UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE CUENCA

CARRERA DE TELECOMUNICACIONES

ACTUALIZACIÓN DE EQUIPOS ACTIVOS PARA LA RED DE DATOS DE LA UETS

Trabajo de titulación previo a la obtención del título de Ingeniero en Telecomunicaciones

AUTOR: MATEO SEBASTIÁN CASTRO CALLE
ROBERTH VINICIO PACHECO VALDIVIEZO

TUTOR: ING. JUAN PAÚL INGA ORTEGA, MsC.

Cuenca – Ecuador
2024

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Nosotros, Mateo Sebastián Castro Calle con documento de identificación N° 0104676192 y Roberth Vinicio Pacheco Valdiviezo con documento de identificación N° 0706702966; manifestamos que:

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

Cuenca, 22 de julio de 2024

Atentamente,

Mateo Sebastián Castro Calle

0104676192

Roberth Vinicio Pacheco Valdiviezo

0706702966

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

Nosotros, Mateo Sebastián Castro Calle con documento de identificación N° 0104676192 y Roberth Vinicio Pacheco Valdiviezo con documento de identificación N° 0706702966, expresamos nuestra voluntad y por medio del presente documento cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del Proyecto Técnico: "Actualización de equipos activos para la red de datos de la UETS" el cual ha sido desarrollado para optar por el título de: Ingeniero en Telecomunicaciones, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

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

Cuenca, 22 de julio de 2024

Atentamente,

Mateo Sebastián Castro Calle

0104676192

Roberth Vinicio Pacheco Valdiviezo

0706702966

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Juan Paúl Inga Ortega con documento de identificación N° 0104166491, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: ACTUALIZACIÓN DE EQUIPOS ACTIVOS PARA LA RED DE DATOS DE LA UETS, realizado por Mateo Sebastián Castro Calle con documento de identificación N° 0104676192 y Roberth Vinicio Pacheco Valdiviezo con documento de identificación N° 0706702966, obteniendo como resultado final el trabajo de titulación bajo la opción Proyecto Técnico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Cuenca, 22 de julio de 2024

Atentamente,

Ing. Juan Paúl Inga Ortega
0104166491

AGRADECIMIENTOS

Con profunda gratitud, dedico este trabajo a mi familia, cuyo inquebrantable apoyo, amor y comprensión han sido fundamentales en cada etapa de este arduo camino.Su confianza en mis capacidades ha sido la fuerza motriz que me ha permitido superar los desafíos y alcanzar este logro.
Agradezco sinceramente al Ing. Juan Inga, por su excepcional guía durante el desarrollo de este proyecto. Su comprensión y empatía hacia mi persona han sido cruciales para enfrentar los desafíos del proceso. Aprecio sinceramente su dedicación, paciencia y el valioso asesoramiento que me brindó. Gracias por su constante apoyo y por hacer una diferencia significativa en mi experiencia académica.
Extiendo mi agradecimiento a la Unidad Educativa Técnico Salesiano por brindarme la confianza para llevar a cabo este proyecto en sus instalaciones. Su completo respaldo y apoyo han sido fundamentales para el éxito de esta iniciativa. Gracias por su colaboración y por confiar en mi trabajo.
No puedo dejar de expresar mi agradecimiento a mi compañero de tesis, con quien he tenido el honor de transitar este proceso educativo desde su inicio. Su colaboración y compromiso han sido esenciales para el éxito de nuestro proyecto. Le extiendo mis mejores deseos de éxito y bendiciones en su futuro.

Mateo Sebastián Castro Calle

Quiero expresar mi más profundo agradecimiento a mi tutor, cuyas correcciones y sugerencias han sido fundamentales para que este trabajo alcance el nivel de profesionalismo deseado. Sus palabras y orientación no solo me han permitido cumplir con los requerimientos necesarios, sino que también han enriquecido mi comprensión y habilidades en el ámbito académico. Gracias por sus valiosas enseñanzas y por ser un mentor excepcional, tanto en su rol de tutor como de docente.

Extiendo mi gratitud a todos mis profesores, quienes han compartido generosamente sus conocimientos y experiencias a lo largo de mi trayectoria universitaria. Cada uno de ustedes ha dejado una huella imborrable en mi formación, y llevaré con orgullo sus enseñanzas a lo largo de toda mi vida profesional. Sus esfuerzos y dedicación han sido esenciales para que hoy pueda estar culminando esta importante etapa.

Finalmente, quiero agradecer profundamente a mi compañero de tesis. Tu colaboración, apoyo y dedicación han sido cruciales para sacar adelante este proyecto. Gracias de corazón por tu compromiso y por ser un verdadero compañero en este viaje. Espero sinceramente que podamos seguir contando el uno con el otro, tanto en nuestra vida diaria como en el ámbito laboral.

Roberth Vinicio Pacheco Valdiviezo

DEDICATORIAS

Dedicatoria de Mateo Sebastián Castro Calle

A mi querida familia,

Dedico este trabajo a ustedes por su constante apoyo y amor a lo largo de todo este proceso. Su ayuda ha sido fundamental en cada etapa, desde las noches largas hasta los días de agotamiento. Cada gesto de apoyo ha sido crucial para mantenerme enfocado y motivado.

Han estado a mi lado en los momentos de alegría y en las dificultades, compartiendo mis avances y dándome consuelo en los obstáculos. Su presencia constante y su confianza en mí han sido la motivación para seguir adelante y alcanzar mis objetivos.

Gracias por su sacrificio y por estar siempre dispuestos a escucharme y celebrar mis logros. Este éxito es tanto suyo como mío, ya que sin su apoyo, no habría sido posible.

Dedicatoria de Roberth Vinicio Pacheco Valdiviezo

Este trabajo está dedicado con todo mi corazón a mis padres y hermanos, quienes han sido mi pilar fundamental desde el inicio de esta etapa universitaria. Su apoyo incondicional y sus constantes palabras de aliento han sido la fuerza motriz que me ha impulsado a seguir adelante, superar los desafíos y formarme como una persona íntegra.

A mis padres, agradezco profundamente sus sacrificios y su amor inagotable. Gracias por enseñarme el valor del esfuerzo, la perseverancia y la importancia de la educación. Sus enseñanzas han sido la brújula que ha guiado cada uno de mis pasos.

A mis hermanos, agradezco su compañía y su ejemplo. Su confianza en mis capacidades y su constante motivación me han dado el valor necesario para enfrentar cualquier obstáculo y seguir persiguiendo mis sueños.

Este trabajo no solo representa el conocimiento adquirido durante mi formación académica, sino también el crecimiento personal y los valores inculcados por mi familia. Cada página, cada idea y cada esfuerzo invertido en esta tesis lleva consigo un pedazo de todo lo que he aprendido y experimentado a lo largo de estos años.

A ustedes, que han estado a mi lado en cada momento, les dedico este logro con gratitud y amor. Esta tesis es tanto suya como mía, pues sin ustedes, este viaje no habría sido posible.

Índice general

Índice de figuras

Índice de tablas

Resumen

Este proyecto se basó en actualizar los equipos activos de red de datos de la UETS. Para ello, se realizó una recopilación exhaustiva de datos que permitió verificar el estado actual de los equipos y su funcionamiento. Se identificaron deficiencias en la red inalámbrica debido a la cobertura inadecuada de los AP, lo que limitaba la conectividad en diversas áreas de la institución.

Se analizaron las necesidades y requerimientos de la UETS, revelando que la mayoría de los equipos estaban obsoletos. Con base en este análisis, se determinaron las necesidades específicas de actualización para cada zona de la institución. Posteriormente, se establecieron nuevas topologías de red, abarcando todas las áreas que requerían acceso a internet.

Se llevó a cabo un proceso de selección de equipos, eligiendo aquellos que se ajustaban a las políticas y al presupuesto financiero de la UETS. La instalación y configuración incluyó la implementación de varios switches de acceso y AP en la mayoría de las zonas, además de la instalación de un switch de core y un firewall en el cuarto de equipos principal.

Finalmente, se verificaron los cambios mediante simulaciones y mediciones, constatando mejoras significativas en la confiabilidad y calidad del servicio de la red. Los nuevos AP proporcionaron una cobertura casi total, permitiendo a los colaboradores de la UETS disfrutar de una conectividad a internet confiable y sin interrupciones, maximizando el uso del ancho de banda disponible.

Palabras clave: Actualización; Cobertura; Implementación; Despliegue de Redes de Computadoras; TIC; Topología de Red.

Abstract

This project was based on updating the active data network equipment at UETS. For this purpose, an exhaustive data collection was carried out to verify the current state of the equipment and its operation. Deficiencies were identified in the wireless network due to inadequate coverage of the access points, which limited connectivity in various areas of the institution.

The needs and requirements of UETS were analyzed, revealing that most of the equipment was obsolete. Based on this analysis, specific upgrade needs were determined for each area of the institution. Subsequently, new network topologies were established, covering all areas requiring Internet access.

An equipment selection process was carried out, choosing those that fit the policies and financial budget of UETS. The installation and configuration included the implementation of several access switches and APs in most areas, in addition to the installation of a core switch and a firewall in the main equipment room.

Finally, the changes were verified through simulations and measurements, showing significant improvements in network reliability and quality of service. The new APs provided almost total coverage, allowing UETS collaborators to enjoy reliable and uninterrupted Internet connectivity, maximizing the use of the available bandwidth.

Keywords: Upgrade; Coverage; Implementation; ICT; Deployment of Computer Network; Network Topology .

Antecedentes

La necesidad de contar con una red de datos, también llamada red informática, en instituciones educativas en principio surgen como una respuesta para mejorar la eficiencia administrativa, por ejemplo dando seguimiento a la asistencia o a la gestión de inventario para responder de forma más precisa a los cambios. Esta eficiencia administrativa también se ve mejorada al permitir compartir recursos como impresoras y escáneres, lo que puede llevar a un uso más eficiente del equipo escolar y a reducir los costos. Gracias a la creación de redes, los profesores y los alumnos pueden comunicarse fácilmente a través del correo electrónico y otras plataformas en línea, lo que fomenta un ambiente de aprendizaje colaborativo También, incluir redes informáticas permite a las instituciones educativas acceder a recursos didácticos novedosos que están surgiendo frente al ingreso de las tecnologías de la información y la comunicación (TIC) [1], [2].

Así, es posible identificar que el uso de las redes de datos y por tanto de las TIC, permiten mejoras a los entornos de aprendizaje a través del incremento de la calidad de la educación, flexibilidad y accesibilidad en el apoyo al aprendizaje electrónico. La integración de tecnologías emergentes, como los laboratorios de computación móviles y los dispositivos Bluetooth, mejora la experiencia educativa y mantiene la participación de los estudiantes [3].

Además, con el incremento del uso de dispositivos móviles y la adopción de plataformas educativas en línea, la demanda de contenido multimedia interactivo esta en constante crecimiento [4]. Estos cambios requieren una infraestructura de red adaptable y escalable para satisfacer las nuevas necesidades educativas [4], [5]. Por lo tanto, las entidades educativas están buscando de aprovechar el uso de las TIC y deben estar preparadas para integrar estas tecnologías de manera efectiva

en su práctica pedagógica y administrativa. Esto enfatiza la importancia de una actualización integral de su infraestructura de red [6].

En este sentido, la modernización de dispositivos activos de red es crucial para garantizar un rendimiento óptimo y una conectividad confiable. La mejora de la infraestructura de red no solo implica la actualización del cableado estructurado y los medios de transmisión para soportar mayores tasas de transmisión de datos, sino también la renovación de los equipos activos de red [7], [8]. Estos equipos desempeñan un papel fundamental en la administración del tráfico de red, la seguridad y la preparación para futuras tecnologías.

Entonces, en busca de brindar una respuesta tecnológica que diera soporte al uso adecuado de las TIC, varias instituciones educativas en Ecuador llevaron a cabo iniciativas de actualización de sus infraestructuras de red con resultados positivos [7]. La actualización de los equipos activos de red, combinada con la implementación de redes de elevada velocidad y de herramientas de gestión centralizada, mejoró de manera significativa la conectividad y el acceso a servicios y aplicaciones [4]. Dicho acceso adecuado con soporte de seguridad y eficiencia operativa oportuna, permitió dar un soporte adecuado para entornos educativos que buscaban migrar al uso de las TIC [4]. Estas experiencias sirvieron como referencia para identificar las mejores prácticas y estrategias de implementación en la Unidad Educativa Técnico Salesiano, fortaleciendo así su capacidad para enfrentar retos presentes y futuros en el campo.

La UETS de la ciudad de Cuenca enfrentaba varios desafíos en relación con su infraestructura de red. Entre estos, se encontraban la insuficiencia de ancho de banda para satisfacer el creciente número de dispositivos conectados. Además, enfrentaba la obsolescencia de los equipos de red, cobertura inalámbrica limitada en ciertas áreas del campus y un tendido de fibra óptica no utilizado. Estas deficiencias en cuanto a las garantías de operación de la red de datos impactaban de manera negativa en la experiencia de estudiantes, docentes y administrativos, dificultando el acceso a recursos educativos digitales que requerían conectividad [8]. También dificultaban la comunicación efectiva y la gestión eficiente de los procesos institucionales.

Una infraestructura de red sólida era fundamental para impulsar las prácticas educativas innovadoras y fomentar las competencias digitales en los alumnos [8], [9].

Además, facilitaría la colaboración entre docentes, el acceso a materiales educativos en línea y la implementación de herramientas tecnológicas para la enseñanza personalizada. En la educación 4.0, donde la incorporación de la tecnología en el proceso educativo es crucial, una infraestructura de red robusta se convertiría en un requisito imprescindible para garantizar la excelencia educativa y la preparación de los estudiantes para los retos del siglo XXI [4].

Justificación

La actualización de equipos activos para la infraestructura de red de datos de la Unidad Educativa Técnico Salesiano, específicamente en el campus Yanuncay, se presentó como una necesidad imperativa para garantizar un entorno educativo eficiente y seguro. Este trabajo de titulación se enfocó en abordar esta necesidad crítica mediante la implementación de medidas técnicas y estratégicas destinadas a optimizar la infraestructura de datos del campus.

La relevancia de este proyecto radicó en la creciente dependencia tecnológica en el campo educativo y la necesidad de contar con equipos activos robustos y confiables para respaldar las actividades académicas y administrativas. La infraestructura de red existente en el campus Yanuncay presenta deficiencias significativas que impactan negativamente en la experiencia de aprendizaje de estudiantes, docentes y personal administrativo.

Entre los principales problemas que determinaron la relevancia de este trabajo se encontraban:

- Obsolescencia tecnológica: La infraestructura de red actual del campus Yanuncay se había quedado rezagada en términos de tecnología y capacidad, lo que resultaba en un rendimiento deficiente y una falta de seguridad adecuada.

- Inestabilidad y fallos: Los equipos de red obsoletos presentaban fallos recurrentes que afectaban la estabilidad de la red y comprometían la integridad de los datos.

- Limitaciones de cobertura y velocidad: La insuficiente cantidad de puntos de acceso inalámbrico y el desperdicio del tendido de fibra óptica existente limitaban la cobertura y la rapidez de la red, dificultando el acceso a recursos

en línea y la realización de actividades educativas que requerían una conexión rápida y confiable.

- Preparación para el futuro: Con la rápida evolución de las tecnologías de la información y las comunicaciones, era fundamental que la infraestructura de red de la UETS estuviera preparada para adaptarse y soportar futuras innovaciones y necesidades educativas.

La pertinencia de este trabajo se evidenciaba en la urgente necesidad de actualizar los equipos de red activos y mejorar la infraestructura de red para asegurar un entorno educativo ideal y favorable para el aprendizaje. Además, dado el impacto directo que tenía la infraestructura de red en la calidad de la educación y en la seguridad de la información, abordar estos problemas era fundamental para el éxito continuo de la institución.

Este proyecto serviría como prueba piloto y proyección de implementación en los campus Carlos Crespi y María Auxiliadora de la UETS, también en otras instituciones de la Comunidad Salesiana como Pases, Agronómico Salesiano y Yumancay.

Objetivos

Objetivo General

- Actualizar los equipos activos para la red de datos de la UETS.

Objetivos específicos:

- Analizar los problemas en la red de datos de la UETS para determinar las características de los equipos activos de red que den respuesta a los requisitos de la institución.
- Establecer e implementar la topología física de la red de datos de la UETS para permitir el correcto funcionamiento de los equipos activos.
- Evaluar el correcto funcionamiento de los equipos conectados en la UETS.

Introducción

La infraestructura de red de una institución educativa es fundamental para asegurar la conectividad, protección y eficacia en el manejo de información y recursos tecnológicos [2]. En el caso del campus Yanuncay de la UETS, enfrentó desafíos significativos con su red de datos, lo que comprometió la operatividad y calidad del servicio educativo. La actualización de equipos activos de red se convirtió en una necesidad estratégica para asegurar una infraestructura moderna y alineada con las demandas tecnológicas actuales y futuras.

Este proyecto consistió en evaluar, seleccionar e implementar nuevos equipos para resolver deficiencias críticas y optimizar la conectividad y seguridad en la red, con el fin de facilitar el aprendizaje y la administración institucional.

La importancia del proyecto radicó en la necesidad de una red de alto rendimiento para apoyar la transición hacia la Educación 4.0. Artículos destacan que las instituciones educativas enfrentan retos significativos debido a infraestructuras obsoletas que afectan la calidad del servicio educativo [4] [7]. En la UETS, se identificaron deficiencias en equipos activos, restricciones en el ancho de banda, cobertura y enlaces de fibra óptica no utilizados.

Los problemas de conectividad y seguridad se debieron a equipos obsoletos y mal implementados, afectando tanto el proceso educativo como las operaciones administrativas. La red existente no soportaba el creciente volumen de usuarios y datos.

El proyecto enfrentó limitaciones como el tiempo disponible para la actualización y la integración de nuevas tecnologías sin interrumpir las actividades diarias. También se presentaron desafíos en la capacitación del personal y la adaptación a los cambios tecnológicos.

Capítulo 1

Fundamentación Teórica

La infraestructura de red en edificaciones institucionales es esencial para garantizar un funcionamiento eficiente y seguro a las exigencias actuales de las aplicaciones tecnológicas usadas en los procesos de enseñanza aprendizaje. Así, con la creciente demanda de conectividad y el constante avance tecnológico, las redes de comunicación educativas se han vuelto indispensables para soportar servicios de plataformas digitales y aplicaciones diversas. Una infraestructura de red bien diseñada, mejora la productividad, asegura la protección de la información y permite la expansibilidad y adaptabilidad necesarias para adaptarse a las demandas cambiantes y la integración de nuevas tecnologías. En el presente capítulo, se analiza la actualización tecnológica en las instituciones educativas, así como la influencia de las nuevas tecnologías y la infraestructura de red en estos entornos.

1.1. Infraestructura de red en edificaciones

La infraestructura de red en edificaciones institucionales o empresariales representa un componente fundamental para el funcionamiento eficiente y seguro de cualquier construcción moderna [10]. En la actualidad, con la creciente necesidad de conectividad y el avance constante de la tecnología, las redes de comunicación dentro de los edificios se han vuelto indispensables para soportar una variedad de servicios y aplicaciones, desde la conexión a internet hasta la automatización y el control de sistemas.

1.1.1. Componentes de la Infraestructura de Red

La infraestructura de red en edificaciones está compuesta por varios elementos fundamentales que trabajan en conjunto para proporcionar conectividad y comunicación.

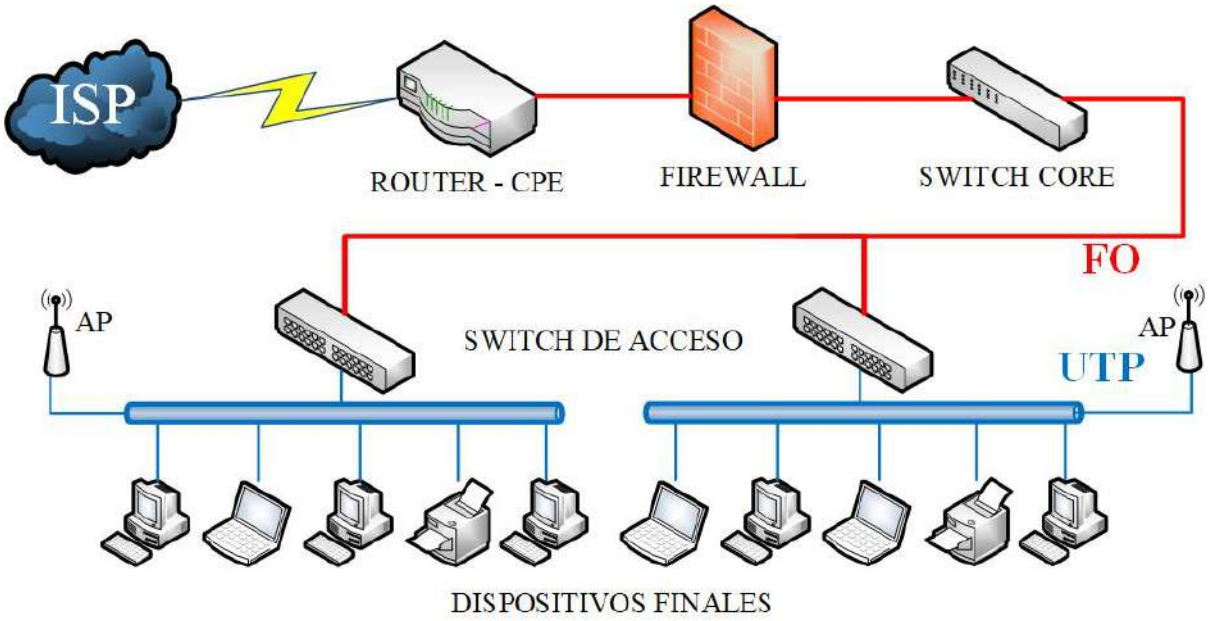

Figura 1.1: Composición de una infraestructura de red en edificaciones.
Fuente: Autor.

La figura 1.1 muestra los componentes activos de red principales, los secundarios y los tipos de cableado más comunes a ser utilizados en una institución educativa. Estos componentes son fundamentales para controlar el tráfico de datos e interconectar equipos activos, asegurando una transmisión eficiente y proporcionar seguridad frente a entidades externas. De este modo, se garantiza que toda la red tenga una conectividad segura y un rendimiento óptimo.

Cableado UTP Cat6

El cableado para redes con cable UTP cat 6 ofrece velocidades de hasta diez gigabits por segundo, superando a las categorías más antiguas. Este tipo de cable es ideal para redes de datos robustas y de gran tamaño, ya que permite una transmisión de datos eficiente y fiable. Es especialmente adecuado para entornos comerciales, residenciales o cualquier lugar donde se requiera un acceso a la red estable y con

gran capacidad de transmisión para múltiples dispositivos finales [11]. En la figura 1.1 el cableado UTP está representado en color azul y es aplicado en enlaces de corta distancia.

Cableado Fibra Óptica (FO)

La FO es un medio de transmisión cableado para datos que utiliza la luz como medio de comunicación. Este es el canal más utilizado en la actualidad para transmitir datos de gran capacidad a alta velocidad. La fibra óptica tiene la ventaja de poder transmitir audio y vídeo en tiempo real. Además, lo que hace que la fibra sea la más usada es que ofrece una transmisión segura, sin perturbaciones, debido a que las fibras están hechas de materiales que no conducen electricidad y el material que las recubre es apto para soportar condiciones climáticas y ambientales [12]. En la figura 1.1 el cableado FO está representado en color rojo y es aplicado en enlaces de corta y larga distancia.

Router CPE

El equipo CPE es un dispositivo administrable instalado en las instalaciones del cliente, ya sea una casa, una empresa o una institución educativa. Permite la conexión a una red de internet proporcionada por el ISP. El CPE distribuye el acceso a Internet brindado por el proveedor hacia otros dispositivos o equipos dentro de la institución educativa, la empresa o la vivienda [13]. La figura 1.1 muestra que el equipo que le da entrada a la red de datos.

Firewall

El firewall, representado en la figura 1.1, conocido también como corta fuegos, es un equipo, sistema o dispositivo de seguridad que existe entre una red privada y el Internet. Este crea una barrera no física que controla el tráfico de red, permitiendo únicamente el acceso autorizado. Todo el tráfico de datos debe pasar por el firewall, donde es inspeccionado y verificado según las reglas de seguridad implementadas.

Sin embargo, existe vulnerabilidad en estos sistemas cuando un agresor ya está dentro de la red privada y ha evadido el firewall. Por lo tanto, es necesario tener un

nivel de protección adicional para los elementos de la red interna, como hardware, software y datos. Además, se puede restringir el acceso a ciertos usuarios mediante claves de acceso. El firewall ofrece la ventaja de permitir la supervisión de la seguridad en la red y, en caso de actividad sospechosa, puede generar alertas [14].

Switch Core

Un conmutador (en inglés *switch*) es un dispositivo que conecta varios dispositivos dentro de una red local (LAN, del inglés *Local Area Network*) y dirige el tráfico de datos entre ellos. El switch recibe paquetes de datos de un dispositivo y los envía solo al dispositivo de destino, optimizando el uso de la red y reduciendo colisiones de datos. Ya que todos los equipos formarían parte del mismo segmento de red, no se necesitaría de un enrutador o *router*. En resumen, un switch permite que los dispositivos de una red se comuniquen de manera eficiente y segura, gestionando el tráfico de manera inteligente [15].

Por otra parte, un switch de núcleo de red (*core*), considerados el corazón de las redes empresariales, son responsables del enrutamiento y la conmutación a alta velocidad. Jerárquicamente, los switches de core se sitúan en la cima, y niveles de acceso y distribución dependen de ellos como se observa en la figura 1.1.

El switch de core se encarga de agregar grandes flujos de tráfico de datos a altas velocidades. Deben ofrecer un rendimiento excepcional, ya que los demás equipos intermedios dependen de ellos. La capacidad de rendimiento de estos switches debe ser muy alta y contar con múltiples puertos para manejar el enorme tráfico de la red. Estos puertos pueden ser de 1, 10, 40, 100 o 400 Gbps. Además, la seguridad y calidad del servicio son aspectos cruciales para que los equipos permanezcan operativos, reduzcan la latencia y aseguren la correcta distribución de los datos [16].

Switch de Acceso

Estos switches se encuentran en la capa de acceso de una red de interconexión de redes como se observa en la figura 1.1. Se encarga de conectar los usuarios finales o dispositivos finales como computadores, teléfonos, puntos de red, teléfonos celulares con los equipos que se presentan en la capa de distribución. Es decir que en la capa

de distribución donde se pueden encontrar el swith de core, reenvía el trafico de red y los distribuye a los switches de acceso para poder fluir el tráfico asignado ya hacia los dispositivos finales. Estos puertos o salidas del switch manejan trafico de 10, 100 o 1000 Mbps. Estos en comparación son menos costosos que los de core [16].

Punto de acceso

La figura 1.1,muestra que es un dispositivo de red, permite establecer una conexión inalámbrica desde una red cableada hacia los dispositivos finales, como computadoras, teléfonos celulares, o cualquier otro dispositivo que requiera conexión a Internet [16].

El uso de APs permite crear una red local inalámbrica WLAN, que evita la necesidad de conexiones cableadas y reduce los costos de implementación. Los AP funcionan reenviando el tráfico de datos desde la red interna cableada, que puede ser de fibra óptica, hacia los dispositivos de los usuarios que se conectan al AP [10].

Sistema de Alimentación Ininterrumpida

Es un sistema de control que no necesariamente debe estar implementado en una infraestructura de red, sin embargo puede ser de gran ayuda. Estos sistemas garantizan que el equipo de red activo continúe funcionando durante cortes de energía [10]. Son cruciales para mantener la continuidad del servicio y proteger los dispositivos de daños causados por variaciones en el suministro eléctrico. El la figura 3.30, muestra un esquema de conexión de este dispositivo.

Centros de Datos y Cuartos de Telecomunicaciones

Estos son espacios dedicados donde se alojan los equipos de red y los servidores. Están diseñados para proporcionar un entorno controlado y seguro, con sistemas de refrigeración, alimentación y medidas de seguridad física adecuadas [10].

Redes DMZ

Las empresas o instituciones de gran tamaño con el afán de evitar posibles intrusiones en su red interna, plantean una red de zona desmilitarizada (DMZ, del

inglés *Demilitarized Zone*). Una DMZ se trata de una red perimetral que se utiliza para separar la red interna de una organización (privada y segura) de la red externa, generalmente Internet (pública y menos segura). Por tanto, la DMZ permite que ciertos servicios accesibles desde el exterior, como servidores web, servidores de correo electrónico o servidores de nombre de dominio (DNS, del inglés *Domain Name System*), se aíslen de la red interna para mejorar la seguridad [17].

En una red DMZ, los recursos accesibles públicamente se colocan en una red separada. Esto significa que si un atacante compromete uno de estos recursos, no tendrá acceso directo a la red interna, limitando así el impacto del ataque. Para lograrlo, se usan los firewalls de manera que se pueda controlar el tráfico entre la red externa y la DMZ, así como entre la DMZ y la red interna. El tráfico permitido es cuidadosamente controlado para minimizar el riesgo [15], [17].

También puede usarse un switch DMZ que se coloca dentro de la zona DMZ para conectar los diferentes dispositivos dentro de la DMZ entre sí, y también a los firewalls que la protegen. Al igual que otros switches, gestiona el tráfico de red entre dispositivos conectados, pero en este caso, dentro de un entorno que está diseñado para ser más seguro y controlado [17].

1.1.2. Tipos de Redes en Edificaciones

Dentro de una edificación, pueden existir diversos tipos de redes, cada una con sus características específicas.

Redes de Área Local (LAN)

Las LAN conectan dispositivos dentro de un edificio o campus, permitiendo la comunicación rápida y eficiente entre computadoras, impresoras y otros dispositivos [10]. Son fundamentales para el funcionamiento interno de las instituciones.

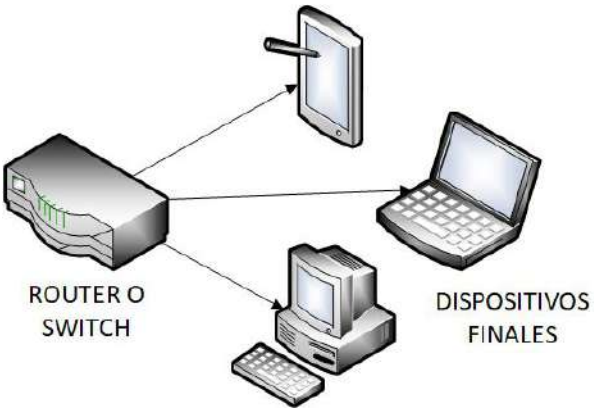

Figura 1.2: Red LAN.
Fuente: Autor.

Redes de Área Amplia (WAN)

Las WAN conectan varias LAN en diferentes ubicaciones geográficas. Son utilizadas para interconectar edificios corporativos, sucursales y oficinas remotas, facilitando la comunicación entre diferentes sedes de una misma organización [10].

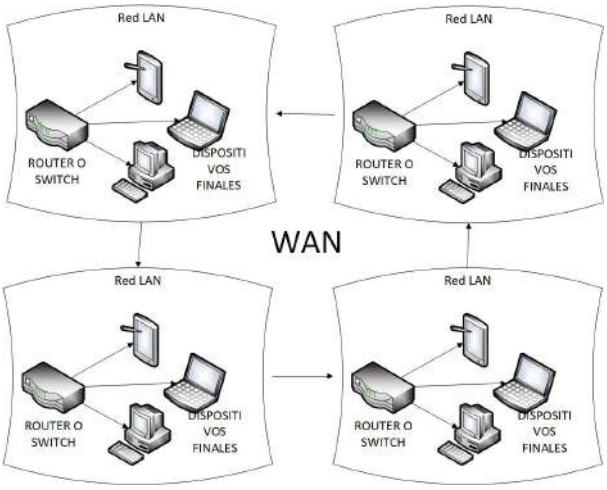

Figura 1.3: Red WAN.
Fuente: Autor.

Redes Inalámbricas (WLAN)

Estas redes facilitan la conexión de dispositivos móviles y portátiles sin necesidad de cables físicos, utilizando tecnologías como Wi-Fi [10]. Ofrecen conectividad flexible y conveniente, siendo ideales para entornos donde la movilidad es crucial.

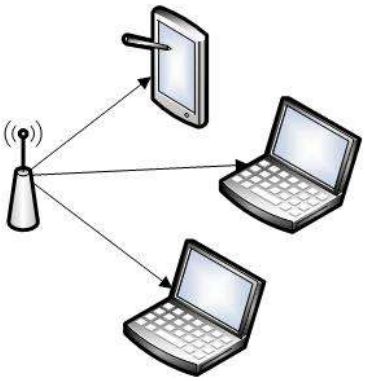

Figura 1.4: Red WLAN.
Fuente: Autor.

1.1.3. Importancia de una Infraestructura de Red Sólida

Contar con una infraestructura de red bien diseñada y mantenida es esencial por varias razones. A continuación, se presentara algunos puntos a consideración para mantener una infraestructura de red fiable.

Conectividad y Productividad

Permite la comunicación eficiente y el intercambio de información entre usuarios y sistemas, mejorando la productividad al facilitar el acceso rápido y confiable a los recursos y servicios necesarios [18].

En la actualidad, con el constante desarrollo de sistemas y dispositivos para la comunicación y transferencia de datos, se requiere tener redes que garanticen una alta calidad de servicio. Esto asegura que todos los participantes en la red puedan acceder a los recursos de manera estable y eficiente para las tareas diarias. Además, una red de datos bien implementada permite una mayor productividad en el entorno en el que está instalada.

Seguridad de la Información

Una infraestructura robusta incluye medidas de seguridad para proteger los datos y prevenir accesos no autorizados [19]. La implementación de firewalls, sistemas de identificación de intrusos y políticas de seguridad es esencial para mantener la integridad y confidencialidad de la información.

A medida que avanza el desarrollo de nuevos equipos de seguridad para redes, también se necesitan nuevos métodos y aplicaciones para una seguridad de red más robusta, orientada hacia una virtualización que permita un control de seguridad de manera dinámica y autónoma. Por ello, se proyecta en tecnologías que permitan gestionar la red mediante software y tecnologías en la nube. Esto permite la existencia de más capas de protección para acceder a la red [20].

Escalabilidad y Flexibilidad

Facilita la expansión y actualización de la red para satisfacer las crecientes demandas de conectividad [21]. Además, permite la integración de nuevas tecnologías y dispositivos, adaptándose a las necesidades cambiantes del entorno.

Siempre existirá un crecimiento en el número de usuarios a medida que pasa el tiempo, especialmente en redes dedicadas a empresas o instituciones donde la demanda de usuarios suele ser mayor. Por lo tanto, es crucial tener en cuenta que cualquier red es susceptible a un aumento en la cantidad de usuarios y, por ende, debe estar diseñada para manejar este crecimiento sin comprometer el rendimiento.

Una infraestructura de red debe ser planificada y dimensionada adecuadamente para permitir la incorporación gradual de nuevos dispositivos, ya sean intermedios (como switches) o finales (computadoras, teléfonos, etc), sin sacrificar la calidad del servicio. Esto implica diseñar la red con suficiente capacidad y flexibilidad para adaptarse a la expansión futura.

1.2. Tecnologías emergentes en infraestructura de red

Para tener una idea, en el mundo de las telecomunicaciones, cada vez surgen nuevas tecnologías y su infraestructura para asegurar que los usuarios tengan acceso a los servicios ofrecidos. Esto se logra implementando tecnologías emergentes que adaptan su diseño a las necesidades actuales, gestionando de manera más eficiente el área de redes, y permitiendo ofrecer mayor velocidad, seguridad y tolerancia a fallos.

1.2.1. Redes Mesh con Wi-fi 6

La tecnología MESH es muy aceptada actualmente para las redes inalámbricas. La red de malla es un tipo de topología de red local que permite usar un rango más amplio de cobertura, ya que los nodos que intervienen en la red se conectan de manera directa, sin jerarquización de equipos. Todos los nodos trabajan en conjunto de tal forma que el proceso de envío de datos en la red sea rápido, evitando problemas de sobrecargas de tráfico de datos y, sobre todo, garantizando una tolerancia a fallos que permite ofrecer una alta calidad de servicio. Esta red MESH se autoconfigura de manera dinámica [22]. La red estaría compuesta por un router o estación base y puntos de acceso o nodos, como se mencionó anteriormente, donde cada nodo se comunica entre sí. Así, un usuario puede cambiar de nodo al movilizarse por la red. Al tener más nodos, la capacidad de cobertura es mayor. Es importante mencionar que todos los nodos deben estar conectados a una única red Wi-Fi. Podría pensarse que es lo mismo usar routers y equipos repetidores, pero los repetidores solo trabajan con el router principal y no se comunican con otros equipos, es decir, trabajan de manera independiente y no conjunta. En cambio, la red MESH permite que un dispositivo se conecte realizando un análisis de red y eligiendo la ruta más óptima para el tráfico de datos, además de determinar a qué nodo debería conectarse.

Este concepto MESH, combinado con la tecnología Wi-Fi 6, también conocida como estándar IEEE 802.11ax, lanzado en 2018 y actualmente el más utilizado en el mercado, presenta nuevas características. A diferencia del estándar anterior, Wi-Fi 6 funciona en dos bandas de frecuencia, 2.4 y 5 GHz. Además, utiliza la técnica de OFDMA mejorada, donde no usa todo el ancho de banda para la transmisión de una sola trama, sino que emplea unidades de recursos (RU), permitiendo realizar varias transmisiones simultáneas hacia los dispositivos finales. Esta combinación con la tecnología MESH es ventajosa, ya que Wi-Fi 6 ofrece velocidades más rápidas, alrededor de 9.6 Gbps con una modulación más elevada utilizando 1024 QAM, un 40 % más que la tecnología anterior Wi-Fi 5, que alcanzaba 6.9 Gbps [23].

1.2.2. Wifi 7

Las redes inalámbricas para redes locales como hogares, oficinas, centros educativos, etc está cada vez creciendo y requiriendo nuevas ventajas de las normativas pasadas ya sea para mayor capacidad de usuarios, mayor velocidad e incluso en el siglo XXI para nuevas aplicaciones y servicios. Por ejemplo, realidad aumentada, vídeo 8K, gaming, trabajos remotos, computación en la nube, e incluso para nuevas modalidades como el manejo remoto o inteligente para aplicaciones en tiempo real [24].

Para ello se está trabajando para implementar un moderno estándar Wi-Fi IEEE 802.11be o también como Wi-Fi 7, que se procura obtener velocidades de hasta 40 gigabits por segundo por cada punto de acceso. Las nuevas mejoras que implementará Wi-fi 7, es que trabajará como triple banda, con la de 2.4, 5, y 6 GHz y será posible usarlas de manera simultánea implementando la tecnología Multi-Link Operation (MLO), que permite agrupar las bandas de frecuencia y canales para tener mayor velocidad, reducir latencia y así obteniendo estabilidad[25].

A comparación de Wi-Fi 6, el estándar 802.11be utiliza la modulación 4096-QAM, lo que permite transmitir 12 bits por símbolo en lugar de los 10 bits por símbolo de la modulación 1024-QAM utilizada en Wi-Fi 6. Aunque este estándar aún se encuentra en su etapa inicial, Wi-Fi 7 busca dar un salto significativo para mejorar la conectividad y la experiencia del usuario, haciéndolo capaz de integrarse con los nuevos servicios y aplicaciones que ofrece el mundo moderno.

1.3. Actualización tecnológica en la Eduación

En la era digital actual, la integración de tecnologías avanzadas en las instituciones educativas es más crucial que nunca. Las herramientas tecnológicas y las redes de alta velocidad están transformando la manera en que se imparte y se recibe la educación, ofreciendo nuevas posibilidades para optimizar la educación y el aprendizaje [26], [27]. En este contexto, la capacidad de una institución educativa para adaptarse y actualizar sus recursos tecnológicos no solo eleva la calidad de la educación, sino que también garantiza que los alumnos estén preparados para

enfrentar los retos de un mundo cada vez más digitalizado.[28]

1.3.1. Desafíos y consideraciones

La integración de tecnología en los entornos educativos conlleva una serie de ventajas que pueden enriquecer el proceso de enseñanza-aprendizaje. No obstante, este avance también presenta desafíos y consideraciones cruciales que requieren atención para asegurar su efectividad[29].

Uno de los desafíos más notables es el costo asociado con la modernización tecnológica. La adquisición de equipos actualizados y el mantenimiento de una infraestructura adecuada pueden suponer una carga financiera considerable para las instituciones educativas. Por ejemplo, aquellas con recursos limitados. Asimismo, la formación continua del cuerpo docente para utilizar de forma eficiente estas herramientas tecnológicas también demanda inversión de tiempo y recursos [30].

Otro desafío significativo es la brecha digital, la cual puede exacerbar las desigualdades existentes si no se aborda. A pesar de que la tecnología puede mejorar el acceso a la enseñanza, existe el riesgo de que los alumnos menos privilegiados enfrenten dificultades para aprovechar al máximo estas herramientas [31]. Por ende, es esencial que las instituciones educativas implementen medidas inclusivas para asegurar que todos los alumnos dejando de lado su situación socio-económica, puedan acceder de manera igualitaria a los recursos tecnológicos necesarios [32].

Capítulo 2

Diagnóstico de Equipos Activos de la Infraestructura de Red

El diagnóstico de equipos activos de la infraestructura de red del campus Yanuncay de la UETS fue una tarea crucial que permitió evaluar el estado y funcionamiento de los dispositivos tecnológicos fundamentales para la conectividad y protección de la red. Este proceso reveló las deficiencias y vulnerabilidades existentes, proporcionando una visión clara de las áreas que requerían actualización y mejora.

2.1. Recopilación de datos sobre los equipos activos de red actuales

En la infraestructura de red del campus Yanuncay, había equipos de red que ya no funcionaban adecuadamente, estaban obsoletos o habían sido implementados de manera deficiente. Esta situación representaba un desafío significativo para la operatividad y eficiencia de la infraestructura tecnológica de la institución, requiriendo medidas urgentes para su actualización y correcta implementación.

2.1.1. Equipos obsoletos

Switch de Core - Cisco Catalyst 4503

En el centro de datos del campus Yanuncay, el switch de core, que es un componente central de la infraestructura de red, estaba quemado. Este equipo era muy antiguo (fabricación - año 2007), había sufrido daños severos, lo que afectó la conectividad y la operatividad de la red. Para solventar este problema, nuestro proveedor de internet configuró un router cisco 891 para funcionar como switch, permitiendo mantener la conectividad básica mientras se buscaba una solución permanente.

