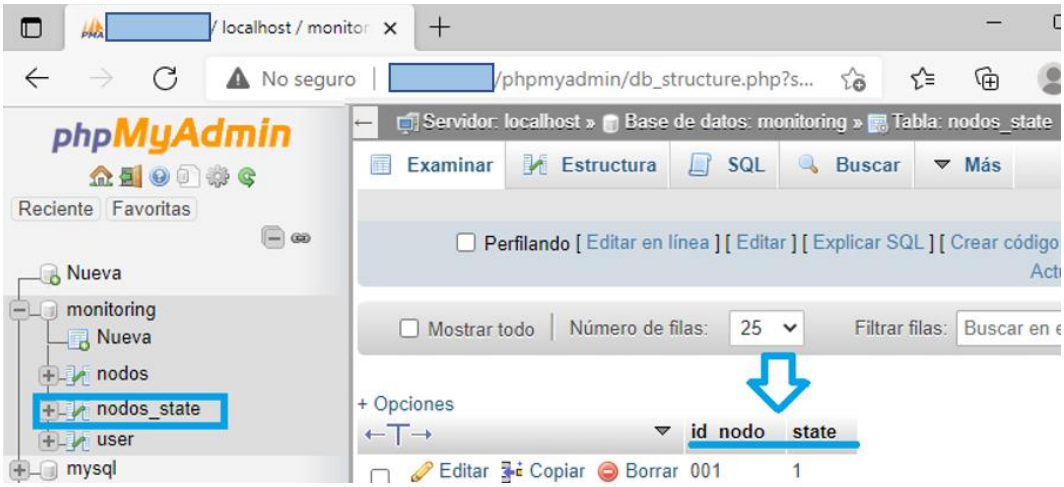
Fuente: *BDD del SCYNODE*

En la tabla “nodos_state” se almacenará el estado de los nodos, estos se los puede identificar por el id_nodo que se les asigna al momento de su registro en la base de datos, además en la columna state se usa el número uno para indicar que la OLT del nodo está encendida y cero para el caso contrario, como se observa en la Figura 28.

Esta tabla es importante para el reinicio remoto de la OLT, ya que, mediante esta información el nodo puede ser reiniciado mediante la activación del actuador lo que permitirá el paso o corte de la corriente que circula a través de la OLT reiniciándola y a su vez levantando el servicio de internet de los abonados.

Figura 28

Tabla "nodos_state" de la BDD del SCYNODE

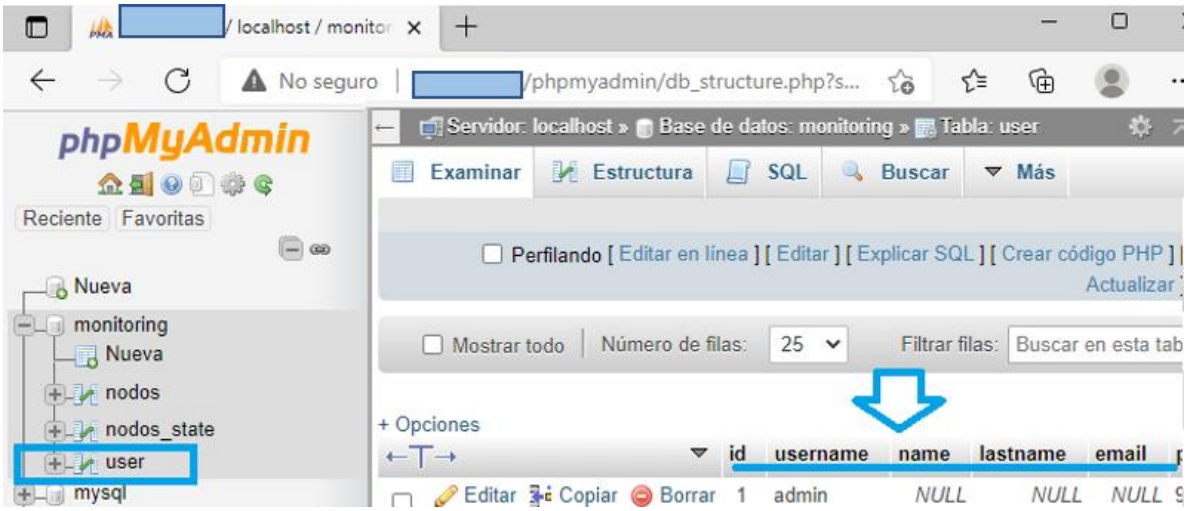


Fuente: *BDD del SCYNODE*

La Tabla “user” se utiliza para el almacenamiento de usuarios que pueden tener acceso a la información, estos usuarios solamente podrán ser creados por la cuenta del administrador. Entre la información de usuario se tiene: nombre, correo y número de identificación. La Figura 29 muestra el contenido de la tabla “user”.

Figura 29

Tabla "user" de la BDD del SCYNODE



Fuente: *BDD del SCYNODE*

El dimensionamiento de la base de datos permite conocer de una manera estimada la cantidad de espacio que ocuparán los datos en la BDD, además de su costo de almacenamiento en el servicio web de Amazon.

3.2.5. Módulo de seguridad

El módulo de seguridad se encargará del control y monitoreo de los niveles de temperatura en el gabinete de equipos, el reinicio remoto de la OLT-Caranqui y el control de acceso. Aquí se programará el código de Arduino para que se conecte con el módulo GSM/GPRS y se envíen las alertas al personal de la empresa SAITEL encargado de la administración del SCYNODE.

En la Figura 30 se presenta parte del código de programación del módulo de seguridad.

Figura 30

Código de programación del módulo de seguridad del SCYNODE

```
#include <SoftwareSerial.h>
SoftwareSerial SIM900(7, 8); //Seleccionamos los pines 7 como Rx y 8 como Tx

void setup()
{
 SIM900.begin(19200);
 Serial.begin(19200);
 delay(1000);
}

void loop()
{
 //Envíamos y recibimos datos
 if (Serial.available() > 0)
 SIM808.write(Serial.read());
 if (SIM808.available() > 0)
 Serial.write(SIM808.read());
}
```

Fuente: *Código fuente de Arduino para el SCYNODE*

3.2.6. Módulo servidor web (Visualización de resultados)

El propósito de este módulo es la presentación de la información obtenida en el módulo central, dentro de una página web.

La página web contará con algunos servicios para el administrador y usuario de la misma. Entre los servicios está la presentación de información de marketing de la empresa SAITEL, así como el acceso por usuario y contraseña a la información proveniente de la base de datos.

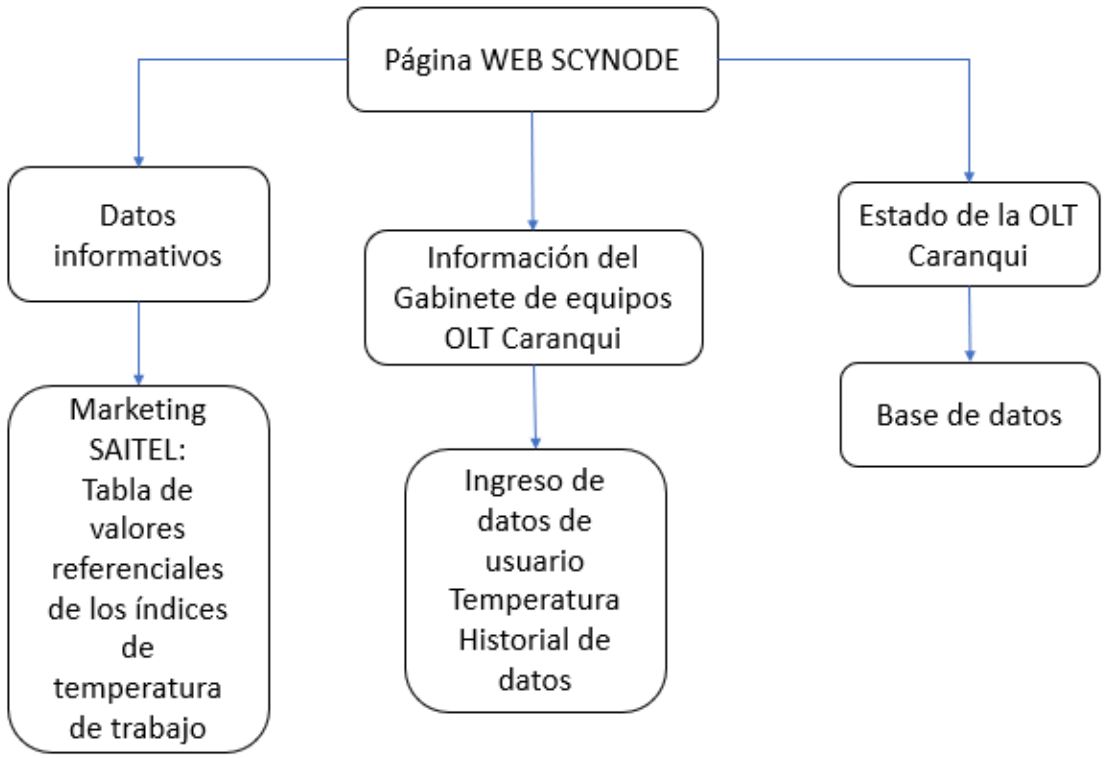
El diseño esquemático de la página web se presenta en la Figura 31, en este esquema se detalla el contenido a mostrar en la página web.

El módulo servidor web está dedicado a la presentación del estado de la OLT-Caranqui, entre la información mostrada está el nivel de temperatura, reinicio de OLT y acceso al gabinete de equipos. La información solamente está disponible para personal autorizado, por lo que es necesario la autenticación de usuarios y contraseñas.

La dirección IP de la página web es la siguiente: http://x.xx.xxx.xx/nodos esta es la dirección IP pública generada en AWS al crear la instancia en donde se alojó el servidor de base de datos y el servidor web. Las funciones y procesos de este módulo se ilustran en el diagrama de flujo de la Figura 31.

Figura 31

Diagrama del contenido de la página web para el diseño del sistema SCYNODE



Fuente: *Autoría*

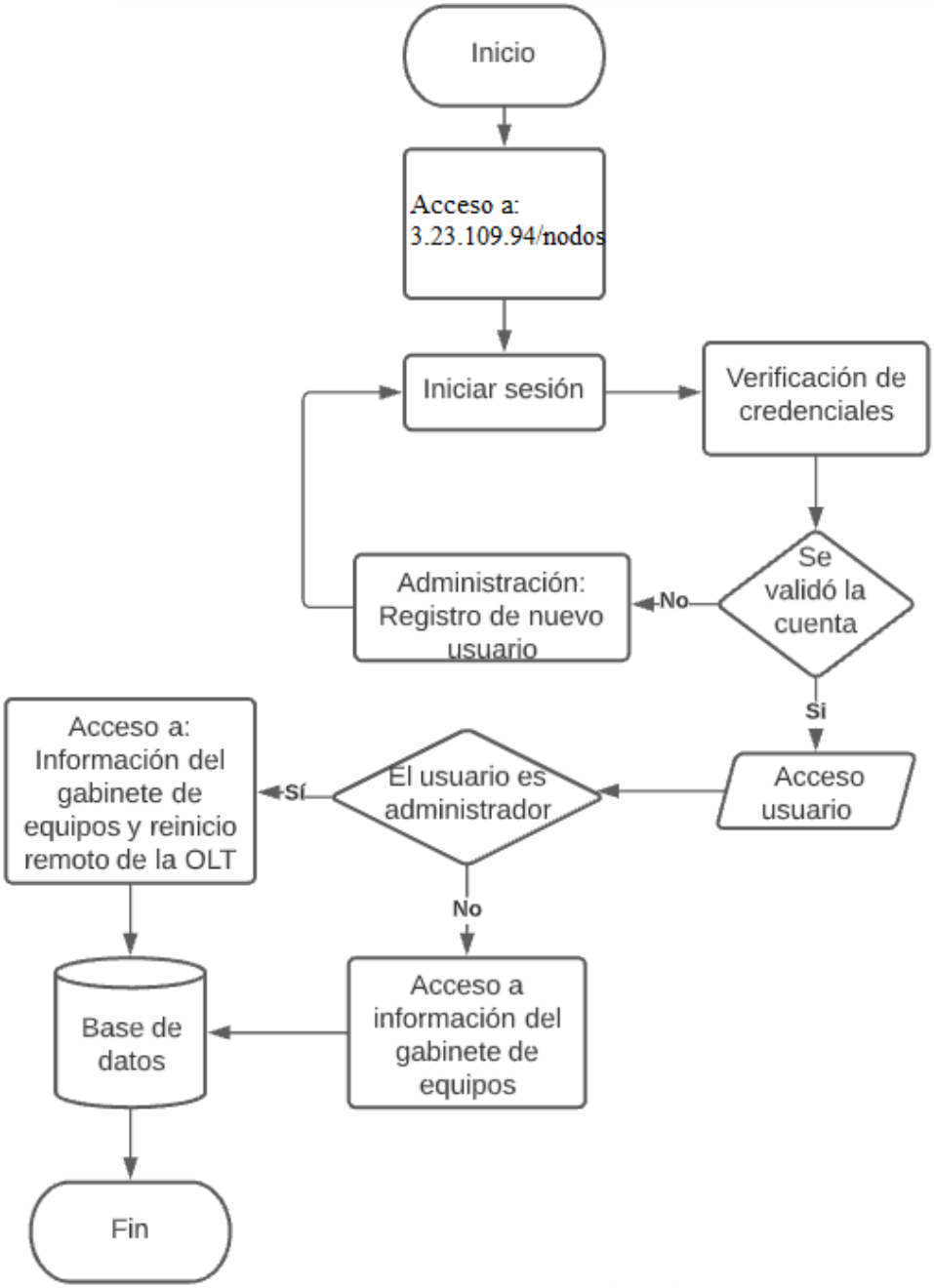
La página WEB alojada en AWS se nutre de la base de datos MySQL (MariaDB) la cual mediante una interfaz gráfica interactiva muestra datos importantes que se puede dividir en tres partes principales como: cuentas de usuarios, datos informativos (frontend) y la estructura (backend).

