UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TEMA:

ESTABLECIMIENTO DE POLÍTICAS PARA LA GESTIÓN Y ADMINISTRACIÓN DE LOS RECURSOS DE LA RED DE LA UNIVERSIDAD TÉCNICA DEL NORTE, A TRAVÉS DEL MODELO DE GESTIÓN FCAPS DE LA ISO.

Trabajo de Grado previo a la obtención del título de Ingeniería en Electrónica y Redes de Comunicación.

AUTOR:

AXEL ESTEBAN ALMEIDA VINUEZA

DIRECTOR:

Msc. CARLOS ALERTO VÁSQUEZ AYALA

Ibarra, 2023

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

IDENTIFICACIÓN DE LA OBRA

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

DATOS DEL CONTACTO			
CÉDULA DE IDENTIDAD:	100278881-6		
APELLIDOS Y NOMBRES:	Almeida Vinueza Axel Esteban		
E-MAIL:	aealmiedav@utn.edu.ec		
TELÉFONO FIJO:	_	**TELÉFONO MÓVIL:**	0992972587
TÍTULO:	Establecimiento de políticas para la gestión y administración de los recursos de la red de la Universidad Técnica del Norte, a través del modelo de gestión FCAPS de la ISO		
AUTOR(ES):	Almeida Vinueza Axel Esteban		
FECHA: dd/mm/aa	22/03/2023		
PROGRAMA:	■ PREGRADO ☐ POSGRADO		
TÍTULO POR EL QUE OPTA:	Ingeniero en Electrónica y Redes de Comunicación		
TUTOR:	Msc. Carlos Alberto Vásquez Ayala		

CONSTANCIAS

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

Ibarra, a los 8 días del mes de junio de 2023.

EL AUTOR:

Axel Esteban Almeida Vinueza

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCAS APLICADAS

CERTIFICACIÓN:

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

Que el presente trabajo de Titulación ESTABLECIMIENTO DE POLÍTICAS PARA LA GESTIÓN Y ADMINISTRACIÓN DE LOS RECURSOS DE LA RED DE LA UNIVERSIDAD TÉCNICA DEL NORTE, A TRAVÉS DEL MODELO DE GESTIÓN FCAPS DE LA ISO, ha sido desarrollado por el señor Almeida Vinueza Axel Esteban bajo mi supervisión.

Es todo cuanto puedo certificar en honor a la verdad.

MSc. Carlos Alberto Vásquez
DIRECTOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

DEDICATORIA

El presente trabajo de titulación va dedicado a mis padres, ya que ellos han sido el soporte sustancial en este proceso, brindándome siempre su apoyo en las buenas y en las malas, creyendo siempre en mí y valorando cada esfuerzo realizado, soportando mi carácter en los días más difíciles de este difícil proceso, para así llegar a cumplir este tan grande y anhelado objetivo que me he propuesto en esta época de mi vida.

A mis abuelitos que siempre estuvieron al pendiente de mí y siempre brindándome consejos y un cariño incondicional que aprecio y valorare toda mi vida.

Y como no dedicar este logro a todas las personas que estuvieron siempre pendiente del proceso de formación académica.

Axel Esteban Almeida Vinueza

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

AGRADECIMIENTO

Agradezco de todo corazón a toda mi familia, quienes fueron parte de este proceso académico, ya que estuvieron siempre pendiente de mi bienestar y progreso, brindándome un apoyo incondicional para crecer como persona y profesional, a mi madre y padre quienes sin dudar ni un segundo creyeron en mí, a mis hermanos que estuvieron al pendiente de alguna u otra manera y como no, a mi persona por haber mantenido en pie a pesar de toda adversidad para así lograr llegar a cumplir esta meta y así llegar a ser un gran ejemplo a seguir.

A mi querido amigo de 4 patas, Donky, ya que fue uno de los grandes compañeros que me acompañaron durante las duras, frías e interminables madrugadas de esta etapa.

A mi mejor amigo Alejandro Meza y Alejandra Collantes, los cuales me ayudaron a superar muchas etapas de mi vida y me ayudaron a crecer tanto personal como profesional, brindándome un apoyo incondicional con todas sus energías y siempre confiando en mí.

A mis dos grandes mentores: Brian Tracy quien me enseño el gran sentido de la responsabilidad y el TEMACH que me enseñó a valorar mi propio esfuerzo y que, a pesar de ya no querer seguir, debemos confiar en nosotros mismos y llegar a vivir en el modo guerra.

Un gran agradecimiento especial a mi director de tesis el Msc. Carlos Alberto Vásquez ya que a través de sus conocimientos y consejos supo guiarme y aconsejarme a lo largo del desarrollo y culminación de este proyecto.