Figura 2.1: Equipo Cisco Catalyst 4503.
Fuente: [33].

Equipo Cisco Catalyst 2960G

El switch DMZ funcionaba como firewall, era un dispositivo diseñado para crear una zona desmilitarizada dentro de una red, separando y protegiendo los servidores públicos de los internos. En el centro de datos, este equipo ya no cumplía su objetivo debido a su antigüedad (fabricado - año 2007) y estaba dañado al punto que no estaba conectado a ningún dispositivo.

Figura 2.2: Equipo Cisco Catalyst 2960G.
Fuente: [33].

Access Point - Ubiquiti UniFi AP

En el campus Yanuncay, algunos de estos equipos antiguos de acceso, instalados en el año 2016, ya no funcionaban y otros presentaban fallos intermitentes. En el año 2019, la mayoría de estos AP fueron reemplazados por equipos más modernos. Sin embargo, algunos de los AP instalados en 2019 estaban mal ubicados, lo que afectaba su eficiencia y la cobertura en la institución.

Figura 2.3: Equipo Ubiquiti UniFi AP.
Fuente: [34].

2.2. Análisis de problemas y deficiencias identificadas

La UETS enfrentaba múltiples problemas relacionados con la obsolescencia y el deterioro de su infraestructura de red del campus Yanuncay. Estos problemas no solo afectaban la conectividad y la operatividad de la red, sino que también comprometían la seguridad de los datos y la eficiencia en el uso de recursos tecnológicos. La necesidad urgente de actualización y mejora de estos componentes era evidente para asegurar un entorno de red estable, seguro y eficiente para la comunidad educativa y administrativa.

Para abordar estas problemáticas, se procedió a analizar detalladamente

cada problema y deficiencia encontrada. Este análisis permitió tomar decisiones informadas y efectivas para implementar las soluciones necesarias que garantizaran una infraestructura de red robusta y confiable.

2.2.1. Problemas y deficiencias de Switch de Core

El switch de core, observado con anterioridad en la figura 2.1 presentaba múltiples deficiencias y problemas que comprometían la operatividad y seguridad de la red. Antes de su falla total, este dispositivo ya mostraba fallos significativos en la asignación de subredes, lo cual afectaba la eficiencia y la organización de la red. Estas fallas indicaban un deterioro progresivo del equipo y una necesidad urgente de revisión y actualización.

La situación se agravó cuando una falla eléctrica provocó que el switch de core se quemara completamente, dejando a la red sin su componente central y crítico. Este evento subrayó aún más la urgencia de reemplazar el equipo defectuoso.

Temporalmente, nuestro proveedor de internet nos conectó un router Cisco 891 configurado como switch para mantener la operatividad mínima de la red. Sin embargo, esta solución es solo una medida provisional y no puede sustituir las capacidades y la eficiencia de un switch de core adecuado. Un switch de core eficiente debe proporcionar alta capacidad de procesamiento, gestión avanzada de tráfico, soporte para múltiples subredes y VLANs, y características de redundancia y seguridad robustas. Además, debe ser capaz de manejar grandes cantidades de datos con mínima latencia y alta disponibilidad, asegurando una red estable y confiable.

En respuesta a esta crisis, se tomó la decisión de adquirir un nuevo switch de core que no solo reemplazara al dispositivo dañado, sino que también solventara las necesidades de subneteo. Esta nueva adquisición permitirá una asignación de subredes más eficiente y mejorará la estabilidad y seguridad de la red en general.

2.2.2. Problemas y deficiencias de Switch DMZ

El switch DMZ, utilizado como firewall de la institución y observado en la figura 2.2, no se encontró en uso debido a su antigüedad y las múltiples fallas en todos

sus puertos. Su mal funcionamiento comprometió la seguridad y eficiencia de la red. Esta situación crítica evidenció la necesidad urgente de actualizar la infraestructura de red para asegurar una administración efectiva de los recursos y protección de los datos.

Ante estos problemas, se decidió adquirir un equipo de firewall completo. Esta nueva solución no solo proporcionaría una mayor protección a la red, sino que también permitiría segmentar los permisos de acceso de manera efectiva, asegurando la adecuada protección de las diferentes áreas de la red frente a posibles amenazas.

El nuevo firewall también permitiría monitorear el uso de la red, bloquear hosts de manera remota y ver en tiempo real el contenido que se está consumiendo. Además, se espera que mejore la seguridad al bloquear sitios web inapropiados, promoviendo un entorno seguro para la educación y mejorando la importancia de la educación digital al proporcionar acceso seguro a recursos en línea.

2.2.3. Problemas y deficiencias de Puntos de Acceso Inalámbrico

La institución enfrentó múltiples problemas con los puntos de acceso (AP, del inglés *Access Point*) instalados en su red. Varios de estos AP como los de la figura2.3 estaban quemados, lo que se atribuyó a la falta de supresores de picos en los dispositivos con alimentación a través de Ethernet (PoE, del inglés *Power over Ethernet*), lo que comprometió su funcionamiento y la estabilidad de la red.

Además, algunos AP instalados en 2019 estaban desconectados, lo que indicaba una falta de mantenimiento y atención a la infraestructura existente. Otros estaban mal ubicados, lo que afectó la cobertura y la calidad de la señal en diversas áreas de la institución. Asimismo, varios de los AP presentaban configuraciones incorrectas, lo que generó fallos en la asignación de subredes y limitó la eficiencia de la red.

Dada esta circunstancia, se tomó la decisión de adquirir nuevos AP para reemplazar los que estaban obsoletos. La nueva adquisición permitiría mejorar la cobertura, optimizar la configuración y asegurar un entorno de red más confiable y eficiente para toda la comunidad educativa.

2.2.4. Otras problemas y deficiencias

Fue crucial reconocer que la actualización de equipos activos no era la única cuestión que requería atención. A pesar de la necesidad de modernizar la infraestructura tecnológica, existieron otros problemas subyacentes que obstaculizaron un funcionamiento óptimo. Entre estos, la limitada capacidad de ancho de banda y la falta de conexión de los enlaces de fibra óptica, que ya estaban disponibles y un sistemas de alimentación ininterrumpida. Abordar estas cuestiones resultó esencial para asegurar que, al cambiar los equipos activos, estos tuvieran un buen funcionamiento y pudieran contribuir realmente a optimizar la excelencia del servicio y la eficacia de las operaciones institucionales.

Limitado Ancho de Banda

La UETS había establecido un contrato con la empresa CEDIA por un ancho de banda de 200 megas para el campus Yanuncay. Sin embargo, este ancho de banda no era suficiente para cubrir las necesidades de la institución, que incluían 14 laboratorios de computación, más de 60 aulas de clases, más de 20 oficinas administrativas y espacios de recreación. La demanda de servicios de internet, especialmente con el uso intensivo de recursos en línea y plataformas educativas, era cada vez más creciente.

Se identificaron serias deficiencias en el contrato entre la UETS y la empresa CEDIA, ya que esta capacidad resultó insuficiente para satisfacer las necesidades operativas de la institución. Esto derivó en una serie de problemas significativos, como la lentitud en el acceso a internet, interrupciones frecuentes en el servicio y caídas de conexión, que afectaron tanto el proceso educativo como las actividades administrativas diarias. Además, la insuficiencia de ancho de banda podría afectar de manera significante al funcionamiento de nuevos equipos de red activos, comprometiendo aún más la eficiencia y la calidad del servicio.

Con el constante crecimiento de la cantidad de usuarios y la expansión de la oferta educativa, la demanda de ancho de banda seguía aumentando, haciendo evidente la necesidad de una revisión del contrato. Por ello, se propuso solicitar un nuevo contrato con CEDIA que contemplara un ancho de banda de al menos 500 megas. Esta mejora no solo permitiría satisfacer las necesidades actuales, sino

que también proporcionaría un margen adecuado para el crecimiento futuro de la institución.

Tendido de fibra óptica no utilizado

El campus Yanuncay contaba con una infraestructura de red avanzada, la cual incluía una extensa red de fibra óptica instalada a lo largo de sus instalaciones. Estos enlaces se habían tendido desde el centro de datos hasta los cuartos de comunicación de los edificios de la institución, y desde estos cuartos hasta el gabinete correspondiente de cada planta. Esta disposición técnica garantizaba la capacidad de soportar una conectividad de alta velocidad.

Sin embargo, a pesar de la disponibilidad de esta tecnología avanzada, dichos enlaces de fibra óptica no habían sido conectados y, como resultado, no estaban en uso. Esta situación se debía a que no contaban con personal capacitado para realizar las conexiones y el switch de core no tenía conectores SFP ópticos o eléctricos. Esta situación limitaba el potencial de la red y afectaba la experiencia de quienes consumían el servicio en la institución, evidenciando la necesidad de una integración efectiva de la infraestructura existente para optimizar el rendimiento y la conectividad en toda la institución.

Ante este problema, se tomó la decisión de utilizar los enlaces de fibra óptica y se consideró este requerimiento al momento de adquirir el nuevo switch de core, asegurándose de que contara con los conectores SFP necesarios para su correcta integración.

Carencia de sistema de alimentación ininterrumpida

El centro de datos del campus Yanuncay carecía de un sistema de alimentación ininterrumpida (SAI) en su centro de datos, lo que generaba serias preocupaciones sobre la continuidad operativa de sus servicios tecnológicos. Sin un SAI, cualquier corte de energía podía interrumpir de manera abrupta el funcionamiento de los servidores y equipos de red, resultando en la pérdida de datos críticos y un tiempo de inactividad significativo. Esta situación limitaba el acceso a plataformas educativas y administrativas, afectando directamente la calidad del servicio.

Además, la falta de un SAI complicaba la recuperación de sistemas tras un apagón y aumentaba el riesgo de daños en los equipos electrónicos, lo que podía elevar los costos de mantenimiento y reemplazo. En este contexto, incluso había ocurrido un incendio dentro del centro de datos debido al uso de regletas eléctricas, lo que incrementó aún más la necesidad de una solución adecuada.

Por esto, se tomó la decisión de implementar un sistema SAI en el centro de datos que opere con voltajes entre 110V-220V para asegurar la correcta alimentación y protección de los equipos de red y servidores físicos. Esta medida fue esencial para prevenir la pérdida de datos, asegurar la estabilidad de la conectividad y permitir apagados controlados durante cortes de energía. La implementación del SAI permitiría a la red de datos operar de manera más confiable y continua, mejorando así la experiencia de usuarios y personal.

2.3. Expectativas sobre la actualización de Red

La expectativa para la UETS era alcanzar el paradigma de la Educación 4.0. Este enfoque se centra en la integración de tecnologías avanzadas en el proceso educativo, promoviendo un aprendizaje más personalizado, interactivo y eficiente[35]. Para que la UETS implementara este paradigma de manera efectiva, era crucial actualizar sus equipos activos de red, por las problemáticas analizadas previamente. Esta actualización resultaba esencial para resolver los problemas de conectividad actuales y cumplir con los requerimientos técnicos necesarios para soportar las tecnologías emergentes que caracterizaban la Educación 4.0.

En primer lugar, el campus Yanuncay necesitaba actualizar sus equipos de red para garantizar un rendimiento óptimo y una conectividad confiable. La Educación 4.0 depende de plataformas en línea, simulaciones y laboratorios virtuales que requieren una red robusta y de alta velocidad [36]. Los equipos obsoletos no podían manejar el gran volumen de datos y las demandas de ancho de banda, lo que resultaba en interrupciones y una experiencia de docentes, estudiantes y personal administrativo deficiente. La actualización permitiría una conectividad más rápida y estable, mejorando la calidad del aprendizaje y la formación.

La personalización del aprendizaje, un componente clave de la Educación 4.0, requiere una red de alta capacidad y baja latencia [37]. Las tecnologías modernas, como la inteligencia artificial y los sistemas de aprendizaje adaptativo, necesitan procesar elevados volúmenes de datos en tiempo real para crear rutas de aprendizaje personalizadas. Los equipos actuales de la UETS no estaban equipados para manejar estas demandas, lo que limitaba la capacidad para ofrecer una educación personalizada. La actualización de los equipos de red permitiría una mayor flexibilidad y eficiencia en el proceso educativo.

La colaboración y el trabajo en grupo son aspectos esenciales de la Educación 4.0, facilitados por herramientas digitales y entornos virtuales de trabajo. Estas herramientas requieren una red confiable y de alto rendimiento. Sin una infraestructura de red adecuada, la UETS enfrentaba desafíos en la implementación de estos entornos colaborativos, afectando la interacción y el trabajo en equipo entre estudiantes y profesores. La modernización de los equipos de red garantizaría que estas herramientas funcionaran de manera óptima, promoviendo un entorno educativo más colaborativo y conectado.

La seguridad de los datos es crítica en la transición hacia la Educación 4.0 [38]. Con el aumento del uso de herramientas digitales y el intercambio de datos personales y académicos, era vital proteger esta información contra amenazas cibernéticas. Los equipos de red obsoletos podían ser vulnerables a ataques, poniendo en riesgo la integridad y la privacidad de los datos. La actualización mejoraría el rendimiento de la red y reforzaría las medidas de seguridad, proporcionando una protección robusta contra los riesgos cibernéticos.

En cuanto a los requerimientos mínimos sobre el rendimiento de la red, la UETS estableció que sus procesos educativos debían acercarse al paradigma de Educación 4.0 en los próximos años. Según [6], [37], [39], los requerimientos técnicos mínimos incluyen una capacidad de ancho de banda adecuada, baja latencia, alta disponibilidad y robustez en la seguridad de la red. Frente a los problemas de conectividad que la UETS había estado sufriendo en los últimos años, era evidente que una intervención en los equipos activos de la red de datos era necesaria para cumplir con estos estándares.

Por lo tanto, la actualización de los equipos de red en la UETS resultaba esencial para superar los problemas de conectividad actuales y cumplir con los requerimientos técnicos necesarios para implementar la Educación 4.0. Una red moderna y eficiente apoyaría el uso de tecnologías avanzadas, la personalización del aprendizaje, la colaboración en línea y la seguridad de la información, proporcionando una base sólida para una educación innovadora y de alta calidad. Las expectativas futuras sobre esta actualización incluían mejoras significativas en la calidad educativa, la seguridad de la información y la sostenibilidad operativa, asegurando que la UETS continuara siendo una institución líder en la educación tecnológica en la ciudad de Cuenca.

Capítulo 3

Establecimiento y Planificación y Actualización de Equipos de Red Activos

En este capítulo, se abordaron los aspectos fundamentales para el establecimiento y la planificación de los equipos de red activos en el campus Yanuncay de la UETS. Se definieron las diferentes zonas de la institución y se estableció la topología física más adecuada para optimizar la conectividad. Además, se realizó la selección y adquisición de equipos de red que cumplieron con los requerimientos específicos del entorno educativo. La instalación y configuración de estos equipos fueron cruciales para garantizar su correcto funcionamiento. Asimismo, se integraron enlaces de fibra óptica para mejorar la capacidad de transmisión de datos y se ajustó la configuración del ancho de banda para asegurar una experiencia de usuario eficiente. Este enfoque integral permitió desarrollar una infraestructura de red robusta y ajustada a las necesidades presentes y futuras de la institución.

3.1. Establecimiento de zonas de interés del campus Yanuncay

El establecimiento de zonas dentro del campus Yanuncay de la UETS era un paso fundamental para la organización y optimización de la red. Esta clasificación no solo facilitaría una mejor gestión de los recursos tecnológicos, sino que también aseguraría una distribución eficiente del servicio de conectividad en toda la institución.

3.1.1. Seccionamiento de zonas por edificios

Con la ayuda de la herramienta "Google Earth"se obtuvo una vista satelital real de lo que compone todo el campus Yanuncay. Como se puede observar en la figura 3.1 el campus esta dividido en ocho zonas de interés con demanda de acceso a internet.

Figura 3.1: Vista satelital del campus Yanuncay.
Fuente: Autor.

Tabla 3.1: Seccionamiento por zonas campus Yanuncay.

Fuente: Autor.

Color	Zona	Descripción
	A	Edificio Miguel Rua
	B	Edificio Carlos Crespi
	C	Edificio Mamá Margarita
	D	Edificio Tecni Club
	E	Edificio Cancha Cubierta
	F	Edificio Coliseo
	G	Edificio Piscina
	H	Edificio Comunicación y Música

3.1.2. Seccionamiento de subzonas

Como se puede observar en la tabla 3.1, cada una de las zonas corresponde a un edificio. Todos los edificios debían ser intervenidos, ya que existían problemáticas en sus aulas, oficinas, talleres y laboratorios.

Puesto que algunos de los edificios estaban comprendidos por varias plantas o niveles, se decidió realizar un seccionamiento adicional de zonas para obtener una visión más específica. Esto permitió identificar de manera más efectiva las ubicaciones adecuadas para los equipos de red activos, facilitando así una mejor planificación de la infraestructura tecnológica en cada espacio de la unidad educativa.

Tabla 3.2: Seccionamiento por subzonas campus Yanuncay.

Fuente: Autor.

Color	Zona	Descripción
	A	Edificio Miguel Rua
	A1	Planta Baja MRUA
	A2	Primera Planta MRUA
	A3	Segunda Planta MRUA
	A4	Tercera Planta MRUA
	B	Edificio Carlos Crespi
	B1	Planta Baja CC
	B2	Primera Planta CC
	B3	Segunda Planta CC
	C	Edificio Mamá Margarita
	D	Edificio Tecni Club
	E	Edificio Cancha Cubierta
	E1	Planta Baja C Cubierta
	E2	Primera Planta C Cubierta
	F	Edificio Coliseo
	F1	Escenario y Graderíos
	F2	Pasillos Coliseo
	G	Edificio Piscina
	H	Edificio Comunicación y Música

El seccionamiento por subzonas fue crucial, ya que se estableció los fundamentos para la realización de la topología física de la red. Este enfoque detallado permitió identificar las necesidades específicas de cada área, facilitando la colocación y reubicación de los puntos de acceso de manera estratégica. Al tener una visión clara de la distribución de espacios, se lograría optimizar el alcance y desempeño de la red, garantizando una conectividad más efectiva en todas las zonas de la institución.

Además, este seccionamiento permitiría una mejor planificación de la infraestructura tecnológica, asegurando que cada edificio y planta recibiera la atención adecuada en función de sus requerimientos.

En la tabla 3.2, se puede observar cada una de las subzonas que comprenden los edificios de la institución, las cuales serían de ayuda para continuar con los siguientes puntos del proyecto.

3.2. Establecimiento de topología de red

La UETS nunca había contado con una topología física de red definida, lo que generó una falta de claridad sobre la estructura y el funcionamiento de su infraestructura tecnológica. Esta situación dificultaba la gestión adecuada de los recursos y la identificación de posibles problemáticas en la conectividad. Por esta razón, se decidió establecer una topología de red que considerara tanto los equipos existentes como aquellos que se están reemplazando y los nuevos que se están integrando al sistema.

Para llevar a cabo la representación gráfica del establecimiento de la topología de red del campus Yanuncay de la UETS, se utilizó la herramienta Cisco Packet Tracer, junto con la implementación de clústeres. Esta plataforma permitió visualizar de manera efectiva las interconexiones de los equipos de red, facilitando la creación de diagramas precisos y detallados.

Es importante destacar que en esta topología no se configuraron equipos, ya que el objetivo no fue realizar una simulación funcional, sino ofrecer una representación física de la infraestructura de red, además que Cisco Packet Tracer no cuenta con todos los equipos que se iban a actualizar en la red.

Para la topología del campus, se desarrolló una tabla (3.3) de colores detallada para identificar los diferentes tipos de cableado, proporcionando así una visión más clara y organizada. Esta tabla facilitó la identificación rápida y precisa del cableado.

Tabla 3.3: Código de colores utilizados en topología.

Fuente: Autor.

Color	Tipo de Cable
	Fibra Óptica
	UTP
	UTP(Varios)

Se elaboró una representación gráfica para cada zona y subzona de la institución, lo que permitió tener una visión clara y estructurada de la red en su totalidad. La incorporación de clústeres ayudó a optimizar la organización y gestión de los recursos, mejorando la eficiencia de la red.

Figura 3.2: Topología del campus Yanuncay seccionado en zonas.
Fuente: Autor.

En la figura 3.2 se presenta la topología física del campus Yanuncay, seccionada en diversas zonas. Dada la gran extensión de la institución y las limitaciones del software empleado, no ha sido posible exportar una imagen de mayor calidad. No obstante, es posible visualizar las nomenclaturas de cada enlace que parte desde la

zona A (Edificio Miguel Rúa) hacia las distintas zonas (B-C-D-E) con las que está conectada mediante enlaces de fibra. Asimismo, se puede observar la zona E (Edificio Cancha Cubierta) con sus correspondientes enlaces de fibra óptica y UTP hacia otras zonas(F-G-H). Además, se observan las dos acometidas de fibra óptica proporcionadas por la empresa CEDIA: la acometida principal por la Av. Felipe II (PuntoNet) y la acometida Back Up por la Av. Don Bosco (TelcoNet).

3.2.1. Topología zona A

Se realizó la topología de la zona A, correspondiente al Edificio Miguel Rúa, así como de sus subzonas. Esta topología detalla las conexiones y enlaces de fibra óptica que parten de esta zona hacia otras zonas del campus. Además, se documentaron las diversas conexiones internas dentro de las subzonas de la zona A, asegurando una comprensión completa de la infraestructura de red en esta área específica.

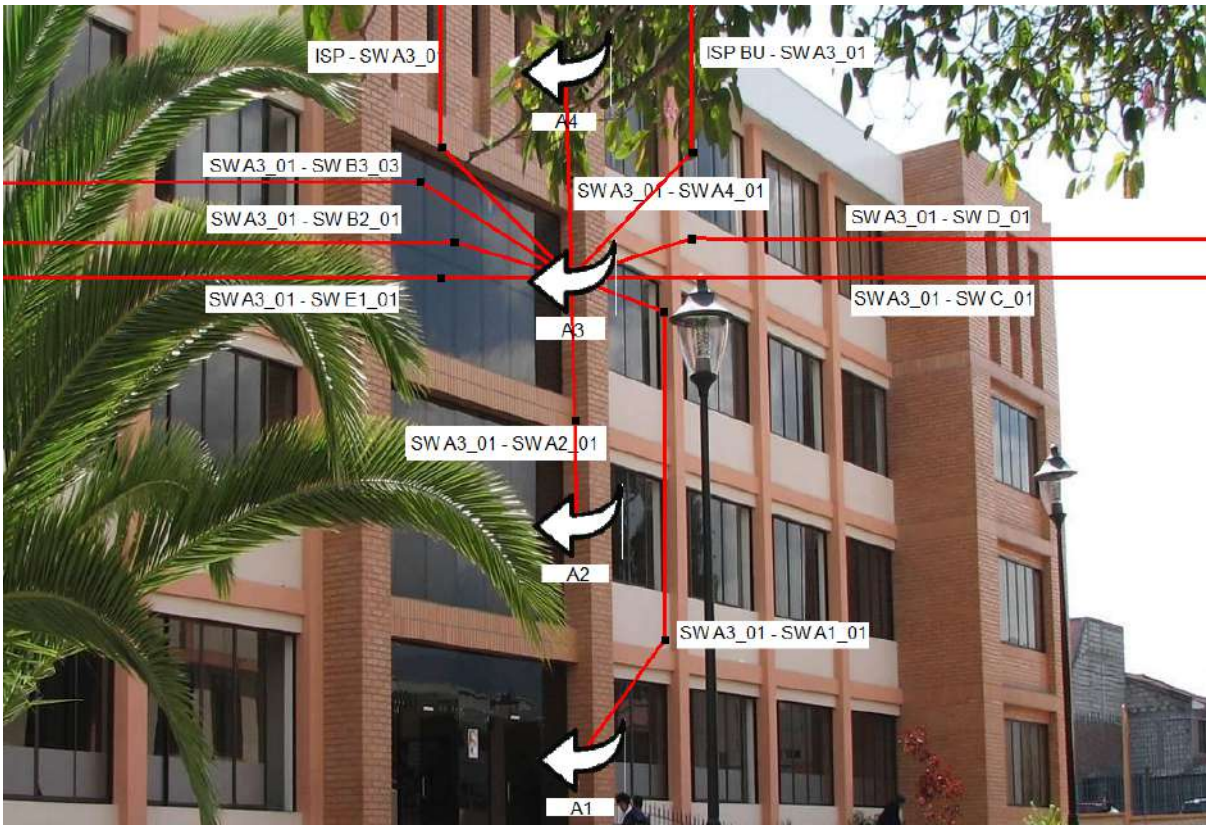

Figura 3.3: Topología zona A.
Fuente: Autor.

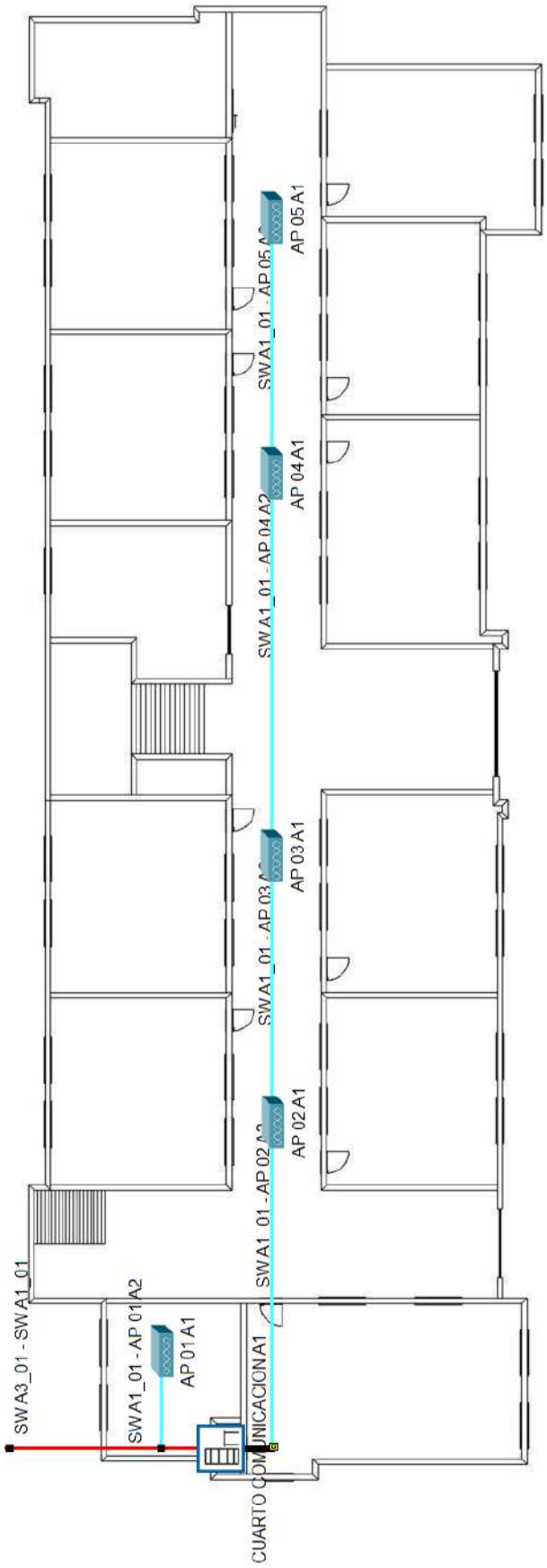

Figura 3.4: Topología zona A1.
Fuente: Autor.

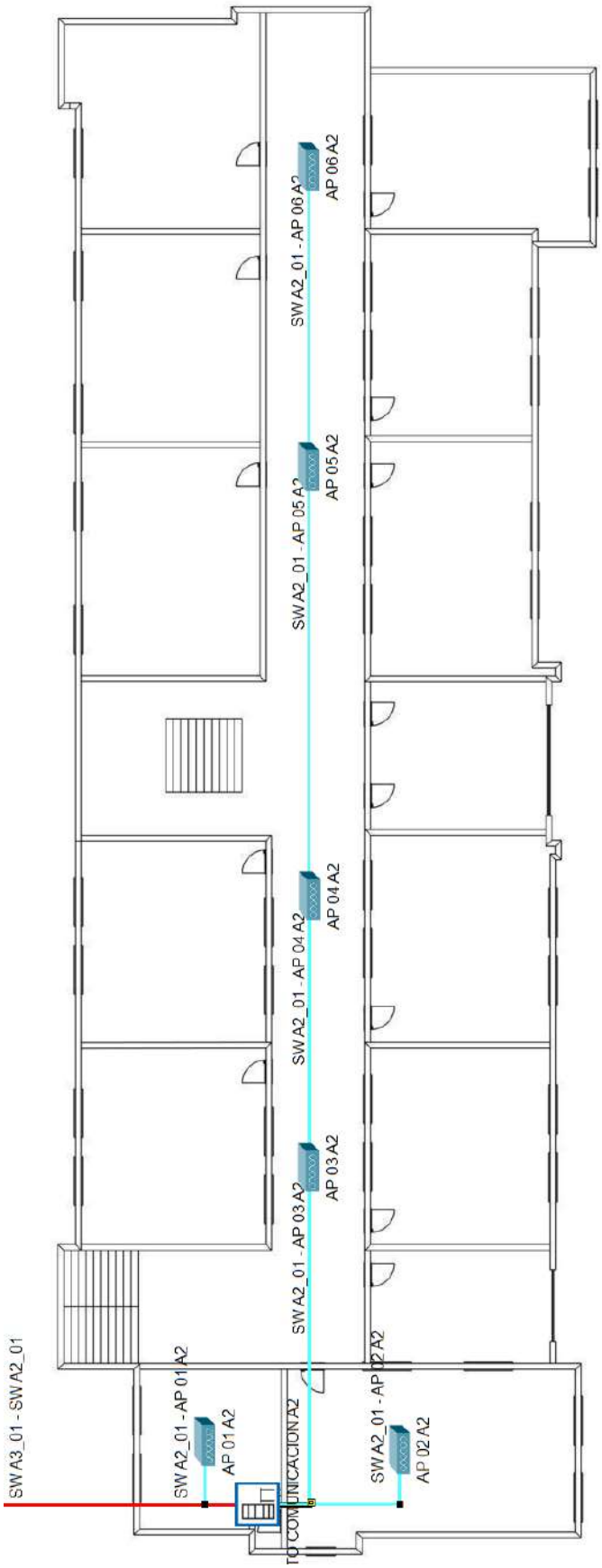

Figura 3.5: Topología zona A2.
Fuente: Autor.

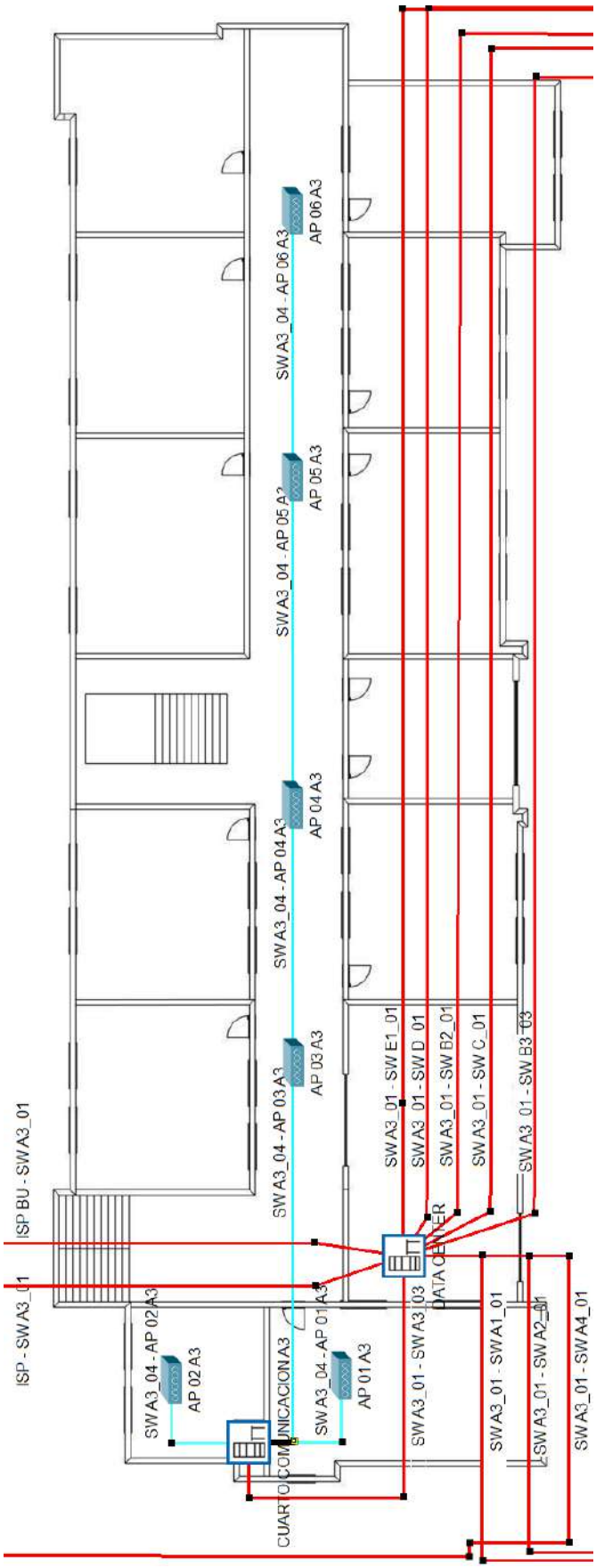

Figura 3.6: Topología zona A3.
Fuente: Autor.

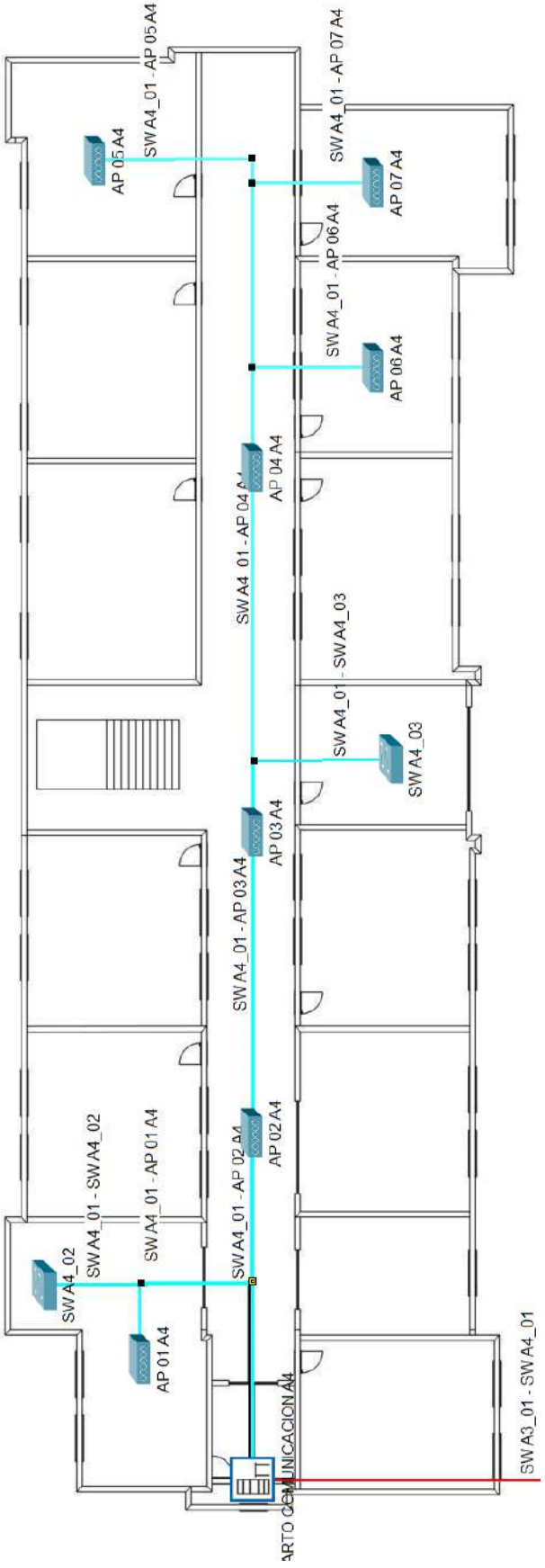

Figura 3.7: Topología zona A4.
Fuente: Autor.

3.2.2. Topología zona B

Se realizó la topología de la zona B, correspondiente al Edificio Carlos Crespi, así como de sus subzonas. Esta topología detalla las conexiones y enlaces de fibra óptica que parten de esta sección hacia otras zonas del campus. Además, se documentaron las diversas conexiones internas dentro de las subzonas de la zona B, asegurando una comprensión completa de la infraestructura de red en esta área específica.

Sin embargo, las gráficas no logran apreciarse con la claridad deseada debido a las limitaciones del software utilizado y a la escala de los planos del edificio, que son demasiado grandes.

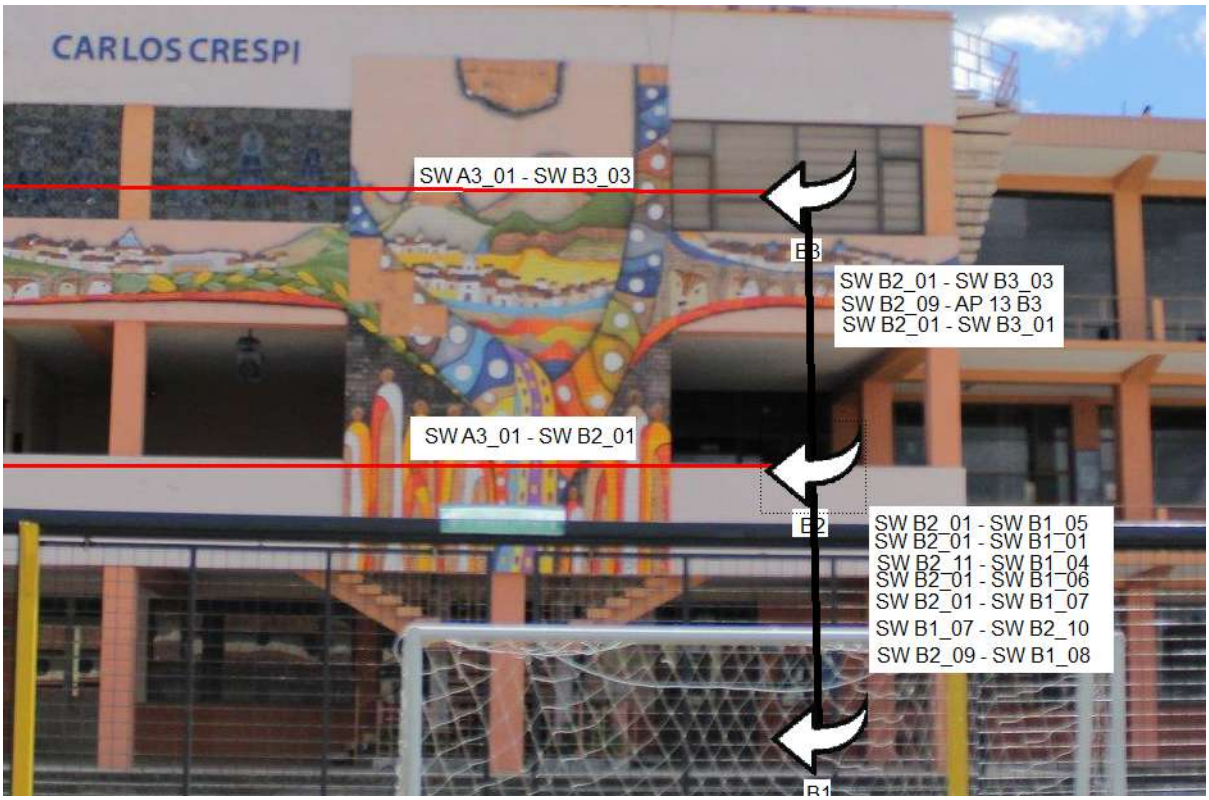

Figura 3.8: Topología zona B.
Fuente: Autor.

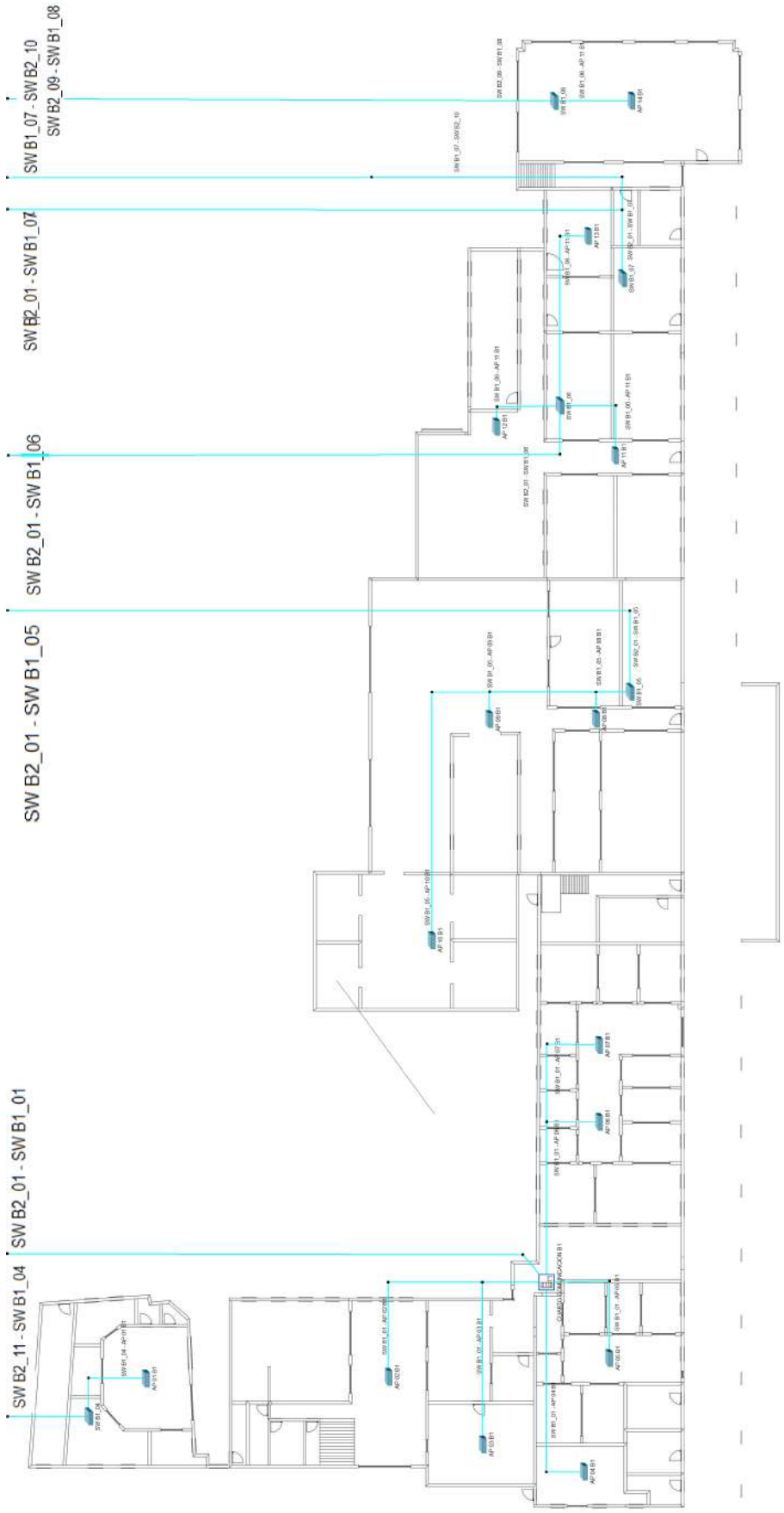

Figura 3.9: Topología zona B1.
Fuente: Autor.