En donde los usuarios puedan logearse y así tener el acceso total al sitio web donde se podrá visualizar la data más importante como es la temperatura y datos de apertura de gabinete como también el APAGADO/ENCENDIDO de este por cada nodo que se haya creado.

En la Figura 32 se muestra el diagrama de flujo de la página Web del sistema SCYNODE.

Figura 32

Diagrama de flujo para el diseño del servidor web del SCYNODE, registro y validación de credenciales

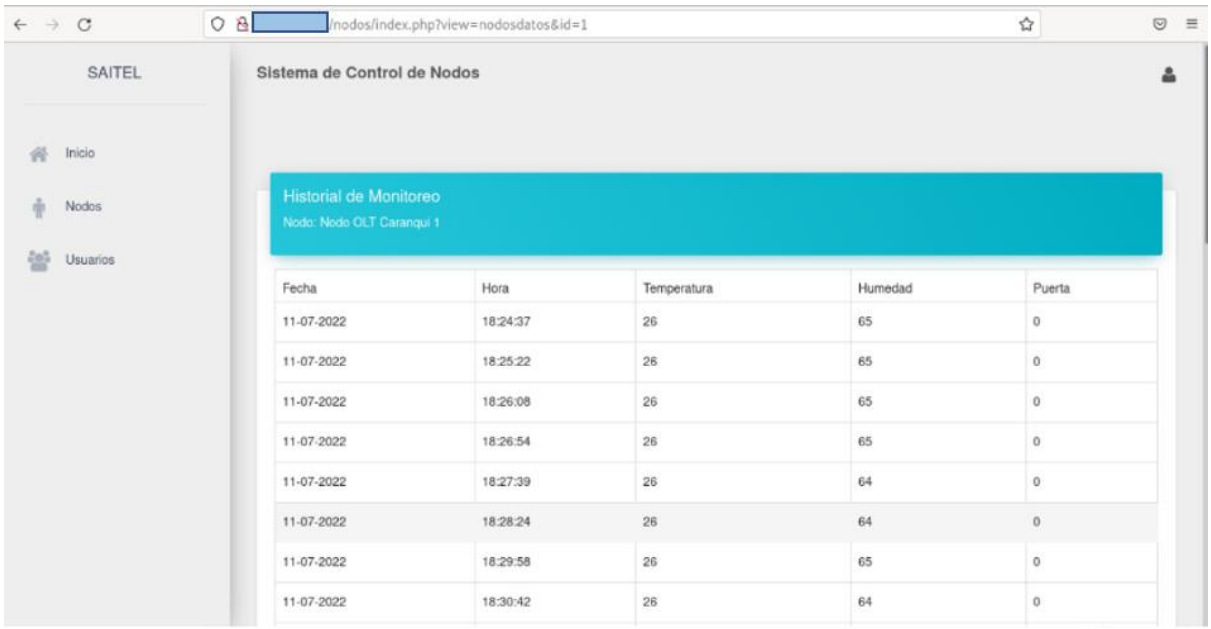


Fuente: *Autoría*

En la Figura 33 se observa el diseño de la interfaz WEB del sistema SCYNODE, en donde se muestra la fecha, la hora, la temperatura y la humedad en el interior del gabinete y el estado de la puerta del mismo.

Figura 33

Interfaz gráfica sistema SCYNODE

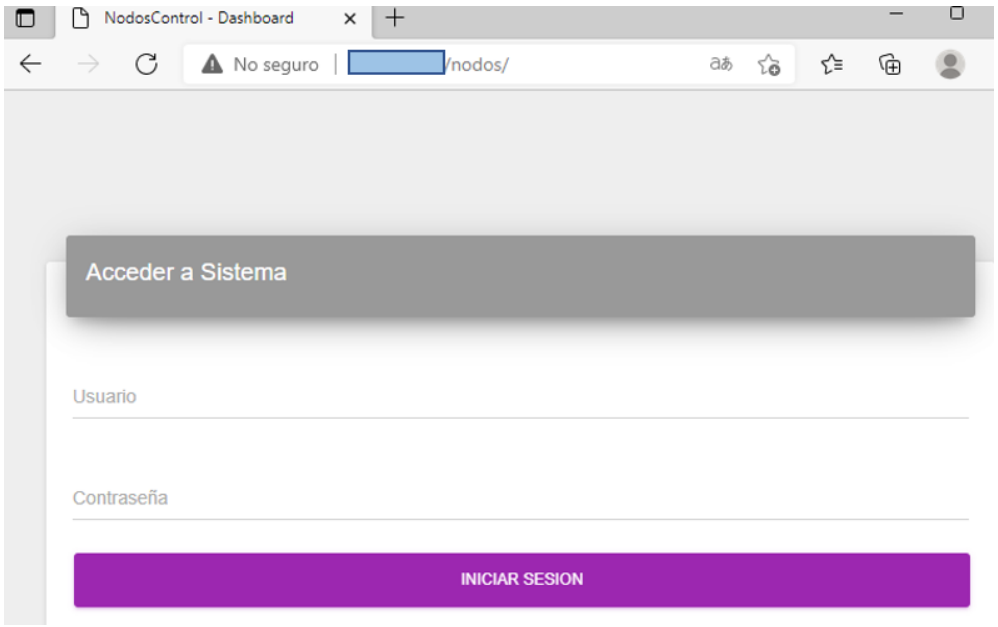


Fuente: *Autoría*

En la Figura 34, se observa el acceso al servidor WEB SCYNODE Mediante la IP pública dada por AWS, el ingreso solo estará permitido a personal autorizado por la empresa.

Figura 34

Diseño y estructura de la página web del SCYNODE



Fuente: *Autoría*

- **Acceso al sistema**

Para la visualización y supervisión remota de los eventos generados por los dispositivos monitoreados en el Nodo se implementa una interfaz web con políticas de seguridad de acceso mediante usuarios y contraseñas. En la Figura 35 se puede observar la interfaz de usuario del Formulario de acceso al sistema con credenciales iniciales de usuario y contraseña por defecto como “admin”.

Figura 35

Formulario de acceso a sistema de control

Fuente: *Autoría*

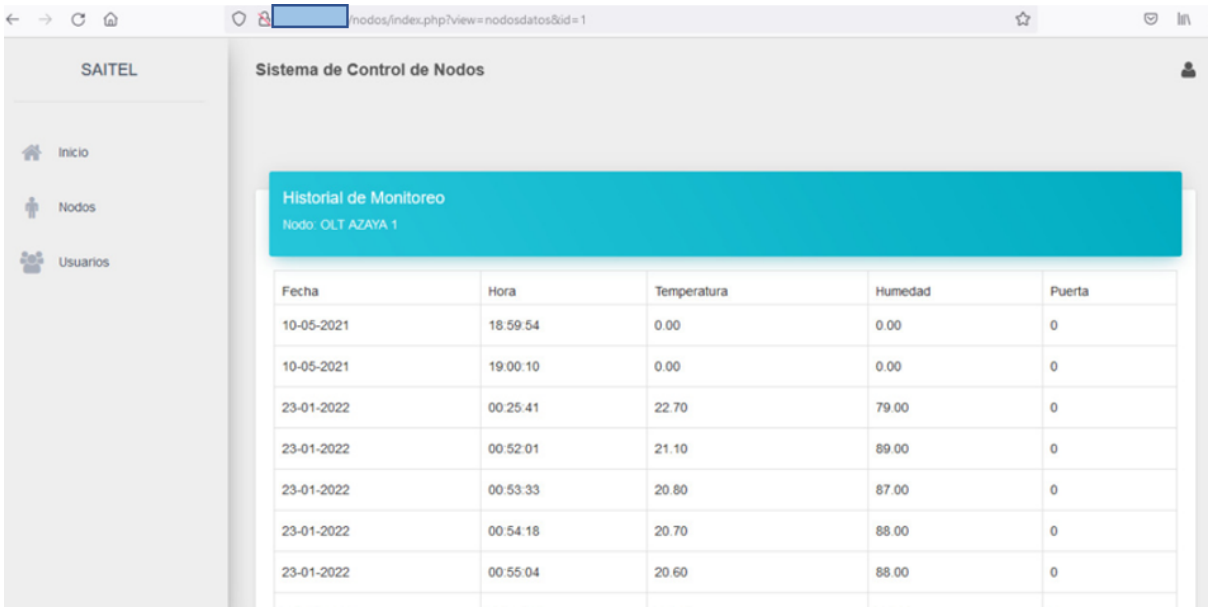
Una vez ingresadas las credenciales de acceso al sistema, se abre la siguiente página que se muestra en la Figura 35 que es el diseño de la interfaz gráfica del servidor WEB en donde se aprecia las variables medias del sistema.

- **Interfaz de usuario del sistema SCYNODE**

La Figura 36 muestra una interfaz web que se implementa con orientación minimalista para que pueda ser de fácil manejo para el usuario y de fácil navegación para que la información pueda ser encontrada rápidamente.

Figura 36

Representación gráfica de datos tomados de MySQL



Fuente: *Autoría*

La pantalla principal corresponde a la opción INICIO del menú principal y consta de un área mayor que presenta en primera instancia un historial de eventos de la OLT que se encuentra como primer elemento en la base de datos conteniendo la información recolectada por el dispositivo SCYNODE. En segunda instancia, como en la Figura 37, se puede observar dos elementos adicionales que complementan el menú principal que consta de Nodos y Usuarios.

Figura 37

Opciones de menú

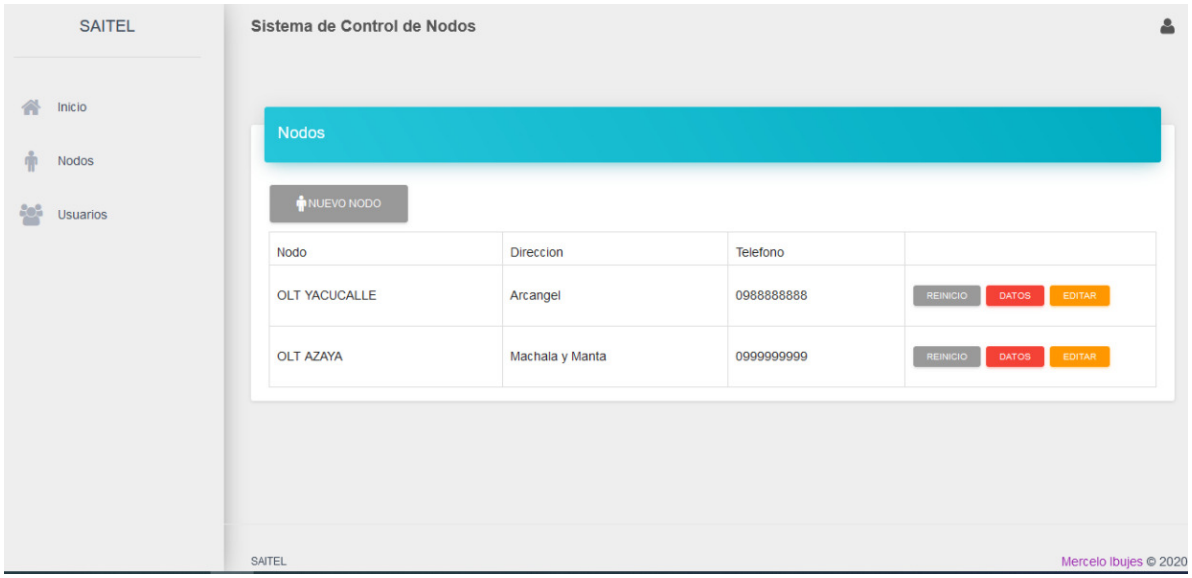
Fuente: *Autoría*

En el menú principal se puede observar la opción usuarios para la creación de estos, dando mayor control de la página, según el nivel que se requiera, al personal autorizado al acceso y manejo remoto de los módulos que se encuentran instalados en los gabinetes/Nodos de la empresa.

La opción nodos permite listar y crear nodos virtuales que representaran a los nodos físicos de la empresa. Cada nodo será representado por su nombre, dirección y número telefónico implementado en el dispositivo SCYNODE. La creación de un nuevo Nodo se resume a apretar el icono correspondiente e ingresar los tres datos enlistados. En la siguiente Figura 38 se puede observar la interfaz de presentación de este apartado.

Figura 38

Vista de Nodos creados en sistema



Nota. ***Botón reinicio:*** *Reinicia el nodo perteneciente a la misma.* ***Botón datos:*** *Permite mirar todos los datos del nodo.* ***Botón editar:*** *Edita los valores del nodo.* Fuente: *Autoría*

3.2.7. Módulo eléctrico o alimentación del sistema

Para calcular el voltaje mínimo necesario que requiere el circuito, es necesario analizar cada elemento que lo conforma es decir, requerimientos de voltaje y corriente de la placa de desarrollo, el sensor de temperatura, los actuadores y el módulo GSM 808, para ello, se muestra en la Tabla 17 los requerimientos de voltaje y corriente de los dispositivos, en este caso, la corriente total será igual a la sumatoria de las corrientes parciales de cada elemento según especificaciones técnicas del fabricante.

Tabla 17

Sumatoria de corrientes consumidas por el nodo 1

Dispositivo	Voltaje	Corriente
Arduino UNO	5-12V	50 mA
DHT11	3,5-5V	2,5 mA
SIM 808	5V	80 mA
Relé 1	5V	90 mA
Relé 2	5V	90 Ma
Total	5V	312,15, mA

Fuente: *Autoría*

Como se evidencia en la Tabla 17, el sistema SCYNODE requiere de una fuente de alimentación de 5 VDC a 300mA para que el sistema pueda operar sin ningún inconveniente y pueda ejecutar la tarea para la que está diseñado.

El módulo de alimentación será el encargado de subministrar energía eléctrica al módulo central y al módulo de seguridad mediante una fuente de 5V a 3 Amperios.