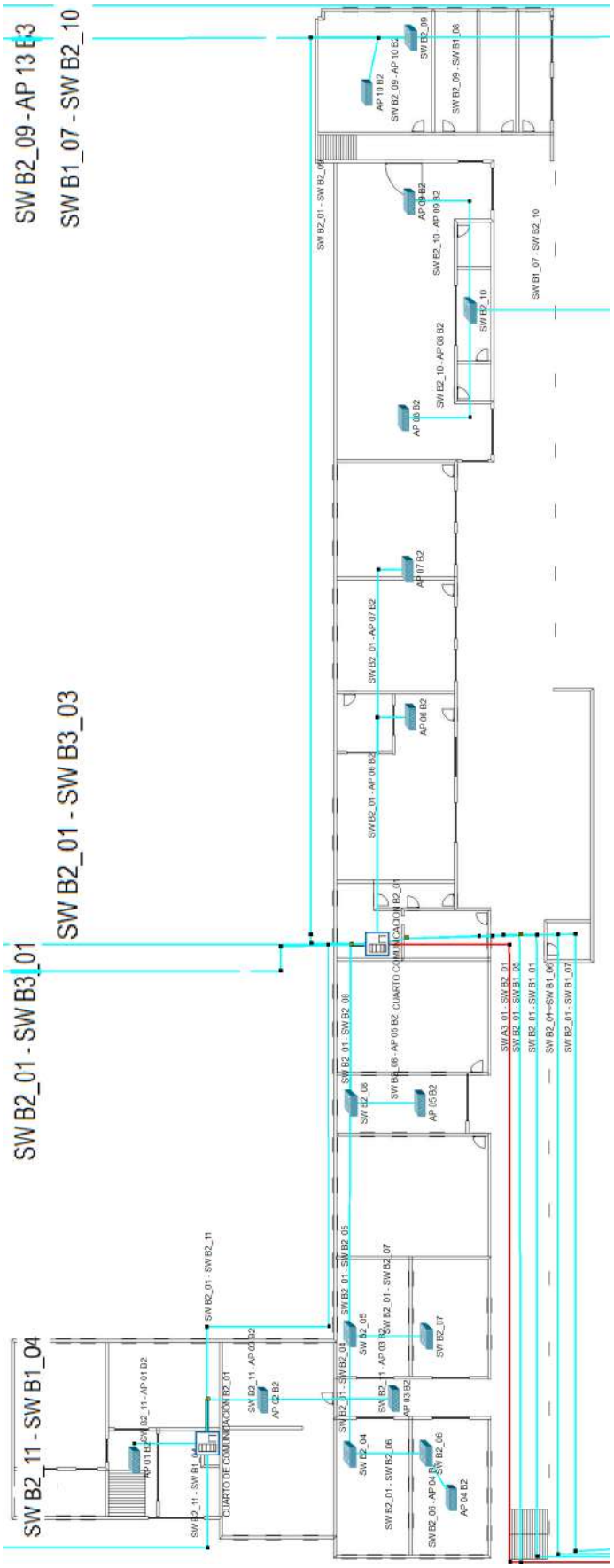

Figura 3.10: Topología zona B2.
Fuente: Autor.

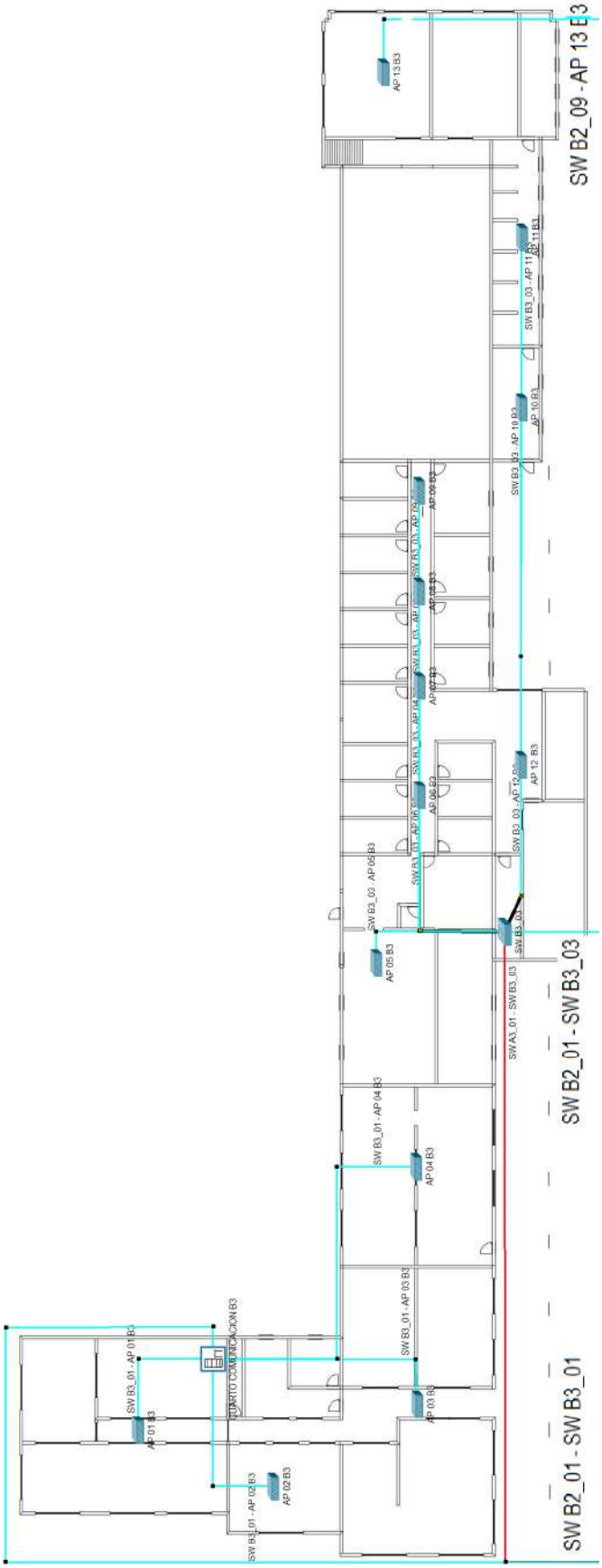

Figura 3.11: Topología zona B3.
Fuente: Autor.

3.2.3. Topología zona C

Se realizó la topología de la zona C, correspondiente al Edificio Mamá Margarita. En esta ocasión no se incluyeron subzonas pero se documentaron las diversas conexiones internas dentro de la zona C, asegurando una comprensión completa de la infraestructura de red en esta área específica.

Figura 3.12: Topología zona C.
Fuente: Autor.

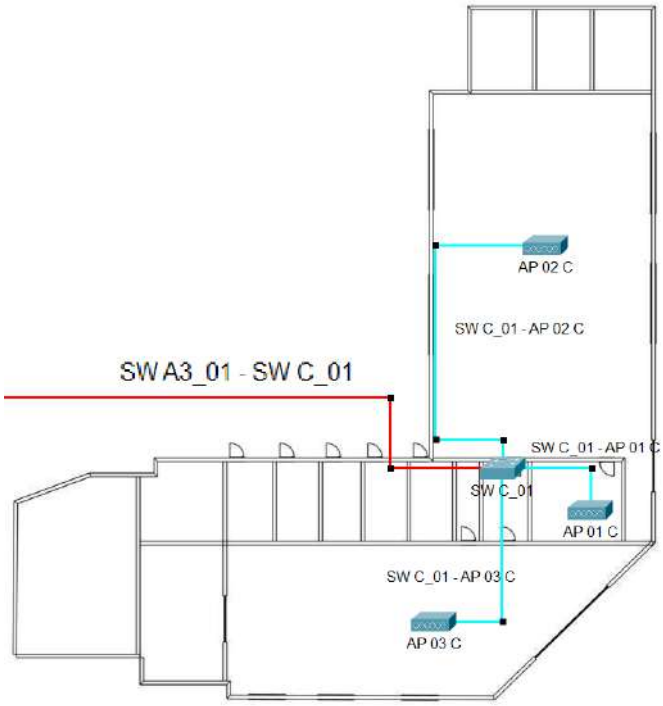

Figura 3.13: Topología zona C interior.
Fuente: Autor.

3.2.4. Topología zona D

Se realizó la topología de la zona D, correspondiente al Edificio Tecni Club. En esta ocasión no se incluyeron subzonas pero se documentaron las diversas conexiones internas dentro de la zona D, asegurando una comprensión completa de la infraestructura de red en esta área específica.

Figura 3.14: Topología zona D.
Fuente: Autor.

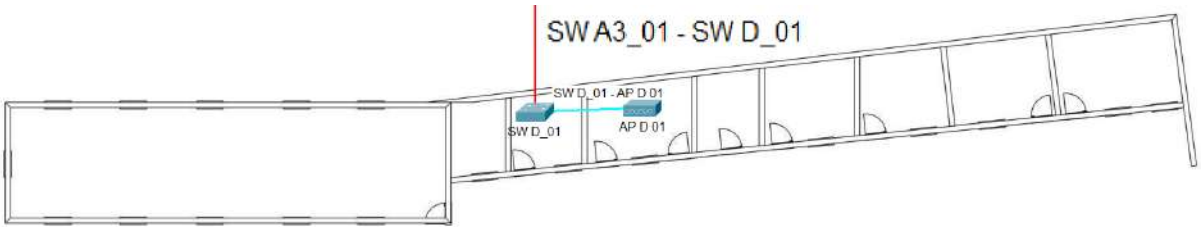

Figura 3.15: Topología zona D interior.
Fuente: Autor.

3.2.5. Topología zona E

Se realizó la topología de la zona E, correspondiente al Edificio Cancha Cubierta, así como de sus subzonas. Esta topología detalla las conexiones y enlaces de fibra óptica que parten de esta zona hacia otras zonas del campus. Además, se

documentaron las diversas conexiones internas dentro de las subzonas de la zona E, asegurando una comprensión completa de la infraestructura de red en esta área específica.

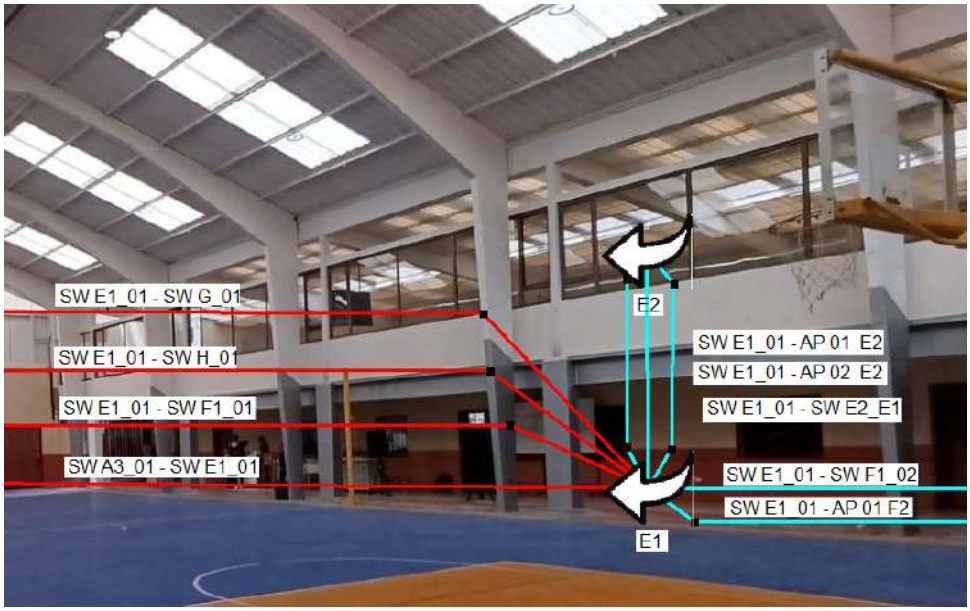

Figura 3.16: Topología zona E.
Fuente: Autor.

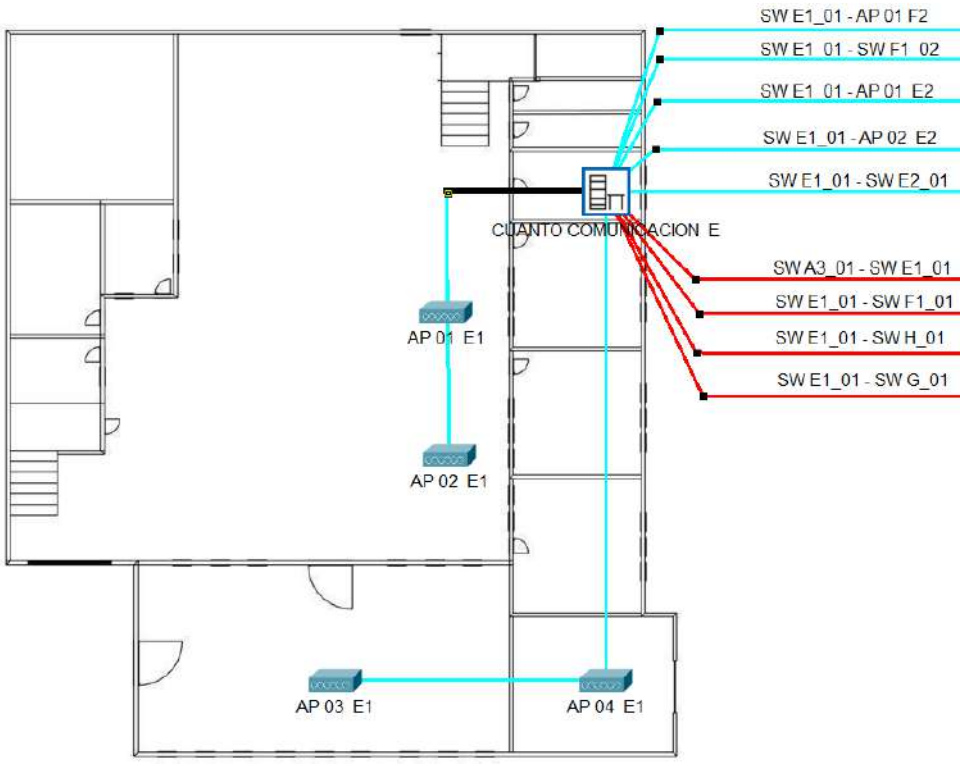

Figura 3.17: Topología zona E1.
Fuente: Autor.

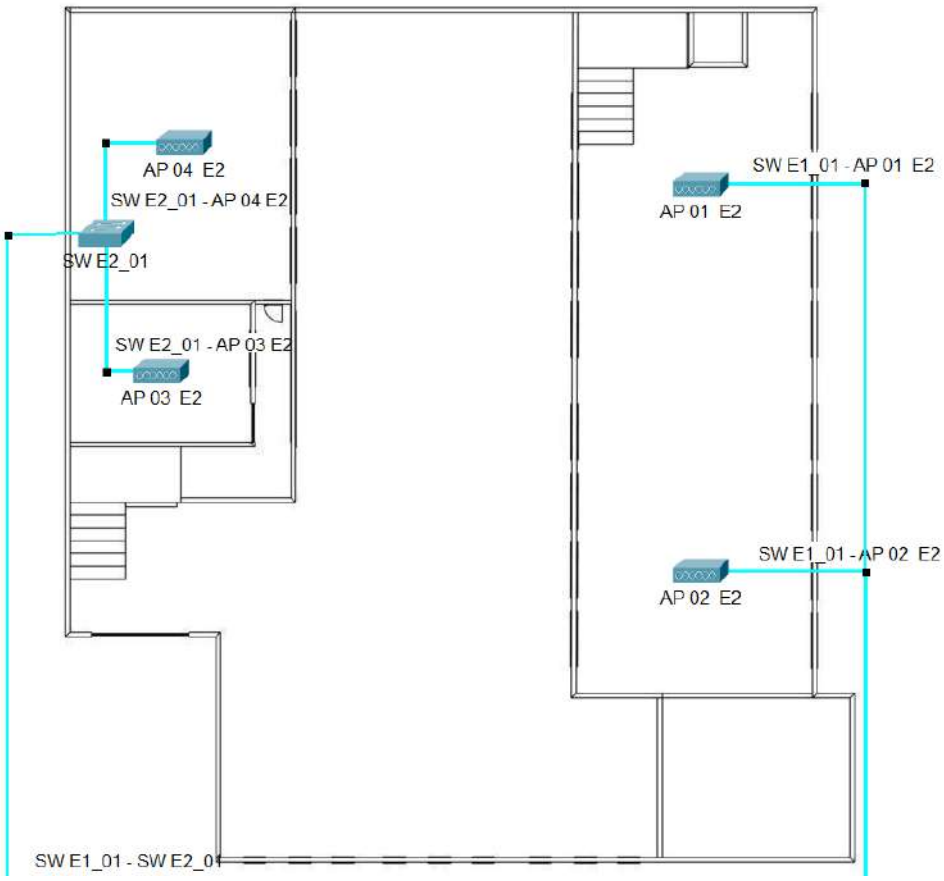

Figura 3.18: Topología zona E2.
Fuente: Autor.

3.2.6. Topología zona F

Se realizó la topología de la zona F, correspondiente al Edificio Coliseo, así como de sus subzonas. Esta topología detalla las conexiones y el enlace de fibra óptica que acomete desde la zona E. Además, se documentaron las diversas conexiones internas dentro de las subzonas de la zona F, asegurando una comprensión completa de la infraestructura de red en esta área específica.

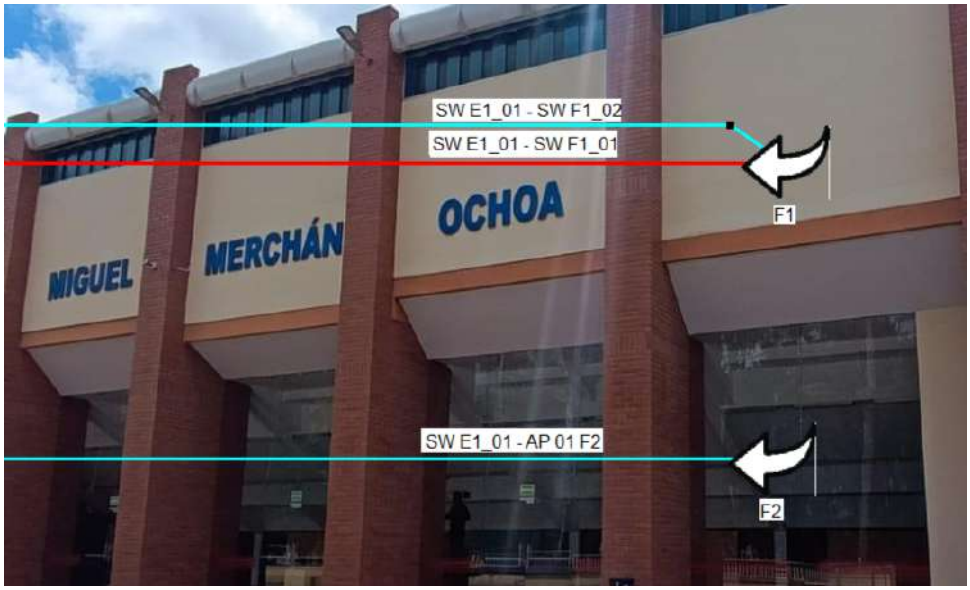

Figura 3.19: Topología zona F.
Fuente: Autor.

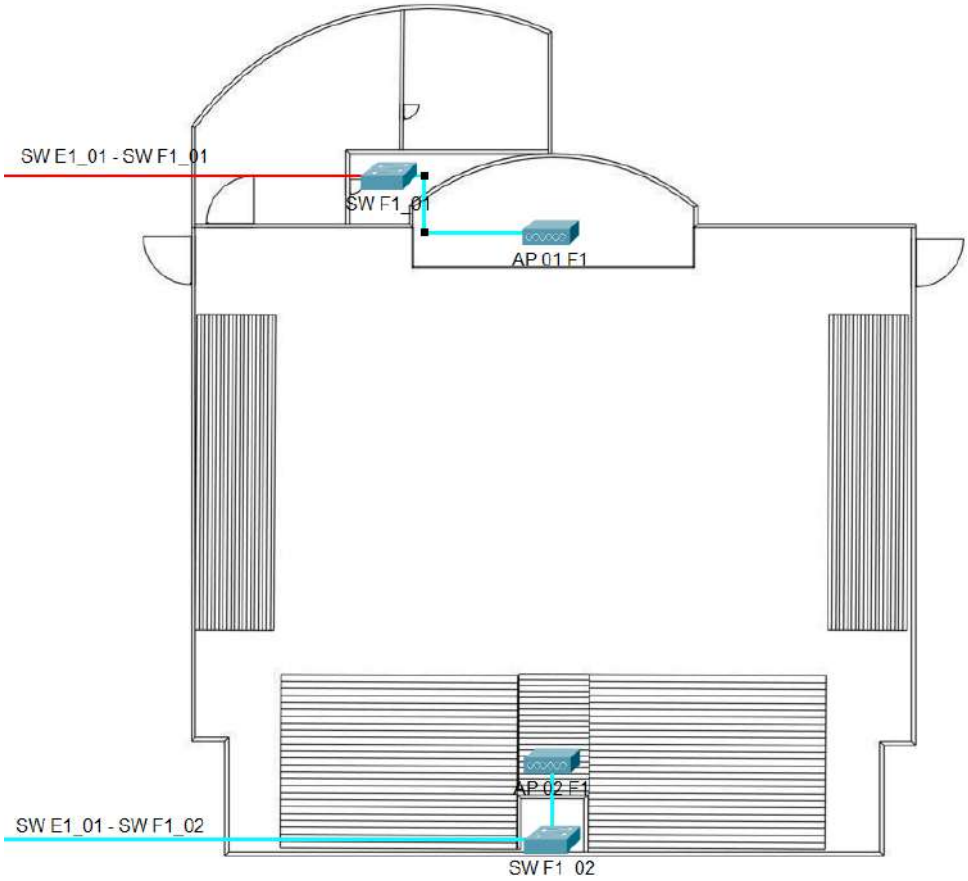

Figura 3.20: Topología zona F1.
Fuente: Autor.

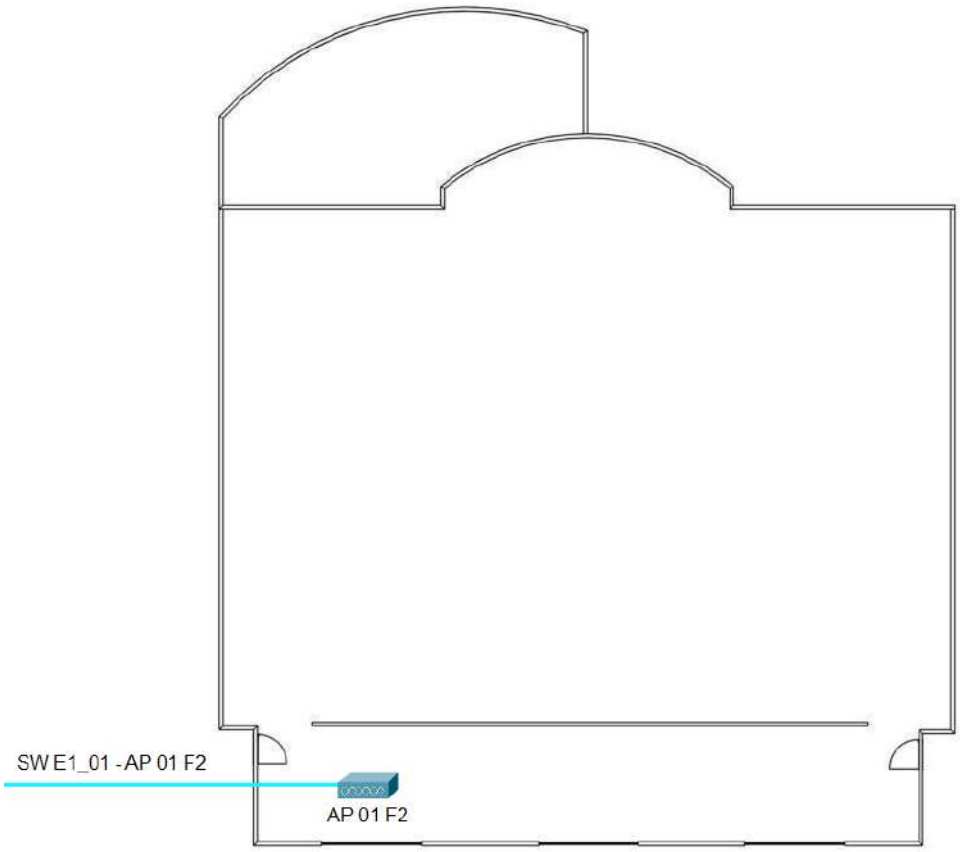

Figura 3.21: Topología zona F2.
Fuente: Autor.

3.2.7. Topología zona G

Se realizó la topología de la zona G, correspondiente al Edificio Piscina. En esta ocasión no se incluyeron subzonas pero se documentaron las diversas conexiones internas dentro de la zona G, asegurando una comprensión completa de la infraestructura de red en esta área específica.

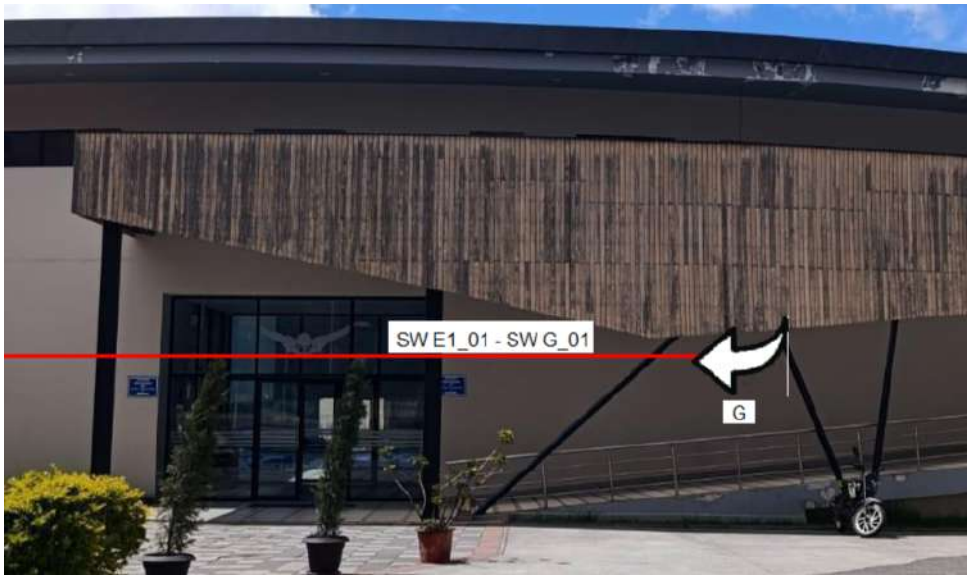

Figura 3.22: Topología zona G.
Fuente: Autor.

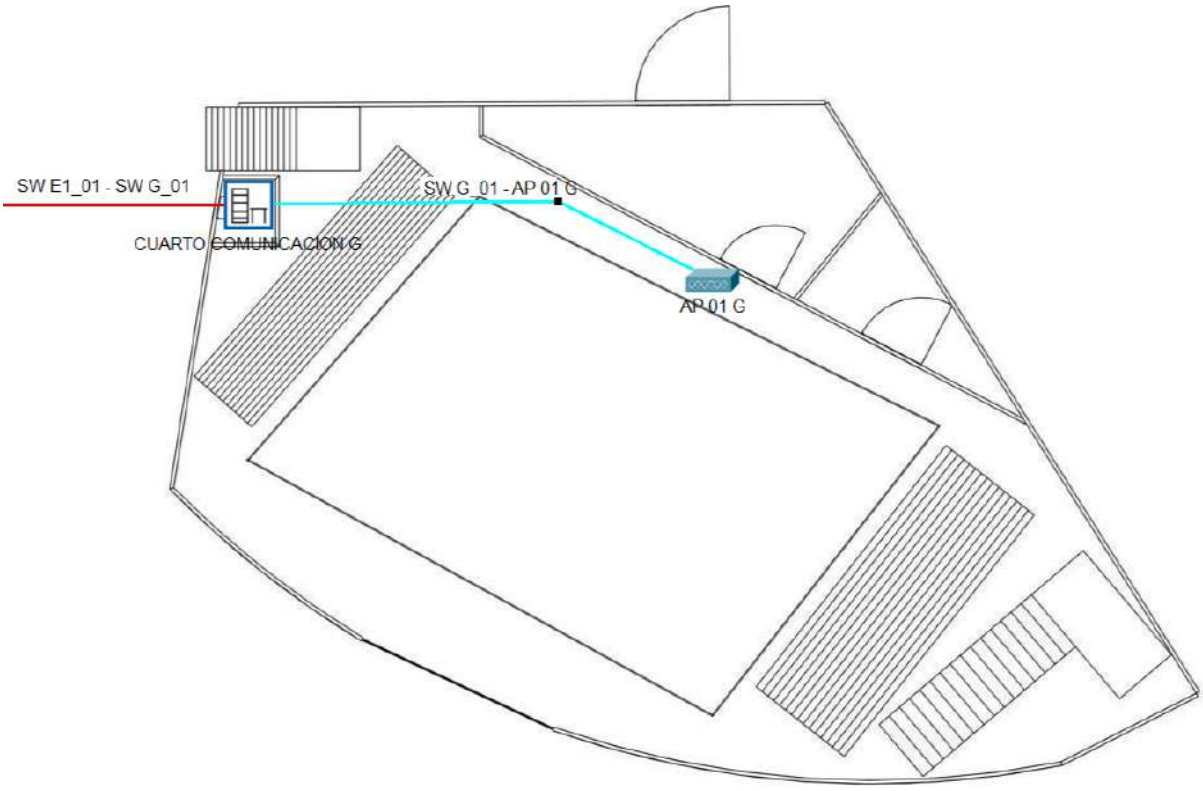

Figura 3.23: Topología zona G interior.
Fuente: Autor.

3.2.8. Topología zona H

Se realizó la topología de la zona H, correspondiente al Edificio Comunicación. En esta ocasión no se incluyeron subzonas pero se documentaron las diversas conexiones internas dentro de la zona H, asegurando una comprensión completa de la infraestructura de red en esta área específica.

Figura 3.24: Topología zona H.
Fuente: Autor.

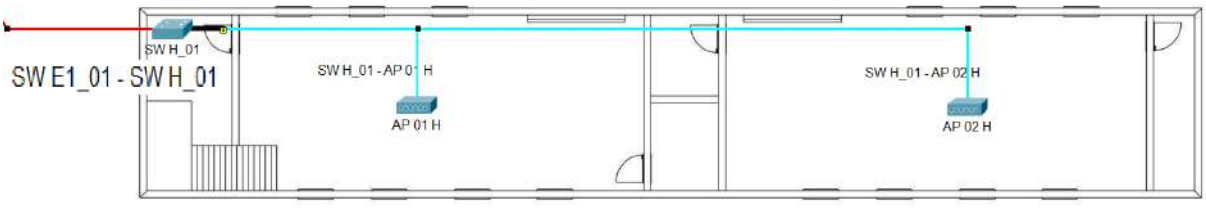

Figura 3.25: Topología zona H interior.
Fuente: Autor.

3.2.9. Descripción de códigos en topología por zonas

En la topología de equipos activos de red, cada equipo estaba meticulosamente descrito mediante tablas que aportaban una descripción detallada. Estos

códigos permitían una gestión eficiente y un mantenimiento preciso de nuestra infraestructura. Esta descripción facilitaba la identificación rápida de fallos, la planificación de actualizaciones y la optimización continua del rendimiento de nuestra red.

Descripción de equipos activos zona A

Tabla 3.4: Descripción de equipos activos zona A1.

Fuente: Autor.

Zona	Descripción	Equipo	#	Edificio	Planta
A1	SW A1_01	Switch	1	Miguel Rúa	Planta Baja
A1	SW A1_02	Switch	2	Miguel Rúa	Planta Baja
A1	AP 01 A1	Access Point	1	Miguel Rúa	Planta Baja
A1	AP 02 A1	Access Point	2	Miguel Rúa	Planta Baja
A1	AP 03 A1	Access Point	3	Miguel Rúa	Planta Baja
A1	AP 04 A1	Access Point	4	Miguel Rúa	Planta Baja
A1	AP 05 A1	Access Point	5	Miguel Rúa	Planta Baja

Tabla 3.5: Descripción de equipos activos zona A2.

Fuente: Autor.

Zona	Descripción	Equipo	#	Edificio	Planta
A2	SW A2_01	Switch	1	Miguel Rúa	Primera Planta
A2	SW A2_02	Switch	2	Miguel Rúa	Primera Planta
A2	AP 01 A2	Access Point	1	Miguel Rúa	Primera Planta
A2	AP 02 A2	Access Point	2	Miguel Rúa	Primera Planta
A2	AP 03 A2	Access Point	3	Miguel Rúa	Primera Planta
A2	AP 04 A2	Access Point	4	Miguel Rúa	Primera Planta
A2	AP 05 A2	Access Point	5	Miguel Rúa	Primera Planta
A2	AP 06 A2	Access Point	6	Miguel Rúa	Primera Planta

Tabla 3.6: Descripción de equipos activos zona A3.

Fuente: Autor.

Zona	**Descripción**	**Equipo**	**#**	**Edificio**	**Planta**
A3	RT 01 A3	Router	1	Miguel Rúa	Segunda Planta
A3	RT 02 A3	Router	2	Miguel Rúa	Segunda Planta
A3	SW 01 A3	Switch Core	1	Miguel Rúa	Segunda Planta
A3	SW 02 A3	Switch Core	2	Miguel Rúa	Segunda Planta
A3	SW 03 A3	Switch	1	Miguel Rúa	Segunda Planta
A3	SW 04 A3	Switch	2	Miguel Rúa	Segunda Planta
A3	SW 05 A3	Switch	3	Miguel Rúa	Segunda Planta
A3	SW 06 A3	Switch	4	Miguel Rúa	Segunda Planta
A3	FW 01 A3	Firewall	1	Miguel Rúa	Segunda Planta
A3	FW 02 A3	Firewall	2	Miguel Rúa	Segunda Planta
A3	AP 01 A3	Access Point	1	Miguel Rúa	Segunda Planta
A3	AP 02 A3	Access Point	2	Miguel Rúa	Segunda Planta
A3	AP 03 A3	Access Point	3	Miguel Rúa	Segunda Planta
A3	AP 04 A3	Access Point	4	Miguel Rúa	Segunda Planta
A3	AP 05 A3	Access Point	5	Miguel Rúa	Segunda Planta
A3	AP 06 A3	Access Point	6	Miguel Rúa	Segunda Planta

Tabla 3.7: Descripción de equipos activos zona A4.

Fuente: Autor.

Zona	Descripción	Equipo	#	Edificio	Planta
A4	SW 01 A4	Switch	1	Miguel Rúa	Tercera Planta
A4	SW 02 A4	Switch	2	Miguel Rúa	Tercera Planta
A4	SW 03 A4	Switch	3	Miguel Rúa	Tercera Planta
A4	AP 01 A4	Access Point	1	Miguel Rúa	Tercera Planta
A4	AP 02 A4	Access Point	2	Miguel Rúa	Tercera Planta
A4	AP 03 A4	Access Point	3	Miguel Rúa	Tercera Planta
A4	AP 04 A4	Access Point	4	Miguel Rúa	Tercera Planta
A4	AP 05 A4	Access Point	5	Miguel Rúa	Tercera Planta
A4	AP 06 A4	Access Point	6	Miguel Rúa	Tercera Planta
A4	AP 07 A4	Access Point	7	Miguel Rúa	Tercera Planta
Total Equipos			**41**	**Edificio Miguel Rúa**	

Descripción de equipos activos zona B

Tabla 3.8: Descripción de equipos activos zona B1.

Fuente: Autor.

Zona	Descripción	Equipo	#	Edificio	Planta
B1	SW B1_01	Switch	1	Carlos Crespi	Planta Baja
B1	SW B1_02	Switch	2	Carlos Crespi	Planta Baja
B1	SW B1_03	Switch	3	Carlos Crespi	Planta Baja
B1	SW B1_04	Switch	4	Carlos Crespi	Planta Baja
B1	SW B1_05	Switch	5	Carlos Crespi	Planta Baja
B1	SW B1_06	Switch	6	Carlos Crespi	Planta Baja
B1	SW B1_07	Switch	7	Carlos Crespi	Planta Baja
B1	SW B1_08	Switch	8	Carlos Crespi	Planta Baja
B1	AP 01 B1	Access Point	1	Carlos Crespi	Planta Baja
B1	AP 02 B1	Access Point	2	Carlos Crespi	Planta Baja
B1	AP 03 B1	Access Point	3	Carlos Crespi	Planta Baja
B1	AP 04 B1	Access Point	4	Carlos Crespi	Planta Baja
B1	AP 05 B1	Access Point	5	Carlos Crespi	Planta Baja
B1	AP 06 B1	Access Point	6	Carlos Crespi	Planta Baja
B1	AP 07 B1	Access Point	7	Carlos Crespi	Planta Baja
B1	AP 08 B1	Access Point	8	Carlos Crespi	Planta Baja
B1	AP 09 B1	Access Point	9	Carlos Crespi	Planta Baja
B1	AP 10 B1	Access Point	10	Carlos Crespi	Planta Baja
B1	AP 11 B1	Access Point	11	Carlos Crespi	Planta Baja
B1	AP 12 B1	Access Point	12	Carlos Crespi	Planta Baja
B1	AP 13 B1	Access Point	13	Carlos Crespi	Planta Baja
B1	AP 14 B1	Access Point	14	Carlos Crespi	Planta Baja

Tabla 3.9: Descripción de equipos activos zona B2.

Fuente: Autor.

Zona	Descripción	Equipo	#	Edificio	Planta
B2	SW B2_01	Switch	1	Carlos Crespi	Primera Planta
B2	SW B2_02	Switch	2	Carlos Crespi	Primera Planta
B2	SW B2_03	Switch	3	Carlos Crespi	Primera Planta
B2	SW B2_04	Switch	4	Carlos Crespi	Primera Planta
B2	SW B2_05	Switch	5	Carlos Crespi	Primera Planta
B2	SW B2_06	Switch	6	Carlos Crespi	Primera Planta
B2	SW B2_07	Switch	7	Carlos Crespi	Primera Planta
B2	SW B2_08	Switch	8	Carlos Crespi	Primera Planta
B2	SW B2_09	Switch	9	Carlos Crespi	Primera Planta
B2	SW B2_10	Switch	10	Carlos Crespi	Primera Planta
B2	SW B2_11	Switch	11	Carlos Crespi	Primera Planta
B2	SW B2_12	Switch	12	Carlos Crespi	Primera Planta
B2	AP 01 B2	Access Point	1	Carlos Crespi	Primera Planta
B2	AP 02 B2	Access Point	2	Carlos Crespi	Primera Planta
B2	AP 03 B2	Access Point	3	Carlos Crespi	Primera Planta
B2	AP 04 B2	Access Point	4	Carlos Crespi	Primera Planta
B2	AP 05 B2	Access Point	5	Carlos Crespi	Primera Planta
B2	AP 06 B2	Access Point	6	Carlos Crespi	Primera Planta
B2	AP 07 B2	Access Point	7	Carlos Crespi	Primera Planta
B2	AP 08 B2	Access Point	8	Carlos Crespi	Primera Planta
B2	AP 09 B2	Access Point	9	Carlos Crespi	Primera Planta
B2	AP 10 B2	Access Point	10	Carlos Crespi	Primera Planta

Tabla 3.10: Descripción de equipos activos zona B3.

Fuente: Autor.

Zona	Descripción	Equipo	#	Edificio	Planta
B3	SW B3_01	Switch	1	Carlos Crespi	Segunda Planta
B3	SW B3_02	Switch	2	Carlos Crespi	Segunda Planta
B3	SW B3_03	Switch	3	Carlos Crespi	Segunda Planta
B3	AP 01 B2	Access Point	1	Carlos Crespi	Segunda Planta
B3	AP 02 B2	Access Point	2	Carlos Crespi	Segunda Planta
B3	AP 03 B2	Access Point	3	Carlos Crespi	Segunda Planta
B3	AP 04 B2	Access Point	4	Carlos Crespi	Segunda Planta
B3	AP 05 B2	Access Point	5	Carlos Crespi	Segunda Planta
B3	AP 06 B2	Access Point	6	Carlos Crespi	Segunda Planta
B3	AP 07 B2	Access Point	7	Carlos Crespi	Segunda Planta
B3	AP 08 B2	Access Point	8	Carlos Crespi	Segunda Planta
B3	AP 09 B3	Access Point	9	Carlos Crespi	Segunda Planta
B3	AP 10 B3	Access Point	10	Carlos Crespi	Segunda Planta
B3	AP 11 B3	Access Point	11	Carlos Crespi	Segunda Planta
B3	AP 12 B3	Access Point	12	Carlos Crespi	Segunda Planta
B3	AP 13 B3	Access Point	13	Carlos Crespi	Segunda Planta
Total Equipos			**60**	**Carlos Crespi**	

Descripción de equipos activos zona C.

Tabla 3.11: Descripción de equipos activos zona C.

Fuente: Autor.

Zona	Descripción	Equipo	#	Edificio	Planta
C	SW C_01	Switch	1	Mamá Margarita	Planta Baja
C	AP 01 C	Access Point	1	Mamá Margarita	Planta Baja
C	AP 02 C	Access Point	2	Mamá Margarita	Planta Baja
C	AP 03 C	Access Point	3	Mamá Margarita	Planta Baja
Total Equipos			**4**	**Mamá Margarita**	

Descripción de equipos activos zona D.

Tabla 3.12: Descripción de equipos activos zona D.

Fuente: Autor.

Zona	Descripción	Equipo	#	Edificio	Planta
D	SW D_01	Switch	1	Tecni Club	Planta Baja
D	AP 01 D	Access Point	1	Tecni Club	Planta Baja
Total Equipos			**2**	**Tecni Club**	

Descripción de equipos activos zona E.

Tabla 3.13: Descripción de equipos activos zona E.

Fuente: Autor.

Zona	Descripción	Equipo	#	Edificio	Planta
E1	SW E1_01	Switch	1	Cancha Cubierta	Planta Baja
E1	SW E1_02	Switch	2	Cancha Cubierta	Planta Baja
E1	AP 01 E1	Access Point	1	Cancha Cubierta	Planta Baja
E1	AP 02 E1	Access Point	2	Cancha Cubierta	Planta Baja
E1	AP 03 E1	Access Point	3	Cancha Cubierta	Planta Baja
E1	AP 03 E1	Access Point	4	Cancha Cubierta	Planta Baja
E2	SW E2_01	Switch	1	Cancha Cubierta	Primera Planta
E2	AP 01 E2	Access Point	1	Cancha Cubierta	Primera Planta
E2	AP 02 E2	Access Point	2	Cancha Cubierta	Primera Planta
E2	AP 03 E2	Access Point	3	Cancha Cubierta	Primera Planta
E2	AP 03 E2	Access Point	4	Cancha Cubierta	Primera Planta
Total Equipos			**11**	**Cancha Cubierta**	

Descripción de equipos activos zona F

Tabla 3.14: Descripción de equipos activos zona F.

Fuente: Autor.

Zona	Descripción	Equipo	#	Edificio	Planta
F1	SW F1_01	Switch	1	Coliseo	Cancha & Escenario
F1	SW F1_02	Switch	2	Coliseo	Cancha & Escenario
F1	AP 02 F1	Access Point	1	Coliseo	Cancha & Escenario
F1	AP 02 F1	Access Point	2	Coliseo	Cancha & Escenario
F2	AP 01 F2	Access Point	1	Coliseo	Pasillo
Total Equipos			**5**	**Coliseo**	

Descripción de equipos activos zona G

Tabla 3.15: Descripción de equipos activos zona G.

Fuente: Autor.

Zona	Descripción	Equipo	#	Edificio	Planta
G	SW G_01	Switch	1	Piscina	Planta Baja
G	SW G_02	Switch	2	Piscina	Planta Baja
G	AP 01 G	Access Point	1	Piscina	Planta Baja
Total Equipos			**3**	**Piscina**	

Descripción de equipos activos zona H

Tabla 3.16: Descripción de equipos activos zona H.

Fuente: Autor.

Zona	Descripción	Equipo	#	Edificio	Planta
H	SW H_01	Switch	1	Comunicación	Planta Baja
H	AP 01 H	Access Point	1	Comunicación	Planta Baja
H	AP 02 H	Access Point	2	Comunicación	Planta Baja
Total Equipos			**3**	**Comunicación**	

Conteo de equipos activos

Tabla 3.17: Conteo de equipos activos.

Fuente: Autor.

Zona	Edificio	Equipo	Cantidad
A	Miguel Rúa	Router CPE	2
		Firewall	2
		Switch Core	2
		Switch	11
		Access Point	24
B	Carlos Crespi	Switch	23
		Access Point	37
C	Mamá Margarita	Switch	1
		Access Point	3
D	Tecni Club	Switch	1
		Access Point	1
E	Cancha Cubierta	Switch	3
		Access Point	8
F	Coliseo	Switch	2
		Access Point	3
G	Piscina	Switch	2
		Access Point	1
H	Comunicación	Switch	1
		Access Point	2
Total Campus Yanuncay			**129**

3.3. Elección de equipos para actualización

En esta sección, se analizaron los equipos más adecuados para la actualización de nuestra red institucional, con un enfoque en asegurar la robustez y facilidad de mantenimiento de los mismos. La elección de los equipos fue un paso crucial para garantizar que la infraestructura tecnológica cumpliera con los requisitos de desempeño, seguridad y escalabilidad necesarios para soportar las operaciones

actuales y futuras de la institución.

Además, se elaboraron tablas comparativas con diferentes marcas de equipos para identificar cuál sería la más conveniente para nuestra red. Estas tablas incluyeron una evaluación detallada de las características técnicas, precios, garantías y soporte post-venta de cada marca. Al comparar estos aspectos, se determinaría de manera objetiva cuál opción ofrecía el mejor equilibrio entre calidad y costo, facilitando así una decisión informada.

Switch de Core

Tabla 3.18: Comparativa de Switch Core.

Fuente: Autor.

Especificación	**Huawei S6730S-S24X6Q-A**	**Cisco Catalyst 9500-24Y4C**	**Juniper EX4650-48Y-AFI**
Velocidad de Transmisión	10 Gbps, 40 Gbps	25 Gbps, 100 Gbps	25 Gbps, 100 Gbps
Memoria	4GB de RAM, 2GB de Flash	16GB de RAM, 16GB de Flash	16GB de RAM, 64GB de SSD
Consumo Máximo de Energía	249 W	650 W	500 W
Temperatura de Operación	-5°C a 45°C	-5°C a 40°C	0°C a 40°C
Puertos SFP	24 x 10GE SFP+	24 x 25GE SFP28	48 x 25GE SFP28
Estandares SFP	SFP+	SFP28	SFP28
Estandares IEEE	802.3, 802.3u, 802.3ab, 802.3z, 802.3ae	802.3, 802.3ae, 802.3ba, 802.3by	802.3, 802.3z, 802.3ae, 802.3ba
Precio	$8,500	$21,000	$38,000

Con el análisis de los respectivos datasheet de los equipos en comparación [40]-[42], se eligió actualizar el equipo antiguo por el Huawei S6730S-S24X6Q-A debido a varias razones fundamentales que aseguraron una mejor performance y confiabilidad el campus Yanuncay.

Figura 3.26: Switch Huawei S6730S-S24X6Q-A.
Fuente:[40].

Entre las razones por las cuales elegir este equipo fue una decisión acertada se encuentra:

- Precio: Con un precio de $8,500, el Huawei S6730S-S24X6Q-A fue más económico en comparación con el Cisco Catalyst 9500-24Y4C ($21,000) y el Juniper EX4650-48Y-AFI ($38,000). Esto representó una excelente relación calidad-precio para la institución o empresas que tenía un presupuesto más ajustado.

- Rendimiento: Aunque ofrecía una velocidad de transmisión de 10 Gbps y 40 Gbps, en comparación con los 25 Gbps y 100 Gbps de los otros modelos, esta velocidad era más que suficiente para la institución puesto que cubriría las necesidades de soportar aplicaciones de alta demanda como la transmisión de video, laboratorios virtuales, platadormas y sistemas de gestión de aprendizaje.

- Consumo Energético: El Huawei S6730S-S24X6Q-A tenía un consumo máximo de energía de 249 W, que era considerable en comparación de los 650 W del Cisco Catalyst y los 500 W del Juniper EX4650. Un menor consumo de energía no solo reducía los costos operativos a largo plazo

- Memoria: Con 4 GB de RAM y 2 GB de Flash, aunque no fue la mayor capacidad entre los competidores, fue suficiente para manejar múltiples tareas y procesos al mismo tiempo en el campus Yanuncay, asegurando un rendimiento fluido en la mayoría de las demandas de la institución.

- Especificaciones SFP y IEEE: Aunque contaba con puertos SFP+ en lugar de SFP28, seguía cumpliendo con los estándares IEEE 802.3, 802.3u, 802.3ab, 802.3z

y 802.3ae, asegurando la compatibilidad y la interoperabilidad con otros equipos de red y manteniendo una infraestructura de red sólida y eficiente.

- Garantía: Una garantía extendida de 8 años, la UETS podía beneficiarse al saber que cualquier problema técnico o fallo del equipo sería cubierto sin costos adicionales durante un periodo prolongado.

- Equipo Back Up: Contar con un equipo de respaldo era crucial para garantizar la continuidad del servicio. En caso de que el equipo principal experimentara fallos, entraría en funcionamiento el equipo de respaldo, minimizando el tiempo de inactividad y asegurando que las actividades académicas y administrativas no se viesen interrumpidas.

- Capacitación: La empresa CEDIA proporcionaría una capacitación asegurando que el personal técnico de la institución estuviera completamente preparado para operar y mantener el equipo de manera eficiente. Esto no solo mejoraría la autonomía y la capacidad de respuesta ante problemas, sino que también reduciría la dependencia de soporte externo, lo que podía ser costoso y lento.

Firewall

Tabla 3.19: Comparativa de Firewall.

Fuente: Autor.

Característica / Firewall	SonicWall NSA 4600	Cisco ASA 5525-X	Fortinet FortiGate 100E
Rendimiento de Firewall	6 Gbps	2 Gbps	7 Gbps
Rendimiento de IPS	1.5 Gbps	600 Mbps	2.4 Gbps
Rendimiento de VPN	2.75 Gbps	300 Mbps	1.8 Gbps
Rendimiento de NGFW (Firewall + IPS)	1.8 Gbps	400 Mbps	1.5 Gbps
Máximo de Sesiones	500	750	800
Interfaces	12 x 1 GbE, 4 x 10 GbE SFP+	8 x 1 GbE, 4 x 1 GbE SFP	22 x 1 GbE, 2 x 10 GbE SFP+
VLANs	512	2000	4096
Gestión	Web, CLI, GMS	ASDM, CLI, Firepower	FortiManager, FortiAnalyzer
Seguridad Avanzada	DPI, SSL Inspection, App Control	Firepower, AMP, URL Filtering	AV, IPS, App Control
Precio Aproximado	$9,5010 USD	$4,020 USD	$3,220 USD

Al seleccionar la mejor solución para la seguridad de la red y analisando los respectivos datasheet [43]-[45], se decidió optar por el SonicWall NSA 4600, destacándose frente a otros modelos como el Cisco ASA 5525-X y el Fortinet FortiGate 100E por varias razones clave.

Figura 3.27: Firewall SonicWall NSA 4600.
Fuente: [43].

- Rendimiento Superior en Firewall: Se eligió el SonicWall NSA 4600 porque

ofrecía un rendimiento de firewall de hasta 6 Gbps, superando al Cisco ASA 5525-X, que alcanzaba 2 Gbps, y al Fortinet FortiGate 100E, con 7 Gbps. Este alto rendimiento aseguraría que la red pudiera manejar grandes volúmenes de tráfico sin comprometer la velocidad o la seguridad.

- Equilibrio en Rendimiento de IPS y VPN: Aunque el Fortinet FortiGate 100E ofrecía el mejor rendimiento de IPS con 2.4 Gbps, el SonicWall NSA 4600 se ubicó en una sólida segunda posición con 1.5 Gbps, comparado con los 600 Mbps del Cisco ASA 5525-X. En términos de VPN, el SonicWall NSA 4600 también destacaba con un rendimiento de 2.75 Gbps, muy por encima del Cisco ASA 5525-X y sus 300 Mbps, y superior al Fortinet FortiGate 100E con 1.8 Gbps.

- Capacidad de NGFW y Escalabilidad: Se optó por el SonicWall NSA 4600 debido a su capacidad para manejar un rendimiento de NGFW (Firewall + IPS) de 1.8 Gbps, superando al Cisco ASA 5525-X con 400 Mbps, y al Fortinet FortiGate 100E con 1.5 Gbps. Aunque el SonicWall ofrecía una capacidad máxima de 500 sesiones, que fue menor que los 750 y 800 del Cisco ASA 5525-X y Fortinet FortiGate 100E, su flexibilidad y escalabilidad en el manejo de VLANs y interfaces compensaban esta diferencia.

- Funciones de Seguridad Avanzada: Se eligió el SonicWall NSA 4600 por su capacidad para proporcionar una protección integral con características avanzadas como DPI (Inspección Profunda de Paquetes), Inspección SSL y Control de Aplicaciones. Aunque el Fortinet FortiGate 100E también brindaba una sólida seguridad avanzada, el SonicWall se destacó por ofrecer una protección más amplia y eficaz.

- Capacitación y Soporte: Al elegir el SonicWall NSA 4600, también aseguramos recibir capacitación completa para el uso del equipo. Esta capacitación garantizaría que el equipo de sistemas y telecomunicaciones pudiera gestionar y configurar el firewall de manera óptima. Además, el SonicWall NSA 4600 venía con un firewall de respaldo, proporcionando una capa adicional de seguridad y continuidad en caso de fallos.

- Costo-Efectividad: A pesar de su precio aproximado de $9,500, el SonicWall NSA 4600 ofrecía una excelente relación calidad-precio, considerando su alto rendimiento y características avanzadas. Aunque era más costoso que el Cisco ASA 5525-X y el Fortinet FortiGate 100E, la combinación de su rendimiento superior y características adicionales justificaba la inversión.

Access Point

Tabla 3.20: Comparación de Equipos para Puntos de Acceso.

Fuente: Autor.

	Aruba 515	**Aruba AP 505**	**Cisco Catalyst 9115AXI**	**Ubiquiti UniFi 6 Pro**
Estándar Wi-Fi	Wi-Fi 6 (802.11ax)	Wi-Fi 6 (802.11ax)	Wi-Fi 6 (802.11ax)	Wi-Fi 6 (802.11ax)
Bandas de frecuencia	2.4GHz y 5GHz	2.4GHz y 5GHz	2.4GHz y 5GHz	2.4GHz y 5GHz
MIMO	4x4:4 (5 GHz), 2x2:2 (2.4 GHz)	2x2:2 (5 GHz), 2x2:2 (2.4 GHz)	4x4:4 (5 GHz), 2x2:2 (2.4 GHz)	4x4:4 (5 GHz), 2x2:2 (2.4 GHz)
Velocidad máxima	Hasta 4.8 Gbps (5 GHz), 575 Mbps (2.4 GHz)	Hasta 1.2 Gbps (5 GHz), 574 Mbps (2.4 GHz)	Hasta 5 Gbps (5 GHz), 600 Mbps (2.4 GHz)	Hasta 4.8 Gbps (5 GHz), 573.5 Mbps (2.4 GHz)
Puertos Ethernet	1x 2.5GBASE-T, 1x 1GBASE-T	1x 1GBASE-T	1x 2.5GBASE-T, 1x 1GBASE-T	1x 2.5GBASE-T
Antenas	Internas, omnidireccionales	Internas, omnidireccionales	Internas, omnidireccionales	Internas, omnidireccionales
Número máximo de clientes	Hasta 256 por radio	Hasta 256 por radio	Hasta 200 por radio	Hasta 300 por radio
Seguridad	WPA3, WPA2, Aruba Policy Enforcement Firewall	WPA3, WPA2, Aruba Policy Enforcement Firewall	WPA3, WPA2, Cisco Umbrella	WPA3, WPA2
Precio	$943.00	$663.00	$900.00	$150.00

Tras evaluar varias opciones para la actualización de nuestros equipos de red y tras revisar los datasheet de los equipos [46]-[48], se decidió que los puntos de acceso Aruba 515 y Aruba AP 505 eran las mejores opciones disponibles.

Figura 3.28: Access Point Aruba serie 500.
Fuente: [46].

- Desempeño de MIMO y Velocidad: Los AP Aruba 515 y 505 ofrecieron un rendimiento MIMO que satisfacía las necesidades de cobertura y capacidad de la institución. El Aruba 515 proporcionaba una configuración MIMO de 4x4:4 en banda de 5 GHz y 2x2:2 en la banda de 2.4GHz, lo que permitiría una velocidad máxima de hasta 4.8Gbps en la banda de 5GHz. El Aruba AP 505, aunque con un MIMO de 2x2:2 en ambas bandas, resultó adecuado para entornos con menos demanda de ancho de banda, proporcionando velocidades máximas de hasta 1.2Gbps en banda de 5GHz.

- Capacidad de Clientes: Los AP Aruba 515 y 505 soportaban hasta 256 clientes por radio, lo que las hacía ideales para entornos con alta densidad de usuarios. Esto era crucial para garantizar un rendimiento óptimo en áreas con muchos dispositivos conectados, superando la capacidad máxima de 200 clientes por radio del Cisco Catalyst 9115AXI y alcanzando la capacidad de 300 clientes por radio del Ubiquiti UniFi 6 Pro.

- Seguridad y Gestión: Ambas antenas Aruba proporcionaron robustas características de seguridad con soporte para WPA3 y WPA2, además de la Aruba Policy Enforcement Firewall. Esto ofreció una capa adicional de protección para la red. Aunque el Cisco Catalyst 9115AXI también incluyó

características de seguridad avanzadas como Cisco Umbrella, la integración con las políticas de Aruba era más adecuada para la infraestructura existente.

- Costo: Los AP Aruba 505 y 515 ofrecían una excelente relación costo-beneficio, con precios competitivos en comparación con el Cisco Catalyst 9115AXI, que resultaba más caro. El Aruba 505, con un costo aproximado de $670, proporcionaba un equilibrio entre rendimiento y precio. En contraste, el Cisco Catalyst 9115AXI, con un costo aproximado de $1,000, superaba nuestras necesidades actuales en términos de capacidad y características. Además, el Aruba 515, aunque más cara con un costo de como $977.50, justificaba su precio por sus especificaciones avanzadas.

Switch de acceso

Tabla 3.21: Comparativa Switch de Acceso.

Fuente: Autor.

Característica / Switch	**Aruba J9776A 2530 24G**	**Cisco Catalyst 9300-24T**	**HPE OfficeConnect 1950 24G**
Puertos Totales	24 puertos Gigabit Ethernet	24 puertos Gigabit Ethernet	24 puertos Gigabit Ethernet
Puertos SFP	4 puertos SFP	4 puertos SFP+	4 puertos SFP
Estándares SFP	1000BASE-X	1000BASE-X, 10GBASE-X	1000BASE-X
Capacidad de Transmisión (Gbps)	56 Gbps	56 Gbps	52 Gbps
Velocidad de Transmisión (Mpps)	41.7 Mpps	41.66 Mpps	38.69 Mpps
Estándares IEEE soportados	802.3, 802.3u, 802.3ab, 802.3az	802.3, 802.3u, 802.3ab, 802.3at	802.3, 802.3u, 802.3ab, 802.3az
Capacidad de Usuarios	512 usuarios	1024 usuarios	No especificado
Precio	$1,503 USD	$2,224 USD	$1,302 USD

Tras una evaluación exhaustiva de varias opciones con su respectivo datasheet[49]-[51], se decidió que el Aruba J9776A 2530 24G era la mejor opción frente a otros modelos.

Figura 3.29: Switch de Acceso Aruba 2530 24G.
Fuente: [49].

- Compatibilidad e Infraestructura Existente: Un factor determinante en la decisión fue que ya se contaba con numerosos switches Aruba J9776A 2530 24G instalados en la red. Esta infraestructura existente permitió una integración fluida y sin problemas de compatibilidad con los nuevos equipos. La continuidad con el mismo modelo simplificaría administración y cuidado de la red, minimizando el impacto operativo y garantizando una transición más eficiente.
- El Aruba J9776A 2530 24G ofrecía una capacidad de transmisión de 56 Gbps y una velocidad de transmisión de 41.7 Mpps, que cumplieron con las necesidades de rendimiento de red. Aunque el Cisco Catalyst 9300-24T también proporcionó una capacidad de 56 Gbps, su mayor costo no justificaba el incremento marginal en el rendimiento. El HPE OfficeConnect 1950 24G, con una capacidad de 52 Gbps y una velocidad de 38.69 Mpps, resultó menos competitivo en términos de rendimiento frente al Aruba J9776A 2530 24G.
- El Aruba J9776A 2530 24G soportaba estándares SFP de 1000BASE-X, lo que fue adecuado para nuestras aplicaciones y requerimientos de red. Aunque el Cisco Catalyst 9300-24T ofrecía soporte adicional para 10GBASE-X, esta capacidad no era necesaria para las necesidades actuales y su costo más alto no se justificaba. El HPE OfficeConnect 1950 24G también soportó 1000BASE-X, pero con menos flexibilidad en comparación con el Cisco.
- El Aruba J9776A 2530 24G soportaba hasta 512 usuarios, lo que resultaba suficiente para las necesidades en comparación con el Cisco Catalyst 9300-24T,

que soportaba hasta 1024 usuarios, pero a un precio más alto. El HPE OfficeConnect 1950 24G no especificaba claramente su capacidad de usuarios, lo que generó incertidumbre en su aplicabilidad a gran escala.

- Costo: El Aruba J9776A 2530 24G presentaba un costo aproximado de $1,500 USD, lo que lo posicionaba a favor en comparación con el Cisco Catalyst 9300-24T, que costaba alrededor de $2,200 USD, y el HPE OfficeConnect 1950 24G, con un costo de alrededor de $1,300 USD. La relación costo-beneficio del Aruba J9776A 2530 24G era óptima, ofreciendo un equilibrio entre rendimiento y precio, dado el hecho de que ya estaba bien integrado en nuestra infraestructura.

Sistema SAI

En la institución se encontraba almacenado un equipo UPS MPS de 5 kVA, el cual opera con un sistema de 48V. Dado que el equipo ya estaba disponible, se solicitó al departamento de mantenimiento solo cuatro baterías de 12V. Estos componentes eran los necesarios para implementar un sistema SAI.

Figura 3.30: Equipos MPS 5kVA.
Fuente: [52].

3.4. Costo de actualización

Se realizó la compra de equipos activos de red y componentes necesarios para la implementación de actualización de equipos activos de red de datos. Esta adquisición incluyó los equipos y elementos indispensables para garantizar un rendimiento óptimo y una integración efectiva con la infraestructura existente.

Tabla 3.22: Presupuesto del Proyecto

USO DEL PRESUPUESTO			
U	**Descripción del Elemento**	**Costo Unitario**	**Costo Total**
1	Switch Core Huawei con BackUp	$ 9.000,00	$ 9.000,00
1	Firewall SonicWall con BackUp	$ 9.500,00	$ 9.500,00
8	Switch Aruba Administrable 24 puertos	$ 800,00	$ 6.400,00
3	Switch Aruba Administrable 8 puertos	$ 250,00	$ 750,00
2	Switch Aruba Administrable 16 puertos	$ 380,00	$ 760,00
10	Ap Aruba 515	$ 943,00	$ 9.430,00
5	Ap Aruba 505	$ 663,00	$ 3.315,00
1	Ap Aruba P17	$ 400,00	$ 400,00
3	Ap Ubiquiti Direccional	$ 320,00	$ 960,00
1	SAI MPS	$ 500,00	$ 500,00
4	Batería 12V	$ 300,00	$ 1.200,00
2	Gabinete Rack 9U	$ 250,00	$ 500,00
1	Gabinete Rack 6U	$ 160,00	$ 160,00
10	Caja PatchCords Panduit	$ 100,00	$ 1.000,00
1	Implementos Extras	$ 1.000,00	$ 1.000,00
2	Kit de Herramientas Básicas	$ 200,00	$ 400,00
720	Costo Diseño y Mano de Obra /H	$ 6,00	$ 4.320,00
TOTAL QUE CUBRE LA INSTITUCIÓN			**$ 49.595,00**

Capítulo 4

Implementación de Actualización de Equipos Activos de Red

Como parte del proyecto de actualización de la infraestructura de red del campus Yanuncay, se llevó a cabo una implementación integral de equipos activos de red, los cuales fueron actualizados y configurados. Este proceso fue fundamental para optimizar la conectividad y el desempeño de la red, adaptándose a las necesidades crecientes de la institución.

4.1. Implementación de equipos principales

Para garantizar una alta disponibilidad y robustez en la implementación de los equipos principales (firewall y switch de core), se siguió un esquema de alta disponibilidad (4.1) que incluye un enlace de acometida principal por parte del ISP PuntoNet y un enlace de respaldo proporcionado por el ISP TelconNet, los cuales fueron subcontratados por nuestro proveedor principal CEDIA. Esto garantizó una continuidad en el servicio y una mayor resiliencia en la infraestructura de red de datos en caso de falla en alguno de los dos enlaces.

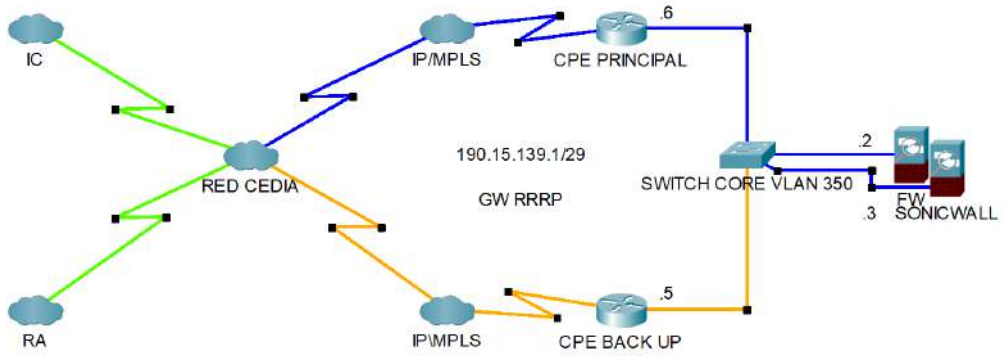

Figura 4.1: Esquema de alta disponibilidad.
Fuente: Autor.

Como muestra la Figura la 4.1, se implementó el protocolo RRRP (Redundant Router Routing Protocol). Este protocolo permite que múltiples routers trabajen juntos para proporcionar redundancia y conmutación por error en caso de que uno de los routers falle.

4.1.1. Implementación de Switch de Core

Se llevó a cabo la actualización del switch de core Huawei 6730S-S24X6Q-A 3.26 como parte del proceso de mejora de la infraestructura de red. A lo largo del proceso de actualización, se realizaron configuraciones detalladas para adaptar el switch a las necesidades específicas de la red y garantizar su integración efectiva con los equipos existentes. Como configuración principal se le asigno una dirección IP estática que serviría para identificar al equipo en la red, como segundo paso se configuró y probo los puertos de las respectivas interfaces, puesto que éste equipo tiene puertos SFP, luego se configuraron VLAN's y DHCP y luego se instaló el equipo en el rack del centro de datos, conectando los enlaces de fibra óptica en los SFP.

Configuración IP estática

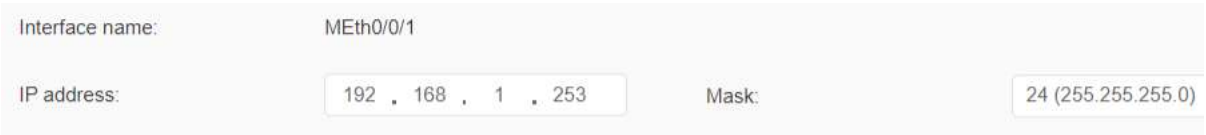

Figura 4.2: Configuración IP estática Switch Core.
Fuente: Autor.

Configuración de interfaces

Se configuraron las interfaces del switch de core para optimizar su funcionamiento y adaptarlo a las necesidades que requería la red. Cabe mencionar que se prestó especial atención a la correcta asignación y ajuste de los parámetros de cada interfaz. Además, se revisó a detalle para asegurar que los transceptores utilizados fueran reconocidos por el equipo. Se utilizaron transceptores ópticos (figuras 4.3 y 4.4) para los enlaces que llegaban directamente del ODF, asegurando una conexión de mayor velocidad y calidad usando fibra óptica. Para los enlaces que llegaban a través de convertidores de medios, se emplearon transceptores eléctricos, adaptando la señal de fibra óptica a un formato eléctrico adecuado para su procesamiento. Esta combinación de transceptores ópticos y eléctricos permitió la conexión de enlaces que antes no estaban conectados, optimizando la integración y eficiencia de toda la infraestructura de red para así garantizar una conectividad eficiente y fiable.

Figura 4.3: SFP Óptico Multimodo Huawei.
Fuente:[53].

Figura 4.4: SFP Eléctrico Huawei.
Fuente: [54].

Figura 4.5: SFP Óptico Monomodo Huawei.
Fuente:[53].

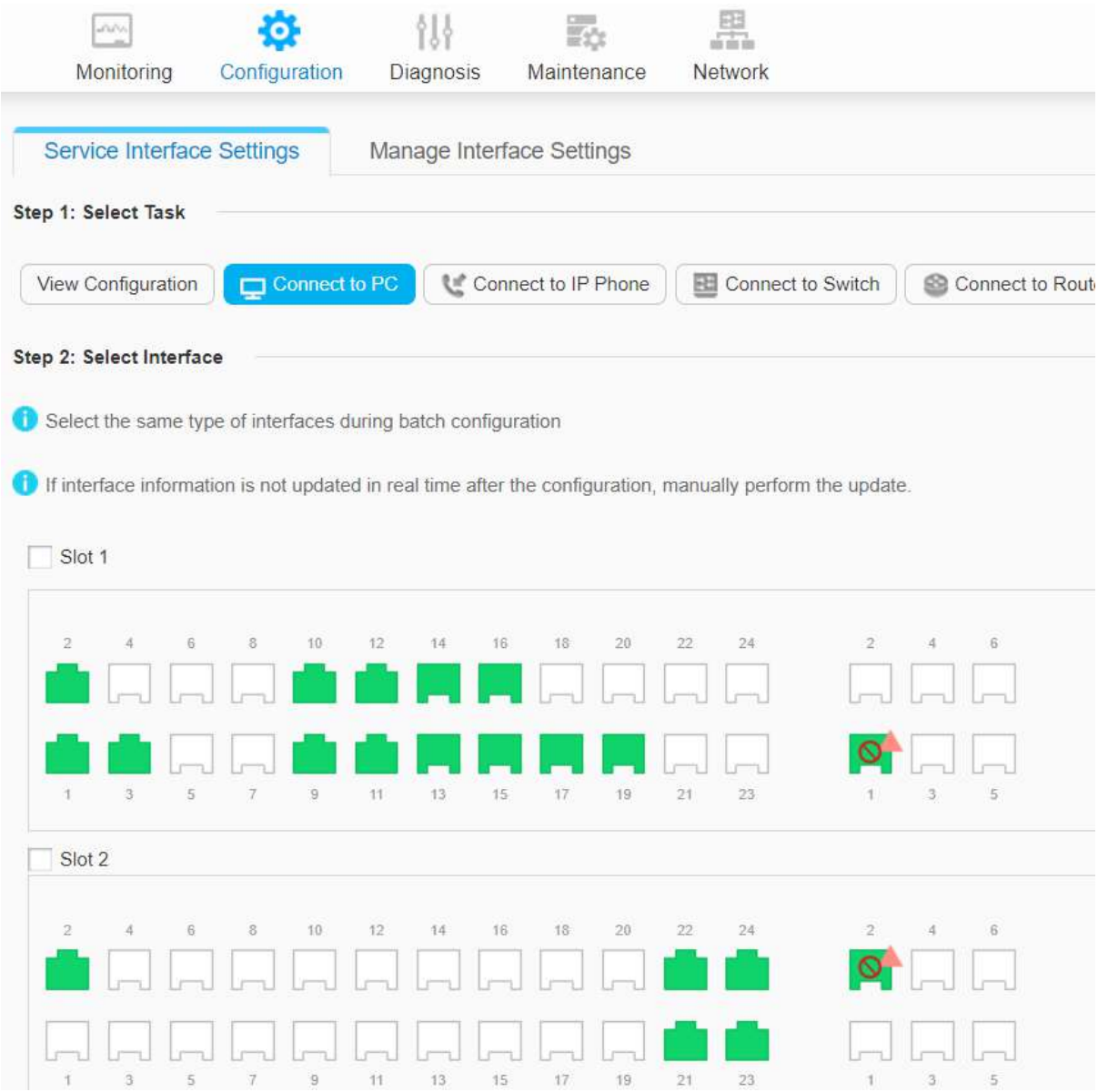

Figura 4.6: Puertos SFP reconocidos por el equipo.
Fuente: Autor.

Interface	Status	Transceiv...	Connector...	Center Wavele...	Transmission Dista...
XGigabitEthernet1/0/1	Normal	1000_BASE_T...	-	-	100(copper)
XGigabitEthernet1/0/2	Normal	1000_BASE_T...	-	-	100(copper)
XGigabitEthernet1/0/3	Normal	1000_BASE_T...	-	-	100(copper)
XGigabitEthernet1/0/9	Normal	1000_BASE_T...	-	-	100(copper)
XGigabitEthernet1/0/10	Normal	1000_BASE_T...	-	-	100(copper)
XGigabitEthernet1/0/11	Normal	1000_BASE_T...	-	-	100(copper)
XGigabitEthernet1/0/12	Normal	1000_BASE_T...	-	-	100(copper)
XGigabitEthernet1/0/13	Normal	1000_BASE_S...	LC	0	275(OM1),550(OM2),10...
XGigabitEthernet1/0/14	Normal	1000_BASE_S...	LC	0	275(OM1),550(OM2),10...
XGigabitEthernet1/0/15	Normal	1000_BASE_S...	LC	0	275(OM1),550(OM2),10...

10 Total record(s): 20

Figura 4.7: Parámetros de interfaces.
Fuente: Autor.

Configuración de VLAN's y DHCP

VLAN ID	VLAN Description	IPv4 Address/Mask
1	VLAN 0001	
2	VLAN2	192.168.2.254/255.255.255.0
3	VLAN3	
4	VLAN4	192.168.4.254/255.255.255.0
5	VLAN5-WAN	
30	VLAN30	192.168.30.254/255.255.255.0
31	VLAN31	192.168.31.254/255.255.255.0
32	VLAN32	192.168.32.254/255.255.255.0
33	VLAN33	192.168.33.254/255.255.255.0
34	VLAN34	192.168.34.254/255.255.255.0

Figura 4.8: Configuración de VLAN's parte 1.
Fuente: Autor.

VLAN ID	VLAN Description	IPv4 Address/Mask
35	VLAN35	192.168.35.254/255.255.255.0
36	VLAN36	192.168.36.254/255.255.255.0
37	VLAN37	192.168.37.254/255.255.255.0
38	VLAN38	192.168.38.254/255.255.255.0
39	VLAN39	192.168.39.254/255.255.255.0
40	VLAN40	192.168.40.254/255.255.255.0
41	VLAN41	192.168.41.254/255.255.255.0
42	LAB. FISICO-QUIMICA	192.168.42.254/255.255.255.0
43	LAB. BIOLOGIA	192.168.43.254/255.255.255.0
44	WLAN LAB. BIOLOGIA	192.168.44.254/255.255.255.0

Figura 4.9: Configuración de VLAN's parte 2.
Fuente: Autor.

Create Delete Batch Create Batch Delete Refresh

VLAN ID	VLAN Description	IPv4 Address/Mask
45	VLAN45	192.168.45.254/255.255.255.0
46	VLAN46	192.168.46.254/255.255.255.0
47	VLAN47	192.168.47.254/255.255.255.0
48	VLAN48	192.168.48.254/255.255.255.0
49	WIFI-PATIO	192.168.49.254/255.255.255.0
50	VLAN50	192.168.50.254/255.255.255.0
60	VLAN60	192.168.60.254/255.255.255.0
61	VLAN 0061	
62	VLAN 0062	
70	VLAN70	192.168.70.254/255.255.255.0

Figura 4.10: Configuración de VLAN's parte 3.
Fuente: Autor.

VLAN ID	VLAN Description	IPv4 Address/Mask
71	VLAN71-PRUEBAS	192.168.71.254/255.255.255.0
80	VLAN80	192.168.80.254/255.255.255.0
90	VLAN90	192.168.90.254/255.255.255.0
91	VLAN91	192.168.91.254/255.255.255.0
92	VLAN92	192.168.92.254/255.255.255.0
100	VLAN100	
101	VLAN101	192.168.101.254/255.255.255.0
102	VLAN102	192.168.102.254/255.255.255.0
103	VLAN103	192.168.103.254/255.255.255.0
104	VLAN104	

Figura 4.11: Configuración de VLAN's parte 4.
Fuente: Autor.

VLAN ID	VLAN Description	IPv4 Address/Mask
105	VLAN105	
106	VLAN106	
107	VLAN107	192.168.107.254/255.255.255.0
108	VLAN108	192.168.108.254/255.255.255.0
109	VLAN109	192.168.109.254/255.255.255.0
110	VLAN110	192.168.110.254/255.255.255.0
111	VLAN111	192.168.111.254/255.255.255.0
112	VLAN112	192.168.112.254/255.255.255.0
113	VLAN113	192.168.113.254/255.255.255.0
114	VLAN114	

Figura 4.12: Configuración de VLAN's parte 5.
Fuente: Autor.

VLAN ID	VLAN Description	IPv4 Address/Mask
115	VLAN115	192.168.115.254/255.255.255.0
116	VLAN116	192.168.116.254/255.255.255.0
117	VLAN117	192.168.117.254/255.255.255.0
118	VLAN118	192.168.118.254/255.255.255.0
130	VLAN130	192.168.130.254/255.255.255.0
150	VLAN150	192.168.150.254/255.255.255.0
200	VLAN200	192.168.200.254/255.255.255.0
230	VLAN230	192.168.230.254/255.255.255.0
237	VLAN237	192.168.237.254/255.255.255.0
240	VLAN240	192.168.240.254/255.255.255.0

Figura 4.13: Configuración de VLAN's parte 6.
Fuente: Autor.

VLAN ID	VLAN Description	IPv4 Address/Mask
242	VLAN242	192.168.242.254/255.255.255.0
243	VLAN243	192.168.243.254/255.255.255.0
253	VLAN253	192.168.253.254/255.255.255.0
254	VLAN254	192.168.254.254/255.255.255.0
300	VLAN300	192.168.1.210/255.255.255.248
310	VLAN310	192.168.223.254/255.255.252.0

Figura 4.14: Configuración de VLAN's parte 7.
Fuente: Autor.

Se configuró el tiempo de duración del DHCP para cada una de las VLANs asignadas, ajustando así la asignación de direcciones IP según las necesidades para cada sección de la red.

Address Pool Name	Subnet Address	Subnet Mask	Lease
vlanif108	192.168.108.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s
Vlanif91	192.168.91.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s
Vlanif71	192.168.71.0	255.255.255.0	0 Day(s) 1 Hour(s) 0 Minute(s
Vlanif30	192.168.30.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s
Vlanif31	192.168.31.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s
Vlanif32	192.168.32.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s
Vlanif33	192.168.33.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s
Vlanif34	192.168.34.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s
Vlanif35	192.168.35.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s
Vlanif36	192.168.36.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s

Figura 4.15: Configuración DHCP parte 1.
Fuente: Autor.

Address Pool Name	Subnet Address	Subnet Mask	Lease
Vlanif37	192.168.37.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)
Vlanif38	192.168.38.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)
Vlanif39	192.168.39.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)
Vlanif40	192.168.40.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)
Vlanif41	192.168.41.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)
Vlanif42	192.168.42.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)
Vlanif43	192.168.43.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)
Vlanif44	192.168.44.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)
Vlanif45	192.168.45.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)
Vlanif46	192.168.46.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)

Figura 4.16: Configuración DHCP parte 2.
Fuente: Autor.

Address Pool Name	Subnet Address	Subnet Mask	Lease
Vlanif47	192.168.47.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)
Vlanif48	192.168.48.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)
Vlanif49	192.168.49.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)
Vlanif50	192.168.50.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)
Vlanif60	192.168.60.0	255.255.255.0	0 Day(s) 8 Hour(s) 0 Minute(s)
Vlanif70	192.168.70.0	255.255.255.0	0 Day(s) 8 Hour(s) 0 Minute(s)
Vlanif80	192.168.80.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)
Vlanif90	192.168.90.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)
Vlanif101	192.168.101.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)
Vlanif102	192.168.102.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)

Figura 4.17: Configuración DHCP parte 3.
Fuente: Autor.

Address Pool Name	Subnet Address	Subnet Mask	Lease
Vlanif103	192.168.103.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)
Vlanif107	192.168.107.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)
Vlanif109	192.168.109.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)
Vlanif110	192.168.110.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)
Vlanif111	192.168.111.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)
Vlanif112	192.168.112.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)
Vlanif113	192.168.113.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)
Vlanif115	192.168.115.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)
Vlanif116	192.168.116.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)
Vlanif117	192.168.117.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)

Figura 4.18: Configuración DHCP parte 4.
Fuente: Autor.

Address Pool Name	Subnet Address	Subnet Mask	Lease
Vlanif118	192.168.118.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)
Vlanif130	192.168.130.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)
Vlanif150	192.168.150.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)
Vlanif200	192.168.200.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)
Vlanif237	192.168.237.0	255.255.255.0	0 Day(s) 8 Hour(s) 0 Minute(s)
Vlanif240	192.168.240.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)
Vlanif242	192.168.242.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)
Vlanif243	192.168.243.0	255.255.255.0	1 Day(s) 0 Hour(s) 0 Minute(s)
Vlanif310	192.168.220.0	255.255.252.0	1 Day(s) 0 Hour(s) 0 Minute(s)

Figura 4.19: Configuración DHCP parte 5.
Fuente: Autor.

Instalación de Switch de Core

Con la configuración del switch de core, se realizó su instalación en el centro de datos. Esta fase incluyó la integración del switch con la infraestructura existente (figura 4.20). Seguido a eso se conectaron los enlaces de fibra óptica que no estaban en uso (figura 4.21). Esta incorporación de enlaces permitió ampliar la capacidad de la red, mejorar la tasa de transmisión de datos y fortalecer la redundancia y fiabilidad del sistema. La conexión de estos enlaces optimizó la conectividad entre las diferentes zonas del campus Yanuncay, promoviendo que la comunicación sea fluida y eficiente entre los diversos dispositivos y sistemas. Este proceso no solo mejoró el rendimiento general, sino que también preparó la infraestructura para soportar futuras expansiones y demandas crecientes.