3.3.Costo de implementación del dispositivo

Para realizar el cálculo del costo de implementación del sistema SCYNODE, se toma en cuenta el costo de los elementos necesarios para el ensamblaje del mismo, para ello en la Tabla 18 se muestra en detalle el valor de los sensores, la placa de desarrollo, el módulo para la comunicación inalámbrica, los actuadores, la carcasa, el sistema de ventilación y el costo de la investigación.

Tabla 18

Costo de implementación del sistema SCYNODE

Dispositivo	Valor
Placa Arduino UNO	$21,30
Módulo GSM/GPRS 808	$31,45
Relé 1	$7,25
Relé 2	$7,25
Ventilador	$24,59
Sensor DHT11	$3,50
Sensor MC38	$1,50
Licencia Plataforma AWS	$50
Carcasa	$70
Costo de investigación	$1283,16
Total	$1500

Fuente: *Autoría*

Como se aprecia en la Tabla 18 el costo de implementación del dispositivo SCYNODE es de $1500, un costo extremadamente bajo en relación con el beneficio y utilidad que representa para la empresa SAITEL.

Capítulo 4. Pruebas de funcionamiento y resultados

Se muestran las pruebas del sistema realizadas primero en un ambiente controlado simulando el nodo y las pruebas de funcionamiento en el nodo en cuestión; se verifica el funcionamiento del sistema SCYNODE probando todos los subsistemas que conforman el dispositivo verificando la funcionalidad del dispositivo; en cada iteración se realiza las pruebas respectivas para modificar el diseño en caso de ser necesario para luego realizar la siguiente en base a los resultados previos. Este apartado es la retroalimentación del capítulo de diseño.

4.1. Pruebas de funcionalidad primera iteración

A continuación, se detallan una serie de pruebas de cada subsistema, mismos que, en base a los requerimientos se determina si cumplen o no el objetivo planteado de acuerdo con el modelo Iterativo de investigación. Las pruebas que se realizarán son: test eléctrico, test del subsistema pasivo, test de hardware, test de software, test de aplicación y finalmente test de funcionalidad.

4.1.1. Test eléctrico

Esta prueba tiene como finalidad verificar si se cumplen los requerimientos de alimentación del dispositivo, verificar que la fuente de alimentación sea capaz de proveer al dispositivo del voltaje necesario para el correcto funcionamiento del módulo SIM808, el sensor DHT11, el sensor magnético, los actuadores y la placa de desarrollo de Arduino, en la Tabla 19 se muestran la descripción del test eléctrico.

Tabla 19

Test del subsistema eléctrico

Pruebas del subsistema eléctrico	
Prerrequisitos	**Pasos**
1. Adquisición de adaptador de 5 voltios DC a 300 mA 2. Cableado de distribución desde el adaptador hasta la placa de desarrollo y los sensores y actuadores. 3. Verificar posiciones de dispositivos.	• Verificación de encendido del Arduino UNO • Verificación de encendido de los sensores • Verificación de encendido de los actuadores • Comprobación de voltaje en el adaptador

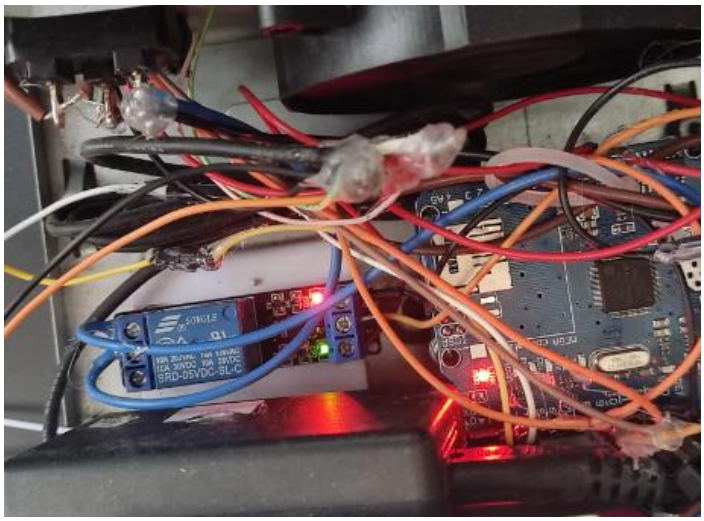
Fuente: *Autoría*

El resultado de esta prueba es positivo, se cuenta con la fuente de alimentación necesaria para alimentar todos los dispositivos que conforman el sistema SCYNODE con la finalidad

que el sistema cumpla los objetivos para los cuales fue diseñado, todos los dispositivos encienden su led indicador de encendido, lo que demuestra que las conexiones realizadas están óptimas y el sistema está listo para funcionar, así como se observa en la Figura 39.

Figura 39

Verificación del subsistema eléctrico



Fuente: *Autoría*

4.1.2. Test subsistema pasivo

Los dispositivos que conforman el dispositivo deben estar interconectados de acuerdo a las especificaciones de diseño planteadas en el capítulo 3, cada elemento tiene una finalidad específica, mediante esta prueba se verifica que todo esté correctamente conectado y en orden. En la Tabla 20, se muestran los parámetros necesarios para realizar el test del subsistema pasivo.

Tabla 20

Pruebas del subsistema pasivo

Pruebas del subsistema pasivo	
Prerrequisitos	**Pasos**
1. Adquisición de cables USB 2. Adquisición de conectores para la conexión de los sensores	• Verificación del estado de los cables • Verificación de las conexiones

Fuente: *Autoría*

Se verifica que las conexiones son exitosas, continuas y sin intrrupciones, se conecta adecuadamente los sensores con la placa de desarrollo, se demuestra mediante la lectura de datos y el envío de los mismos a la base de datos.

4.1.3. Test subsistema activo

Esta prueba consiste en verificar si la placa de desarrollo está trabajando adecuadamente, mediante esta prueba se verifica el reconocimiento de la Placa Arduino UNO en el computador, la carga del sketch y el establecimiento de conexión a la red GPRS. En la Tabla 21 se muestran los parámetros de la prueba del subsistema activo.

Tabla 21

Pruebas del subsistema activo

Pruebas del subsistema activo	
Prerrequisitos	**Pasos**
1. Adquisición de la placa Arduino 2. Verificación de los puertos COM 3. Carga del sketch de manera exitosa 4. Conectarse a la red GPRS	• Carga del sketch a la placa ARDUINO • Establecimiento de conexión inalámbrica • Lectura de datos de los sensores • Envío de Información • Apreciación de resultados en servidor WEB

Fuente: *Autoría*

Los resultados de la prueba son satisfactorios, la placa de desarrollo de Arduino UNO es reconocida por el computador, por lo tanto, el sketch de programación se cargó a plenitud; la conexión entre el dispositivo y la red GPRS es exitosa, la lectura de los sensores es correcta.

4.1.4. Test de aplicación

Consiste en evaluar la integración del sistema con su funcionalidad, en donde se verifica que el SCYNODE es un sistema de comunicación de datos y reinicio remoto. Según el propósito del proyecto mediante esta prueba se comprueba que el envió de datos sea óptimo y sea presentado al usuario de forma conveniente y entendible para que, una vez determinada una toma de decisión con respecto al nodo, se cumpla con el reinicio remoto del nodo a criterio del personal de soporte técnico de la empresa SAITEL, así como se muestra en la Tabla 22.

Tabla 22

Pruebas del subsistema de aplicación

Pruebas del subsistema de aplicación	
Prerrequisitos	**Pasos**

1. Crear cuenta en AWS 2. Envío de datos al servidor WEB 3. Apreciación de resultados en el servidor 4. Reinicio remoto del nodo	• Crear cuenta en AWS • Verificar el envío de datos entre el SCYNODE y la ip pública asignada a la cuenta de AWS • Verificar la conectividad entre AWS con el sistema SCYNODE

Fuente: *Autoría*

La apreciación de datos es exitosa, aprecian los datos detectados por los sensores y son visualizados en tiempo real, se reinicia el nodo de forma remota ingresado a la plataforma de AWS, se muestra al usuario de una forma clara y concisa y el sistema cuenta con un botón que permite el reinicio del NODO, el dispositivo debe cortar la energía eléctrica del dispositivo a controlar.

4.1.5. Pruebas de la primera iteración del SCYNODE

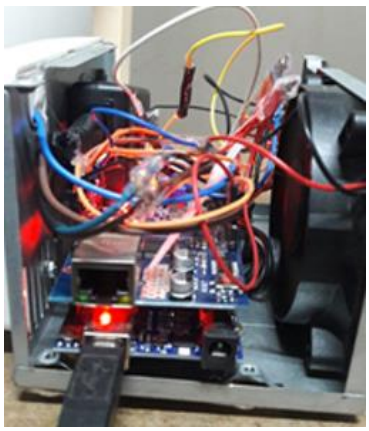
Una vez culminado el diseño del SCYNODE se procede con la valoración del estado actual, esto se lo realiza aplicando las pruebas del sistema. Como primera etapa se va a valorar lo siguiente:

- El envío vía mensaje de texto de los valores de temperatura dentro del gabinete de equipos.
- Publicación de la página web.

En la Figura 40 se observa el hardware del sistema SCYNODE vista interna el cual está conformado por el módulo de toma de datos, módulo eléctrico, módulo de envío y recepción de datos y el sistema de ventilación.

Figura 40

Elementos de hardware para las pruebas de la primera iteración del SCYNODE



Fuente: Autoría

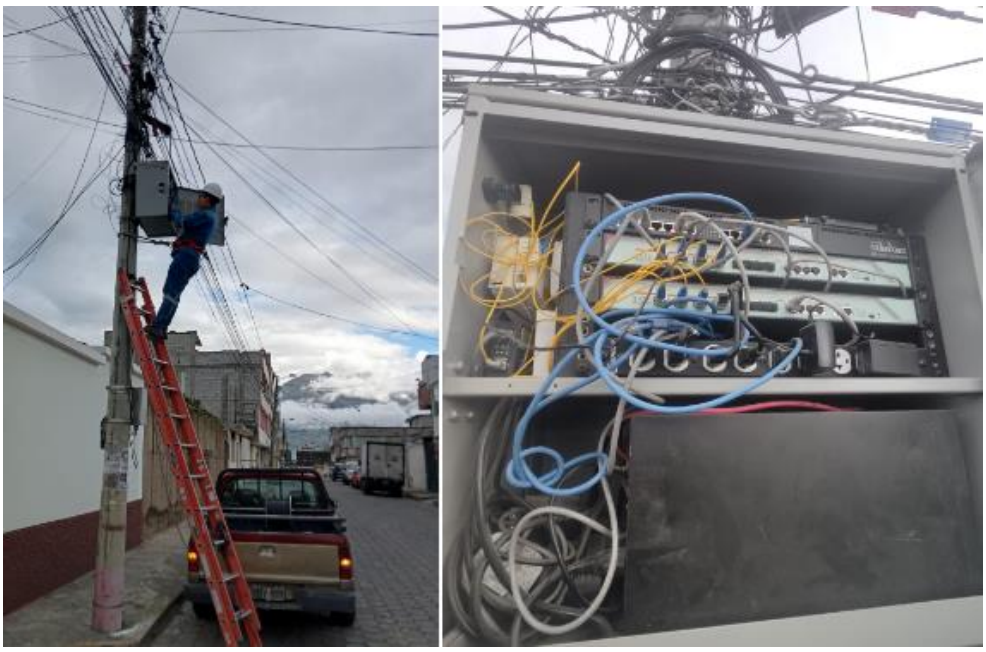
4.2. Pruebas de funcionalidad segunda iteración

En esta iteración se recolecta información por el período de un mes con once muestras diarias de temperatura dentro del gabinete de equipos de la OLT-Caranqui, a partir de las ocho de la mañana hasta las seis de la noche, el horario fue determinado en el análisis del escenario actual. En la Figura 41 se observa la colocación del prototipo SCYNODE en el nodo OLT-Caranqui.

Una vez instalado el dispositivo dentro de la sala de equipos, se procede a realizar las mediciones de temperatura en escala de grados centígrados con diferencia de una hora entre mediciones.

Figura 41

Colocación del prototipo SCYNODE en el gabinete de equipos del nodo OLT-Caranqui, por parte de un técnico de la empresa SAITEL



Fuente: *Autoría*

Ya que el dispositivo se encuentra programado para el envió de las mediciones a través de un mensaje de texto en caso de alertas, en la Figura 42 se puede observar un ejemplo del contenido del mensaje de texto.

Figura 42

Parámetros recibidos desde el módulo central vía mensaje de texto

Fuente: *Autoría*

El conjunto de muestras recolectadas durante el mes de julio se presenta a continuación en la Tabla 23, poniendo de manifiesto los valores máximos de temperaturas durante este periodo de tiempo y representando además los valores máximos del año.

Según (Instituto Nacional de Metereología e Hidrología, 2020), en la región Sierra Norte la temperatura empieza a aumentar desde las 07:00 y a disminuir considerablemente a partir de las 18:00, debido a que la condensación en esta área geográfica es mucho más elevada por la ubicación respecto al nivel del mar.

De acuerdo a la información mencionada se toma en cuenta el horario de 08:00 a 18:00 para la toma de mediciones de la temperatura con un intervalo de una hora en las mismas, este lapso de tiempo fue escogido ya que es el de más tráfico de eventos puntuales en los nodos de la red de fibra óptica de la empresa SAITEL, además como será un prototipo ligado a la infraestructura de telecomunicaciones los datos se actualizarán en simultáneo con los servidores y esto se lo realiza a cada hora.