Figura 4.20: Instalación de Switch de Core.
Fuente: Autor.

Figura 4.21: Conexión de enlaces de Fibra Óptica.
Fuente: Autor.

4.1.2. Implementación de Firewall

Para la implementación del Firewall SonicWall NSA 4600, seguimos el esquema presentado en la figura 4.1 . Después de revisar y ajustar el diseño según las necesidades específicas de nuestra red, procedimos con la configuración del dispositivo. Este enfoque sistemático garantizó que el firewall se integrara de manera eficiente en nuestra infraestructura y cumpliera con los requisitos de seguridad establecidos.

Configuración de VPN's

Se configuraron las VPNs de los diferentes campus de la UETS (figura 4.22), permitiendo la interconexión segura y eficiente entre las redes locales de cada ubicación. Esta configuración facilitó la comunicación y el acceso a recursos comunes mediante una red privada virtual, garantizando que todos los campus estuvieran integrados de manera segura y operativa.

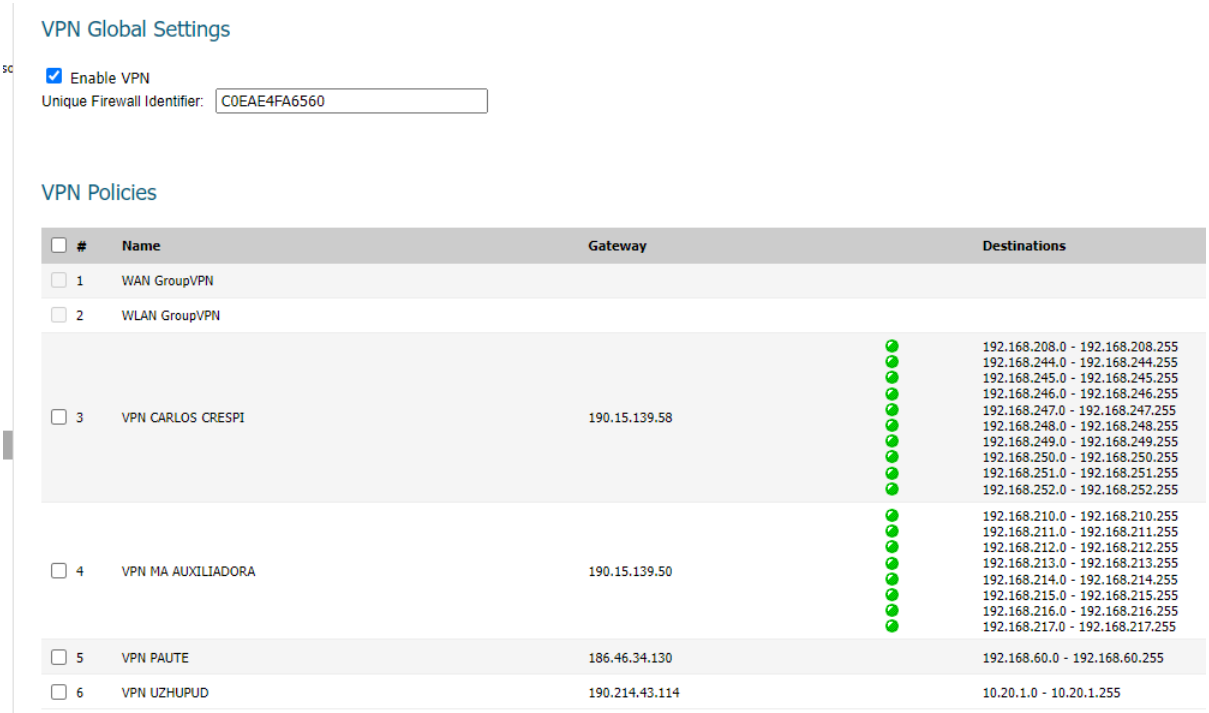

Figura 4.22: Configuración de VPN's UETS.
Fuente: Autor.

Configuración de reglas de acceso

Se configuraron las reglas de acceso para el firewall con el objetivo de controlar y gestionar de mejor manera el tráfico que circula en la red educativa. Estas reglas fueron diseñadas no solo para permitir o bloquear el tráfico según direcciones IP, puertos y protocolos específicos, sino también para restringir el acceso a páginas web prohibidas, protegiendo así a los alumnos de contenidos inapropiados. Además, se implementaron políticas de seguridad para prevenir accesos no autorizados, amenazas externas y optimizar el desempeño general del sistema.

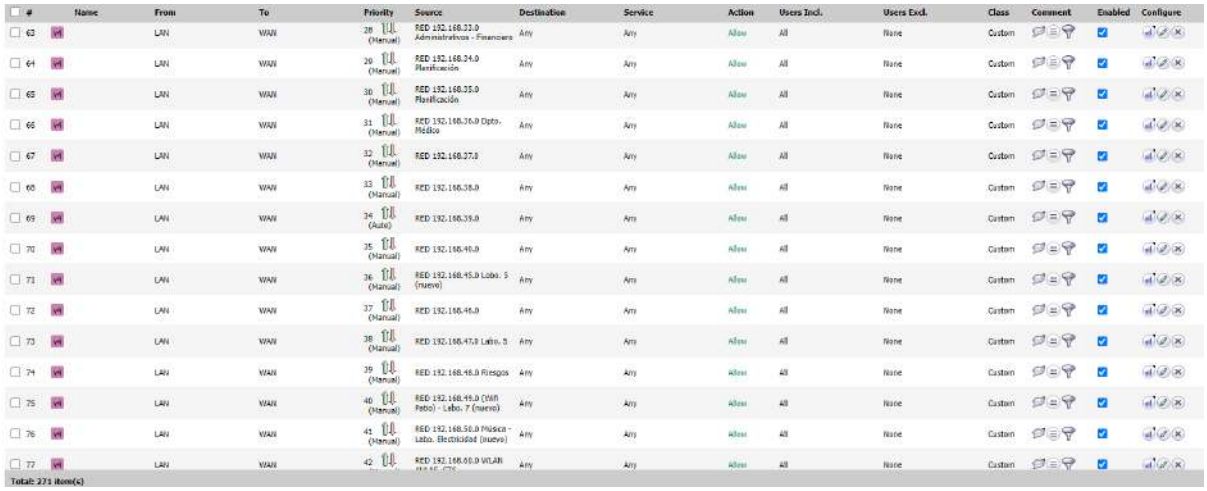

Figura 4.23: Configuración general de reglas de acceso.
Fuente: Autor.

Figura 4.24: Configuración de políticas de seguridad.
Fuente: Autor.

#	Nombre	Lista de URL permitidas	Lista de URL prohibidas	Categorías de bloques	Categorías de frases de cont...	Confirmar categorías	Categorías de BMW	Categorías Permitidas
1	CAPACITACIÓN CFS	URL PERMITIDAS GENERALES	Lista de Bloqueadas	4. Pornografía 28. Sistemas de prevención de piratería y proxy 50. Pago por navegar en sitios 59. Malware				1. Violencia/Odio/Racismo 2. Ropa íntima/Traje de baño 3. Nudismo 5. Armas ...
2	Perfil predeterminado de CFS	URL PERMITIDAS GENERALES	Ninguno	1. Violencia/Odio/Racismo 2. Ropa íntima/Traje de baño 3. Nudismo 4. Pornografía ...				13. Chat/Mensajería instantánea (MI) 14. Arte/Entretenimiento 15. Negocios y economía 17. Educación ...
3	CFS DEFECTO POLÍTICO	URL PERMITIDAS GENERALES	Lista de Bloqueadas	1. Violencia/Odio/Racismo 2. Ropa íntima/Traje de baño 3. Nudismo 4. Pornografía ...				13. Chat/Mensajería instantánea (MI) 14. Arte/Entretenimiento 15. Negocios y economía 17. Educación ...
4	LABORATORIOS CFS	Ninguno	URL BLOQUEADAS LABORATORIOS	1. Violencia/Odio/Racismo 2. Ropa íntima/Traje de baño 3. Nudismo 4. Pornografía ...				13. Chat/Mensajería instantánea (MI) 14. Arte/Entretenimiento 15. Negocios y economía 16. Aborto/Grupos de defensa ...
5	LABORATORIOS CTS CFS	URL PERMITIDAS GENERALES	Ninguno	1. Violencia/Odio/Racismo 2. Ropa íntima/Traje de baño 3. Nudismo 4. Pornografía ...				14. Arte/Entretenimiento 15. Negocios y Economía 16. Aborto/Grupos de Defensa 17. Educación ...
6	PRUEBAS POLÍTICAS DEL CFS	Ninguno	Ninguno	2. Ropa íntima/trajes de baño 3. Nudismo 4. Pornografía 6. Contenido para adultos/maduros ...				1. Violencia/Odio/Racismo 5. Armas 7. Culto/Ocultismo 9. Habilidades ilegales/Habilidades cuestionables ...

Figura 4.25: Configuración de filtro de contenido parte 1.
Fuente: Autor.

#	Nombre	Lista de URL permitidas	Lista de URL prohibidas	Categorías de bloques	Categorías de frases de cont...	Confirmar categorías	Categorías de BMW	Categorías Permitidas
				...				...
5	LABORATORIOS CTS CFS	URL PERMITIDAS GENERALES	Ninguno	1. Violencia/Odio/Racismo 2. Ropa íntima/Traje de baño 3. Nudismo 4. Pornografía ...				14. Artes/Entretenimiento 15. Negocios y Economía 16. Aborto/Grupos de Defensa 17. Educación ...
6	PRUEBAS POLÍTICAS DEL CFS	Ninguno	Ninguno	2. Ropa íntima/trajes de baño 3. Nudismo 4. Pornografía 6. Contenido para adultos/maduros ...				1. Violencia/Odio/Racismo 5. Armas 7. Culto/Ocultismo 9. Habilidades ilegales/Habilidades cuestionables ...
7	CFS PRUEBAS BLOQUEO	Ninguno	Ninguno	1. Violencia/Odio/Racismo 2. Ropa íntima/Traje de baño 3. Nudismo 4. Pornografía ...				13. Chat/Mensajería instantánea (MI) 14. Artes/Entretenimiento 15. Negocios y economía 16. Aborto/Grupos de defensa ...
8	SFC restringido	URL PERMITIDAS GENERALES	Lista de Bloqueadas	1. Violencia/Odio/Racismo 2. Ropa íntima/Traje de baño 3. Nudismo 4. Pornografía ...				17. Educación 31. Comunicaciones web 58. Redes sociales
9	VIP del SFC	URL PERMITIDAS GENERALES	Ninguno	1. Violencia/Odio/Racismo 2. Ropa íntima/Traje de baño 3. Nudismo 4. Pornografía ...				13. Chat/Mensajería instantánea (MI) 14. Artes/Entretenimiento 15. Negocios y economía 16. Aborto/Grupos de defensa ...
10	CFS VIP SIN REDES SOCIALES	URL PERMITIDAS GENERALES	Lista de Bloqueadas	1. Violencia/Odio/Racismo 2. Ropa íntima/Traje de baño 3. Nudismo 4. Pornografía ...				14. Artes/Entretenimiento 15. Negocios y Economía 16. Aborto/Grupos de Defensa 17. Educación ...

Figura 4.26: Configuración de filtro de contenido parte 2.
Fuente: Autor.

Configuración de ancho de banda

Dentro de las reglas de acceso del firewall (Figura 4.23), se configuró el ancho de banda para las diferentes redes del campus, asignando prioridades específicas según las necesidades de cada área. Se dio mayor prioridad a las oficinas administrativas, las cabinas de comunicación, la comunidad salesiana y los laboratorios de computación. Esta configuración aseguró que las áreas críticas para el funcionamiento y la administración del campus contaran con suficiente ancho de banda para operar de manera eficiente, mientras se gestionaron de manera adecuada los recursos

disponibles para otras redes dentro del campus.

Figura 4.27: Configuración de ancho de banda.
Fuente: Autor.

Gracias a la actualización del contrato con CEDIA, el campus dispuso de una conexión de 500 megas en lugar de 200 megas. Esta mejora permitió reasignar el ancho de banda de forma ideal entre las diferentes redes del campus.

Tabla 4.1: Asignación de anchos de banda.

Fuente: Autor.

Área	**Prioridad**	**Ancho de Banda Asignado**
Oficinas Administrativas	1	200Mbps
Comunidad Salesiana	2	100Mbps
Cabinas de Comunicación	3	80Mbps
Laboratorios de Computación	4	60Mbps
Aulas	5	40Mbps
Sala de Profesores	6	20Mbps

Los anchos de banda fueron configurados para funcionar de manera óptima durante el horario laboral, asignando prioridad a las oficinas administrativas, la

comunidad salesiana, las cabinas de comunicación, los laboratorios de computación, las aulas y la sala de profesores, de acuerdo con su importancia. Fuera del horario laboral, 400 megas serán destinados a la comunidad salesiana, mientras que el restante se asignará al resto de la red para asegurar una distribución eficiente y equitativa de los recursos

Instalación de Firewall

Luego de realizar las configuraciones del firewall, se procedió a instalar el equipo en el rack del centro de datos (figura 4.28). Esta instalación permitió integrar el firewall de manera efectiva en la infraestructura de red, garantizando un funcionamiento adecuado para la protección de red del campus.

Figura 4.28: Instalación de firewall.
Fuente: Autor.

Se creó una VLAN específica en el switch de core para administrar el enlace entre los CPE del proveedor y el firewall. Esta VLAN, identificada como VLAN 5, fue configurada para garantizar una conexión eficiente y segura entre los dispositivos del proveedor y el sistema de firewall, optimizando el manejo del tráfico e integridad de la red.

4.2. Implementación de Switch de Acceso

Se realizó la actualización y configuración de los switches de acceso que se encontraban en mal estado en la red del campus Yanuncay. Para este proceso, se

utilizaron los switches utilizados (3.29), los cuales demostraron ser una excelente opción debido a su compatibilidad con la infraestructura existente y su capacidad para manejar las demandas de la red educativa. Esta mejora garantizó un rendimiento óptimo y una mayor fiabilidad en las conexiones, beneficiando a todos los usuarios del campus Yanuncay.

Asignación de IP estática

A cada switch de acceso se le asignó una IP estática para asegurar una administración eficiente y preciso de los dispositivos conectados.

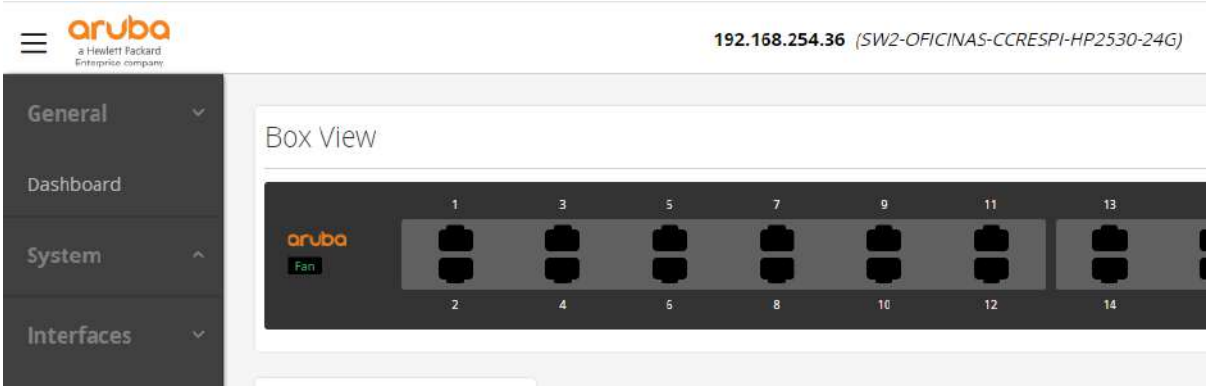

Figura 4.29: Configuración de IP estática en Switch de acceso.
Fuente: Autor.

Configuración de puertos de Switch de Acceso

Se realizó la configuración de puertos del switch asignando las VLAN's correspondientes a cada uno de los puertos. Esta configuración se llevó a cabo de manera detallada para garantizar que cada puerto esté correctamente asociado a la VLAN específica que requiere, asegurando así una segmentación adecuada y un funcionamiento óptimo de la red.

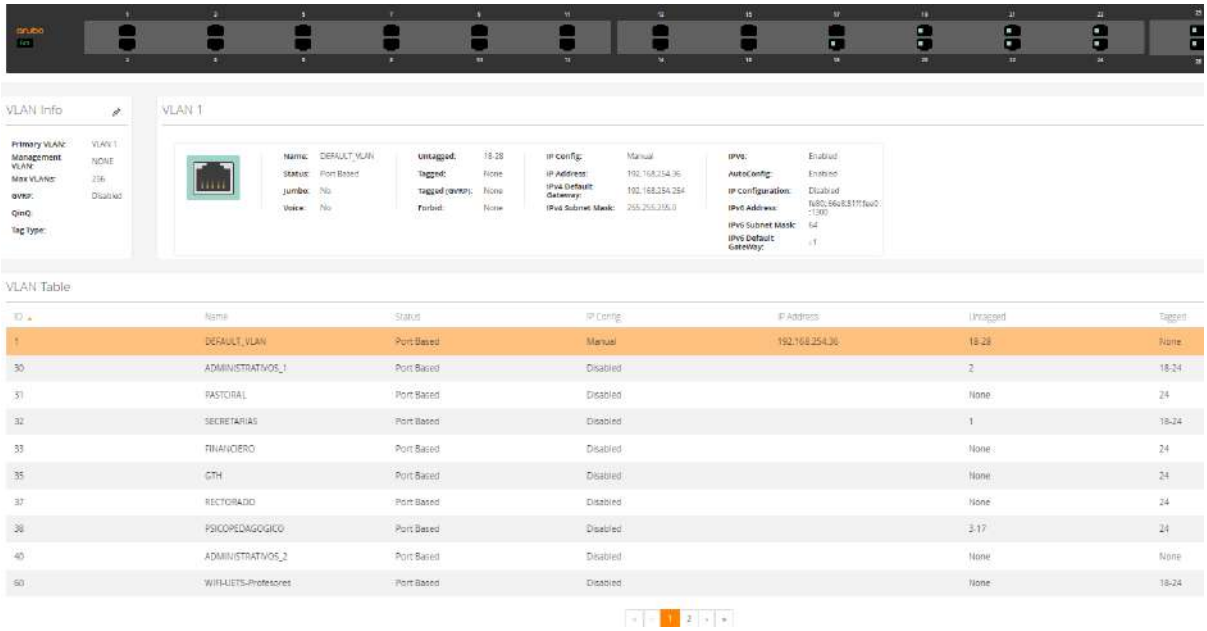

Figura 4.30: Configuración de puertos en Switch de Acceso.
Fuente: Autor.

Instalación de Switch de Acceso

Todos los switches de acceso Aruba que necesitaban ser actualizados fueron instalados en sus respectivos gabinetes, con la finalidad de garantizar una mayor eficiencia y capacidad en nuestra red educativa, proporcionando a los usuarios una experiencia más robusta y confiable. Además, se aseguró que todos los equipos se integraran de forma correcta con la infraestructura existente, lo que permitió una transición sin problemas y avance sustancial en el rendimiento general de la red.

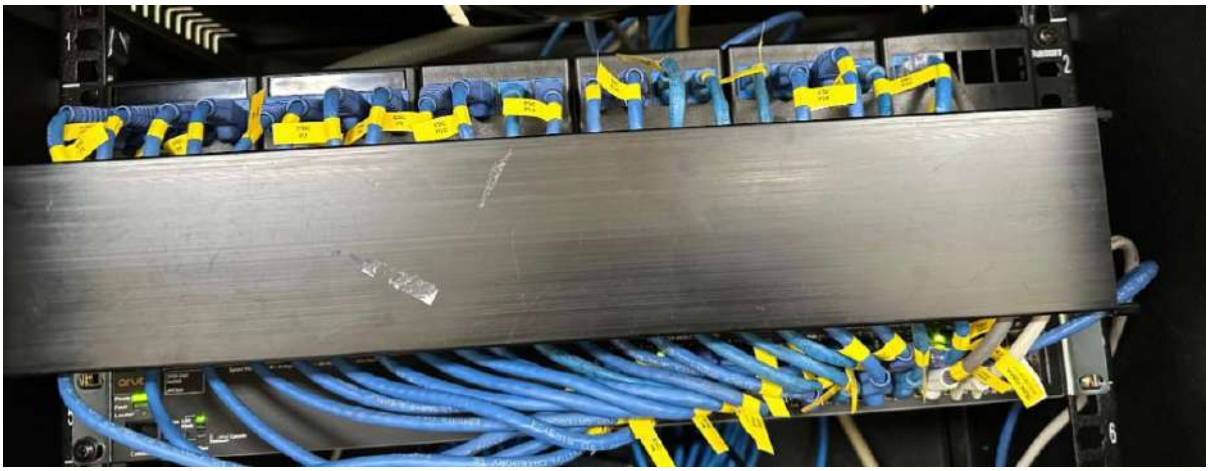

Figura 4.31: Instalación de Switch de Acceso.
Fuente: Autor.

4.3. Implementación de Access Point

En el campus Yanuncay, se llevó a cabo una actualización completa de los AP que se encontraban en mal estado. Además, se implementaron nuevos AP para garantizar una cobertura y rendimiento óptimos en toda la infraestructura.

4.3.1. Agregación de dispositivo a portal

Cada nuevo dispositivo fue registrado, incluyendo el identificador de serie y la dirección MAC, y agregado al portal Aruba Central para una gestión centralizada y eficiente.

Figura 4.32: Registro de credenciales de dispositivos en Aruba central.
Fuente: Autor.

4.3.2. Configuración de asignación por zonas

Se asignaron las zonas correspondientes en el portal Aruba Central para cada punto de acceso (AP) que se configuró. Esta asignación garantizó una gestión precisa y eficiente de la red, permitiendo una supervisión y control más detallado de cada AP en sus respectivas ubicaciones. Esta organización optimizó el rendimiento de la red y aseguró una cobertura uniforme en todo el campus.

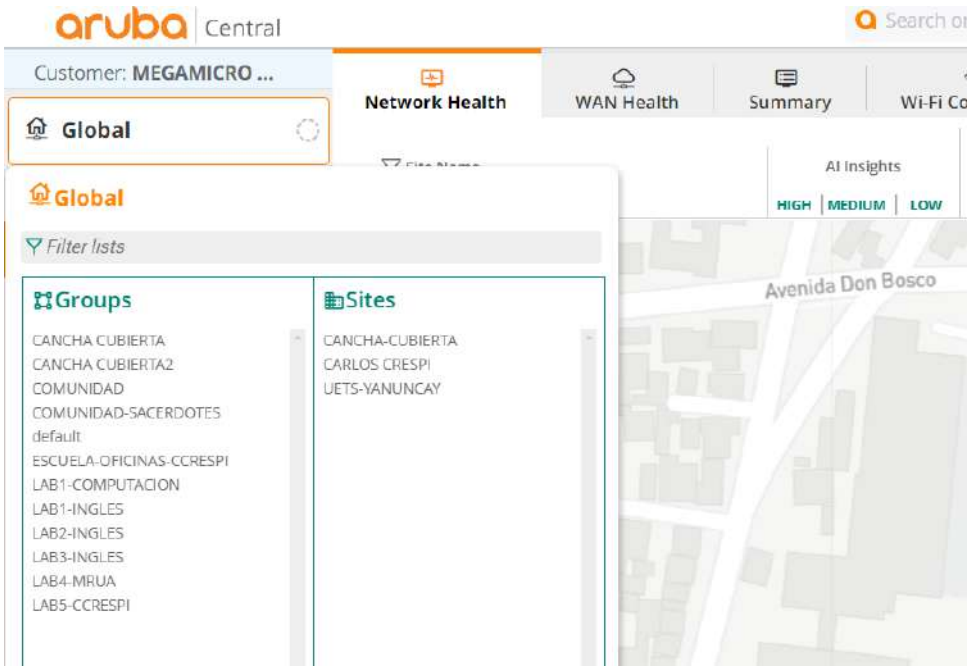

Figura 4.33: Asignación de zonas de funcionamiento de AP.
Fuente: Autor.

4.3.3. Configuración final de AP

Se configuró la licencia de funcionamiento y la dirección IP de los AP en el portal Aruba Central. Esta tarea incluyó la asignación de las licencias correspondientes para asegurar la operación óptima de cada dispositivo y la configuración precisa de las direcciones IP para asegurar su integración efectiva en la red existente. La gestión a través de Aruba Central permitió un control centralizado, facilitando la supervisión en tiempo real, la actualización remota del firmware y la resolución de problemas de manera eficiente. Esta implementación mejoró la estabilidad de la red y proporcionó una plataforma unificada para el monitoreo y mantenimiento de todos los puntos de acceso.

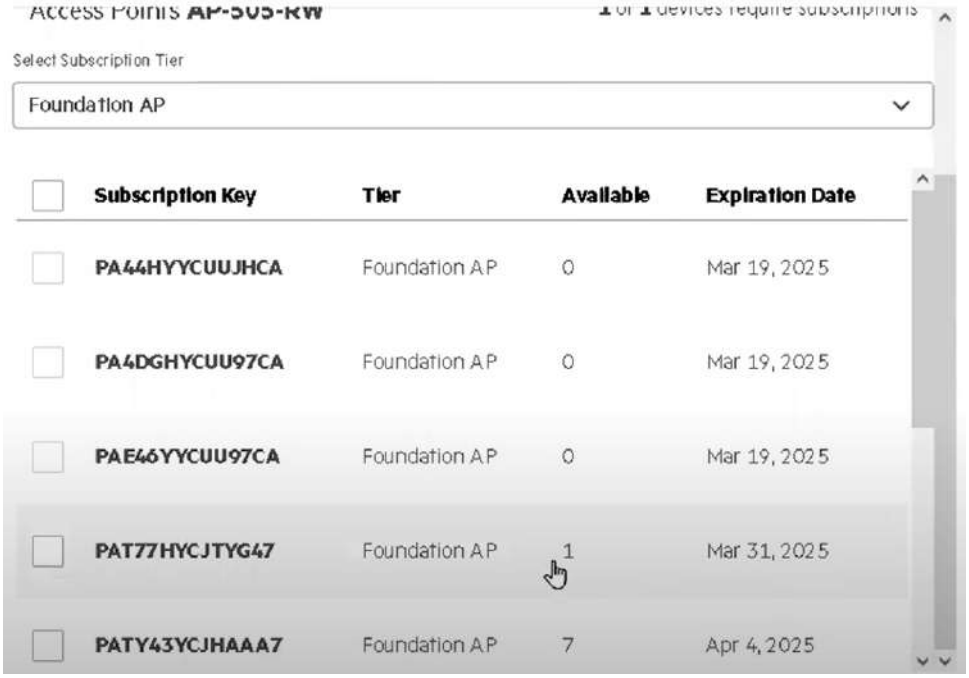

Figura 4.34: Asignación de licencia de operación.
Fuente: Autor.

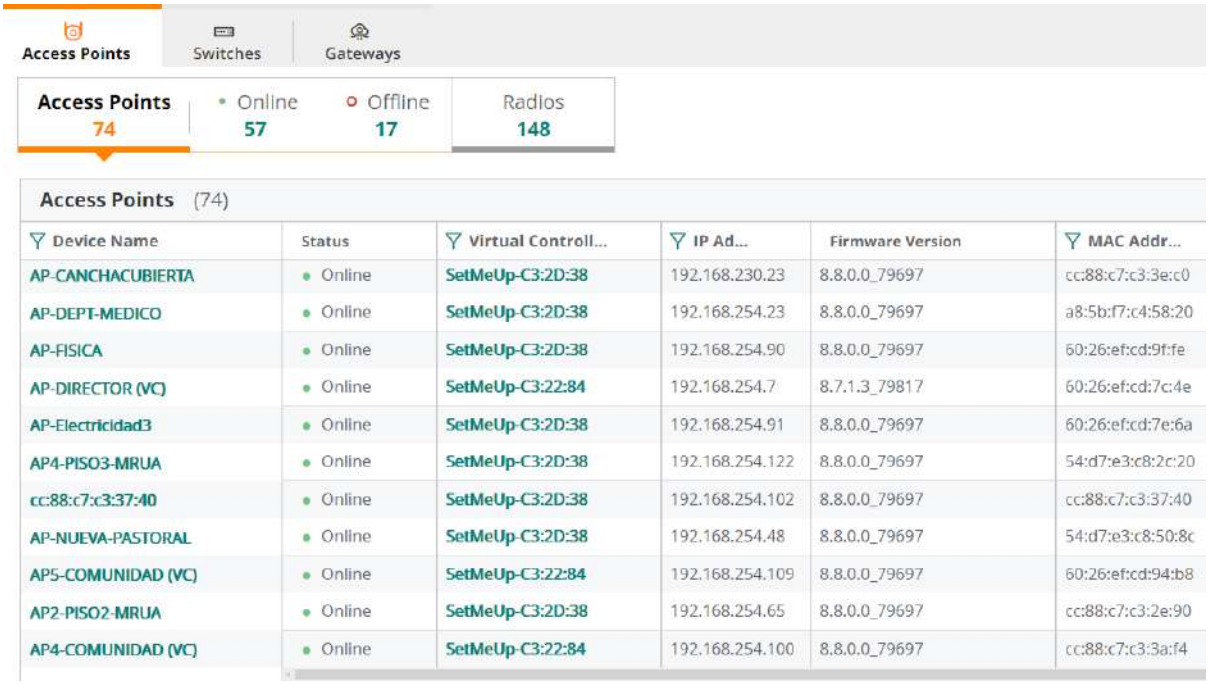

Figura 4.35: Configuración IP de AP.
Fuente: Autor.

Figura 4.36: Instalación de AP.
Fuente: Autor.

4.4. Implementación de SAI

Se implementó un sistema SAI para proteger los equipos activos de red del data center y asegurar su funcionamiento continuo. Además, se instaló un banco de baterías de 48V necesario para alimentar el SAI, proporcionando 2 horas de servicio eléctrico cada que suceda corte de energía. Para la instalación, se siguió un esquema planificado que garantizó la correcta implementación y funcionamiento del sistema. El equipo suministrará 110V a los equipos principales, que son los CPE, switch de core y firewall.

Figura 4.37: Esquema eléctrico de alta disponibilidad.
Fuente: Autor.

4.4.1. Instalación de SAI

Características de Equipo UPS

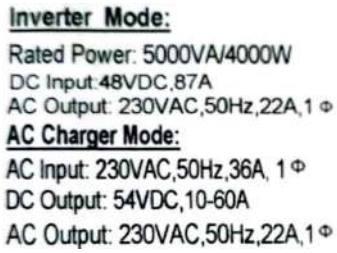

Figura 4.38: Características de equipo MPS 5kva.
Fuente: [52].

Instalación de banco de baterías para SAI

Se instalaron 4 baterías de 12V en serie para obtener los 48 voltios necesarios para alimentar el equipo UPS del sistema SAI. Este arreglo asegura una alimentación continua y estable, protegiendo así los equipos activos de red del data center frente a posibles interrupciones en el suministro eléctrico.

Figura 4.39: Instalación de banco de baterías de 48V.
Fuente: Autor.

Instalación de UPS del sistema SAI

Figura 4.40: Instalación de Equipo MPS 5kva.
Fuente: Autor.

Capítulo 5

Análisis de Resultados

En este capítulo se dio a conocer los resultados obtenidos del proyecto de actualización de los equipos activos de red en el campus Yanuncay de la UETS. La actualización logró mejoras significativas en varias áreas clave: se optimizó la cobertura de la red inalámbrica, proporcionando una señal más estable y uniforme para todo el campus; el ancho de banda disponible aumentó, garantizando velocidades de conexión aun mas rápidas y una mayor eficiencia en el uso de la red; y se implementaron nuevas herramientas y técnicas para una gestión más eficaz de la red, mejorando la administración y supervisión de los equipos y el tráfico de datos.

5.1. Áreas de cobertura WiFi por APs

Para poder entender las gráficas de simulación y pruebas en el entorno real, se han tomado en cuenta las zonas seccionadas que se detallan en la tabla 3.2 para la UETS. Al analizar estas gráficas, se analiza el desempeño para las distintas secciones bajo condiciones simuladas y compararlas con los resultados obtenidos en pruebas reales. Esto nos permite identificar posibles discrepancias y ajustar los parámetros de simulación para obtener una representación más fiel de la realidad.

5.1.1. Resultados obtenidos en Zona A1

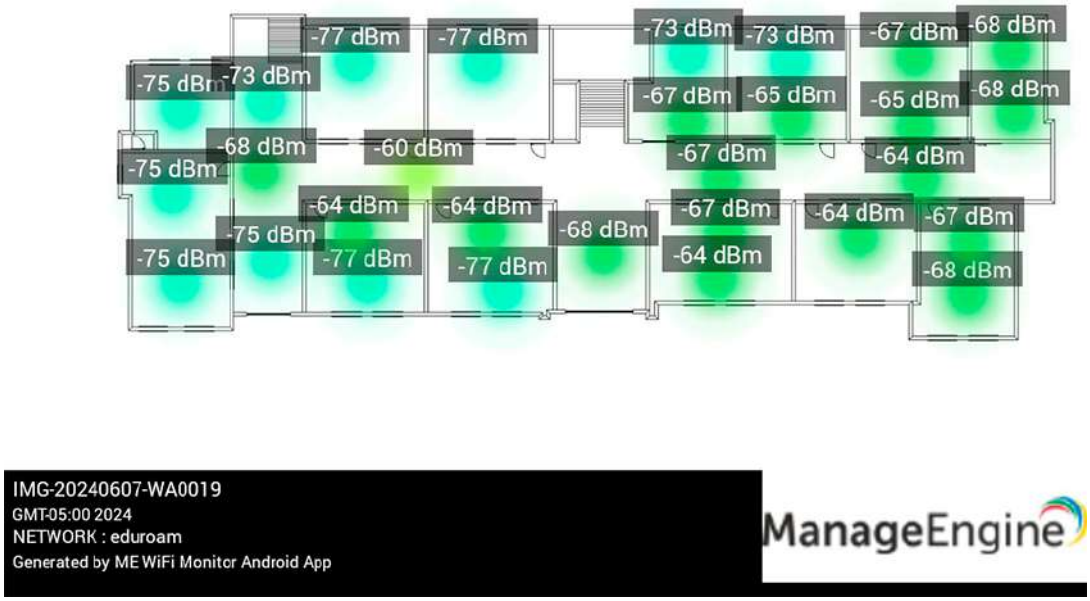

Figura 5.1: Mediciones de cobertura previo a la actualización en A1.
Fuente: Autor.

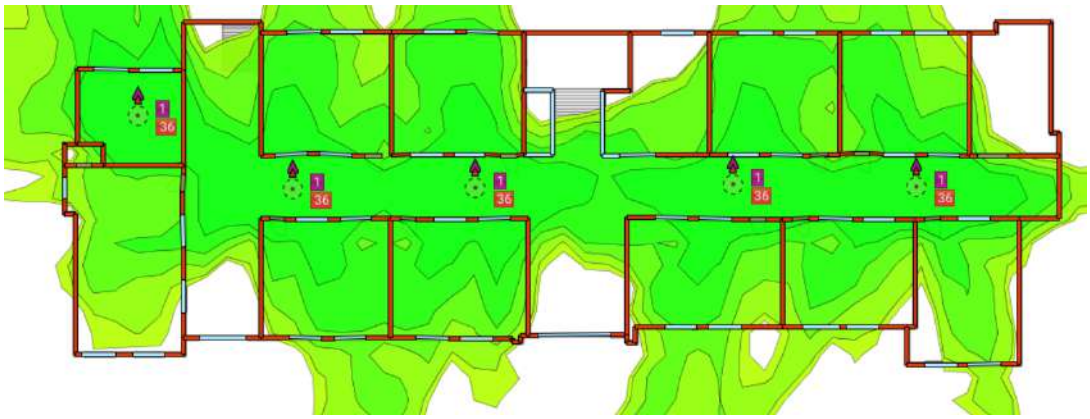

Figura 5.2: Simulación del área de cobertura en A1.
Fuente: Autor.

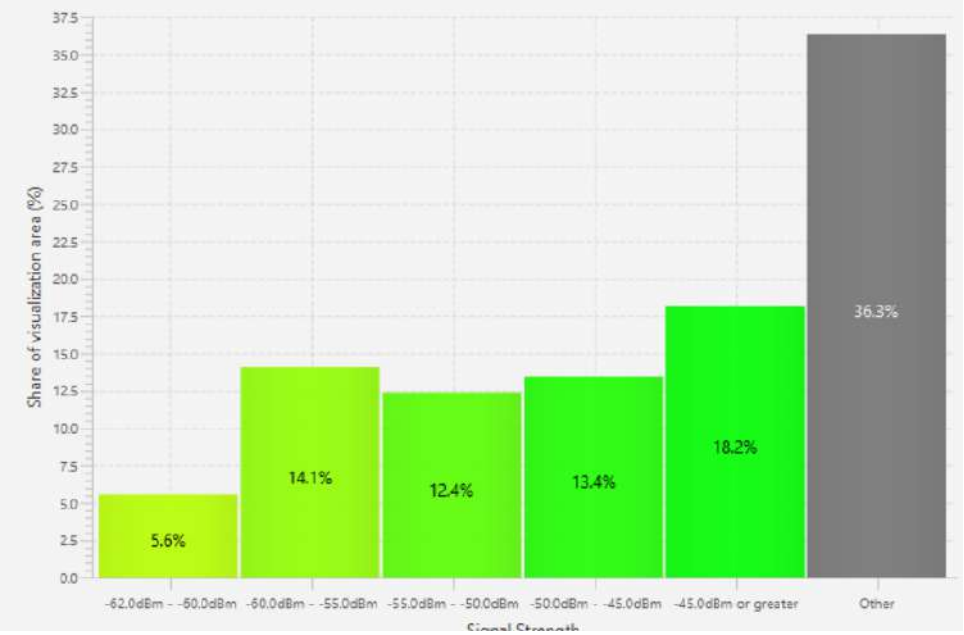

Figura 5.3: Simulación porcentual de área de cobertura en A1.
Fuente: Autor.

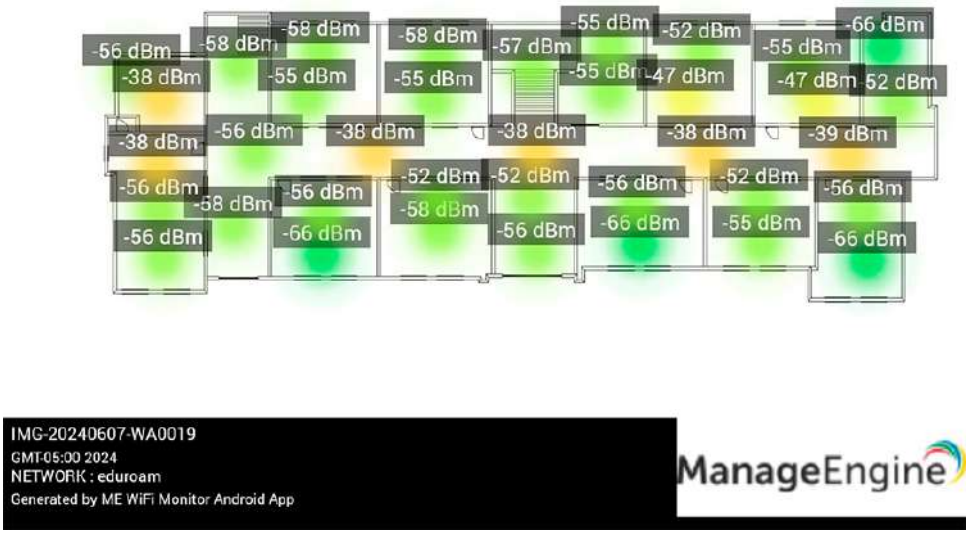

Figura 5.4: Resultado actual WiFi Analyzer en A1.
Fuente: Autor.

En la primera figura 5.1 se denota la falta de cobertura en la zona, ya que anteriormente solo existían tres puntos de acceso (APs) para abastecer la señal. Esto resulta en que los puntos de sensibilidad sean bajos y, por ende, cuando un dispositivo se conectara a la red tenga conexión inestable por estar dentro de zonas con cobertura de señal baja

En la Figura 5.2 se refleja los valores porcentuales de simulación de las zonas

de cobertura junto con su respectivo plano real, donde se observa que la cobertura de la red está casi cubierta usando 5 APs. Esta gráfica nos permite ver, a manera de simulación, que se ha cubierto la totalidad de las aulas y oficinas de los colaboradores. En la Figura 5.3 se muestra el porcentaje de cobertura en relación con los niveles de sensibilidad. Esta información indica que, si se está cerca del punto de acceso más cercano, se alcanzaría el 58 % de toda el área de cobertura, asegurando una calidad de señal buena, que se encuentra entre los -45 a -60 dBm de sensibilidad. En la Figura 5.4 se observa el estado actual y real de la cobertura de la zona. En este caso, se aprecia que todo el interior cuenta con un área de cobertura óptima, lo cual permite navegar sin problema alguno.

5.1.2. Resultados obtenidos en Zona A2

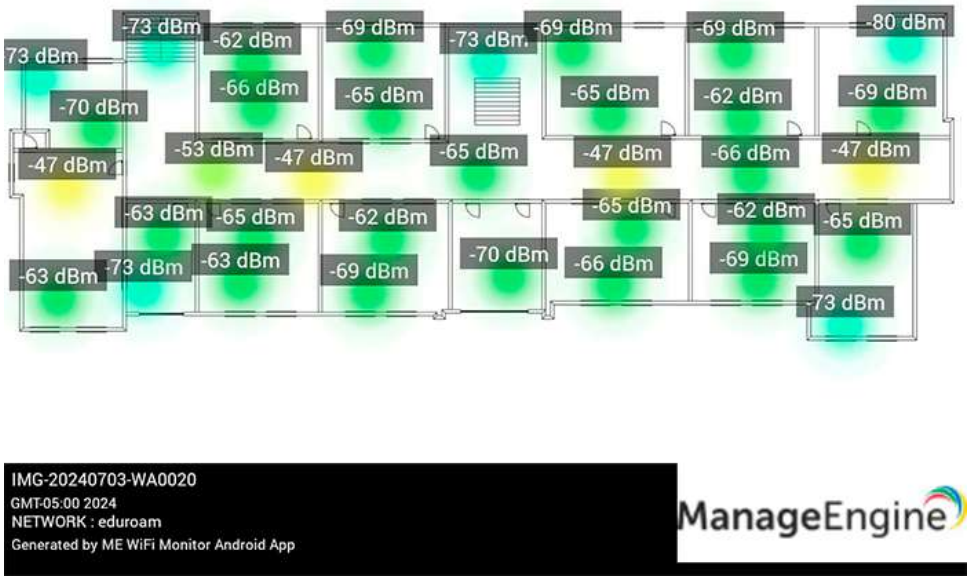

Figura 5.5: Mediciones de cobertura previo a la actualización en A2.
Fuente: Autor.

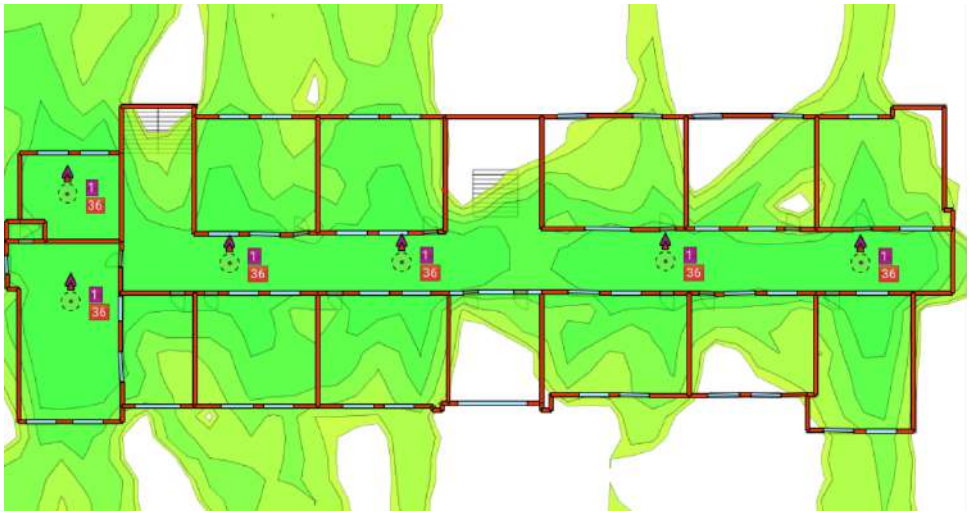

Figura 5.6: Simulación del área de cobertura en A2.
Fuente: Autor.

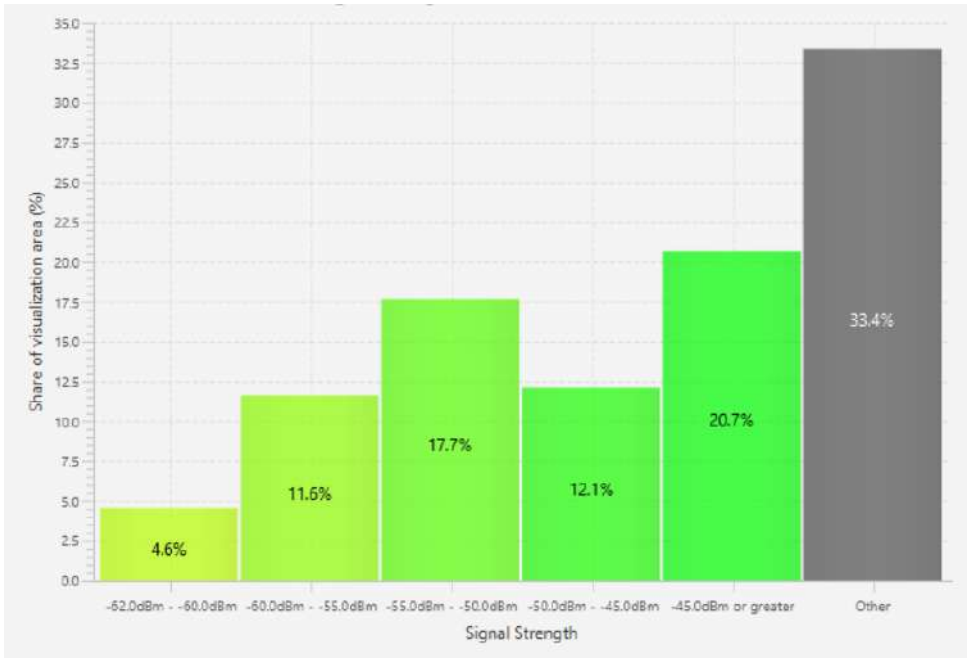

Figura 5.7: Simulación porcentual de área de cobertura en A2.
Fuente: Autor.

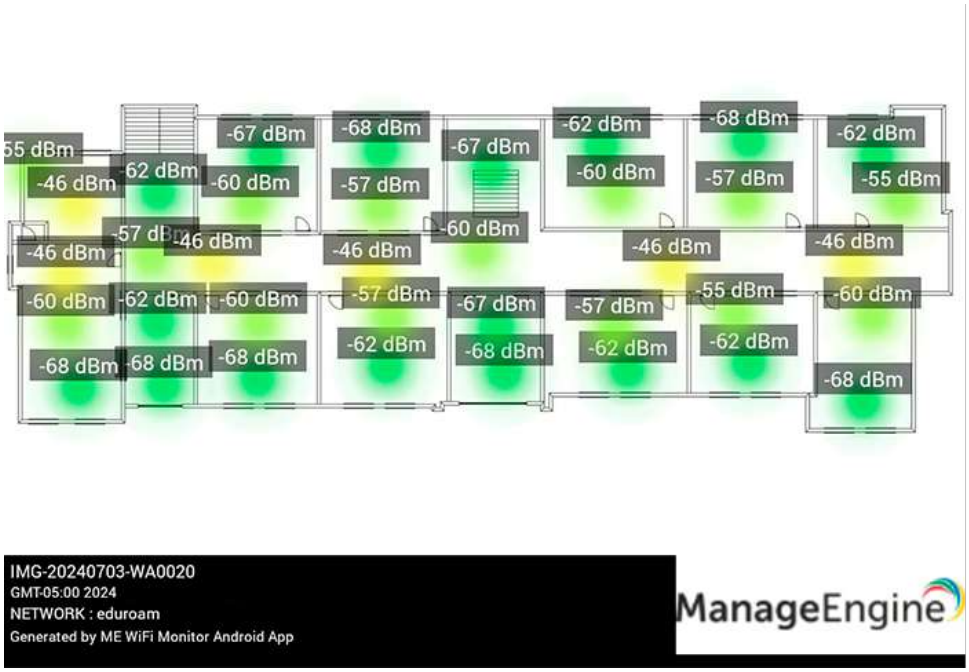

Figura 5.8: Resultado actual WiFi Analyzer en A2.
Fuente: Autor.

En la Figura 5.5 se muestra la cobertura de la señal cuando había cuatro puntos de acceso (APs) funcionando, que era como estaba la zona antes. Por ello, se observa que hay áreas con sensibilidad menor a cero, lo que causa que la conexión sea inestable y las velocidades puedan ser bajas.

Como se ve en la Figura 5.6, se muestran las zonas de cobertura a manera de simulación de la zona A2, donde se puede observar que esta zona cubre en su totalidad todas las aulas, laboratorios y oficinas con 6 APs instalados. Permitiendo un uso eficaz de la conectividad a internet. En la figura 5.7, se observa que alrededor del 62 % del área de cobertura garantiza un buen uso de internet, con una sensibilidad entre -45 a -60 dBm. El resto del área tendría una calidad de señal algo inferior en comparación con la zona más cercana al AP. En la Figura 5.8 se observa el estado actual y real de la cobertura de la zona. En este caso, se aprecia que todo el interior cuenta con un área de cobertura óptima, lo cual permite navegar sin problema alguno.

5.1.3. Resultados obtenidos en Zona A3

Figura 5.9: Mediciones de cobertura previo a la actualización en A3.
Fuente: Autor.

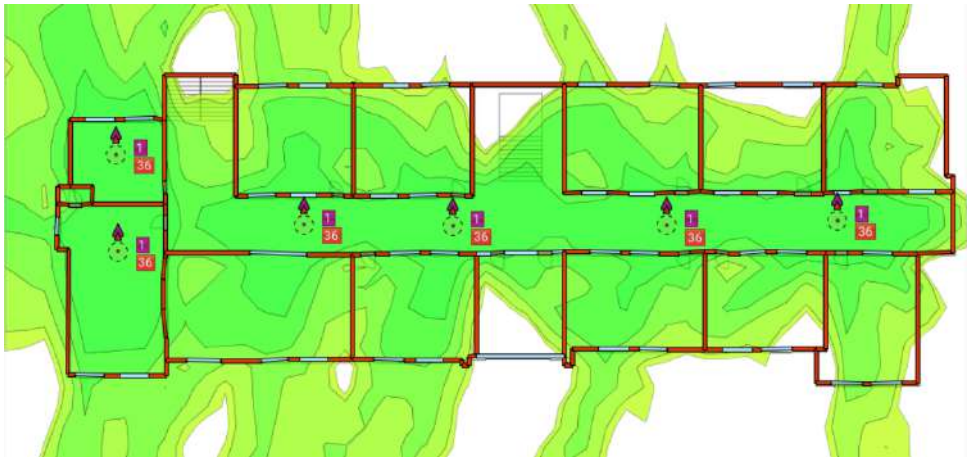

Figura 5.10: Simulación del área de cobertura en A3.
Fuente: Autor.

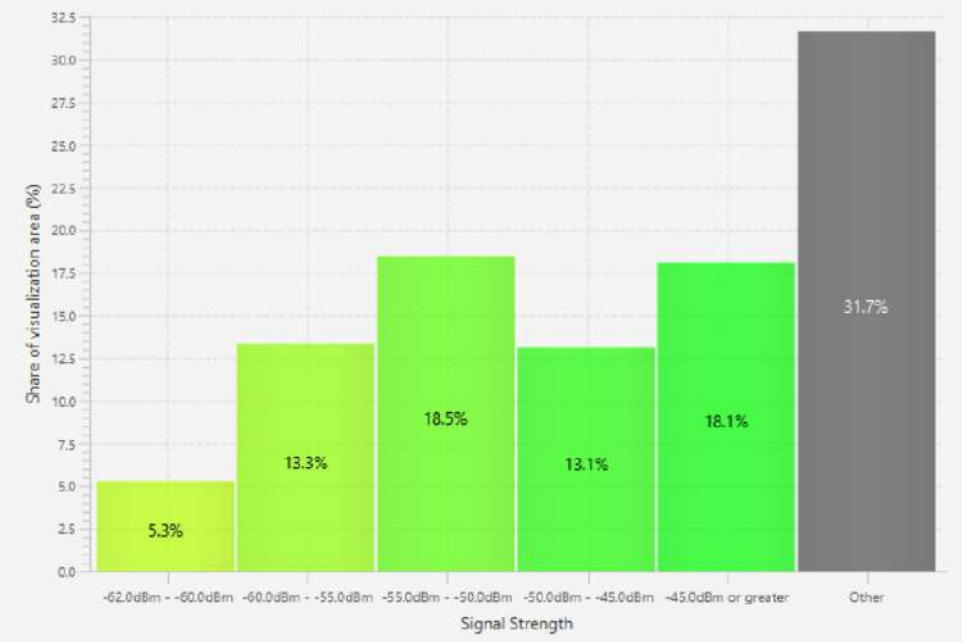

Figura 5.11: Simulación porcentual de área de cobertura en A3.
Fuente: Autor.

Figura 5.12: Resultado actual WiFi Analyzer en A3.
Fuente: Autor.

En la primera Figura 5.9 de la zona se observa que algunos rincones del plano tienen niveles de sensibilidad menores a cero. Esto se debe a que anteriormente solo estaban habilitados cuatro puntos de acceso (APs), lo que causaba una deficiencia de

velocidad y una conexión inestable cuando los dispositivos se conectaban a la red. En la Figura 5.10 se ve las zonas de cobertura de la zona, donde se observa que todas las aulas y oficinas del personal administrativo cuenta con cobertura de la red para poder realizar actividades con uso del servicio a internet con la implementación de 6 APs. En la Figura 5.11 se muestra que el 63 % contaría con calidad de servicio dentro de un rango entre -45 a -60 dBm de sensibilidad para tener conectividad confiable. En la Figura 5.12 se observa el estado actual y real de la cobertura de la zona. En este caso, se aprecia que todo el interior cuenta con un área de cobertura óptima, lo cual permite navegar sin problema alguno.

5.1.4. Resultados obtenidos en Zona A4

Figura 5.13: Mediciones de cobertura previo a la actualización en A4.
Fuente: Autor.

Figura 5.14: Simulación del área de cobertura en A4.
Fuente: Autor.

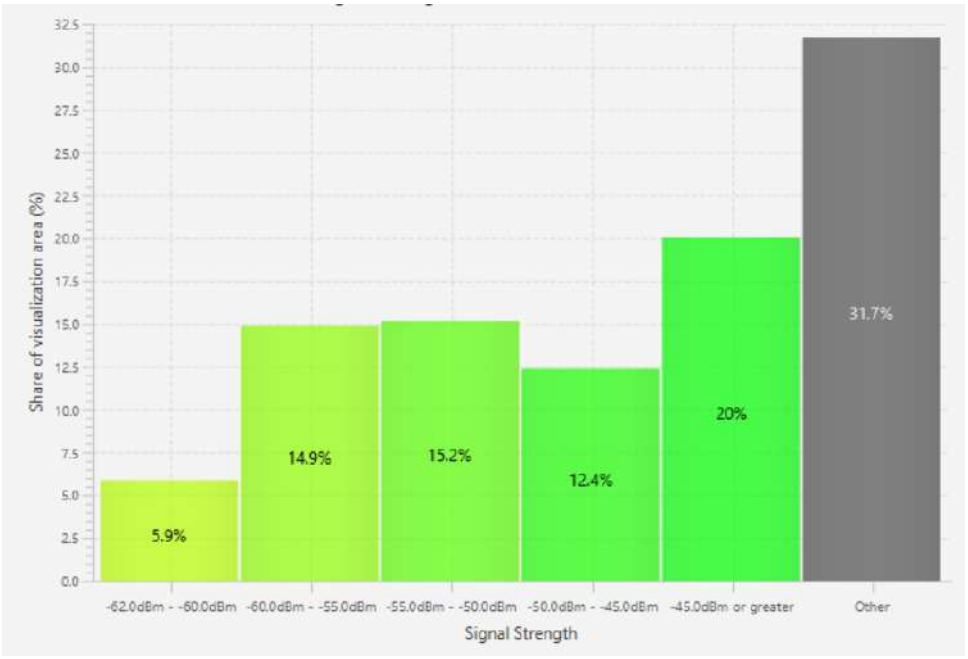

Figura 5.15: Simulación porcentual de área de cobertura en A4.
Fuente: Autor.

Figura 5.16: Resultado actual WiFi Analyzer en A4.
Fuente: Autor.

En la primera Figura 5.13 se muestra que antes solo habían instalados cinco puntos de acceso (APs) para cubrir todo el plano. Sin embargo, se puede observar que los niveles de sensibilidad en los rincones más alejados son bajos, lo que dificultaba que algunos usuarios conectados tuvieran velocidades adecuadas. En la Figura 5.14 se observa, a manera de simulación, que la zona 4 cubre todas las aulas y oficinas del personal administrativo y estudiantes de la UETS con la instalación de 7 APs. La Figura 5.15, en cambio, muestra el porcentaje del área cubierta con el valor de sensibilidad, indicando que el 62 % de la zona tendría una conectividad efectiva dentro del rango de -45 a -60 dBm de sensibilidad. El resto del área presentaría una calidad de señal inferior. En la Figura 5.16 se observa el estado actual y real de la cobertura de la zona. En este caso, se aprecia que todo el interior cuenta con un área de cobertura óptima, lo cual permite navegar sin problema alguno.

5.1.5. Resultados obtenidos en Zona B1

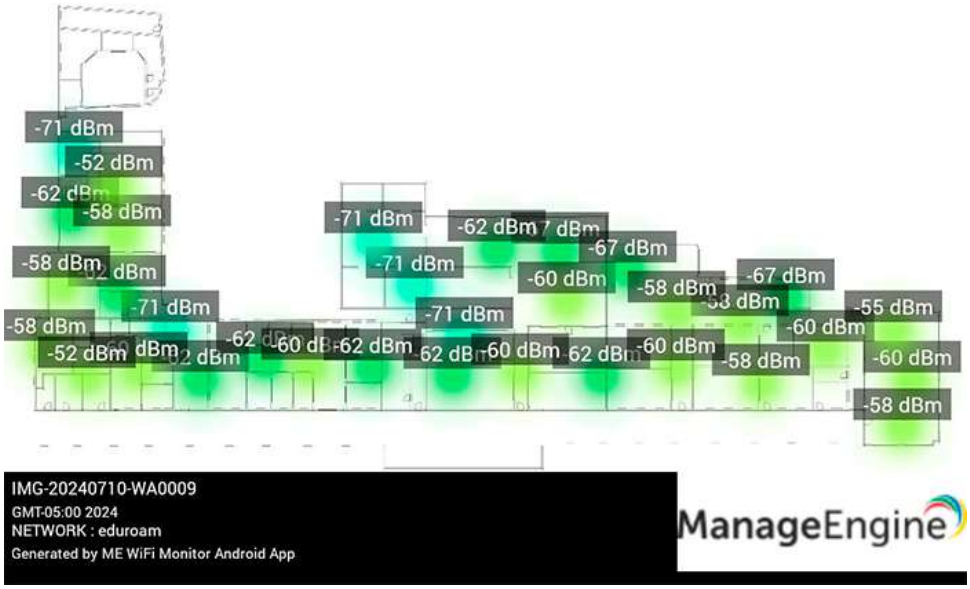

Figura 5.17: Mediciones de cobertura previo a la actualización en B1.
Fuente: Autor.

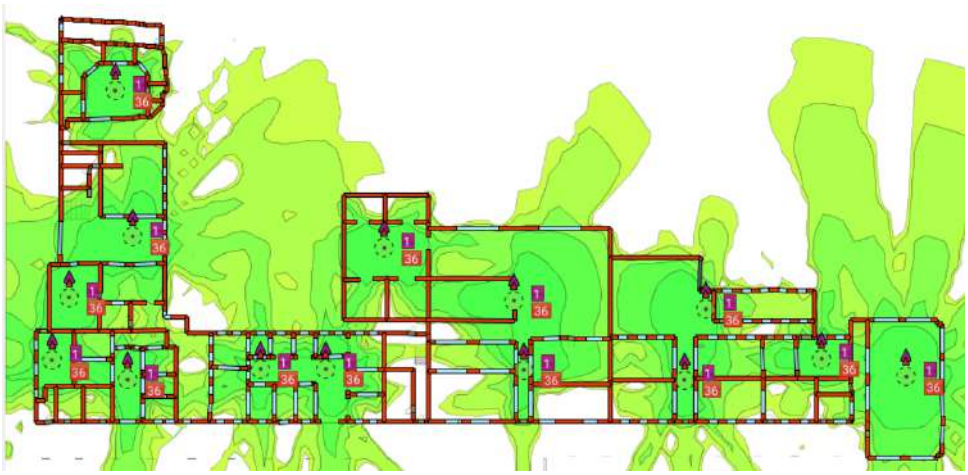

Figura 5.18: Simulación del área de cobertura en B1.
Fuente: Autor.

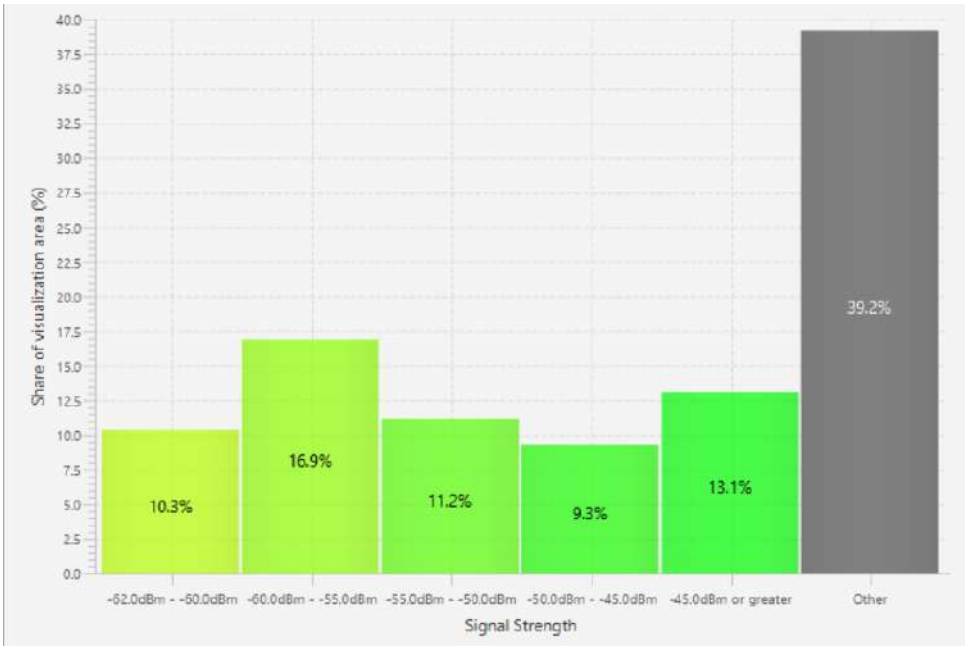

Figura 5.19: Simulación porcentual de área de cobertura en B1.
Fuente: Autor.

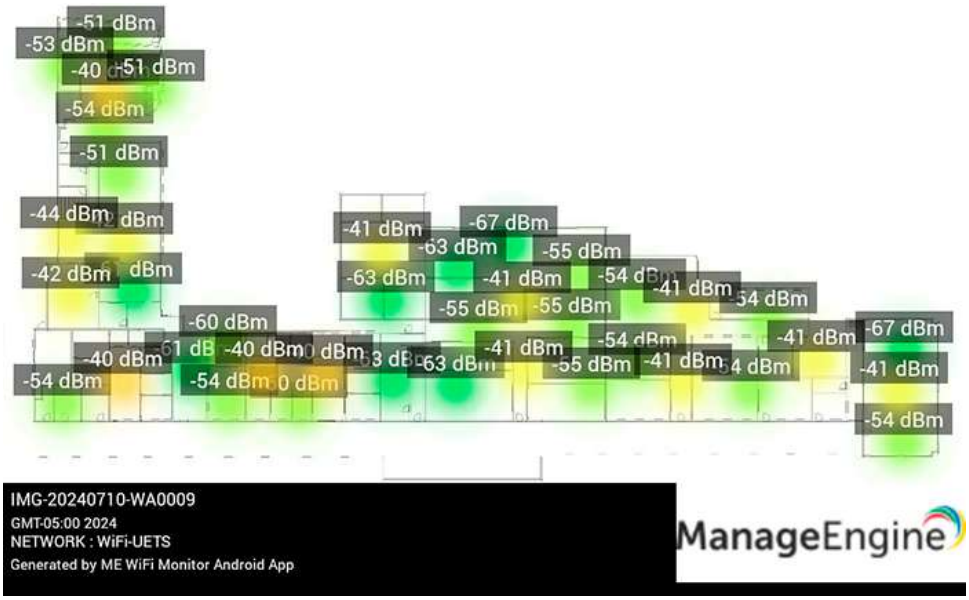

Figura 5.20: Resultado actual WiFi Analyzer en B1.
Fuente: Autor.

En la figura 5.17 se muestra el área de cobertura antes de la actualización de la red y el aumento de puntos de acceso (APs). Antes de los cambios, solo había instalados ocho APs, por lo que esta zona, que era de gran tamaño, no abarcaba todos los rincones y presentaba fallas de conexión, dificultando que el personal accediera a los recursos en línea. Además, como se logra ver en la figura, los niveles de señal eran

bajos en las zonas más distanciadas de los APs. En la Figura 5.18 se muestra la zona más grande a cubrir en cuanto a conectividad, por lo que usando 14 APs se aseguró cubrir toda la zona en cuanto a aulas y oficinas del personal docente y administrativo. En la Figura 5.19 se resalta que en la zona se puede asegurar que el 50 % puede gozar de calidad de conectividad para el uso de internet, dentro del rango de -45 dBm a -60 dBm de sensibilidad. El porcentaje restante tendría una calidad inferior debido al estar a una distancia lejana del AP mas cercano. En la Figura 5.20 se observa el estado actual y real de la cobertura de la zona. En este caso, se aprecia que todo el interior cuenta con un área de cobertura óptima, lo cual permite navegar sin problema alguno.

5.1.6. Resultados obtenidos en Zona B2

Figura 5.21: Mediciones de cobertura previo a la actualización en B2.
Fuente: Autor.

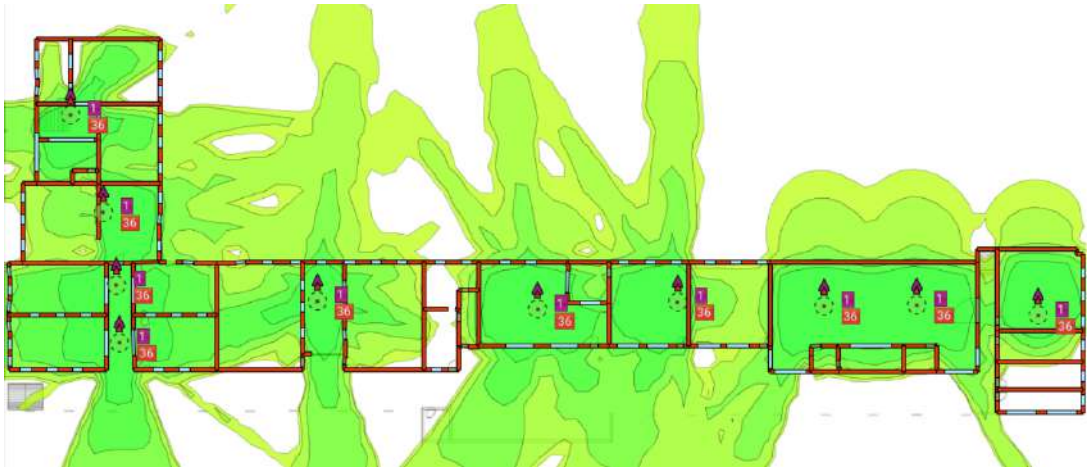

Figura 5.22: Simulación del área de cobertura en B2.
Fuente: Autor.

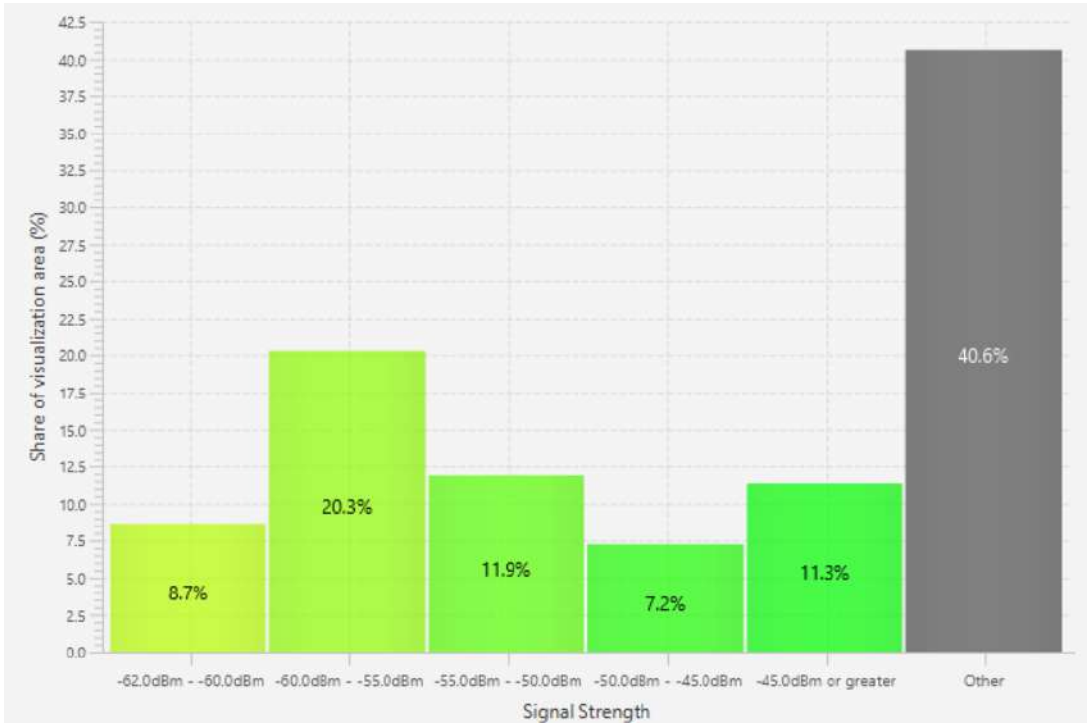

Figura 5.23: Simulación porcentual de área de cobertura en B2.
Fuente: Autor.

Figura 5.24: Resultado actual WiFi Analyzer en B2.
Fuente: Autor.

En la primera Figura 5.21 se muestra la zona de cobertura cuando solo estaban instalados cinco puntos de acceso (APs). Como se puede observar, en algunas partes los niveles de sensibilidad eran menores que cero. Por ende, los usuarios que estaban más lejos del AP experimentaban problemas de inestabilidad en la conexión debido a la cobertura deficiente. En la Figura 5.22 se observa que se trabajó con 10 APs para cubrir por completo el rango de cobertura, asegurando que las oficinas y laboratorios tengan acceso a una conexión a internet fiable. En la Figura 5.23 se demuestra que al menos el 50.7 % del área tendrá la máxima eficacia en cuanto a la velocidad de conexión dentro del rango de -45 a -60 dBm, siempre y cuando estén cerca del AP más cercano a su ubicación. En la Figura 5.24 se observa el estado actual y real de la cobertura de la zona. En este caso, se aprecia que todo el interior cuenta con un área de cobertura óptima, lo cual permite navegar sin problemas. Además, se agregó un switch de ocho puertos.

5.1.7. Resultados obtenidos en Zona B3

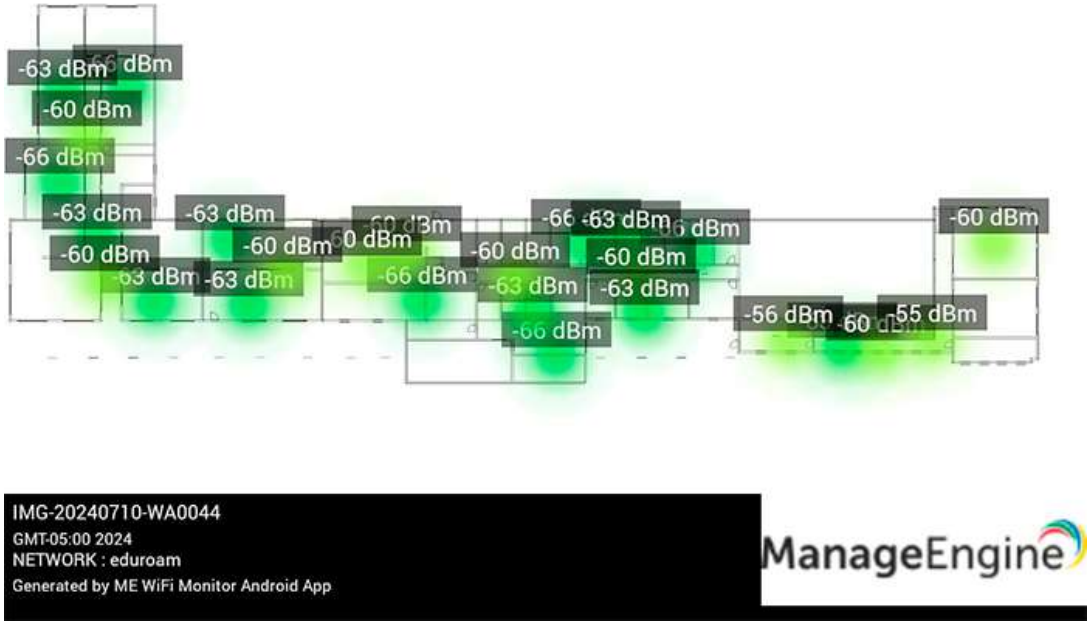

Figura 5.25: Mediciones de cobertura previo a la actualización en B3.
Fuente: Autor.

Figura 5.26: Simulación del área de cobertura en B3.
Fuente: Autor.

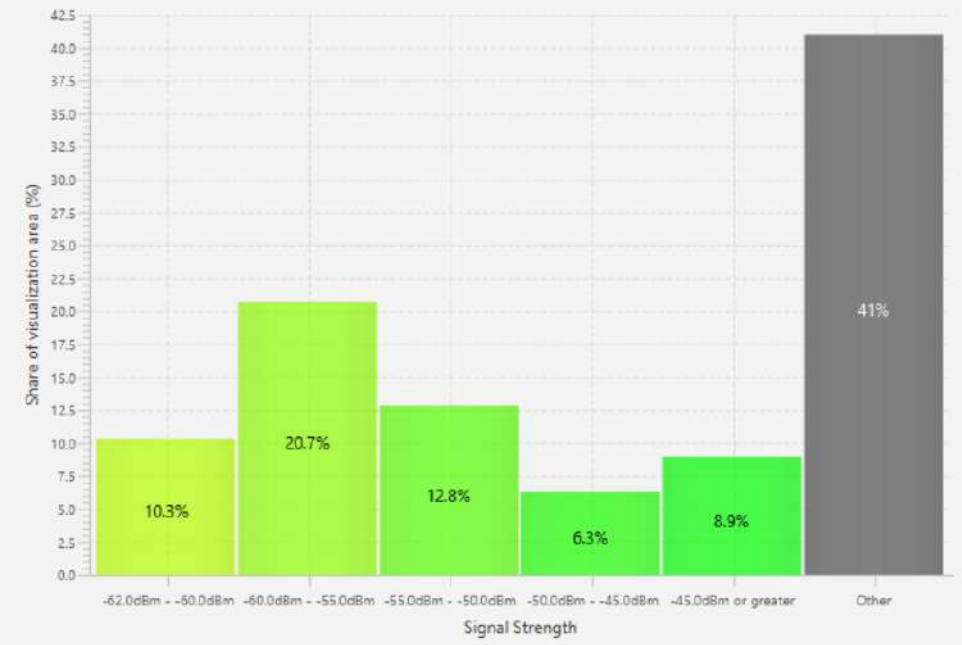

Figura 5.27: Simulación porcentual de área de cobertura en B3.
Fuente: Autor.

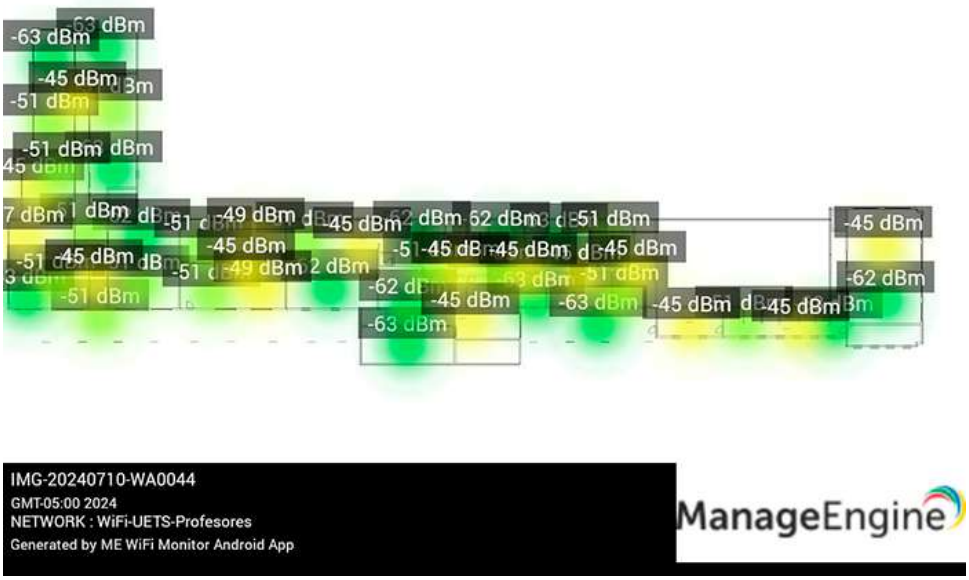

Figura 5.28: Resultado actual WiFi Analyzer en B3.
Fuente: Autor.

En la primera Figura 5.25 de la zona, se observa que el área de cobertura no cubría todo el plano de manera eficiente debido a que solo estaban instalados y funcionando ocho puntos de acceso (APs). Esto causaba problemas de conexión para algunos usuarios en zonas donde la señal no llegaba. Por eso, solo los usuarios que estaban cerca del AP más cercano no presentaban estos inconvenientes. En la Figura

5.26 se muestra que la zona fue cubierta con el uso de 13 APs ubicados en zonas estratégicas, asegurando que cada rincón de las aulas, laboratorios y oficinas tenga una buena conectividad a internet. La Figura 5.27 representa el porcentaje de conectividad en relación a la distancia entre el usuario y el AP más cercano, indicando que el 48.7 % de toda la zona obtendría una buena calidad de conexión que estaría dentro del rango de -45dBm a -60 dBm de sensibilidad. Esto permite una velocidad adecuada para las necesidades diarias de la educación en línea y el uso de recursos basados en internet. El porcentaje restante tendría una conectividad inferior por lo cual no aprovecharía al máximo el ancho de banda brindado. En la Figura 5.28 se observa el estado actual y real de la cobertura de la zona. En este caso, se aprecia que todo el interior cuenta con un área de cobertura óptima, lo cual permite navegar sin problema alguno. Además, se agregó un switch de 24 puertos.

5.1.8. Resultados obtenidos en Zona C

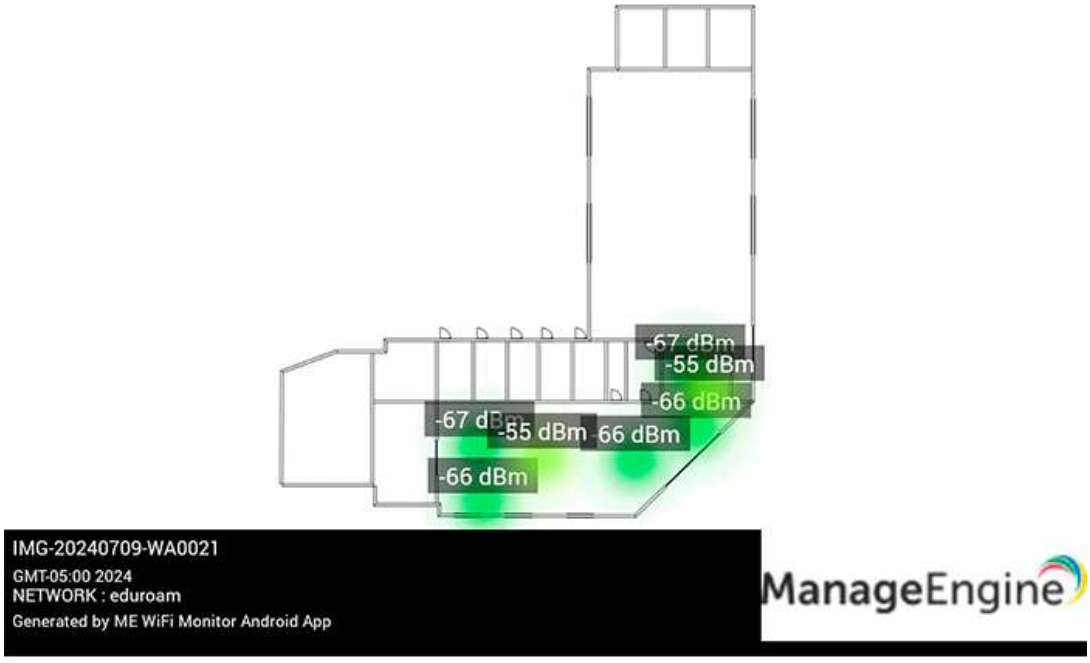

Figura 5.29: Mediciones de cobertura previo a la actualización en C.
Fuente: Autor.

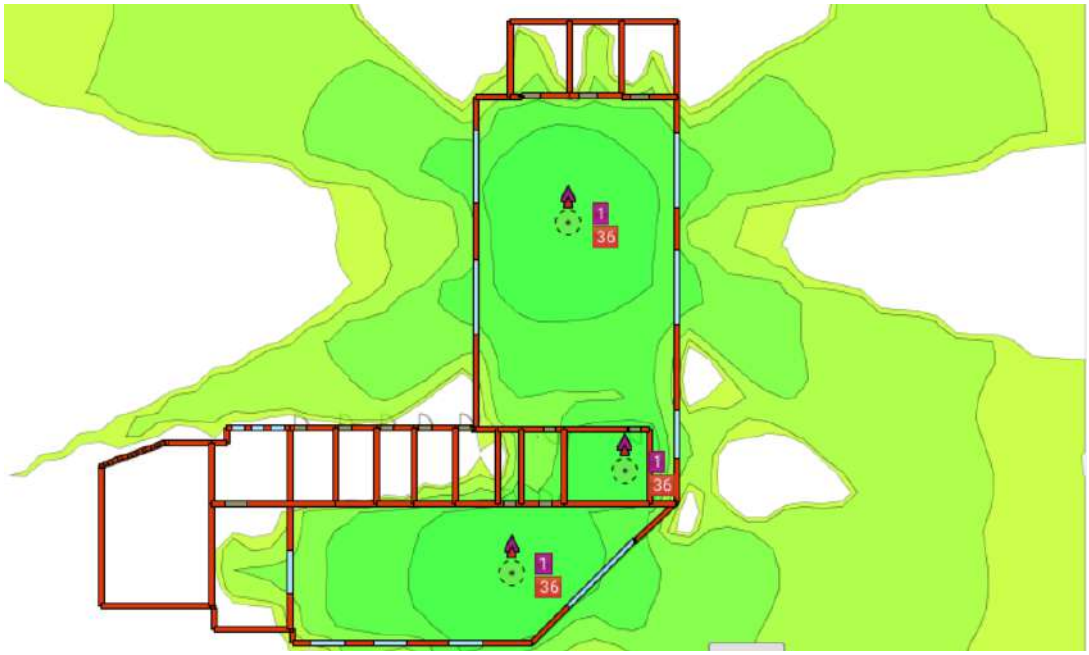

Figura 5.30: Simulación del área de cobertura en C.
Fuente: Autor.