Tabla 23

Resultados de las mediciones de temperatura con el SCYNODE en el gabinete de equipos de la OLT-Caranqui perteneciente a la empresa SAITEL

Hora **Fecha**	**8:00**	**9:00**	**10:00**	**11:00**	**12:00**	**13:00**	**14:00**	**15:00**	**16:00**	**17:00**	**18:00**
1/04/2022	20°C	34°C	44°C	49°C	52°C	56°C	60°C	64°C	68°C	62°C	58°C

2/04/2022	21°C	35°C	46°C	50°C	54°C	57°C	61°C	66°C	70°C	64°C	59°C
3/04/2022	23°C	37°C	48°C	53°C	57°C	61°C	65°C	69°C	74°C	68°C	63°C
4/04/2022	19°C	33°C	43°C	47°C	50°C	54°C	58°C	62°C	66°C	60°C	56°C
5/04/2022	20°C	34°C	44°C	49°C	52°C	56°C	60°C	64°C	68°C	62°C	58°C
6/04/2022	20°C	34°C	44°C	49°C	52°C	56°C	60°C	64°C	68°C	62°C	58°C
7/04/2022	18°C	32°C	42°C	46°C	49°C	52°C	56°C	60°C	64°C	58°C	54°C
8/04/2022	21°C	35°C	46°C	50°C	54°C	57°C	61°C	66°C	70°C	64°C	59°C
9/04/2022	20°C	34°C	44°C	49°C	52°C	56°C	60°C	64°C	68°C	62°C	58°C
10/04/2022	26°C	40°C	52°C	57°C	61°C	65°C	70°C	75°C	80°C	73°C	68°C
11/04/2022	24°C	38°C	49°C	54°C	58°C	62°C	67°C	71°C	76°C	69°C	65°C
12/04/2022	25°C	39°C	51°C	56°C	60°C	64°C	68°C	73°C	78°C	71°C	66°C
13/04/2022	22°C	36°C	47°C	51°C	55°C	59°C	63°C	67°C	72°C	66°C	61°C
14/04/2022	23°C	37°C	48°C	53°C	57°C	61°C	65°C	69°C	74°C	68°C	63°C
15/04/2022	21°C	35°C	46°C	50°C	54°C	57°C	61°C	66°C	70°C	64°C	59°C
16/04/2022	20°C	34°C	44°C	49°C	52°C	56°C	60°C	64°C	68°C	62°C	58°C
17/04/2022	22°C	36°C	47°C	51°C	55°C	59°C	63°C	67°C	72°C	66°C	61°C
18/04/2022	24°C	38°C	49°C	54°C	58°C	62°C	67°C	71°C	76°C	69°C	65°C
19/04/2022	25°C	39°C	51°C	56°C	60°C	64°C	68°C	73°C	78°C	71°C	66°C
20/04/2022	22°C	36°C	47°C	51°C	55°C	59°C	63°C	67°C	72°C	66°C	61°C
21/04/2022	19°C	33°C	43°C	47°C	50°C	54°C	58°C	62°C	66°C	60°C	56°C
22/04/2022	20°C	34°C	44°C	49°C	52°C	56°C	60°C	64°C	68°C	62°C	58°C
23/04/2022	22°C	36°C	47°C	51°C	55°C	59°C	63°C	67°C	72°C	66°C	61°C
24/04/2022	20°C	34°C	44°C	49°C	52°C	56°C	60°C	64°C	68°C	62°C	58°C
25/04/2022	19°C	33°C	43°C	47°C	50°C	54°C	58°C	62°C	66°C	60°C	56°C
26/04/2022	23°C	37°C	48°C	53°C	57°C	61°C	65°C	69°C	74°C	68°C	63°C
27/04/2022	25°C	39°C	51°C	56°C	60°C	64°C	68°C	73°C	78°C	71°C	66°C
28/04/2022	24°C	38°C	49°C	54°C	58°C	62°C	67°C	71°C	76°C	69°C	65°C
29/04/2022	25°C	39°C	51°C	56°C	60°C	64°C	68°C	73°C	78°C	71°C	66°C
30/04/2022	21°C	35°C	46°C	50°C	54°C	57°C	61°C	66°C	70°C	64°C	59°C
31/04/2022	22°C	36°C	47°C	51°C	55°C	59°C	63°C	67°C	72°C	66°C	61°C

Fuente: Prototipo del SCYNODE

Con los datos presentados en la tabla anterior se determina los niveles de temperatura medios a cada hora y con ello poder definir un rango de trabajo aceptable y un límite máximo con el que se deberán accionar los mecanismos de ventilación del gabinete o de la OLT.

En la sala de equipos Caranqui se trabaja con una OLT modelo HUAWEI GPON MA 5680T como se puede observar en la siguiente Figura 43.

Figura 43

OLT HUAWEI GPON MA 5680T

Fuente: *SAITEL*

Este modelo de OLT integra las funciones de conmutación de agregación y enrutamiento de borde, tiene la capacidad de proveer GPON de gran densidad, ethernet P2P y servicio de triple play. En la Tabla 24 se detallan las principales características de este dispositivo.MA5608T

Tabla 24

Características de la OLT HUAWEI SmartAX MA5608T OLT

Característica	Descripción
N° de modelo	MA5680T
Dimensión	490*275.8*447.2mm
Entorno operativo	• La temperatura: -25° ~ +55°C • Humedad: 5% ~ 95% (sin condensación)
Parámetros de la fuente de alimentación	-48 Entrada de V CC, admite protección de alimentación dual. Rango de voltaje de funcionamiento -38.4V ~ -72V
Capacidad de intercambio de backplane	3.2 Tbit/seg
Capacidad de intercambio de la placa de control	1920 Gbit/seg
Capacidad de acceso	128*10G EPON 64*10G GPON 128*EPON 256*GPON 768*GE

Tipo de acceso	Interfaz aguas arriba: 10GE óptico, interfaz comercial óptica/eléctrica de GE: Puerto óptico EPON, puerto óptico GPON, 10Puerto óptico G EPON, puerto óptico P2P FE, puerto óptico P2P GE, Interfaz óptica Ethernet

Fuente*: (YCICT CO , 2021)*

Con los datos recolectados de temperatura se procede a realizar la Tabla 25 en donde se puede observar la media aritmética por cada intervalo de tiempo. Este procedimiento permite tener una comparación con la temperatura nominal de trabajo de la OLT incorporada en el Nodo-Caranqui. de

Tabla 25

Valores medios de temperatura dentro de la sala de equipos del nodo OLT-Caranqui

Hora	**8:00**	**9:00**	**10:00**	**11:00**	**12:00**	**13:00**	**14:00**	**15:00**	**16:00**	**17:00**	**18:00**
Temperatura media	21.8° C	35.8° C	46.6°C	51.1°C	54.8°C	58.6°C	62.8°C	67°C	69.1°C	65.3°C	52°C

Fuente: *Prototipo del SCYNODE*

Teniendo en cuenta que la temperatura máxima de trabajo de la OLT es de 55°C se puede observar que este límite es superado, en promedio, todos los días del mes a partir del mediodía. Esto puede recaer en el desgaste prematuro de los equipos del Nodo, daños y perdida de información.

4.2.1. Pruebas segunda iteración

A continuación, se inicia con el proceso del desarrollo de la segunda iteración para el diseño del SCYNODE, de ser el caso se omitirán pasos que ya fueron realizados en la primera iteración, y se irán agregando otros requerimientos de acuerdo con el análisis del escenario actual detallado en el siguiente apartado.

Debido a que algunas de las temperaturas medias en la sala de equipos del nodo OLT-Caranqui, véase Tabla 25, son más altas que la temperatura de operación recomendada por el fabricante se incluirá en el prototipo, un ventilador con capacidad alta de enfriamiento por su rapidez y potencia.

En esta segunda iteración se incorpora al diseño del dispositivo prototipo, un dispositivo electromecánico que permita identificar el acceso, autorizado o no, al Nodo.

Básicamente el elemento electromecánico se encontrará activo a la espera de su accionamiento, cuando se trata de acceso no autorizado, caso contrario podrá ser desactivado por personal autorizado para no generar ningún tipo de alarma.

4.2.2. Reinicio remoto de la OLT ubicada en el nodo OLT-Caranqui

Como resultado de la superación del régimen de temperatura de trajo de la OLT, el dispositivo cambia del estado activo de funcionamiento a un modo en espera que desactiva todas sus funciones.

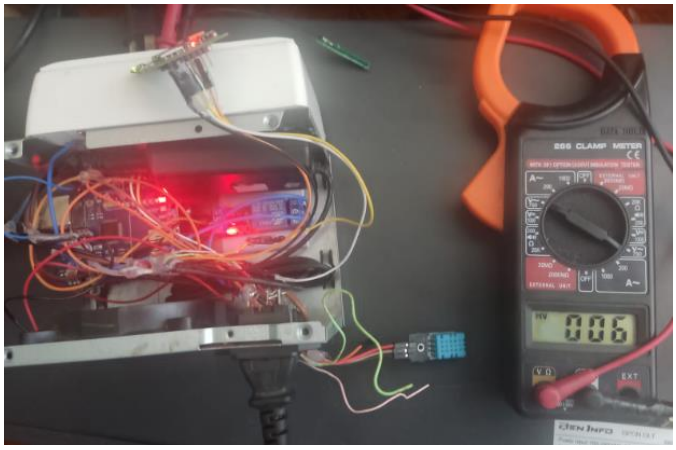
Al activarse el modo de espera entra además en un modo de enclavamiento interno que se mantiene hasta la presencia de un reinicio total.

Al encontrarse en el modo enclavamiento, la OLT no tiene capacidad siquiera de recibir comandos básicos por lo que no es posible ejecutar un reinicio remoto, sino que se debe interrumpir su alimentación energética de forma manual.

Para lograr la interrupción energética de forma automática se integra un relé controlado por una placa Arduino que a su vez tomara en cuenta los siguientes criterios para su activación o desactivación según se muestra en la Figura 44:

Figura 44

Verificación de corte de voltaje AC de manera remota



Fuente: *Autoría*

4.2.3. Codificación del software para el sistema segunda Iteración

En esta etapa se continua con el proceso de codificación del módulo de toma de datos, módulo central y módulo de seguridad mediante el establecimiento de los rangos de temperatura con los cuales se activará el dispositivo de ventilación.

Se diseña un sistema que permita la activación de la ventilación del gabinete desde el primer momento en que se sobrepasa el límite máximo de temperatura de funcionamiento de la OLT para evitar la necesidad de un reinicio total mediante corte de energía eléctrica, esto significa que el reinicio remoto de la OLT siempre será a consideración del Administrador y de criterios técnicos propios de la empresa SAITEL.

Una vez integrado el magnetic-reed al módulo de toma de datos es necesario programar la placa Arduino para que empiece a realizar el monitoreo del acceso a la sala de equipos en el nodo OLT-Caranqui. En la Figura 45 se muestra parte del código fuente para el interruptor de posición magnético tipo reed-switch.

Figura 45

Líneas de código de la programación del magnetic-reed, declaración de variables, inicialización de puertos

sptrwebOLT

```
const int pinSensor = 2;
const int pinLED = 13;

void setup() {
  //configurar pin como entrada con resistencia pull-up interna
  pinMode(pinSensor, INPUT_PULLUP);
  pinMode(pinLED, OUTPUT);
}

void loop() {
  int value = digitalRead(pinSensor);

  if (value == LOW) {
    digitalWrite(pinLED, HIGH);
  } else {
    digitalWrite(pinLED, LOW);
  }

  delay(1000);
}
```

Fuente: *Código de programación de Arduino para el SCYNODE*

4.2.4. Pruebas de base de datos en base a la variable temperatura

Una vez obtenidas las temperaturas del gabinete, en la primera iteración, dentro de la sala de equipos ubicados en el nodo OLT-Caranqui, se continúa con la fase de delimitación de los rangos de temperatura a los cuales se verá sujeto el proceso de activación del dispositivo de ventilación a través de la relación entre los datos recolectados y los rangos permitidos por el dispositivo y especificados por el fabricante.

En la Tabla 26 se muestra el resumen de las dos características mencionadas con anterioridad.

Tabla 26

Definición de valores de temperatura del entorno de trabajo en la sala de equipos ubicada en el nodo OLT-Caranqui

Temperatura del entorno de trabajo recomendada por el fabricante de la OLT	-25° ~ +55°C	
Temperatura media del entorno de trabajo dentro de la sala de equipos del nodo OLT-Caranqui	**Hora**	**Temperatura**
	08:00	21°C
	09:00	35°C
	10:00	46°C
	11:00	51°C
	12:00	54°C
	13:00	56°C
	14:00	62°C
	15:00	67°C
	16:00	69°C
	17:00	65°C
	18:00	52°C
Temperatura del entorno de trabajo a la cual se accionará el proceso de activación del dispositivo de enfriamiento	Temperatura ≥ +45°C	

Fuente: *Autoría*

Ya definidos los rangos de temperatura del entorno de trabajo se procede a integrar el dispositivo de ventilación y el relé controlador correspondiente en el prototipo desarrollado hasta este punto.

En la Figura 46 se muestra parte del código de la programación en Arduino para el control del relé. Véase el Anexo 3 para el código de programación en su totalidad.

Figura 46

Líneas de código de la programación del relé, declaración de variables, inicialización de puertos

```
const int rele = 2;

/***   Setup   ***/
void setup() {
    pinMode(rele,OUTPUT);
}

/***   Loop   ***/
void loop() {
    digitalWrite(rele, HIGH);
```

Fuente: *Código de programación de Arduino para el SCYNODE*

4.3. Pruebas de funcionalidad tercera iteración

En este punto se continúa con el proceso de evaluación del SCYNODE, para ello en la segunda iteración se desarrollarán las siguientes pruebas:

- Las mediciones de temperatura y el envío de esta información a la base de datos con un intervalo de una hora a partir de las ocho de la mañana hasta las seis de la noche.
- El envío de la información a la base de datos al abrir el gabinete de equipos ubicado en el nodo OLT-Caranqui.
- Activación del módulo de refrigeración de acuerdo con los rangos establecidos.
- Reinicio remoto de la OLT y archivo de la información en la base de datos.

Las pruebas planteadas son para la verificación de funcionamiento básico del dispositivo que permita remotamente controlar el reinicio del Nodo, en la Figura 47, se muestra la carcasa del nodo.