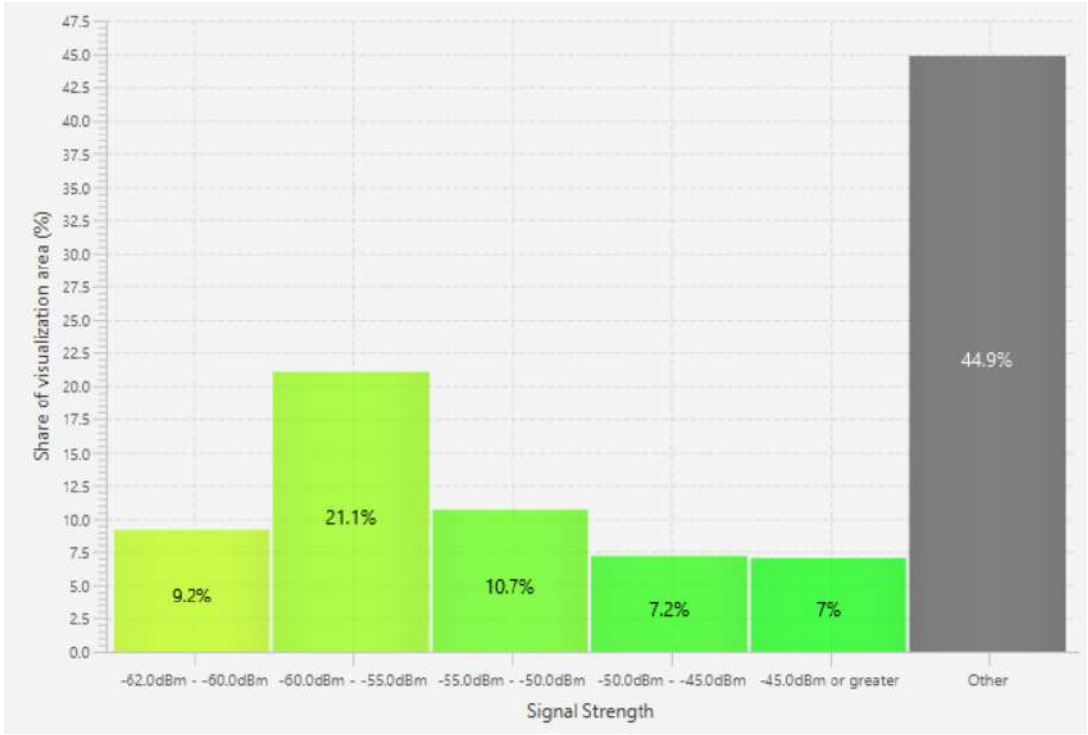

Figura 5.31: Simulación porcentual de área de cobertura en C.
Fuente: Autor.

Figura 5.32: Resultado actual WiFi Analyzer en C.
Fuente: Autor.

En la Figura 5.29 que con anterioridad representaba la zona de cobertura, se observa que la señal solo llegaba a ciertos rincones cercanos al punto de acceso (AP). Más lejos de este, la señal era muy baja. Esto se debía a que solo un AP estaba funcionando, mientras que el otro estaba deshabilitado debido a configuraciones incorrectas, hasta que pudiera ser reconfigurado. En la Figura 5.30 se observa que, con el uso de 3 APs ubicados en zonas específicas, se logra cubrir toda el área requerida, incluyendo las mesas de los bares, la oficina de administración y el centro de actividades de gimnasia. El mapa de calor muestra que casi todos los usuarios en su entorno podrán disfrutar de conectividad a internet. La Figura 5.31 presenta el porcentaje de conexión a la red correspondiente a toda el área dentro del rango de cobertura de los APs. En este caso, el 46 % de toda la zona tendría un nivel de conectividad efectiva, con una señal de calidad dentro del rango de -45 a -60 dBm de sensibilidad. En la Figura 5.32 se observa el estado actual y real de la cobertura de la zona. En este caso, se aprecia que todo el interior cuenta con un área de cobertura óptima, lo cual permite navegar sin problema alguno.

5.1.9. Resultados obtenidos en Zona D

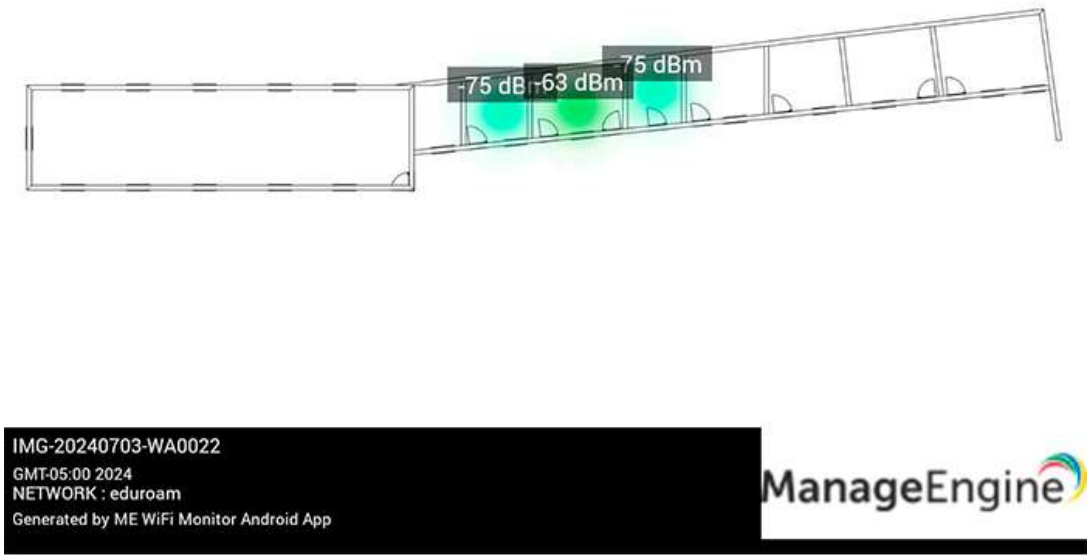

Figura 5.33: Mediciones de cobertura previo a la actualización en D.
Fuente: Autor.

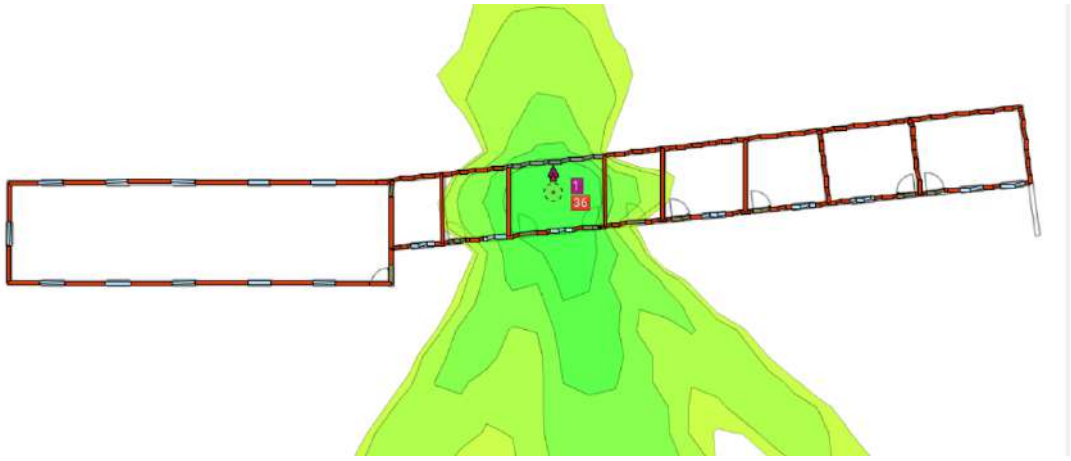

Figura 5.34: Simulación del área de cobertura en D.
Fuente: Autor.

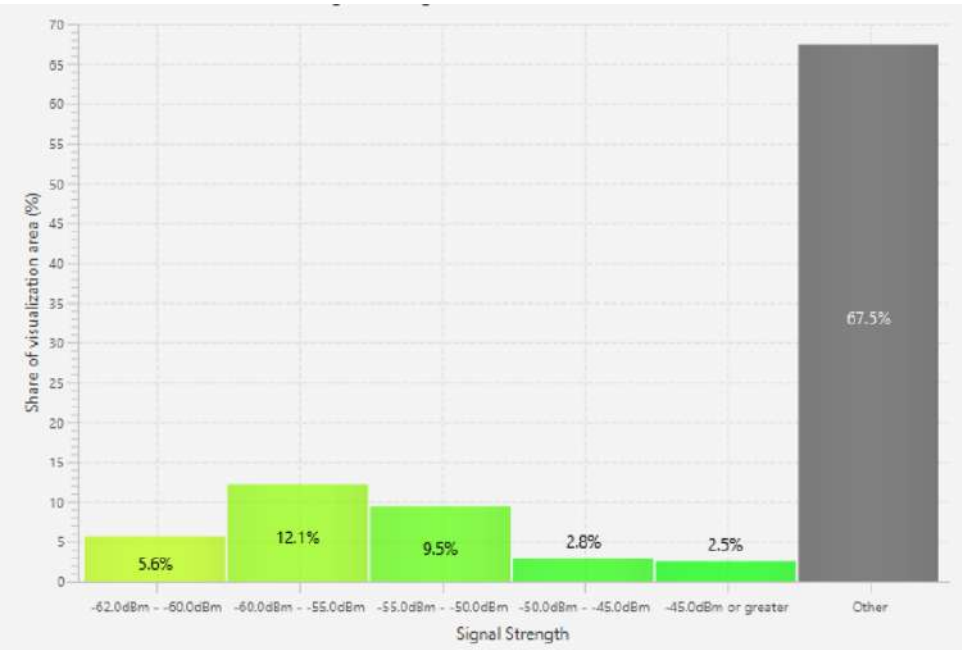

Figura 5.35: Simulación porcentual de área de cobertura en D.
Fuente: Autor.

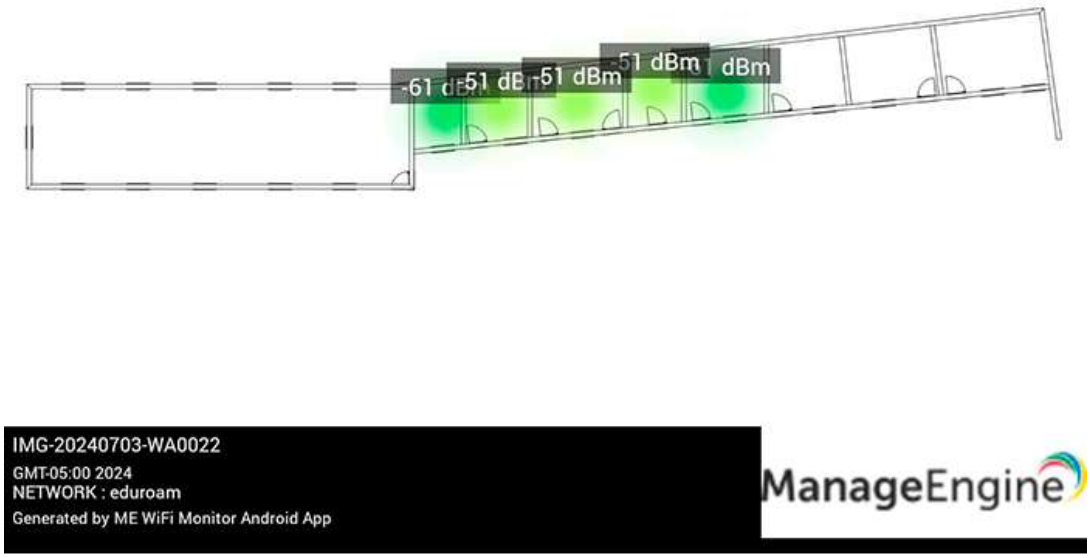

Figura 5.36: Resultado actual WiFi Analyzer en D.
Fuente: Autor.

En la primera Figura 5.33 de la zona, se contaba con un solo punto de acceso (AP) mal ubicado. Por ello, solo la oficina administrativa tenía una señal estable al estar más cerca del AP, mientras que las aulas en los extremos presentaban niveles de

sensibilidad bajos, lo que causaba problemas en la velocidad de navegación en línea. En la Figura 5.34 se muestra que el plano de la zona cubre de manera eficaz la oficina administrativa con un solo AP, priorizando la conectividad en esta área. Las aulas en los extremos no tienen una conexión tan eficaz debido a que son zonas que no siempre están ocupadas. La Figura 5.35 representa el porcentaje de conexión a la red de toda la zona, indicando que el 26.9 % estaría dentro del rango de -45 a -60 dBm de sensibilidad, lo que significa una buena velocidad y una conexión a internet fiable. En la Figura 5.36 se observa el estado actual y real de la cobertura de la zona. En este caso, se aprecia que todo el interior cuenta con un área de cobertura óptima, lo cual permite navegar sin problema alguno.

5.1.10. Resultados obtenidos en Zona E1

Figura 5.37: Mediciones de cobertura previo a la actualización en E1.
Fuente: Autor.

Figura 5.38: Simulación del área de cobertura en E1.
Fuente: Autor.

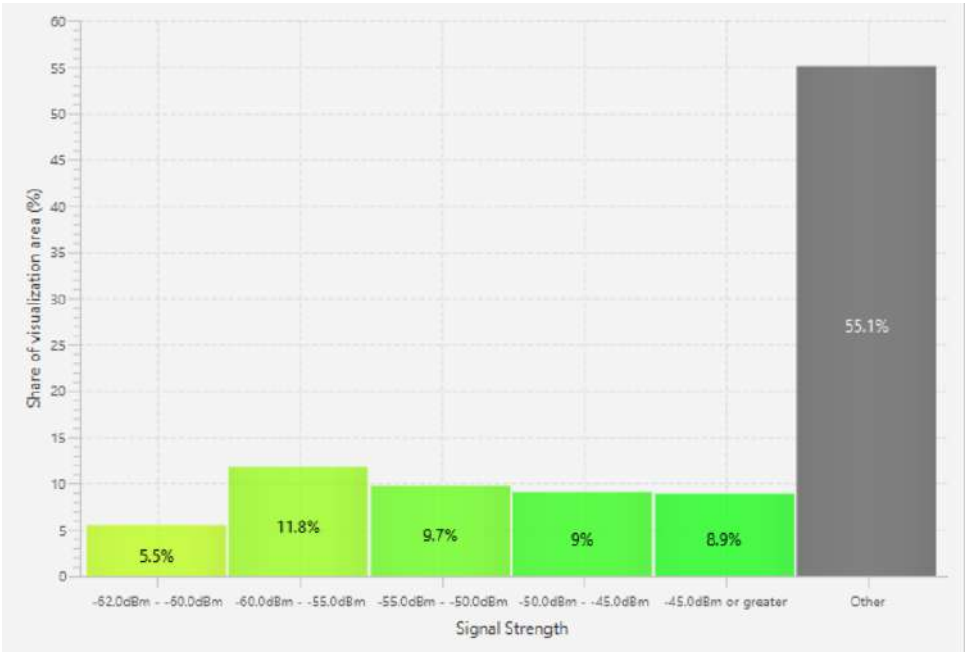

Figura 5.39: Simulación porcentual de área de cobertura en E1.
Fuente: Autor.

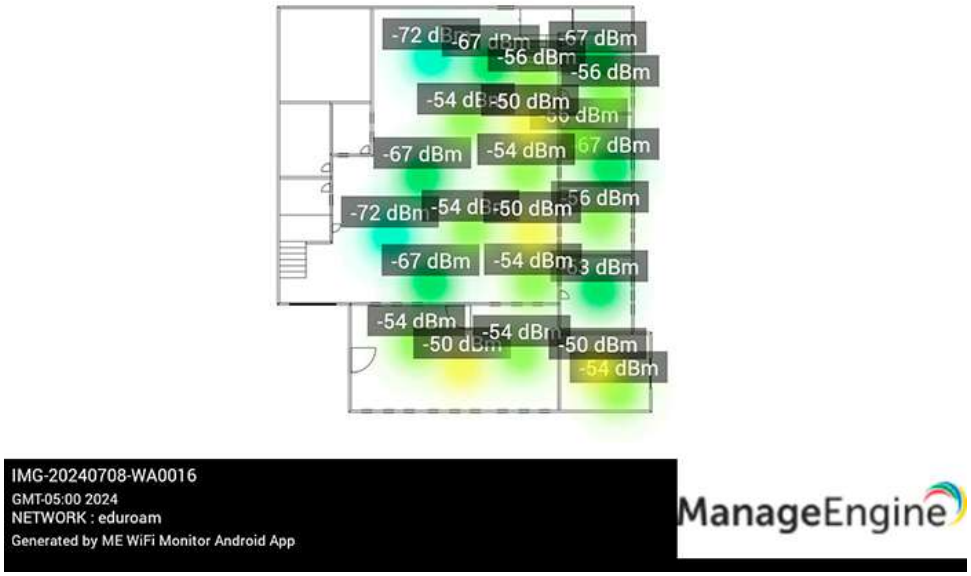

Figura 5.40: Resultado actual WiFi Analyzer en E1.
Fuente: Autor.

En la Figura 5.37 se observa que, cuando solo se trabajaba con dos puntos de acceso (APs), los niveles de sensibilidad eran altos, lo que permitía una conexión estable solo si se estaba cerca del AP más cercano. Sin embargo, el resto de las áreas de la zona presentaban una cobertura deficiente debido a los obstáculos y a las distancias que no se cubrían por completo. En la Figura 5.38 se muestra que el plano de la zona, cubre todas las áreas requeridas correspondientes a las aulas de estudiantes. En el caso de las bodegas en la parte superior izquierda y el salón de la parte superior izquierda, no se prioriza un nivel de señal al máximo debido a que son lugares que no son aulas y son requeridos para otros fines. Por lo tanto, el uso de 4 APs instalados es suficiente para cubrir las áreas requeridas. La Figura 5.39 muestra el rango proporcional de conectividad de toda la zona, indicando que el 39.4 % tendrá un nivel de cobertura de red rápido y fiable, que estará dentro de un rango desde los -45 a -60 dBm de sensibilidad. En la Figura 5.40, se observa el estado actual y real de la cobertura de la zona. En este caso, se aprecia que todo el interior cuenta con un área de cobertura óptima, lo cual permite navegar sin problema alguno. Además, se agregó un switch de 8 puertos.

5.1.11. Resultados obtenidos en Zona E2

Figura 5.41: Simulación del área de cobertura en E2.
Fuente: Autor.

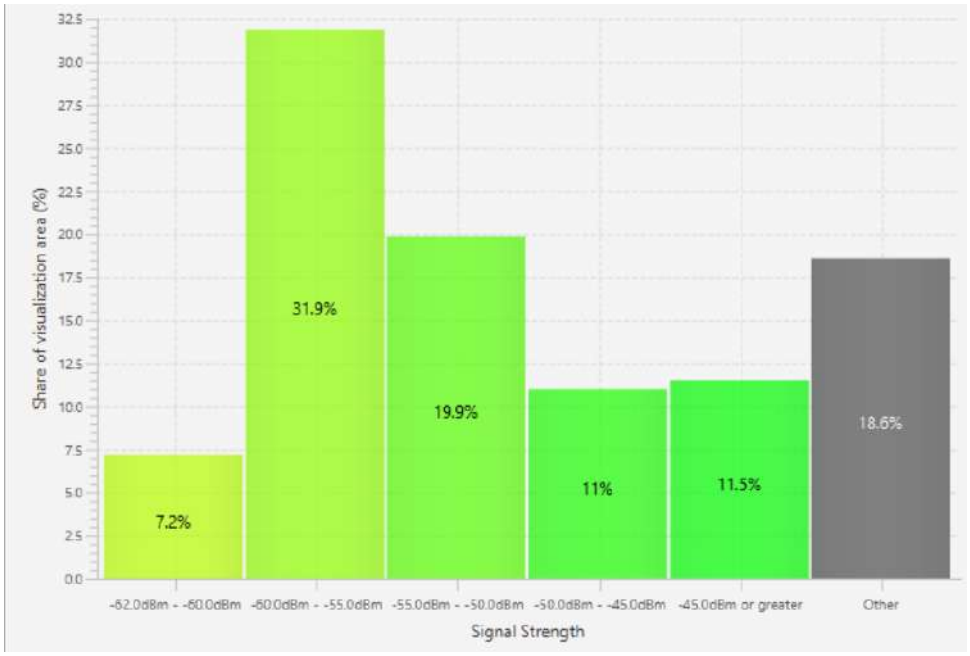

Figura 5.42: Simulación porcentual de área de cobertura en E2.
Fuente: Autor.

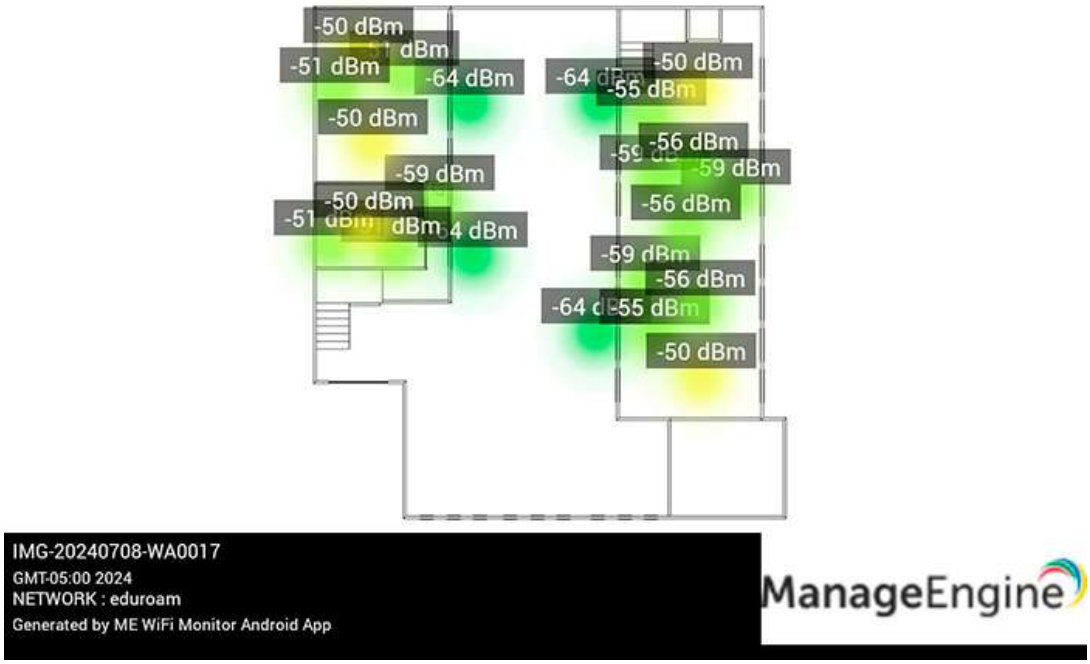

Figura 5.43: Resultado actual WiFi Analyzer en E2.
Fuente: Autor.

En esta zona no había un estado previo de cobertura, ya que no se habían instalado puntos de acceso (APs). Solo se propuso su implementación para proporcionar cobertura en toda el área. En la Figura 5.41 se muestra que el plano de la zona está cubierto en casi su totalidad con el uso de 4 APs, priorizando más la cobertura en las zonas de aulas de la segunda planta. En la Figura 5.42 se presenta el porcentaje de cobertura de toda el área, indicando que el 42.4 % de la zona tendría la mayor calidad de servicio y velocidad de conexión a internet siempre que se encuentre dentro de un rango desde los -45 a -60 dBm de sensibilidad. En la Figura 5.43, se observa el estado actual y real de la cobertura de la zona. En este caso, se aprecia que todo el interior cuenta con un área de cobertura óptima, lo cual permite navegar sin problema alguno. Además, se agregó un switch de 24 puertos.

5.1.12. Resultados obtenidos en Zona F1

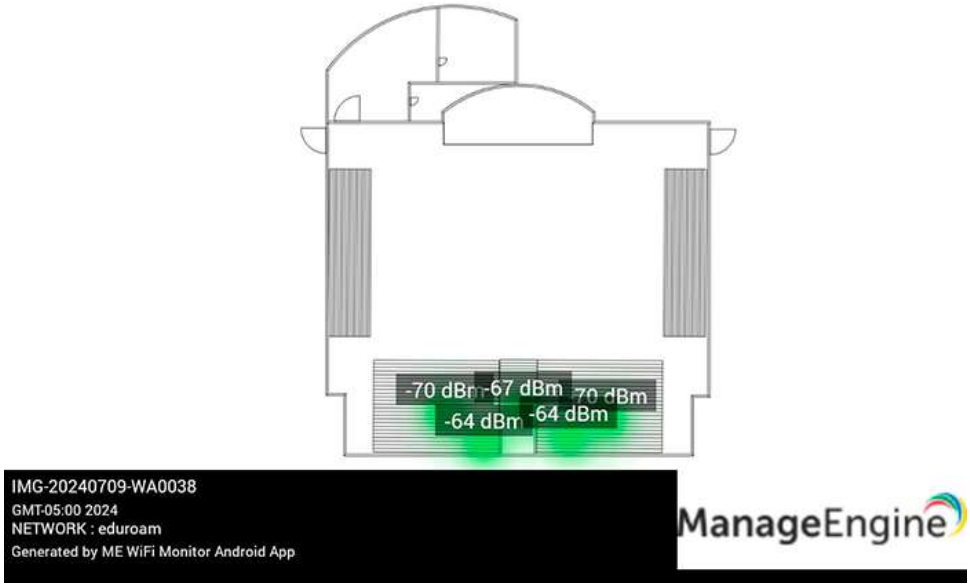

Figura 5.44: Mediciones de cobertura previo a la actualización en F1.
Fuente: Autor.

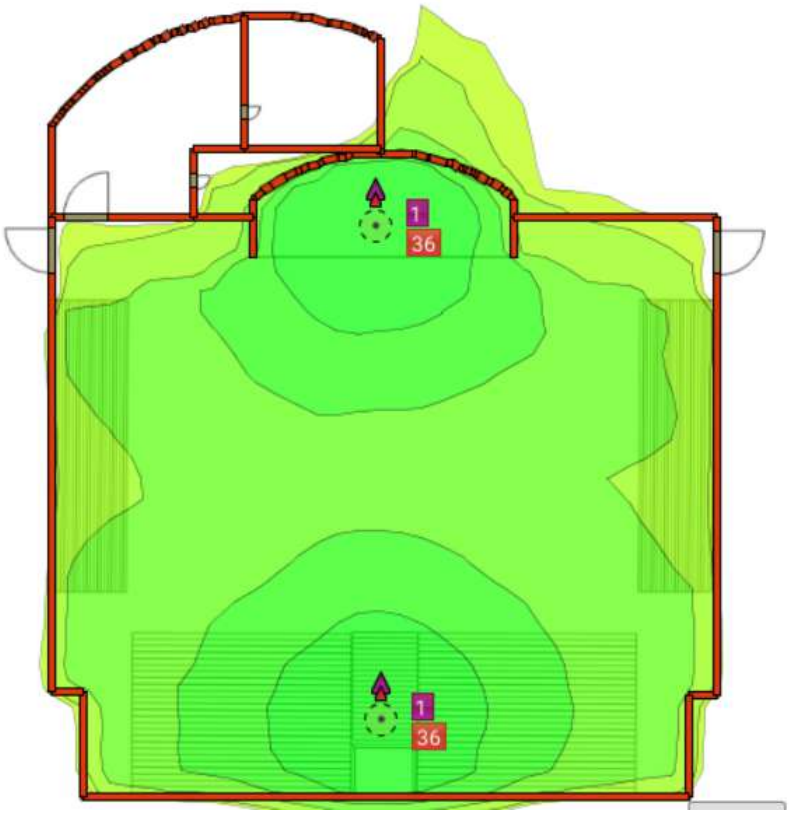

Figura 5.45: Simulación del área de cobertura en F1.
Fuente: Autor.

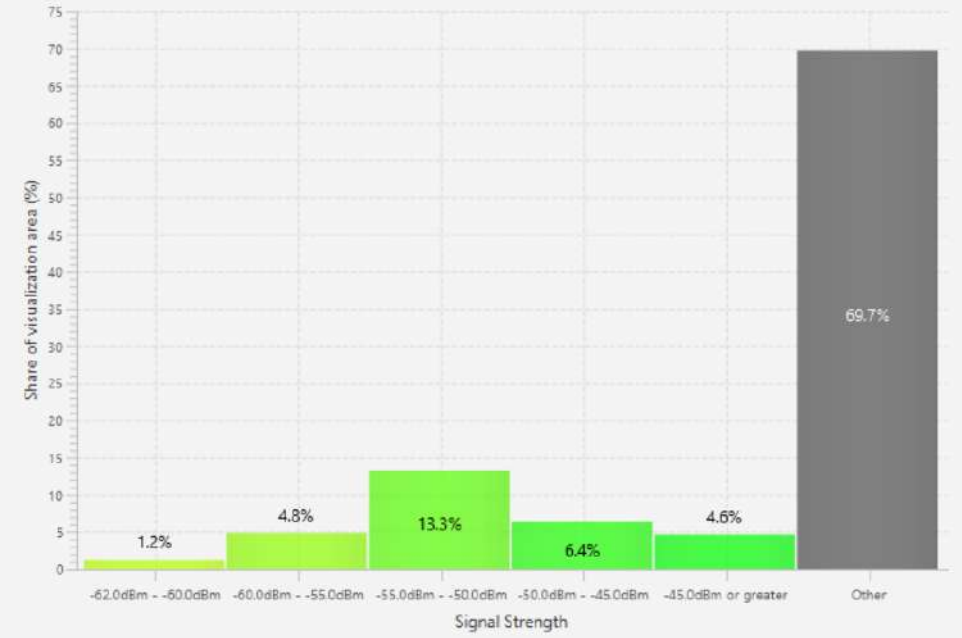

Figura 5.46: Simulación porcentual de área de cobertura en F1.
Fuente: Autor.

Figura 5.47: Resultado actual WiFi Analyzer en F1.
Fuente: Autor.

En la Figura 5.44 se muestra cómo estaban antes los niveles de sensibilidad de la señal en la zona de cobertura. En ese momento, solo se utilizaban dos puntos de acceso (APs) que requerían modificaciones en sus parámetros para mejorar la conectividad. Por ello, la señal solo era estable si los usuarios se encontraban cerca del AP, pero la velocidad era deficiente debido a configuraciones incorrectas realizadas

con anterioridad. En la Figura 5.45 se muestra el plano de toda la zona, donde con el uso de 2 APs se logra cubrir casi en su totalidad para conectar a todos los usuarios presentes. En la Figura 5.46 se observa que el 29.1 % de toda la zona que esta en un rango desde los -45 a -60 dBm de sensibilidad podrá utilizar la conexión de manera fiable y aprovechar el ancho de banda ofrecido; el porcentaje restante será un poco inferior debido a la extensión de la zona y los objetos que obstruyen el paso de las señales. En la Figura 5.47, se observa el estado actual y real de la cobertura de la zona. En este caso, se aprecia que todo el interior cuenta con un área de cobertura óptima, lo cual permite navegar sin problema alguno.

5.1.13. Resultados obtenidos en Zona F2

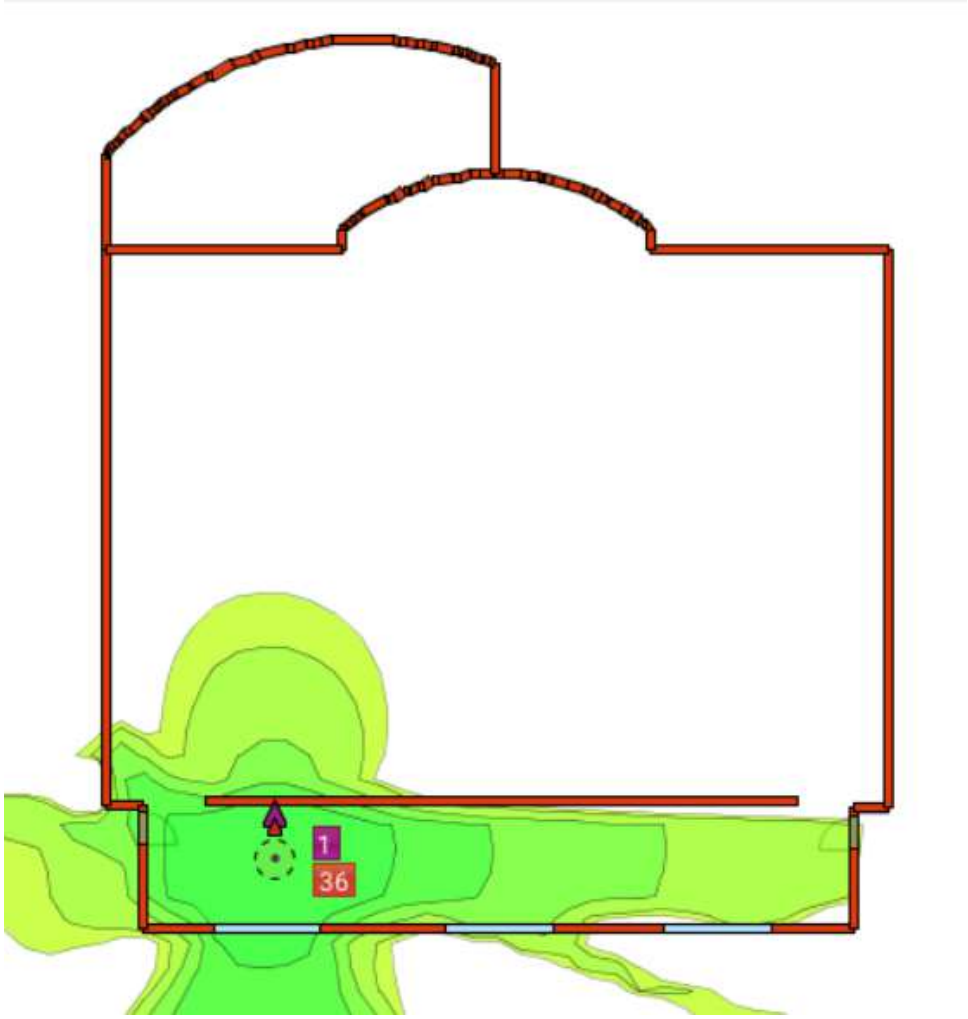

Figura 5.48: Simulación del área de cobertura en F2.
Fuente: Autor.

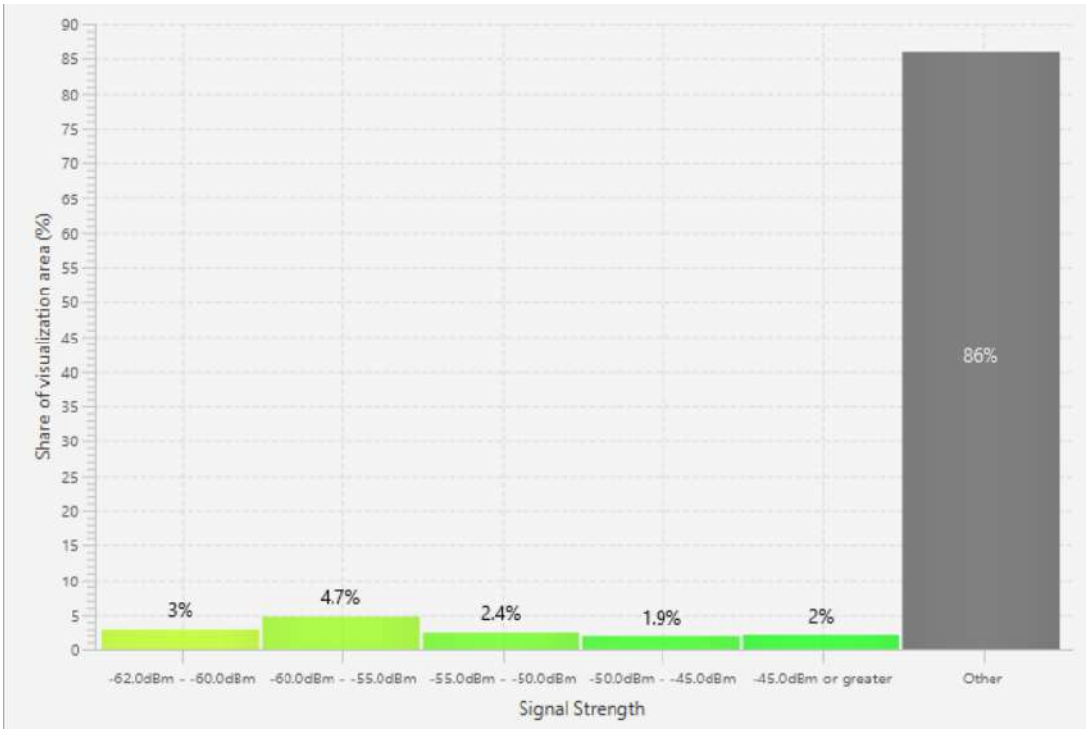

Figura 5.49: Simulación porcentual de área de cobertura en F2.
Fuente: Autor.

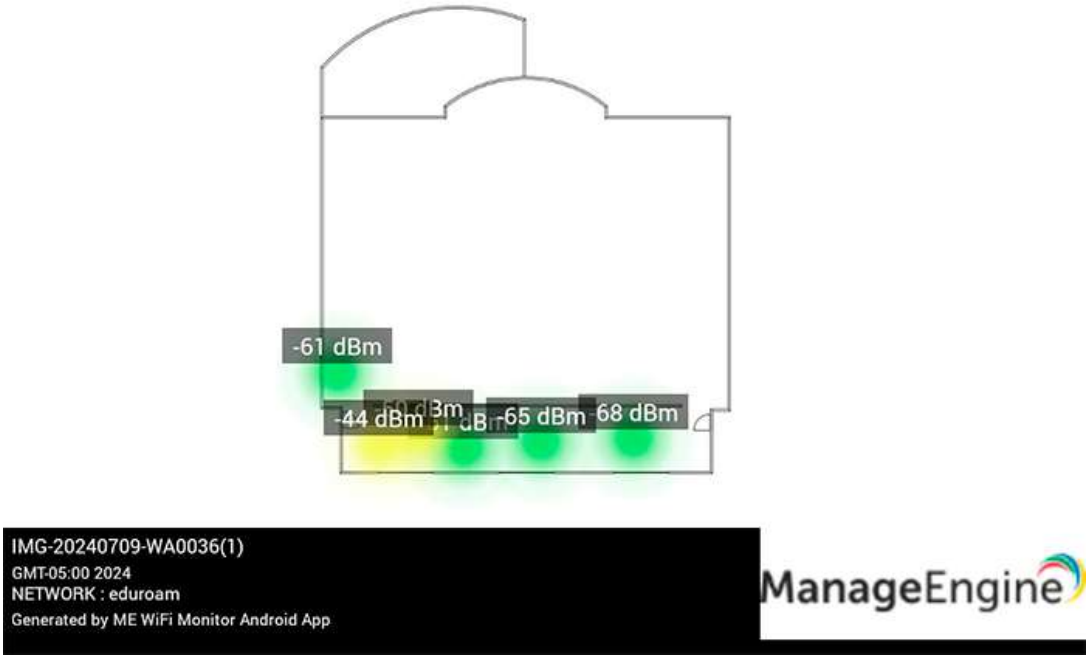

Figura 5.50: Resultado actual WiFi Analyzer en F2.
Fuente: Autor.

En esta zona antes de la actualización el AP estaba desconectado debido a que requería de una reconfiguración para mejorar sus parámetros de transmisión y

rango de cobertura. En esta zona representada por la Figura 5.48, se muestra que el pasillo está cubierto en su totalidad con el uso de 1 AP. En la Figura 5.49 representa el porcentaje de toda la zona, indicando qué nivel de señal obtendría dependiendo de la ubicación del usuario. El 11 % de toda la zona disfrutaría de la mayor velocidad y calidad de servicio, ya que está diseñado para cubrir una zona pequeña y se encuentra en un rango de -45 a -60 dBm de sensibilidad. En la Figura 5.50, se observa el estado actual y real de la cobertura de la zona. En este caso, se aprecia que todo el interior cuenta con un área de cobertura óptima, lo cual permite navegar sin problema alguno.

5.1.14. Resultados obtenidos en Zona G

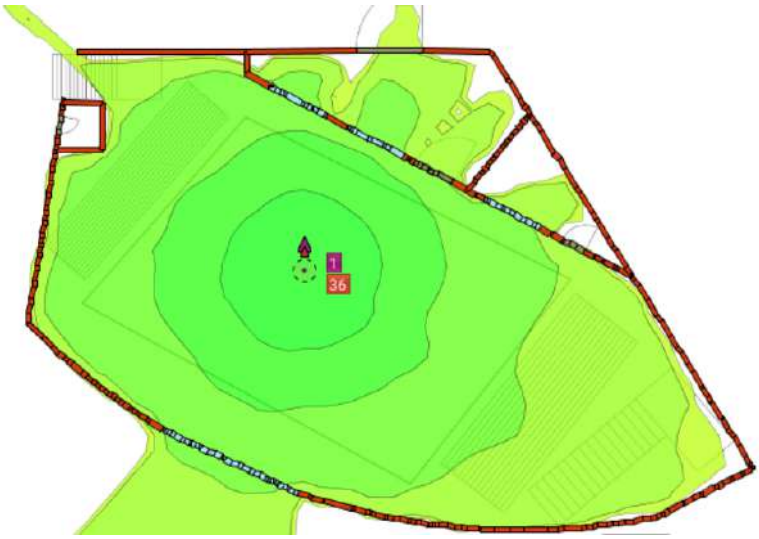

Figura 5.51: Simulación del área de cobertura en G.
Fuente: Autor.

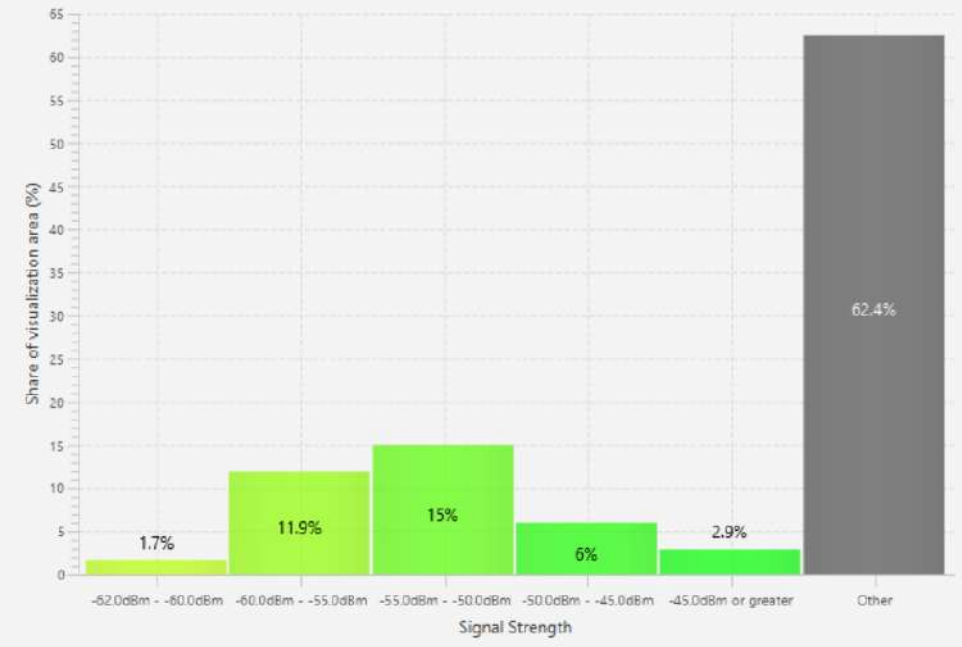

Figura 5.52: Simulación porcentual de área de cobertura en G.
Fuente: Autor.

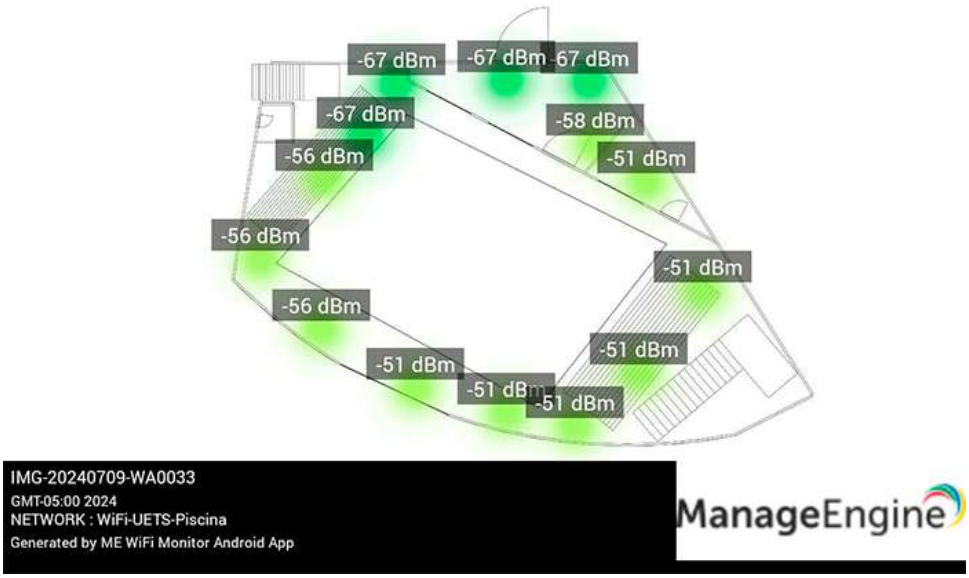

Figura 5.53: Resultado actual WiFi Analyzer en G.
Fuente: Autor.

En esta zona no existió un antes, ya que solo se planifico la implementación de un solo AP. En la Figura 5.51, se observa que la zona está cubierta en su totalidad, incluso las gradas con el uso de un solo AP. Esto se debe a que es una zona abierta que carece de obstáculos como paredes en su parte central, lo que permite un rango

de cobertura más amplio y sin restricciones, a diferencia de las zonas anteriores que tienen paredes intermedias.

En la Figura 5.52, se muestra el porcentaje de conectividad de toda la zona, donde el 35.8 % representa un área de cobertura con un nivel de conectividad fiable, aprovechando todo el ancho de banda dentro del rango de -45 a -60 dBm de sensibilidad. El porcentaje restante cuenta con cobertura para tareas que no requieren una calidad de señal excelente, aunque la velocidad puede ser menor. En la Figura 5.53, se observa el estado actual y real de la cobertura de la zona. En este caso, se aprecia que todo el interior cuenta con un área de cobertura óptima, lo cual permite navegar sin problema alguno. Se resalta que el AP contaba con protección 1P68 para evitar problemas con la lluvia ya que su ubicación no era de manera interna. Además, se agregó un switch de 24 puertos.

5.1.15. Resultados obtenidos en Zona H

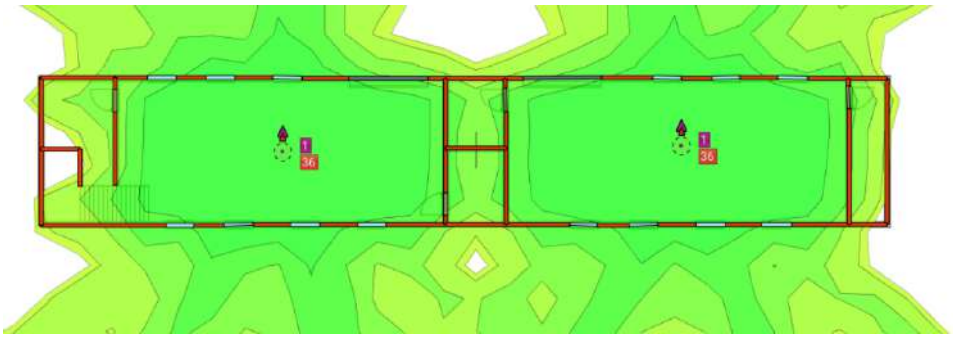

Figura 5.54: Simulación del área de cobertura en H.
Fuente: Autor.

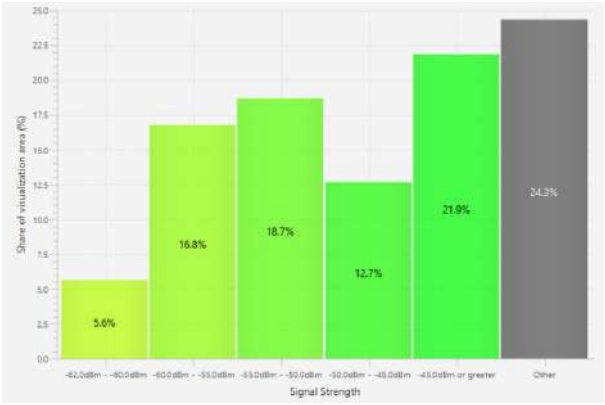

Figura 5.55: Simulación porcentual de área de cobertura en H.
Fuente: Autor.

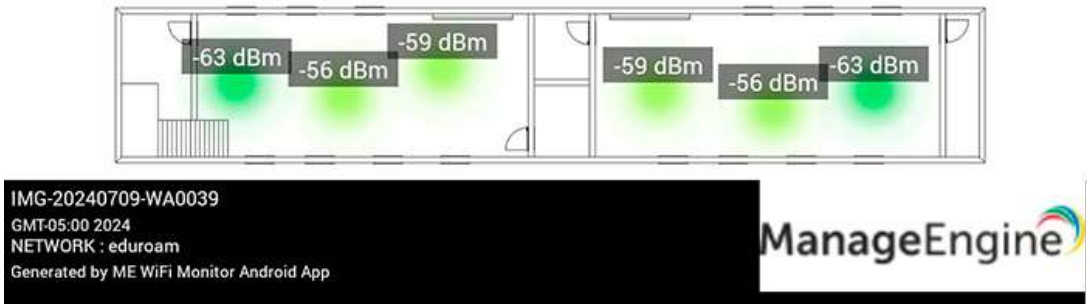

Figura 5.56: Resultado actual WiFi Analyzer en H.
Fuente: Autor.

En esta zona no existió el uso de APs, por ello solo se planificó la instalación de APs según requieran para cubrir todo la zona requerida. En la Figura 5.54 se muestra que el plano de la zona está totalmente cubierto, garantizando así una conectividad en todos los rincones con la presencia de 2 APs instalados en cada departamento, tanto para el de comunicación y de música. En la Figura 5.55, se indica que el 70.1 % tiene la mayor calidad de señal estable, dentro del rango de -45 a -60 dBm de sensibilidad. El resto del porcentaje tendrá una calidad inferior a comparación si estuviese cerca de un AP. En la Figura 5.56 se observa el estado actual y real de la cobertura de la zona. En este caso, se aprecia que todo el interior cuenta con un área de cobertura óptima, lo cual permite navegar sin problema alguno. Además, se agregó un switch de 24 puertos.

5.1.16. Resultados de cobertura simulada y medición real

Los resultados obtenidos en la tabla 5.1 con el programa de simulación Ekahau Site Survey y la aplicación móvil WIFI Analyzer And Survey permitieron comparar los valores de cobertura de la señal. En ambos casos, se observó que los valores de sensibilidad de la señal eran muy similares. La simulación mostró una cobertura de señal con valores de sensibilidad entre -45 dBm a los -60 dBm en en la zona interna, mientras que las mediciones reales arrojaron valores en el rango de -50 dBm a los -72 dBm. Esto indica que la simulación y las mediciones reales coinciden de manera parcial, confirmando exactitud de uso del programa de simulación en la estimación

de la cobertura de la señal para tener una idea de como quedaría la cobertura en cada zona de la UETS.

Tabla 5.1: Valores de sensibilidad simulados y reales.

Fuente: Autor.

Zona	Nivel de señal esperado	Nivel de señal logrado
A1	[-45 dBm a -60 dBm]	[-38 dBm a -66 dBm]
A2	[-45 dBm a -60 dBm]	[-46 dBm a -68 dBm]
A3	[-45 dBm a -60 dBm]	[-54 dBm a -65 dBm]
A4	[-45 dBm a -60 dBm]	[-46 dBm a -62 dBm]
B1	[-45 dBm a -60 dBm]	[-41 dBm a -67 dBm]
B2	[-45 dBm a -60 dBm]	[-46 dBm a -65 dBm]
B3	[-45 dBm a -60 dBm]	[-45 dBm a -63 dBm]
C	[-45 dBm a -60 dBm]	[-51 dBm a -67 dBm]
D	[-45 dBm a -60 dBm]	[-51 dBm a -61 dBm]
E1	[-45 dBm a -60 dBm]	[-54 dBm a -72 dBm]
E2	[-45 dBm a -60 dBm]	[-50 dBm a -64 dBm]
F1	[-45 dBm a -60 dBm]	[-53 dBm a -68 dBm]
F2	[-45 dBm a -60 dBm]	[-44 dBm a -68 dBm]
G	[-45 dBm a -60 dBm]	[-51 dBm a -67 dBm]
H	[-45 dBm a -60 dBm]	[-56 dBm a -59 dBm]

5.2. Optimización del Ancho de Banda

Al reasignar los anchos de banda en toda la institución, se logró una mejora considerable en la capacidad de la red. Este proceso de reasignación implicó una reconfiguración detallada de los recursos de ancho de banda para asegurarse que cada área del campus recibiera la cantidad óptima de capacidad según sus necesidades específicas. Como resultado, se experimentó un aumento notable en la velocidad de conexión, lo que se tradujo en una mayor eficiencia en el uso de la red para actividades académicas y administrativas. La optimización permitió una distribución más equitativa del ancho de banda, reduciendo los cuellos de botella y mejorando la experiencia de usuario al navegar. Este ajuste no solo facilitó una experiencia más fluida y rápida, sino que también contribuyó a una infraestructura de red más robusta y adaptada a las demandas actuales de la institución.

Figura 5.57: Resultado anterior de ancho de banda UETS.
Fuente: Autor.

Figura 5.58: Resultado posterior de ancho de banda UETS.
Fuente: Autor.

En la figura 5.57 ilustra un ejemplo de las velocidades de subida y bajada

antes de la actualización en el coliseo de la institución. Tras la implementación, se logró gestionar el ancho de banda a través del firewall, permitiendo aumentar la velocidad hasta un máximo de 500Mbps, ajustándose a las necesidades específicas de la institución. En la figura 5.58 se presentan las nuevas velocidades de subida y bajada alcanzadas durante el evento Ruleta del Saber realizado de igual manera en el coliseo y organizado por el Ministerio de Educación. Este evento resultó ser un éxito total en términos de transmisión en vivo y en el uso de plataformas que requerían un elevado ancho de banda.

Tabla 5.2: Velocidades de transmisión promedio antes y después de la implementación.

Fuente: Autor

Zona	**Velocidad de Subida y Bajada Antes (Mbps)**	**Latencias (ms) Antes**	**Velocidad de Subida y Bajada Después (Mbps)**	**Latencias (ms) Después**
Administrativo	10 a 25	10 a 1200	100 a 200	5 a 25
Comunidad Salesiana	5 a 25	25 a 1000	50 a 100	5 a 10
Cabinas de Comunicación	1 a 10	25 a 1200	100 a 200	5 a 25
Laboratorios de Computación	5 a 15	40 a 1200	20 a 100	5 a 10
Aulas	1 a 25	25 a 1000	20 a 80	10 a 25
Sala de Profesores	0.5 a 20	10 a 1200	20 a 80	25 a 45

La tabla 5.2 muestra una comparativa de las velocidades promedio de subida y bajada en diversas zonas de la institución antes y después de la actualización del ancho de banda. Los datos muestran una mejora significativa en el rendimiento de la red, con incrementos notables en la capacidad de transferencia de datos tras la actualización.

Antes de la actualización, las velocidades eran bajas en todas las áreas. Con la actualización, se logró un aumento considerable en las velocidades de subida y bajada, reflejando una optimización efectiva del ancho de banda.

Las velocidades promedio presentadas se han calculado para representar el rendimiento general del sistema, ya que la extensión y diversidad de la institución hacen que sea impráctico obtener datos exactos en todos los puntos. Estos valores promedio ofrecen una visión precisa del impacto de la actualización, mostrando cómo la capacidad de la red se ha adaptado para garantizar mejoras con respecto a las necesidades de los usuarios en diferentes zonas de la institución. Aunque las velocidades exactas pueden variar entre ubicaciones y momentos, los promedios reflejan la mejora general en el rendimiento de la red, facilitando una experiencia más eficiente y rápida para todos los usuarios.

5.3. Monitoreo del rendimiento de la infraestructura de red

Con la implementación de plataformas avanzadas de monitoreo en los nuevos equipos activos de red, se logró analizar el desempeño de la infraestructura en tiempo real. Estas herramientas permitieron un seguimiento detallado y continuo de todos los componentes de la red, proporcionando un claro prospecto del estado y eficiencia de la misma. La información en tiempo real facilitó la detección proactiva de posibles problemas, optimizando la gestión y asegurando un rendimiento óptimo para todos los usuarios.

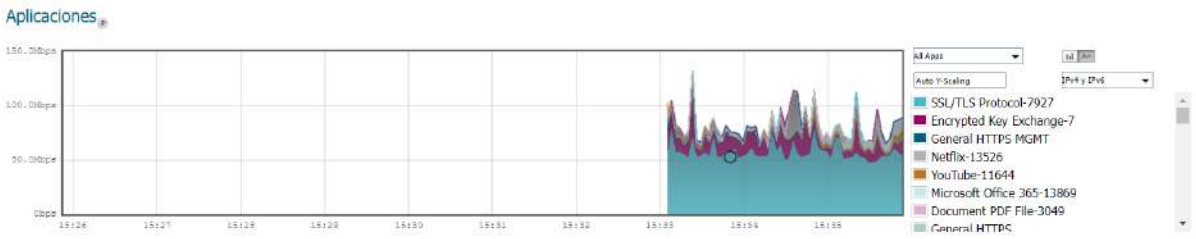

Figura 5.59: Monitoreo de uso de aplicaciones.
Fuente: Autor.

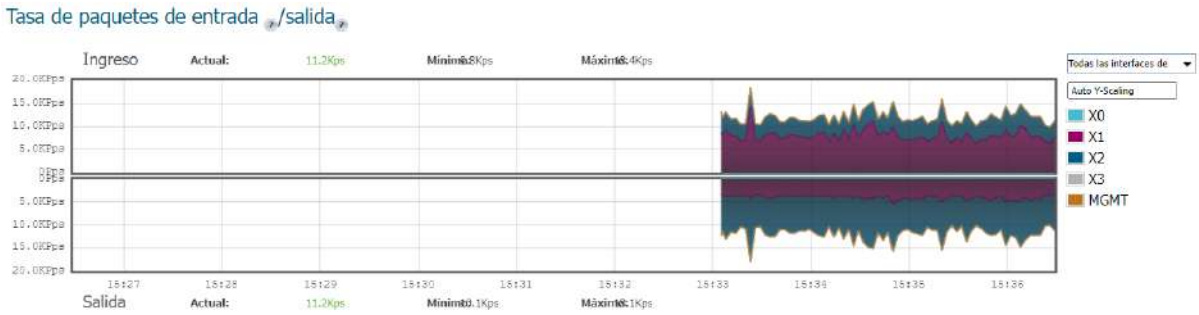

Figura 5.60: Monitoreo de tasa de transmisión de paquetes.
Fuente: Autor.

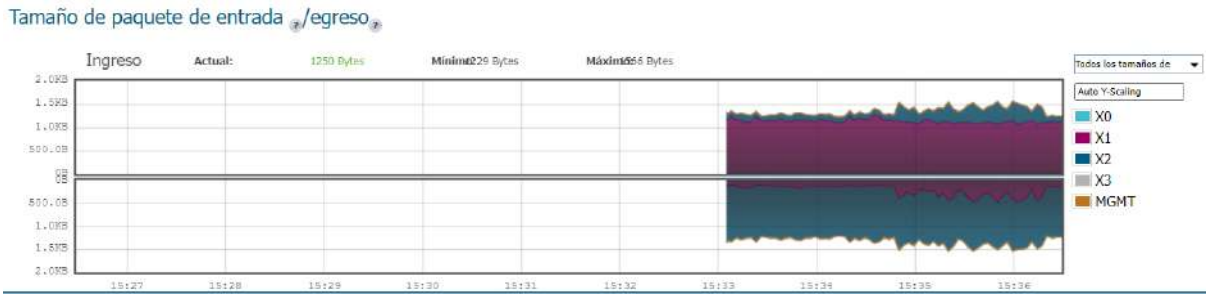

Figura 5.61: Monitoreo de tamaño de paquetes.
Fuente: Autor.

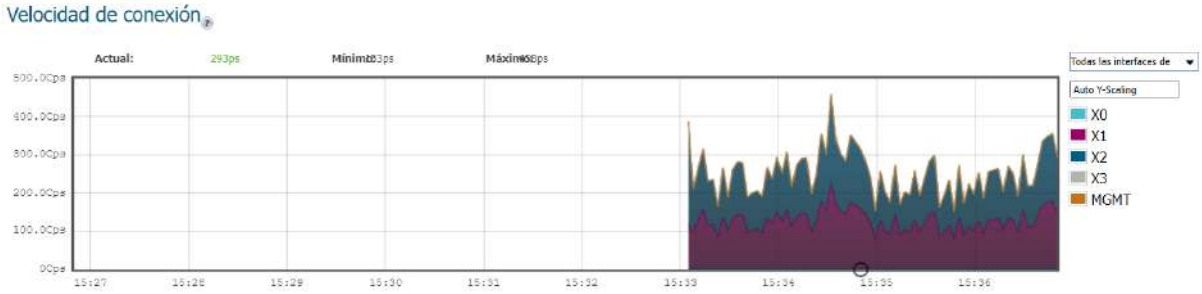

Figura 5.62: Monitoreo de velocidad de conexión.
Fuente: Autor.

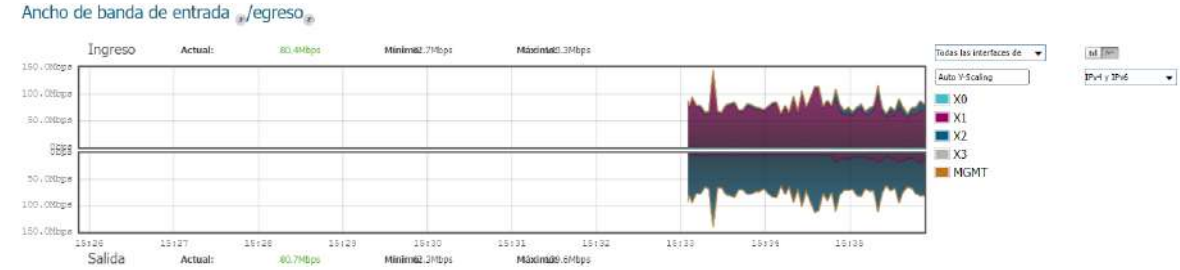

Figura 5.63: Monitoreo de ancho de banda.
Fuente: Autor.

Capítulo 6

Conclusiones y Recomendaciones

6.1. Conclusiones

Es importante destacar que no se consideró el análisis de la zona de cobertura en exteriores para la actualización de la red inalámbrica. Esto se debió a que, al tratarse de una institución salesiana, los patios y áreas al aire libre se destinaban al recreo y actividades físicas de los estudiantes, en lugar de ser utilizados para fines académicos o administrativos que requirieran una conexión constante a la red. La decisión de no incluir estas áreas en el análisis de cobertura se fundamentó en la misión y los valores de la institución, que priorizan la convivencia y el progreso integral de los alumnos a través del juego y la interacción social en espacios abiertos. Además, la cobertura existente en los interiores ya proporcionaba una conectividad óptima para las necesidades tecnológicas de la institución, garantizando que las aulas, cabinas de comunicación, comunidad salesianas, oficinas administrativas contaran con una señal robusta y confiable.

En el futuro, podría tenerse en cuenta la posibilidad de evaluar la cobertura en exteriores si las necesidades de la institución cambian o si se implementan nuevas tecnologías y aplicaciones que requieran una mayor conectividad en todas las áreas del campus. Sin embargo, en el contexto actual, la decisión de enfocar los recursos y esfuerzos en las zonas interiores se alinea con las prioridades y objetivos educativos de la institución.

La simulación de la cobertura de puntos de acceso en distintas zonas del

campus Yanuncay permitió demostrar la importancia y eficacia de la planificación previa en la implementación de redes inalámbricas. A través de simulaciones detalladas, se lograron crear una serie de escenarios que facilitaron el análisis de los rangos de cobertura, identificando áreas con potenciales problemas de conectividad y optimizando las ubicaciones de los AP para lograr una cobertura integral. Esta fase de simulación fue crítica en la planificación y despliegue de la red inalámbrica, asegurando que la implementación en el mundo real fuera exitosa y satisficiera las necesidades de conectividad de la comunidad educativa.

La selección adecuada de equipos de telecomunicaciones y la aplicación de una metodología rigurosa fueron fundamentales para desarrollar una red de datos robusta y eficiente en la UETS. Este enfoque permitió no solo la optimización del rendimiento de la red, sino también la garantía de su sostenibilidad a largo plazo. La infraestructura tecnológica creada apoyó de manera integral tanto el aprendizaje como la administración, proporcionando una base sólida sobre la cual la UETS puede continuar creciendo y evolucionando. Los equipos modernos implementados permitirán monitorear el estado de la red, garantizando su correcto funcionamiento.

El ancho de banda se elevó gracias al cambio de contrato de 200 a 500 Mbps, obteniendo excelentes resultados en términos de velocidad y capacidad de manejo de datos. Con la ayuda del firewall, se pudo gestionar el ancho de banda de acuerdo a las necesidades de la institución. Esto mejoró la capacidad de la institución para manejar grandes volúmenes de datos y facilitó la comunicación y colaboración entre estudiantes, profesores y personal administrativo.

Se debe recalcar que la implementación de un sistema SAI fue crucial para la protección de los equipos de la red contra cortes de energía. Este sistema aseguró que no hubiera interrupciones en el servicio, permitiendo un funcionamiento continuo y estable de la infraestructura tecnológica. El sistema SAI no solo protegió los equipos de posibles daños por fluctuaciones eléctricas, sino que también garantizó que las operaciones críticas pudieran continuar durante cortes de energía, proporcionando tiempo suficiente para la restauración del servicio o para el apagado controlado de los equipos. Esta medida fue vital para garantizar la estabilidad y fiabilidad de la red donde en un entorno educativo la continuidad del servicio es esencial.

6.2. Recomendaciones

Se recomienda continuar con la actualización gradual de los equipos de red activos, incluso si los equipos antiguos siguen funcionando sin problema. Esta práctica asegura que la infraestructura de red permanezca alineada con los avances tecnológicos y las futuras demandas, optimizando el rendimiento, la seguridad y la eficiencia. Los equipos modernos ofrecen mejoras significativas en compatibilidad y capacidades, lo que previene problemas de obsolescencia y facilita la adaptación a nuevas tecnologías, garantizando una red más robusta y escalable a largo plazo.

Para afinar el rendimiento de la red, recomendamos reemplazar todos los enlaces de cableado UTP por enlaces de fibra óptica, incluyendo los que conectan los switches de acceso y otros enlaces relevantes. Aprovechando los puertos libres en el switch de core. Esta actualización mejorará el ancho de banda y la velocidad de transmisión de datos, reduciendo la latencia y eliminando la necesidad de saltos entre equipos.

Recomendamos trasladar los AP ubicados en laboratorios que cuentan con cableado UTP a zonas del campus donde su cobertura pueda ser de mayor utilidad. Este ajuste permitirá aprovechar el cableado existente para optimizar el rendimiento de la red en áreas con alta demanda de conectividad, mientras se maximiza la cobertura y se asegura una distribución más efectiva de los recursos de red en el campus.

Para mejorar la gestión y análisis de la red, se recomienda adquirir la licencia de monitoreo del firewall que permita revisar el estado de la red en tiempo pasado. Por ahora, el monitoreo se limita a tiempo real, por lo que esta licencia adicional proporcionará la capacidad de analizar datos históricos, identificar tendencias y resolver problemas de manera más eficaz al revisar eventos pasados y patrones de tráfico.

Dado el continuo crecimiento de la institución, se recomienda contratar un mayor ancho de banda para anticipar y satisfacer futuras demandas. Los actuales 500 Mbps podrían no ser suficientes para apoyar el aumento en el uso de la red, por lo que una expansión en la capacidad de ancho de banda garantizará un rendimiento óptimo y una experiencia de usuario fluida, alineada con las necesidades en constante

evolución de la UETS.

Para asegurar una fuente de alimentación ininterrumpida en caso de cortes de energía y agotamiento de las baterías, se recomienda adquirir paneles solares para integrar con el sistema SAI. El equipo UPS 3.30 es compatible con alimentación solar, lo que proporcionará un respaldo adicional y redundante, garantizando la continuidad del servicio y la estabilidad de la infraestructura tecnológica durante interrupciones prolongadas o fallos en el suministro eléctrico.

Para consolidar una infraestructura tecnológica uniforme y de alto rendimiento en toda la UETS, es imperativo proceder con la actualización integral de los equipos activos en todos los campus. Esta actualización permitirá una integración coherente y eficaz de los sistemas, optimizando así el rendimiento de la red en toda la institución. Al implementar equipos de última tecnología en cada campus, se garantiza no solo una mayor eficiencia operativa y estabilidad en la conectividad, sino también una base sólida para el soporte continuo de las crecientes demandas educativas y administrativas. Además, esta estandarización facilitará la gestión centralizada de los recursos tecnológicos y la implementación de futuras mejoras, asegurando que todos los campus operen bajo un mismo nivel de excelencia tecnológica y ofreciendo un entorno educativo y administrativo más robusto y resiliente frente a los desafíos tecnológicos futuros.

Glosario

AP Access Point.

CEDIA Corporación Ecuatoriana para el Desarrollo de la Investigación y Academia.

DHCP Protocolo de Configuración Dinámica de Host por sus siglas en inglés Dynamic Host Configuration Protocol.

DMZ Zona Desmilitarizada.

FO Fibra Óptica .

ISP Proveedor de Servicio de Internet .

LAN Red de Área Local por sus siglas en inglés Local Area Network.

MAN Red de Área Metropolitana por sus siglas en inglés Metropolitan Area Network.

Mbps Mega bits por Segundo .

OFDMA Acceso Múltiple por División de Frecuencia Ortogona .

PDF Distribuidor de Fibra Óptico por sus siglas en inglés Optical Distribution Frame.

RRRP Protocolo de Enrutamiento de Router Redundante por sus siglas en inglés Redundant Router Routing Protocol.

SAI Sistemas de Alimentación Ininterrumpida.

SFP Módulo Pluggable de Formato Reducido por sus siglas en inglés Small Form-factor Pluggable.

UETS Unidad Educativa Técnico Salesiano.

UTP Par Trenzado no Apantallado por sus siglas en inglés Unshielded Twisted Pair.

WAN Red de Área Amplia por sus siglas en inglés Wide Area Network.

WLAN Red de Área Local Inalámbrica por sus siglas en inglés Wireless Local Area Network.

Referencias

[1] M. Shea y M. Hentea, «A perspective on wireless networks for education,» en *International Conference on Information Technology: Research and Education, 2003. Proceedings. ITRE2003.*, IEEE, 2003, págs. 640-646.

[2] Q. Zhang, C. Song, Y. Xu y S. Liu, «Research on the Application of Network Technology in Computer Aided Education,» *Highlights in Science, Engineering and Technology*, vol. 92, págs. 432-437, 2024.

[3] D. Hawkridge, *New information technology in education*. Routledge, 2022.

[4] P. S.-C. Goh y N. Abdul-Wahab, «Paradigms to drive higher education 4.0,» *International Journal of Learning, Teaching and Educational Research*, vol. 19, n.º 1, págs. 159-171, 2020. DOI: https://doi.org/10.26803/ijlter.19.1.9.

[5] J. Marugán Merinero, «Diseño de Infraestructura de red y soporte informático para un centro público de educación infantil y primaria,» Universidad Politécnica de Madrid, 2010. dirección: https://oa.upm.es/4976/3/PFC_JUAN_MARUGAN_MERINEROx.pdf.

[6] M. d. R. R. Jiménez, C. E. R. Orozco, J. H. Contreras y M. T. S. Núñez, «educación 4.0: acercamiento a una nueva manera de aprender con herramientas online,» 2020. DOI: https://doi.org/10.33936/cognosis.v5i2.1997.

[7] V. E. Carvajal Barros, «Diseño de cableado estructurado de los laboratorios de la Unidad Educativa Profesor Luis Merani y unión de campus por medio de fibra Óptica,» Universidad de las Américas, Quito, 2018. dirección: http://dspace.udla.edu.ec/handle/33000/8686.

[8] L. I. González-Pérez y M. S. Ramírez-Montoya, «Components of Education 4.0 in 21st century skills frameworks: systematic review,» *Sustainability*, vol. 14, n.º 3, pág. 1493, 2022. DOI: https://doi.org/10.3390/su14031493.

[9] E. A. Yoza Segovia, «Implementación de una Red Inalámbrica para el Acceso a Internet con Tecnología Ubiquiti en la Unidad Educativa Ocho de Enero,» UNESUM, 2020. dirección: http://repositorio.unesum.edu.ec/handle/53000/2265.

[10] TIC NUS, *Infraestructura de una red*, 2023. dirección: https://ticnus.com/noticias/infraestructura-y-redes/infraestructura-de-una-red/.

[11] D. Medianero Huari, «Disponibilidad de datos para trabajo remoto empresa Arteco: actualizando la infraestructura de Red a Cat 6 para implementación de cloud y optimizar la accesibilidad en tiempos de Covid-19,» 2024. dirección: http://repositorio.uigv.edu.pe/handle/20.500.11818/8440.

[12] P. E. G. Trujillo y L. A. C. Quishpe, «Características y ventajas existentes en la conexión inalámbrica y fibra óptica. Una revisión bibliográfica,» *E-IDEA Journal of Engineering Science*, vol. 4, n.º 9, págs. 14-25, 2022. DOI: https://doi.org/10.53734/esci.vol4.id224.

[13] D. M. Andrango Álvaro, «Diseño y simulación de una red MPLS utilizando equipos Mikrotik y el emulador GNS3 en entornos PYMES,» B.S. thesis, Quito: Universidad de las Américas, 2019, 2019. dirección: http://dspace.udla.edu.ec/handle/33000/11528.

[14] J. W. Forero Gandur, «Firewalls a la vanguardia,» B.S. thesis, Universidad Piloto de Colombia, 2015. dirección: http://repository.unipiloto.edu.co/handle/20.500.12277/2875.

[15] W. Odom, *CCENT/CCNA ICND1 100-105 Official Cert Guide* (Official Cert Guide). Pearson Education, 2016, ISBN: 9780134440989. dirección: https://books.google.com.ec/books?id=eeYyDAAAQBAJ.

[16] A. R. Silvera Fernandez, «Implementación de un sistema de acceso a la red de datos para mejorar el control de acceso de los dispositivos microinformáticos en una empresa de fabricación y comercialización de alimentos de consumo masivo-2021,» 2022. dirección: https://hdl.handle.net/20.500.12867/5896.

[17] A. Tanenbaum, N. Feamster, D. Wetherall, V. Campos y J. Gallegos, *Redes de computadoras*. Pearson, 2023, ISBN: 9786073259309. dirección: https://books.google.com.ec/books?id=tU8j0AEACAAJ.

[18] C. A. CHÁVEZ GÓMEZ, «Implementación de Red WiFi en zonas fuera de cobertura del edificio Matriz de la Prefectura de Pichincha,» Tesis doct., Sin Editorial, 2023. dirección: http://repositorio.iti.edu.ec/handle/123456789/842.

[19] IBM, *Network Security*, https://www.ibm.com/es-es/topics/network-security.

[20] D. S. Pacheco, «Seguridad en redes de comunicaciones: Perspectivas y desafíos,» *Ingeniare. Revista chilena de ingeniería*, vol. 30, n.º 2, págs. 215-217, 2022. DOI: http://dx.doi.org/10.4067/S0718-33052022000200215.

[21] L. F. Murcia Fuentes, R. F. Ortiz Pantoja y C. A. Ramírez Gutiérrez, «Optimización integral de infraestructura tecnológica para mejorar la conectividad y accesibilidad en sedes de Murcia SAS mediante servicios de outsourcing de soluciones tecnológicas Ricardo SA,» 2023. dirección: https://hdl.handle.net/20.500.12494/55032.

[22] N. Gangi, «Implementación de redes mesh para IoT,» Tesis doct., Universidad Católica de Córdoba, 2020. dirección: https://pa.bibdigital.ucc.edu.ar/2813/.

[23] B. A. Baque, «Beneficios de implementar una red con tecnología Mesh en las redes inalámbricas Universitarias: Caso de estudio Universidad Estatal del Sur de Manabí,» *Serie Científica de la Universidad de las Ciencias Informáticas*, vol. 13, n.º 11, págs. 185-195, 2020. dirección: https://dialnet.unirioja.es/servlet/articulo?codigo=8590368.

[24] E. Khorov, I. Levitsky e I. F. Akyildiz, «Current Status and Directions of IEEE 802.11be, the Future Wi-Fi 7,» *IEEE Access*, vol. 8, págs. 88 664-88 688, 2020. DOI: 10.1109/ACCESS.2020.2993448.

[25] S. Chauhan, A. Sharma, S. Pandey, K. N. Rao y P. Kumar, «IEEE 802.11be: A Review on Wi-Fi 7 Use Cases,» en *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, 2021, págs. 1-7. DOI: 10.1109/ICRITO51393.2021.9596344.

[26] UNESCO Global Education Monitoring Report, *Tecnología en la educación: ¿Una herramienta en los términos de quién?* 2023. dirección: https://gem-report-2023.unesco.org/es/tecnologia-en-la-educacion/.

[27] H. M. Guimet, «La transformación digital en la educación: la revolución de las TIC,» *Blog de los Estudios de Psicología y Ciencias de la Educación, Universitat Oberta de Catalunya*, 2020. dirección: https://blogs.uoc.edu/epce/es/transformacion-digital-en-la-educaciona-revolucion-tic/.

[28] Universidad Europea, *Tecnología educativa: Importancia y principales usos*, 2023. dirección: https://ecuador.universidadeuropea.com/blog/tecnologia-educativa/.

[29] Leonardo Carvalho, *Nuevas tecnologías en la educación: influencia, ventajas y desafíos*, 2024. dirección: https://www.sydle.com/es/blog/nuevas-tecnologias-en-la-educacion-63ef92977f03ed13ae2d1909.

[30] I. S. Jirikils, «Principales barreras para la modernización de las universidades,» ene. de 2023.

[31] C. Lion, «Los desafíos y oportunidades de incluir tecnologías en las prácticas educativas. Análisis de casos inspiradores,» sep. de 2019. dirección: https://policycommons.net/artifacts/8222378/los-desafios-y-oportunidades-de-incluir-tecnologias-en-las-practicas-educativas/9137178/.

[32] A. Negueruela y B. Torres, *La brecha digital impacta en la educación*, Técnicos de educación en UNICEF España, abr. de 2020. dirección: https://www.unicef.es/educa/blog/covid-19-brecha-educativa.

[33] I. Cisco Systems, *Cisco Support - Switches*, https://www.cisco.com/c/es_mx/support/switches/index.html, 2024.

[34] I. Ubiquiti Networks, *UniFi AP/UAP-LR Quick Start Guide*, 2016. dirección: https://dl.ui.com/guides/UniFi/ES/UAP_UAP-LR_QSG_ES.pdf.

[35] C. E. George Reyes, M. S. Ramírez Montoya, E. O. López Caudana et al., «Imbricación del Metaverso en la complejidad de la educación 4.0: Aproximación desde un análisis de la literatura,» *Pixel-Bit*, 2023. dirección: https://hdl.handle.net/11162/241607.

[36] A. T. S. Ocegueda, E. L. S. Ocegueda y J. M. R. Barajas, «Educación 4.0, modalidad educativa y desarrollo regional integral,» *IE Revista de Investigación Educativa de la REDIECH*, n.º 13, pág. 13, 2022. dirección: https://dialnet.unirioja.es/servlet/articulo?codigo=8626468.

[37] F. Calderón, «FUNDAMENTOS TEORICOS DE EDUCACIÓN 4.0 PARA LA EXCELENCIA ACADEMICA EN EL AMBITO DE LA CUARTA REVOLUCION INDUSTRIAL.,» *TESIS DOCTORALES*, 2021. dirección: https://espacio.digital.upel.edu.ve/index.php/TD/article/view/223.

[38] H. G. Oquendo, L. O. Giraldo et al., «Análisis de riesgos y vulnerabilidades en la educación 4.0 del proceso de enseñanza–aprendizaje.,» *Publicaciones e Investigación*, vol. 16, n.º 1, 2022. DOI: https://doi.org/10.22490/25394088.5615.

[39] E. Muñoz-Guevara, G. Velázquez-García y J. F. Barragán-López, «Análisis sobre la evolución tecnológica hacia la Educación 4.0 y la virtualización de la Educación Superior,» *Transdigital*, vol. 2, n.º 4, págs. 1-14, 2021. DOI: https://doi.org/10.56162/transdigital86.

[40] Huawei Technologies Co., Ltd., *S6730S-S24X6Q Datasheet*, 2024. dirección: https://support.huawei.com/enterprise/en/doc/EDOC1000013621/db1ca75a/s6730s-s24x6q-a-02353ajx-02353ajx-001-02353ajx-003-02353ajx-004.

[41] Cisco Systems, *Cisco Catalyst 9500 Series Switches Data Sheet*, 2019. dirección: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/nb-06-cat9500-ser-data-sheet-cte-en.html.

[42] Juniper Networks, «EX4650 Ethernet Switch Datasheet,» Juniper Networks, inf. téc., 2024. dirección: https://www.juniper.net/content/dam/www/assets/datasheets/us/en/switches/ex4650-ethernet-switch-datasheet.pdf.

[43] Dell SonicWALL, *Dell SonicWALL NSA Series Firewalls*, 2024. dirección: https://www.sonicguard.com/datasheets/nsa/Dell-SonicWALL-NSA-Series-Firewalls-data-sheet.pdf.

[44] Cisco Systems, Inc., *Cisco ASA 5500 Series Next-Generation Firewalls*, https://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/data_sheet_c78-701808.html, 2019.

[45] Fortinet, *FortiGate 100E Series Data Sheet*, 2024. dirección: https://www.avfirewalls.com/datasheets/FortiGate/FortiGate_100E_Series_New.pdf.

[46] A. Networks, «Aruba 500 Series Access Points,» Aruba Networks, inf. téc., 2024. dirección: https://www.arubanetworks.com/es/productos/inalambrico/puntos-de-acceso/puntos-de-acceso-interior/500-series/.

[47] I. Cisco Systems, «Cisco Catalyst 9100AX Access Points,» Cisco Systems, Inc., inf. téc., 2024. dirección: https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access-points/datasheet-c78-741988.html.

[48] U. Inc., *UniFi 6 Pro Datasheet*, 2024. dirección: https://dl.ubnt.com/ds/u6-pro_ds.

[49] Aruba Networks, «Aruba 2530 Switch Series,» Aruba Networks, inf. téc., 2023. dirección: https://www.arubanetworks.com/assets/_es/ds/DS_2530SwitchSeries.pdf.

[50] Cisco Systems, *Cisco Catalyst 9300 Series Switches Data Sheet*, 2023. dirección: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html.

[51] H. P. Enterprise, *HPE OfficeConnect 1950 Series Switches*, 2024. dirección: https://buy.hpe.com/lamerica/es/networking/switches/fixed-port-web-managed-ethernet-switches/1900-switch-products/conmutadores-hpe-officeconnect-de-la-serie-1950/p/7399488.

[52] L. Sungrow Power Supply Co., *Sungrow SG110CX Inverter Datasheet*, 2023. dirección: https://cdn.enfsolar.com/Product/pdf/Inverter/5e69a6523ae49.pdf.

[53] H. Technologies, *125 Gbit/s SFP+ eSFP Optical Module*, Huawei, 2024. dirección: https://support.huawei.com/enterprise/en/doc/EDOC1100043478/9f3a8cfb/125-gbit-s-sfp-esfp-optical-module.

[54] Huawei Technologies Co., Ltd., *1 Gbit/s Electrical Transceiver*, 2024. dirección: https://support.huawei.com/enterprise/en/doc/EDOC1100043478/633dd41/1-gbit-s-electrical-transceiver.