Figura 47

Carcasa del sistema SCYNODE

Fuente: *Autoría*

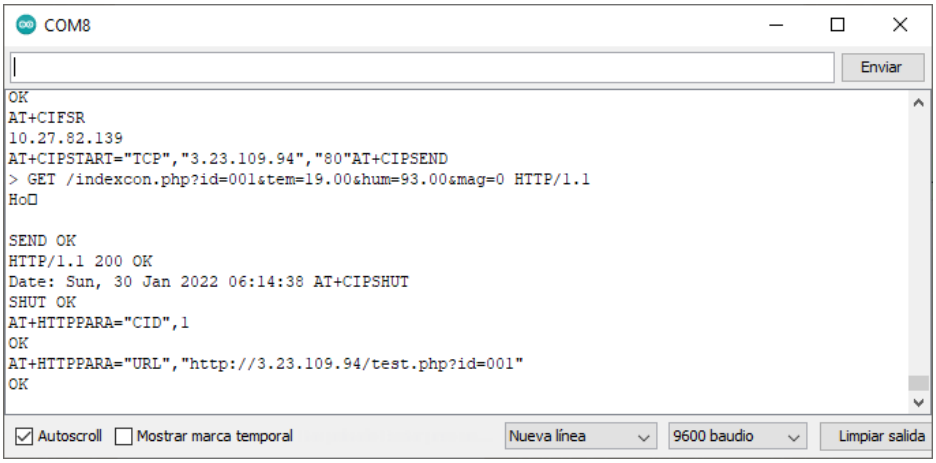
4.3.1. Pruebas lectura de datos y establecimiento de conexión

Este apartado se relaciona con el envío de la temperatura y estado de apertura de puertas de gabinetes con la respectiva fecha y hora del evento. Esta recolección de los datos ayuda para que la lógica de diseño en la programación pueda realizar las respectivas notificaciones mediante la página web.

Mediante la comunicación serial podemos evidenciar el envío de datos hacia la base MySQL colocada en la nube. En la Figura 48 se muestra la lectura de datos en el puerto COM 8 de la placa ARDUINO así como también el mensaje de establecimiento de conexión con la red GPRS.

Figura 48

Recolección de datos (Temperatura y Estado de apertura de puerta) enviados a MySQL

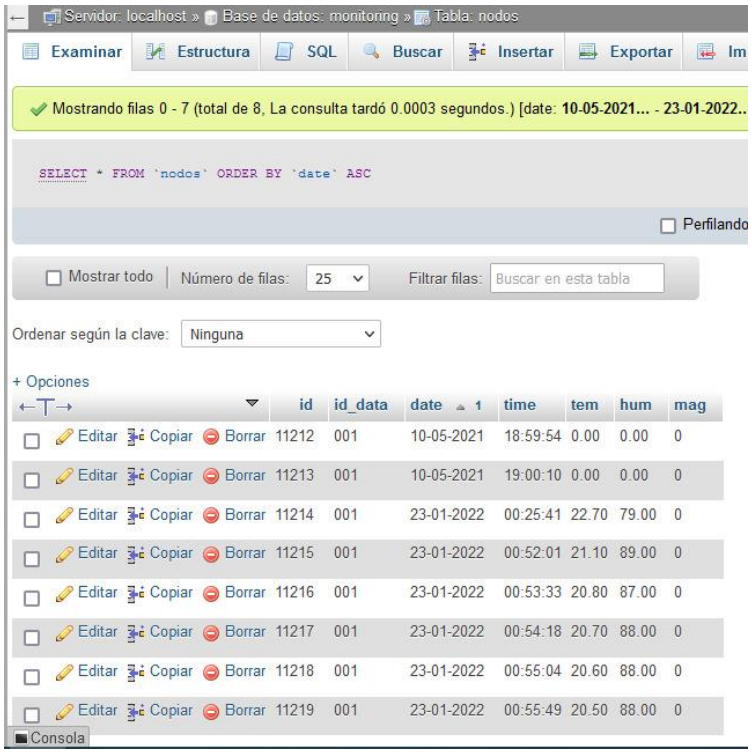


Fuente *Autoría*

En la Figura 49 se muestra que los datos son guardados en la base de MySQL ubicados en la tabla “Nodos”, así el usuario puede acceder a esta información.

Figura 49

Tabla de recolección de datos en MySQL



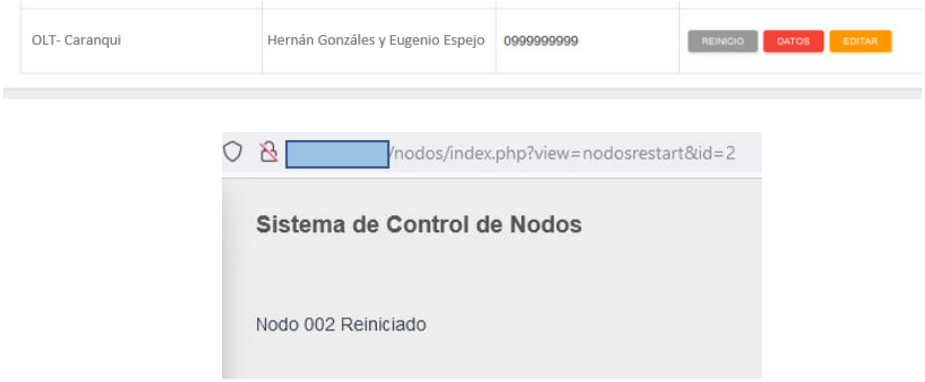
Fuente: *Autoría*

4.3.2. Corte energético remoto de la OLT y registro de actividad en la base de datos

Como se muestra en la Figura 50, la interfaz indica que cada nodo se crea con un botón de reinicio el cual una vez pulsado notifica que fue reiniciado de manera correcta, mediante un mensaje en la página web.

Figura 50

Notificación de nodo reiniciado



Fuente: *Autoría*

La prueba general de su función básica de reinicio la podemos evidenciar conectando a la toma eléctrica un elemento con alimentación eléctrica como se muestra en la siguiente Figura 51.

Figura 51

Prueba de funcionamiento de reinicio

Fuente: *Autoría*

4.3.3. Notificación de apertura de puerta de gabinete.

Para esta notificación se usa de la misma manera la interfaz web la cual notificará que la apertura de la puerta de gabinete fue abierta de manera recurrente sin tener ningún control de acceso. En la base de datos nos registrara en la tabla "Nodo_State" como "1" para la apertura de puerta y "0" como puerta normalmente cerrada, así como se muestra en la Figura 52.

Figura 52

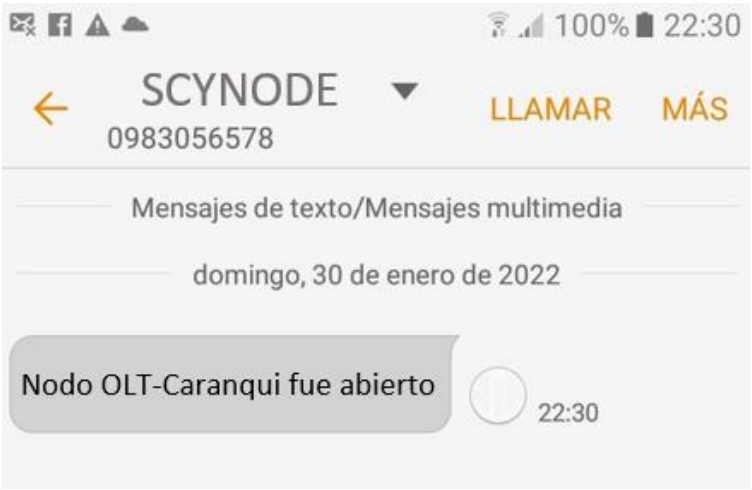
Variable de Dato de apertura de puerta

Fuente: *Autoría*

La Apertura del gabinete del nodo emitirá un mensaje de alerta de texto a un número preconfigurado para que sea el único que pueda saber de dicho evento, así como se muestra en la Figura 53.

Figura 53

Notificación SMS de apertura de Nodo



Fuente: *Autoría*

4.3.4. Activación del módulo de ventilación

Esta opción permitirá de manera automática encender un ventilador que se activará dependiendo de los rangos de temperatura censada por el sistema. En la Figura 54 se muestra el código de activación del actuador que accionará el sistema de ventilación.

Figura 54

Código de verificación de activación del módulo de ventilación

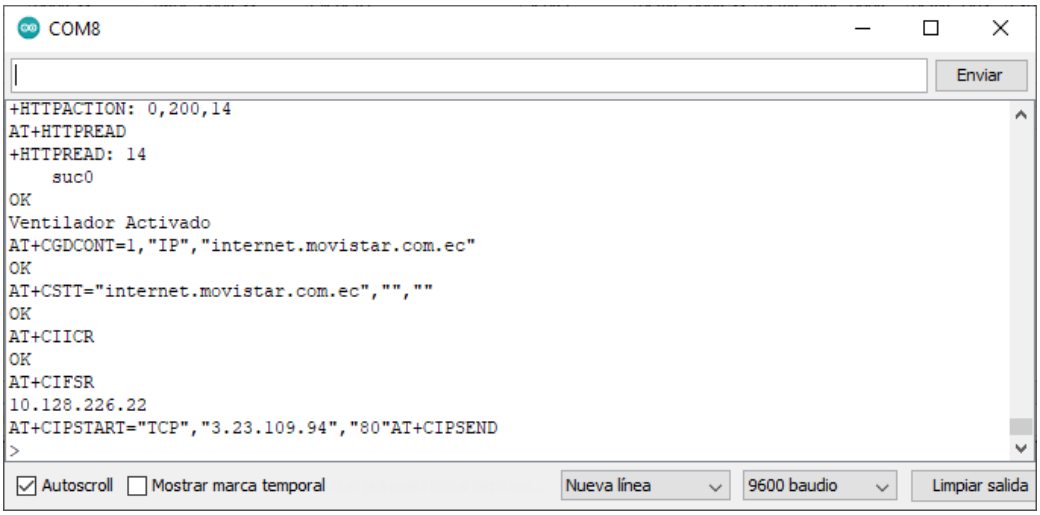
```
/////// Control Temperatura ////////////
void controlTemp()
{
    if (t < 30){      //////Activacion del módulo de ventilación
      digitalWrite(ctemp, LOW);
      Serial.println("Ventilador Activado");
      }       else {
        digitalWrite(ctemp, HIGH);
        }
}
```

Fuente: *Autoría*

La respuesta serial para saber que está en un buen funcionamiento se observa en la Figura 55.

Figura 55

Notificación lógica de activación del módulo de ventilación



Fuente: *Autoría*

De la misma forma y al ser censado de manera recurrente esta notificación no se toma en cuenta para que pueda ser mediante mensajes de texto o notificación web.

4.4. Beneficios de la implementación del sistema SCYNODE

Con la finalidad de evaluar los beneficios que el dispositivo SCYNODE representa a la empresa SAITEL, se realiza un análisis de costos en un periodo de 3 meses antes de la implementación del dispositivo y 3 meses después de haberlo implementado, para este estudio se toma en cuenta los siguientes parámetros: tiempo empleado en solucionar un evento, horas extras, ticket generado en el periodo comprendido entre 04 de enero del 2021 hasta el 24 de marzo del mismo año y a partir del 03 de marzo del 2022 hasta el 31 de mayo del presente año. En la Tabla 27 se observa los eventos registrados en la empresa SAITEL del nodo caranqui con su respectivo detalle antes de implementar el sistema SCYNODE.

Tabla 27

Eventos de F.O. presentados en el nodo Caranqui

Ticket	Fecha	Hora	Problema	Tiempo solución	Costo horas extras
3868	04/01/2021	20:27	Equipos inhibidos	1h30m	$12,86
3927	09/01/2021	10:04	Equipos inhibidos	1h	$2,50
4205	02/01/2021	18:05	Corte de fibra	50m	$10,48
4306	12/01/2021	10:00	Corte de fibra	3h10m	$2,50

4323	14/01/2021	14:00	Fallo energía	5h10m	$2,50
4325	14/01/2021	19:09	Atenuación fibra	2h10m	$14,46
4352	18/02/021	11:43	Equipos inhibidos	4h19m	$2,50
4367	20/02/2021	10:14	Equipos inhibidos	1h32m	$2,50
4392	21/02/2021	20:44	Equipos inhibidos	1h15m	$10,48
4413	28/02/2021	10:53	Equipos inhibidos	1h29m	$2,50
4482	09/03/2021	09:37	Equipos inhibidos	1h	$2,50
4494	11/03/2021	12:59	Organización	3h	$2,50
4518	16/03/2021	17:11	Organización	4h	$34,42
4562	24/03/2021	17:12	Organización	2h25m	$34,42
			Total		**$137,12**

Fuente: *SAITEL*

Como se observa en la Tabla 27, los eventos recurrentes durante un periodo de tres meses han sido el de equipos inhibidos, dicho evento se soluciona con el reinicio manual de los dispositivos que se encuentran en el nodo, además se muestran eventos propios de red con sus respetivos tiempos de solución dependiendo del caso., para el estudio se toma en cuenta los eventos relacionados con la inhibición de equipos y el costo que representa la solución; en la Tabla 28 se muestra el costo total que implican dichos eventos.

Tabla 28

Costo de solución de evento equipos inhibidos

Ticket	Fecha	Hora	Problema	Tiempo solución	Costo horas extras
3868	04/01/2021	20:27	Equipos inhibidos	1h30m	$12,86
3927	09/01/2021	10:04	Equipos inhibidos	1h	$2,50
4352	18/02/021	11:43	Equipos inhibidos	4h19m	$2,50
4367	20/02/2021	10:14	Equipos inhibidos	1h32m	$2,50
4392	21/02/2021	20:44	Equipos inhibidos	1h15m	$10,48
4413	28/02/2021	10:53	Equipos inhibidos	1h29m	$2,50
4482	09/03/2021	09:37	Equipos inhibidos	1h	$2,50
			Total		**$35,84**

Fuente: *SAITEL*

En la Tabla 29 se muestra el detalle de los eventos presentados durante el periodo comprendido entre marzo a mayo del 2022 indicando número de ticket, evento, tiempo de solución y costo.

Tabla 29

Eventos de F.O. después de implementar el sistema SCYNODE

Ticket	Fecha	Hora	Problema	Tiempo solución	Costo horas extras
6752	03/03/2022	18:52	Organización	2h10	$18,46
6853	15/03/2022	17:25	Atenuación fibra	1h	$10,48
6856	16/03/2022	19:31	Corte fibra	2h30	$22,44
6866	18/04/2022	13:27	Corte fibra	3h	$2,5
6929	24/04/2022	09:12	Cambio baterías	1h20m	$2,5
7037	09/05/2022	17:33	Corte fibra	2h15m	$22,10
7136	27/05/2022	18:04	Organización	1h	$10,48
7326	01/05/2022	7:24	Corte fibra	2h	$2,50
Total					**$91,46**

Fuente: *SAITEL*

Como se muestra en la Tabla 29, el evento de equipos inhibidos desaparece de los registros, indicando que durante ese periodo no se ha presentado ese inconveniente, pero sí eventos puntuales propios de la red de fibra óptica.

4.4.1. Beneficio de cumplimiento de metas diarias

El personal de soporte técnico recibe solicitudes de clientes a diario, las mismas que deben ser solucionadas por los técnicos de SAITEL, un promedio de órdenes por día es de 4 las mismas que dependen del sitio donde se encuentre el domicilio del cliente y tipo de trabajo a realizar, cuando un evento de inhibición de equipos de OLTs, se debe acudir al sitio para levantar el servicio, generando un desfase en el cumplimiento de las metas diarias. Con la implantación del sistema SCYNODE, se cumple con las metas diarias ya que el reinicio de las OLTs se lo realiza de forma remota, así los técnicos cumplen con su ruta diaria conforme lo planificó el departamento de soporte.

4.4.2. Beneficio económico

Una vez que el sistema SCYNODE es implementado en el Nodo OLT-Caranqui de la empresa SAITEL, se convierte en una herramienta poderosa que permite a la compañía ahorrar recursos económicos, ya que, con el reinicio remoto de los dispositivos OLT, ya no es necesario que el personal técnico se movilice al sitio ahorrando combustible en el transporte, pago de horas extras al personal técnico designado, pago de horas extras al personal de soporte técnico encargado del monitoreo.

Como se verifica en la Tabla 30, en un periodo de tres meses la empresa gasta $35,84 en solucionar los eventos presentados en el nodo OLT-Caranqui, ahora realizando un cálculo estimado anual se debe multiplicar ese valor por 4 dando como resultado un costo de $143,36.

Además, con el registro de accesos al nodo se conserva el patrimonio de infraestructura de la empresa SAITEL ante cualquier evento de robo, así como se había presentado en situaciones anteriores, información obtenida de la entrevista realizada al Ing. Miguel Cuasapaz Jefe Técnico de la empresa en donde en el año 2021 el nodo OLT-Caranqui fue vulnerado en su seguridad generando pérdidas económicas a la empresa mediante el hurto de los equipos que conforman el nodo, los mismos son mostrados en la Tabla 30 con su respectivo valor económico.

Tabla 30

Pérdidas económicas por robo en nodo OLT Caranqui

Dispositivo	Costo
OLT SamrtAX MA56	$824,37
OLT SamrtAX MA56	$824,37
Batería HR12 V370 VRLA AGM	$232,96
Inversor 12V	$230
Core RB 3011	$90,16
Regulador de voltaje	$11,00
Toma regulada	$25,20
Equipo de energía Nanostation M5	$90
Total	**$2328,06**

Fuente: *SAITEL*

Como se observa en la Tabla 30, la empresa perdió $2328,06 afectando la economía de la compañía y la disponibilidad del servicio a los clientes.

Se realiza la recopilación de información respectiva y se obtiene un registro de 300 clientes que se conectan al nodo OLT Caranqui y reciben el servicio de internet mediante fibra óptica, se han retirado 15 abonados en un periodo de 1 año; durante ese periodo no estaba instalado el sistema SCYNODE y luego de la implementación se tiene que los retirados han sido solo 5 suscriptores motivo por el cual, el dispositivo resulta de gran beneficio económico para la empresa.

Para finalizar, luego de la implementación del sistema SCYNODE, la empresa SAITEL tendrá un beneficio anual de $2471,42, cabe resaltar que el ahorro es por nodo, si se llegara a implementar en toda la infraestructura de la empresa, el beneficio económico es mucho mayor.

4.4.3. Beneficio en relación al factor tiempo

El tiempo estimado en realizar la visita a los nodos para la revisión técnica pertinente en caso de avería es de aproximadamente una hora, dependiendo del lugar donde se encuentre el técnico más el tiempo de notificación entre otros, con el dispositivo de monitoreo remoto ese tiempo se transforma en un minuto aproximadamente en dar una solución, el personal de soporte técnico únicamente ingresa al servidor y realiza el reinicio remoto lo que resulta un beneficio para la empresa y para los usuarios garantizando la disponibilidad del servicio de Internet.

4.4.4. Beneficio de disponibilidad del servicio

La apreciación del cliente es de vital importancia cuando se presta el servicio de Internet; ante cualquier eventualidad, con el simple reinicio del Nodo el cliente no notará la caída del servicio haciendo que su apreciación sea de un servicio continuo y sin intermitencias, lo que resulta favorable para la empresa ante la solución de eventos que se registran en la red.

CAPÍTULO 5. CONLUSIONES Y RECOMENDACIONES

Este es el apartado final del documento en donde se presentan las conclusiones y recomendaciones encontradas a lo largo del desarrollo del proyecto. Es un capítulo corto que sintetiza el resultado de la investigación. También se muestran las recomendaciones con la finalidad de realizar investigaciones futuras y que el investigador tenga una pauta más clara y concisa al momento del desarrollo de dispositivos tecnológicos.

5.1. Conclusiones

- Mediante la fundamentación teórica, se estableció criterios técnicos con respecto al ensamblaje y propuesta de los subsistemas que conforman el dispositivo para un correcto funcionamiento, para luego integrarlos con la finalidad de obtener un resultado final que es contar con un sistema de reinicio remoto de OLTs.
- Mediante la recopilación de información sobre los eventos más relevantes con respecto a equipos de infraestructura de fibra óptica, se logró definir el término usado por la empresa SAITEL “OLT inhibida”, las causas que lo originan, las soluciones a dicho evento y la propuesta ante esa problemática.
- Mediante las técnicas de investigación como la entrevista y la encuesta, se estableció un listado de requerimientos lo que permitió diseñar un sistema que cumple con los objetivos del proyecto.
- Mediante la determinación de requerimientos de usuario, de arquitectura y del sistema, se escogió el Hardware y software más adecuado para dar cumplimiento a los mismos permitiendo que la funcionalidad del dispositivo corresponda al diseño planteado cumpliendo los objetivos del proyecto.
- La finalidad del sistema SCYNODE es el reinicio remoto del nodo Caranqui mediante su interfaz WEB, mismo que logró reestablecer el servicio de Internet a los abonados que se conectan al nodo OLT Caranqui, cuando el dispositivo esté inhibido, ahorrando recursos humanos, económicos y factor tiempo a la empresa SAITEL.
- El sistema SCYNODE ha tenido gran acogida por parte del personal administrativo de la empresa, tal es el caso que se tiene planificado destinar recursos para profundizar en la investigación y realizar prototipos modelo con la finalidad de implementar el sistema en cada uno de los nodos.
- El sistema SCYNODE logró activar el sistema de enfriamiento bajando la temperatura interna del gabinete del nodo mejorando así el rendimiento de los dispositivos.

- El sistema SCYNODE tiene aplicaciones de control remoto a nivel industrial ya que por los componentes electrónicos del mismo es adaptable a situaciones de control de corriente de hasta 10 Amperios de corriente, por ende, puede servir de base modelo para futuras investigaciones del IIOT.
- El sistema SCYNODE permite un ahorro anual de $2471,42 por nodo, lo que resulta beneficioso para la empresa SAITEL, ya que, además de contar con integridad en la infraestructura, se asegura el patrimonio de la misma.

5.2. Recomendaciones

- Se recomienda consultar información bibliográfica en fuentes confiables que muestren datos actualizados, las fuentes a buscar deben haber sido publicadas dentro de los últimos 5 años.
- Se recomienda el uso de la metodología iterativa ya que se puede realizar cambios en las diferentes etapas del proyecto convirtiéndose en una excelente metodología de ensayo y error.
- Se recomienda tomar precaución ante cualquier conexión mal establecida entre los componentes, ya que, se pueden generar cortos circuitos lo que puede afectar los dispositivos que conforman el dispositivo.
- Se recomienda conectar el dispositivo al respaldo de alimentación que cuentan los nodos de fibra óptica para que no exista interrupciones de acceso al sistema por cortes de energía eléctrica.
- Se recomienda contratar un plan contínuo de telefonía móvil para que no exista interrupciones de acceso al dispositivo y así garantizar el correcto funcionamiento de este.
- Se recomienda hacer uso de software y hardware libre con la finalidad de obtener compatibilidad entre la placa de desarrollo y diferentes sensores que conforman el sistema SCYNODE y así contar con una comunidad amplia que colabore con aportes de mejora a la presente investigación.
- Se recomienda realizar pruebas de funcionamiento de cada subsistema de forma separada, para al final integrar todo el dispositivo y verificar el desempeño del sistema en general y mantenerlo en un periodo de operación de 24 horas.
- Adaptar soluciones simples para grandes inconvenientes presentados en las empresas proveedoras de servicios de internet.

- Contratar los servicios de los proveedores de almacenamiento en la nube y estar al pendiente en la fecha de caducidad de los servicios contratados.

REFERENCIAS BIBLIOGRÁFICAS

Referencias

Ahmad, I., Namal, S., Ylianttila, M., & Gurtov, A. (2016). *Security in Software Defined Networks: A Survey.* India: IEEE Communications Surveys and tutorials.

Altexsoft. (18 de Enero de 2018). *Extreme Programming: Values, Principles, and Practices*. Obtenido de https://www.altexsoft.com/blog/business/extreme-programming-values-principles-and-practices/

Amazon. (09 de Julio de 2022). *Transceptor SFP de cobre 10/100/1000Base-T*. Obtenido de Transceptor SFP de cobre 10/100/1000Base-T: https://www.amazon.com/-/es/Transceptor-1000Base-T-negociaci%C3%B3n-autom%C3%A1tica-compatible/dp/B075XC7VL3?th=1

Angulano, J. L. (04 de Septiembre de 2019). *SEGURILATAM*. Obtenido de Protección en infraestuctura crítica en las telecomunicaciones: https://www.segurilatam.com/seguridad-por-sectores/infraestructuras-criticas/infraestructura-critica-telecomunicaciones_20190904.html

ARDUINO CL. (01 de Febrero de 2021). *PLACAS ARDUINO*. Obtenido de https://arduino.cl/producto/arduino-mega-2560/

AWS. (15 de 05 de 2021). *Amazon Web Services*. Obtenido de https://docs.aws.amazon.com/es_es/iot/latest/developerguide/what-is-aws-iot.html

AWS. (10 de Julio de 2022). *Supervisión remota de dispositivos IoT*. Obtenido de Supervisión remota de dispositivos IoT: https://aws.amazon.com/es/solutions/implementations/remote-monitoring-of-iot-devices/

Bt-PON. (09 de Julio de 2022). *4GE 2VoIP 5G CATV Dual Band WiFi ONU BT-711XR*. Obtenido de 4GE 2VoIP 5G CATV Dual Band WiFi ONU BT-711XR: https://www.bt-pon.com/producto/4ge-2voip-5g-catv-dual-band-wifi-onu-bt-711xr

Cánovas Izquierdo, J. L., Díaz , O., Puente, G., & García Molina, J. (2011). *ScheMol: Un lenguaje específico del dominio para extraer modelos de bases de datos relacionales.* España: ONEKIN.

CISCO. (29 de Junio de 2022). *Qué es el monitoreo de red*. Obtenido de Qué es el monitoreo de red: https://www.cisco.com/c/es_mx/solutions/automation/what-is-network-monitoring.html

Claro. (01 de Julio de 2022). *Mapas de cobertura Claro*. Obtenido de Mapas de cobertura Claro: https://www.geodata.com.ec/

Criollo Ortiz, P. J., & Aguirre Carvajar, F. V. (2017). *Diseño de una metodología para el control de servicios convergentes, basada en la calidad de servicio desde el punto de vista del usuario. Propuesta regulatoria para servicios convergentes en el ecuador.* Quito: EPN.

CXR. (09 de Julio de 2022). *GP-2500 GPON OLT*. Obtenido de GP-2500 GPON OLT: https://www.cxr.com/en/produits/gpon-olt-gp2500-215.html

GAIMC. (21 de Febrero de 2021). *Focus on Process Control*. Obtenido de https://www.gaimc.com/

gtlan. (09 de Julio de 2022). *¿Cuáles son las necesidades de ventilación y refrigeración en un rack de comunicaciones?* Obtenido de ¿Cuáles son las necesidades de ventilación y refrigeración en un rack de comunicaciones?: https://www.gtlan.com/cuales-son-las-necesidades-de-ventilacion-y-refrigeracion-en-un-rack-de-comunicaciones/

Guévin, M. (11 de Marzo de 2019). *NUTCACHE*. Obtenido de Principales Métodos, Enfoques y Técnicas de Gestión de Proyectos: https://www.nutcache.com/es/blog/8-principales-metodos-enfoques-y-tecnicas-de-gestion-de-proyectos/

Haworth, S. (15 de Enero de 2021). *thedigitalprojectmanager*. Obtenido de https://thedigitalprojectmanager.com/es/agile-frente-a-waterfall/

Hernández, L. d. (2 de Diciembre de 2019). *PROGRAMARFACIL*. Obtenido de https://programarfacil.com/blog/arduino-blog/leer-el-sensor-de-temperatura-lm35-en-arduino/#comment-4830197541

Horcajo, A. (04 de Abril de 2020). *EL ECONOMISTA*. Obtenido de La seguridad de las telecomunicaciones: nuevos desafíos: https://www.eleconomista.es/firmas/noticias/10464683/04/20/La-seguridad-de-las-telecomunicaciones-nuevos-desafios.html

Instituto Nacional de Metereología e Hidrología. (19 de 01 de 2020). *INAMHI*. Obtenido de https://www.inamhi.gob.ec/dir-de-informacion-hm/

Intellinet. (09 de Julio de 2022). *Módulo Tranceptor SFP Gigabit RJ45 de cobre*. Obtenido de Módulo Tranceptor SFP Gigabit RJ45 de cobre: https://es.intellinetnetwork.eu/products/intellinet-es-modulo-transceptor-sfp-gigabit-rj45-de-cobre-523882

ITU. (2015). *La seguridad de las telecomunicaciones y las tecnologías de la información.* Madrid: ITU.

Llamas, L. (04 de Diciembre de 2015). *INGENIERÍA, informática y diseño*. Obtenido de https://www.luisllamas.es/usar-un-interruptor-magnetico-con-arduino-magnetic-reed/

Mantelero, A. (2017). From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era. 139-158.

MatrixTelcom. (10 de Julio de 2022). *Bandeja de distribución para rack ODF 48 hilos*. Obtenido de Bandeja de distribución para rack ODF 48 hilos: https://matrixtelcom.co/producto/bandeja-de-distribucion-para-rack-odf-48-hilos/

Mikaeil, A. M., Hu, W., Ye, T., & Hussain, S. B. (2017). Performance evaluation of XG-PON based mobile front-haul transport in cloud-RAN architecture. *IEEE Xplore*, 3.

Mikrotik. (09 de Julio de 2022). *Foro Mikrotik*. Obtenido de Foro Mikrotik: https://forum.mikrotik.com/viewtopic.php?t=125574

Mikrotik. (09 de Julio de 2022). *The DUDE*. Obtenido de The DUDE: https://mikrotik.com/thedude

Nagios. (09 de Julio de 2022). *Qué es Nagios*. Obtenido de Qué es Nagios: https://www.nagios.com/

Oracle. (22 de Julio de 2022). *Circulación del aire de enfriamiento desde baldosas perforadas*. Obtenido de Circulación del aire de enfriamiento desde baldosas perforadas: https://docs.oracle.com/cd/E63755_01/html/E63764/gomsm.html

PAESSLER. (08 de Julio de 2022). *PRTG Network Monitor*. Obtenido de PRTG Network Monitor: https://www.paessler.com/prtg

Pasian, B. (2015). *Design Methods and Practices for Research of Project Management.* Surrey: Gower Publishing Company.

PRINCE2. (16 de Junio de 2021). *PRINCE2*. Obtenido de https://www.prince2.com/usa

PROMETEC. (14 de Enero de 2020). *MÓDULO GSM/GPRS: LLAMAR Y ENVIAR SMS*. Obtenido de https://www.prometec.net/gprs-llamar-enviar-sms/

Romero Castro, M. I., Figueroa Morán, G. L., Vera Navarrete, D. S., & Álava Cruzatty, J. E. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades.* Alicante: 3CIENCIAS.

SAITEL. (10 de Julio de 2022). *SAITEL Antecedentes*. Obtenido de SAITEL Antecedentes: https://saitel.ec/antecedentes/

Saleh, M. (2019). *The Three Dimensions of Security*. International Journal of Security.

Santander, P. G. (2019). *Diseño de un sistema de alerta ante estados de hiperglucemia e hipoglucemia, sintomatologías previas a un coma diabético.* Ibarra: UTN.

Silva Ponce de León, C. (2018). *Seguridad de las Redes y Sistemas de Telecomunicaciones Críticos.* Brasil: csilva.

Suárez, J. P. (2021). Sistema de Control Redundante basado en una arquitectura IOT. 17.

Telequismo. (22 de Julio de 2022). *FTTH esquema*. Obtenido de FTTH esquema: https://www.telequismo.com/ftth_esquema2/

UNIR. (2021). No repudio, ¿qué significa en seguridad informática? 1-3.

Valero, A. (28 de Noviembre de 2016). *DIWO*. Obtenido de https://www.areatecnologia.com/electricidad/rele.html

Varela, A., & Ron , S. (2020). *Geografía y Clima del Ecuador.* Quito: PUCE.

Vaseashta, A., Susmann, P., & Braman, E. (2017). *Cyber security and resiliency policy framework.* Northfield: IOS Press.

YCICT CO . (15 de 02 de 2021). *YCICT CO LIMITED*. Obtenido de https://www.ycict.net/es/products/huawei-smartax-ma5608t-olt/

Zenoss. (09 de Julio de 2022). *Modern Network Monitoring*. Obtenido de Modern Network Monitoring: https://www.zenoss.com/product/network-monitoring

Zumba Gamboa, J. P., & León Arreaga, C. A. (2018). *Evolución de las Metodologías y Modelos utilizados en el Desarrollo de Software.* Guayaquil: INNOVA.

ANEXOS

Anexo 1 Encuesta de Stakeholders

UNIVERIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÉA EN CIENCIAS APLICADAS

CIERCOM

Encuesta dirigida a personal de soporte técnico de la empresa SAITEL

El objetivo del presente documento es identificar los requerimientos de Stakeholders para implementar un sistema de reinicio automático.

Marque con una X el casillero correspondiente según su opinión:

1. Dentro de la infraestructura de F.O de la empresa SAITEL, ¿con qué frecuencia ocurren eventos puntuales?

Diario	☐
Semanalmente	☐
Mensualmente	☐
Nunca	☐

2. En caso de existir un evento puntual en nodos es necesario la movilización de personal técnico in situ

Si	☐
No	☐

3. Cree Ud. necesario que se notifique a la empresa y/o personal técnico cuando un gabinete de equipos es abierto

Si	☐
No	☐

4. Qué tipo de eventos son los más recurrentes dentro de los nodos de FO (mencione tres)

1.

2.

3.

5. Para la apreciación de información en general ¿cuál cree que es la mejor opción?

Servidor web	
Aplicaciones Móviles	

6. Que tan necesario considera la implementación de un sistema de control y monitoreo remoto de la OLT.

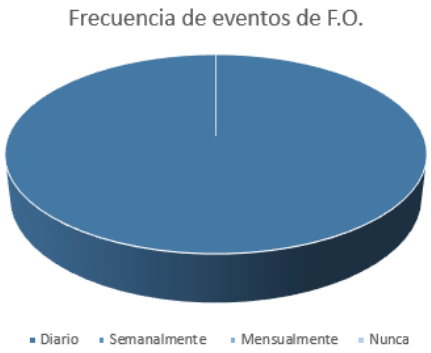
Muy necesario	
Medianamente necesario	
Poco necesario	
Nada Necesario	

Anexo 2. Tabulación de encuestas

En la primera pregunta se solicitó a los encuestados señalar la frecuencia con que ocurren eventos puntuales de infraestructura de F.O. de la empresa SAITEL, en donde el 100% de la muestra señaló que diariamente ocurren eventos de infraestructura de fibra óptica. Los resultados se muestran en la Figura 56.

Figura 56

Frecuencia de eventos puntuales



Fuente: *Autoría*

Durante la encuesta el personal técnico señala que a diario se presentan eventos puntuales de F.O. en donde el evento es monitoreado por el departamento de soporte técnico,

luego es reportado al técnico de soporte de turno para presentar una solución rápida ante esa eventualidad.

El técnico debe movilizarse al sitio para realizar la revisión respectiva, en este caso el levantamiento del servicio de Internet, los resultados se muestran en la siguiente Figura 57.

Figura 57

Movilización personal técnico

Fuente: *Autoría*

La siguiente pregunta sirvió para establecer el grado de necesidad de incorporar un sistema de alarma y notificación de acceso no autorizado al nodo, en donde el 100% de encuestados cree que es necesaria la presencia de un dispositivo que indique cuando un gabinete de equipos es abierto. Los resultados se muestran en la Figura 58.

Figura 58

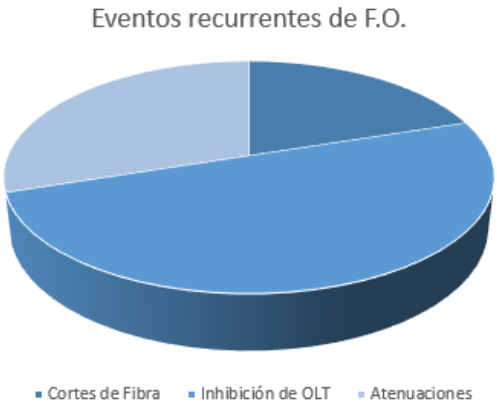
Necesidad de alerta de ingreso al gabinete

Fuente: *Autoría*

La siguiente pregunta sirvió para determinar qué tipo de evento ocurre con más frecuencia en la red de Fibra Óptica de SAITEL, cabe resaltar que se mencionaron 3 eventos recurrentes: Cortes de Fibra, Inhibición de Equipos y Atenuaciones. Los resultados fueron los siguientes: el 20% de la muestra dijo que los eventos más recurrentes son los cortes de Fibra, el 50% manifiesta que son la inhibición de Equipos y el otro 30% restante indicó que las atenuaciones son los eventos más recurrentes dentro de la infraestructura. Los resultados se muestran en la Figura 59.

Figura 59

Eventos recurrentes de F.O.

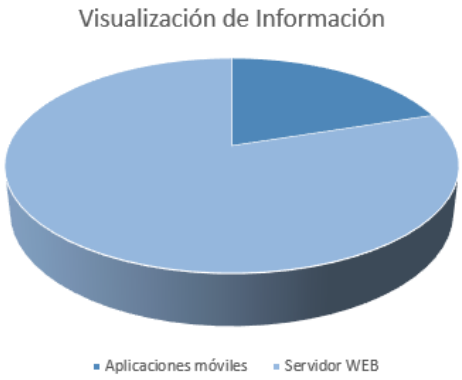


Fuente: *Autoría*

En la siguiente pregunta se indagó sobre como prefiere que sea visualizada la información, como resultado se obtuvo que el 20% de la muestra prefiere aplicaciones móviles y que el 80% de los encuestados optar por el uso de un servidor WEB.

Figura 60

Apreciación de resultados



Fuente: *Autoría*

El grado de necesidad de implantación de un dispositivo de monitoreo remoto de los nodos de fibra óptica se estima mediante la pregunta 6 de la encuesta, en donde, el 80% de la muestra estima que es muy necesario la colocación de un sistema de monitoreo en cada nodo de F.O. y un 20% estima que es medianamente necesario. Los resultados se muestran en la Figura 61.

Figura 61

Necesidad de implementación del sistema SCYNODE

Fuente: *Autoría*

Anexo 3. Líneas de código en la placa de desarrollo

Código para la inicialización de variables

```
#include <SoftwareSerial.h>  //Incluye las librerías necesarias para la ejecución
del programa
#include <string.h>
#include <DHT.h>
 #define DHTPIN 12            // Definimos el pin digital donde se conecta el
sensor de temperatura
#define DHTTYPE DHT11
DHT dht(DHTPIN, DHTTYPE);     // Inicializamos el sensor DHT11
SoftwareSerial sim900(2,3);   // RX, TX
byte buffer[64];              //Buffer para recibir datos del puerto serie
int count=0, m=0;
float h,t ;
#define phonenumber "0983056578    //Número de teléfono autorizado, debe ser el
mismo que el formato que recibe el SMS,
const int Power = 13,Rele = 8, magnetico=11, ctemp=6;  // Definición Power
encendido por software SIM900
char control=' ';
void setup(){
  Serial.begin(9600);
  sim900.begin(9600);
  dht.begin();                     // Comenzamos el sensor DHT
  delay(500);                      // Tiempo suficiente para ingresar a la red
telefónica.
  Sim900_Inti();
  sim900.print("AT+CMGF=1\r");    // Configuración del módulo GSM en modo texto.
  delay(500);
pinMode(magnetico, INPUT);        // declaramos sensor magnético como entrada
pinMode(Rele, OUTPUT) ;           // LedPower como salida
pinMode(ctemp, OUTPUT) ;         // ctemp como salida
digitalWrite(ctemp, HIGH);
digitalWrite(Rele, LOW);
pinMode( Power, OUTPUT) ;        // Power como salida GSM
digitalWrite(Power, HIGH);       //Encendido por Software SIM900
delay(500);
digitalWrite(Power, LOW);
Serial.println("State: INICIANDO.....");
}
```

Código para la lectura de sensores

```
void loop()
{
  delay(5000);                              // Esperamos 5 segundos entre medidas
 m = digitalRead(magnetico);                // Leemos estado de sensor magnético
 h = dht.readHumidity();                    // Leemos la humedad relativa
  t = dht.readTemperature();                // Leemos la temperatura en grados
centígrados (por defecto)
 float f = dht.readTemperature(true);       // Leemos la temperatura en grados
Fahreheit
  if (isnan(h) || isnan(t)) {               // Comprobamos si ha habido algún
error en la lectura
    Serial.println("Error obteniendo los datos del sensor DHT11");
    return;
  }
  float hif = dht.computeHeatIndex(f, h);     // Calcular el índice de calor en
Fahreheit
  float hic = dht.computeHeatIndex(t, h, false);   // Calcular el índice de calor
en grados centígrados
  controlTemp();                             // Verificación módulo de ventilación
   if (Serial.available())                   // Verifica si se dispone de datos en
el puerto serie por hardware
    sim900.write(Serial.read());             // y los escribe en el escudo SIM900
    envioHTTP();
```

```
}
void clearBufferArray()                     // Limpia el buffer
{
  for (int i=0; i<count;i++)
    { buffer[i]=NULL;}                      // borrar todos los índices del
arreglo
}
void Sim900_Inti(void)
{
  sim900.println("AT+CLIP=1");             // Activa la identificación de llamada
 delay(1000);
 sim900.println("AT+CSMP=17,167,0,0");
  delay(1000);
  sim900.println("AT+CMGF=1");             //Configura el modo texto para enviar
o recibir mensajes
  delay(1000);
  sim900.println("AT+CNMI=2,2,0,0,0");     // Saca el contenido del SMS por el
puerto serie del GPRS
  delay(1000);
  sim900.println("AT+CGDCONT=1,\"IP\",\"internet.cnt.net.ec\"");
// Establece parámetros PDP
delay(2000);
mostrarDatosSeriales();
sim900.println("AT+CSTT=\"internet.cnt.net.ec\",\"\",\"\""); //comando configura
el APN, nombre de usuario y contraseña."gprs.movistar.com.ar","wap","wap"-
>Movistar Arg.
delay(2000);
mostrarDatosSeriales();
```

Código para el establecimiento de conexión inalámbrica con la red GPRS

```
sim900.println("AT+CIICR");
//Realizar una conexión inalámbrica con gprs o csd
delay(2000);
mostrarDatosSeriales();
sim900.println("AT+CIFSR");
// Obtenemos nuestra IP local
delay(2000);
  sim900.println("AT+SAPBR=3,1,\"Contype\",\"GPRS\"");
  delay(2000);
  mostrarDatosSeriales();
  sim900.println("AT+SAPBR=3,1,\"APN\",\"www\"");
  delay(2000);
  mostrarDatosSeriales();
  sim900.println("AT+SAPBR=1,1");
  delay(2000);
  mostrarDatosSeriales();
  sim900.println("AT+SAPBR=2,1");
  delay(2000);
  mostrarDatosSeriales();
  sim900.println("AT+HTTPINIT");
  delay(2000);
  mostrarDatosSeriales();
  sim900.println("AT+HTTPPARA=\"CID\",1");
  delay(2000);
}
void Cmd_Read_Act(void)    //Esta función lee los SMS enviados al escudo SIM900 y
actúa en base a lo recibido
{
  char buffer2[64];
  char comparetext[25];
  for (int i=0; i<count;i++)
```

Código para el envío de datos

```
 { buffer2[i]=char(buffer[i]);}
  memcpy(comparetext,buffer2,25);
//copiar el contenido de la matriz
  if (strstr(comparetext,"HTTPREAD"))
//encontrar palabras específicas de una cadena
  {
  if (strstr(buffer2,"suc1"))
//Recibe instrucción On
  {
      digitalWrite(Rele, HIGH) ;
        delay(4000);                // Espera medio segundo
        digitalWrite(Rele, LOW);    // Apaga el pin 13 relé
        delay(4000);                // Espera medio segundo
        reinicioHTTP();
        Serial.println("\nSistema Reiniciado")
  }
}
}
void inicioHTTP()              //Función de envío de datos tomados por sensores
vía HTTP
{
  sim900.println("AT+CGDCONT=1,\"IP\",\"internet.cnt.net.ec\""); // Establece
parámetros PDP
delay(2000);
mostrarDatosSeriales();
sim900.println("AT+CSTT=\"internet.cnt.net.ec\",\"\",\"\"");    //comando
configura el APN, nombre de usuario y
contraseña."gprs.movistar.com.ar","wap","wap"->Movistar Arg.
delay(2000);
mostrarDatosSeriales();
sim900.println("AT+CIICR"); //Realizar una conexión inalámbrica con gprs o csd
delay(2000);
mostrarDatosSeriales();
sim900.println("AT+CIFSR"); // Obtenemos nuestra IP local
delay(2000);
}
void envioHTTP()            //Función de envío de datos tomados por sensores vía
HTTP
{
  inicioHTTP();
sim900.println("AT+CIPSTART=\"TCP\",\"18.118.4.62\",\"80\""); //Indicamos el tipo
de conexión, url o dirección IP y puerto al que realizamos la conexión
delay(3000);
mostrarDatosSeriales();
sim900.println("AT+CIPSEND");   //Envía datos a través de una conexión tcp o udp
delay(10000);
mostrarDatosSeriales();
String datos="GET /indexcon.php?id=001&tem=";
sim900.print(datos);            //Envía datos al servidor remoto
sim900.print(t);
sim900.print("&hum=");
sim900.print(h);
sim900.print("&mag=");
sim900.print(m);
```

Establecimiento de conexión con el servidor de AWS

```
sim900.println(" HTTP/1.1\r\nHost: 18.118.4.62\r\n");
delay(3000);
mostrarDatosSeriales();
sim900.println((char)26);
delay(2000);
//Ahora esperaremos una respuesta pero esto va a depender de las condiciones de
la red y este valor quizá debamos modificarlo dependiendo de las condiciones de
la red
```

```
sim900.println();
mostrarDatosSeriales();
sim900.println("AT+CIPSHUT");  //Cierra la conexión(Desactiva el contexto GPRS
PDP)
delay(2000);
mostrarDatosSeriales();
  sim900.println("AT+SAPBR=2,1");
  delay(2000);
  mostrarDatosSeriales();
  sim900.println("AT+HTTPPARA=\"CID\",1");
  delay(2000);
  mostrarDatosSeriales();
sim900.println("AT+HTTPPARA=\"URL\",\"http://18.118.4.62/test.php?id=001\"");
  delay(2000);
  mostrarDatosSeriales();
  sim900.println("AT+HTTPACTION=0");
  delay(4000);
  mostrarDatosSeriales();
   sim900.println("AT+HTTPREAD");
  delay(3000);
  mostrarDatosSeriales();
}
```

Código para la activación remota del relé

```
void reinicioHTTP()         //Función de envío/recepción de datos de reinicio vía
HTTP
{
 inicioHTTP();
 sim900.println("AT+CGDCONT=1,\"IP\",\"internet.cnt.net.ec\""); // Establece
parámetros PDP
delay(2000);
mostrarDatosSeriales_reinicio();
sim900.println("AT+CSTT=\"internet..ec\",\"\",\"\""); //Comando configura el APN,
nombre de usuario y contraseña."gprs.movistar.com.ar","wap","wap"->Movistar Arg.
delay(2000);
mostrarDatosSeriales_reinicio();
sim900.println("AT+CIICR");     //Realizar una conexión inalámbrica con gprs o
csd
delay(2000);
mostrarDatosSeriales_reinicio();
sim900.println("AT+CIFSR");      // Obtenemos nuestra IP local
delay(2000);
sim900.println("AT+CIPSTART=\"TCP\",\"18.118.4.62\",\"80\""); //Indicamos el tipo
de conexión, url o dirección IP y puerto al que realizamos la conexión
delay(2000);
mostrarDatosSeriales_reinicio();
sim900.println("AT+CIPSEND");    //Envía datos a través de una conexión tcp o udp
delay(10000);
mostrarDatosSeriales_reinicio();
String datos="GET /restart.php?id=001";
sim900.print(datos);             //Envía datos al servidor remoto
sim900.println(" HTTP/1.1\r\nHost: 18.118.4.62\r\n");
delay(3000);
mostrarDatosSeriales_reinicio();
sim900.println((char)26);
delay(2000);         //Ahora esperaremos una respuesta pero esto va a depender de
las condiciones de la red y este valor quizá debamos modificarlo dependiendo de
las condiciones de la red
sim900.println();
mostrarDatosSeriales_reinicio();
sim900.println("AT+CIPSHUT");      //Cierra la conexión(Desactiva el contexto
GPRS PDP)
delay(2000);
mostrarDatosSeriales_reinicio();
```

```
}
void mostrarDatosSeriales()       //Muestra los datos que va entregando el sim900
{
Serial.write(sim900.read());
if (sim900.available())
  {
    while(sim900.available())     //Leyendo datos del arreglo de caracteres
    {
      //Serial.println("phonenumber");
      buffer[count++]=sim900.read();   //Almacenando los datos del arreglo en un
buffer
      if(count == 64)break;
  }
    Serial.write(buffer,count);
    Cmd_Read_Act();
    clearBufferArray();
    count = 0;
  }
}
void mostrarDatosSeriales_reinicio()  //Muestra los datos que va entregando el
sim900
{
Serial.write(sim900.read());
  if (sim900.available())
  {
    while(sim900.available())         //Leyendo datos del arreglo de caracteres
    {
      buffer[count++]=sim900.read();  //Almacenando los datos del arreglo en un
buffer
      if(count == 64)break;
  }
    Serial.write(buffer,count);
    clearBufferArray();
```

Código para la activación del sistema de refrigeración

```
void controlTemp()
{
    if (t < 28){
//Activación del módulo de ventilación
      digitalWrite(ctemp, LOW);
      Serial.println("Ventilador Activado");
      }       else {
        digitalWrite(ctemp, HIGH);
        }
}
```

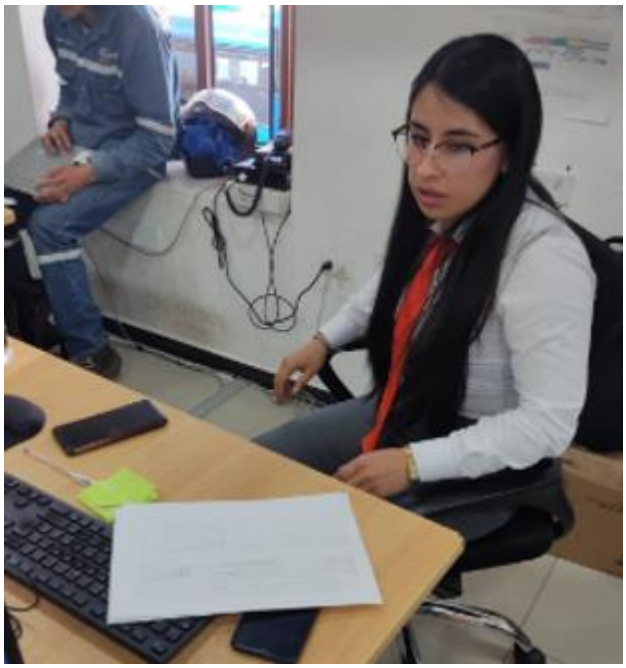
Anexo 4. Evidencias fotográficas

Las evidencias fotográficas son evidencia del trabajo realizado, para ello, se muestran fotos de la toma de datos en el departamento de soporte técnico.

En la Figura 62 se muestra la encuesta dirigida a la encargada del departamento de soporte técnico inalámbrico de la empresa SAITEL.

Figura 62

Encuesta departamento de soporte técnico

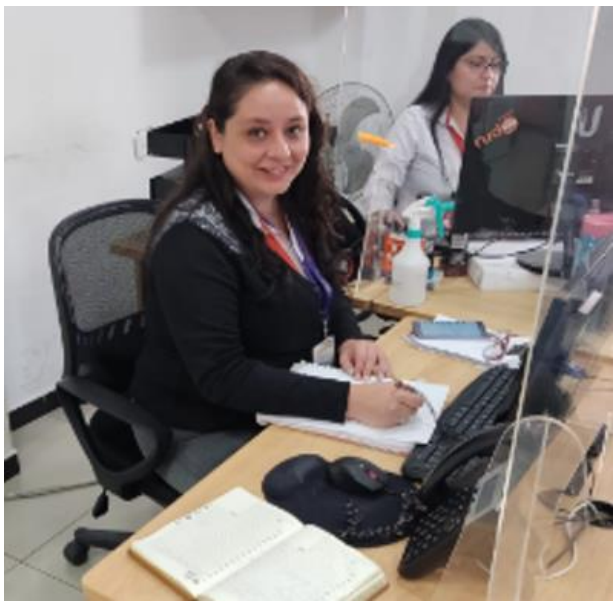


Fuente: *Autoría*

En la Figura 63 se muestra la encuesta dirigida a la encargada del departamento de soporte técnico de fibra óptica de la empresa SAITEL.

Figura 63

Encuesta al departamento de soporte técnico de la empresa SAITEL



Fuente: *Autoría*

En la figura 64 se muestra la encuesta realizada a un técnico de la empresa SAITEL

Figura 64

Encuesta al departamento técnico de la empresa SAITEL

Fuente: *Autoría*

En la Figura 65 se muestra pruebas de funcionamiento en un ambiente controlado, es decir en un gabinete que no se encuentra operativo pero que tiene los mismos dispositivos de red en su interior que el Nodo OLT-Caranqui.

Figura 65

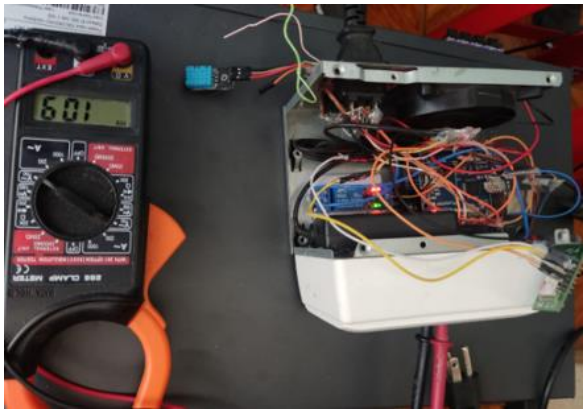
Pruebas del sistema SCYNODE en un ambiente controlado

Fuente: *Autoría*

En la Figura 66 se muestran las conexiones internas del sistema SCYNODE.

Figura 66

Conexiones internas del sistema SCYNODE



Fuente: *Autoría*

En la Figura 67 se muestra la interfaz gráfica del servidor web en donde se evidencia el registro de temperatura del nodo OLT-Caranqui de la empresa SAITEL.

Figura 67

Datos de temperatura mostrados en el servidor web alojado en la nube

Fuente: *Autoría*