A mis amigos de aula: Christofer M, Wilmer B, Jean Carlos R, Andy S, Fredy C, Max C, Bryan C, Adonis N, Alexander G y Kevin E; siendo una parte importante en este camino, compartiendo un sin número de emociones positivas y negativas, sabiendo el gran reto que teníamos, el rendirnos nunca fue una opción, para así llegar a sentirnos orgullosos de cada uno de nosotros y así logar culminar este proceso académico.

También un agradecimiento al personal del DDTI, ya que me abrieron muy cordialmente sus puertas y me impartieron sus conocimientos dentro del proceso de este proyecto.

Axel Esteban Almeida Vinueza

RESUMEN

Este proyecto tiene como finalidad administrar y gestionar los recursos y dispositivos que se encuentren dentro de la red inalámbrica y cableada de la Universidad Técnica del Norte, a través del modelo de gestión FCAPS de la ISO, en el cual, con la ayuda del software de gestión Cisco DNA Center se permitirá obtener más información sobre el estado actual de la red, lo cual permitirá que se realice una gestión adecuada de los recursos físicos y lógicos que se encuentran en la red.

A través de la gestión y el monitoreo constante del software de Gestión Cisco DNA Center se permite visualizar histogramas, mapas unifilares de calor, reportes, generación de alertas a problemas mediante niveles de prioridad, todo esto con la finalidad de mantener un óptimo servicio a los usuarios de la red del campus de la UTN. Las herramientas que posee el software de gestión ayudan a generar una respuesta rápida y eficiente ante problemas que se susciten tanto en la red cableada como inalámbrica, ya que el administrador de red tendrá mayor disponibilidad de información al momento de suscitarse cualquier eventualidad, permitiendo que se disminuyan dichos problemas que ocurren en la red.

Mediante el establecimiento de políticas y manuales de procedimientos, se establecieron guías para cada ámbito del modelo de gestión FCAPS, lo cual ayudará a la planificación, organización, supervisión y control de los dispositivos de la red inalámbrica y cableada, ya que el administrador de red que se encuentre en el Departamento de Desarrollo Tecnología e Informático (DDTI) tendrá el objetivo de brindar un servicio de calidad y siempre en total disponibilidad.

ABSTRACT

The purpose of this project is to manage and administer the resources and devices within the wired and wireless network of the Technical University of the North, through the FCAPS management model of ISO, in which, with the help of the Cisco DNA Center management software, more information about the current state of the network will be obtained, which will allow for proper management of the physical and logical resources within the network.

Through constant management and monitoring of the Cisco DNA Center management software, histograms, heatmaps, reports, and problem alerts can be visualized and generated through priority levels, all with the aim of maintaining optimal service to the users of the UTN campus network. The management software tools help generate a quick and efficient response to any problems that may arise in both the wired and wireless network, as the network administrator will have greater availability of information in case of any eventuality, allowing for the reduction of such network issues.

By establishing policies and procedure manuals, guidelines were established for each area of the FCAPS management model, which will aid in the planning, organization, supervision, and control of the devices within the wired and wireless network. The network administrator in the Technology and Information Development Department (DDTI) aims to provide quality service and always maintain total availability.

ÍNDICE

INDICE DE FIGURAS

INDICE DE TABLAS

1. ANTECEDENTES

1.1. Problema

A menudo que se van retomando las actividades diarias dentro de la Universidad Técnica del Norte, habrá mayor afluencia y congestión en la red por parte de los usuarios que quieran acceder a esta, entonces establecer políticas de gestión y administración para la red de la Universidad técnica del Norte se convierte en un pilar fundamental para que los usuarios tengan un acceso y servicio a la red óptimo, dando así el espacio apto para los usuarios puedan realizar sus diferentes actividades laborarles dentro de la Universidad Técnica del Norte.

La administración actual de la Universidad Técnica del Norte no tiene un enfoque definido de cómo resolver ciertos problemas de red que se susciten con el retorno progresivo a las actividades presenciales, lo cual da el punto de partida para establecer políticas de gestión y administración de la red ya sea cableada o inalámbrica.

A través de la realización de dicho proyecto se quiere llegar a implementar políticas de gestión y administración para los usuarios de la red de la Universidad Técnica del Norte, las cuales permitirán obtener una óptima gestión de la red ya que dicha red requiere de un monitoreo continuo de su estado y así poder obtener una adecuada gestión de los recursos de la red de la universidad Técnica del Norte.

El Departamento de Desarrollo Tecnológico e Informático (DDTI) de la Universidad Técnica del Norte-Ibarra debe estar en constante evolución tecnológica ofreciendo una mejor disponibilidad y funcionalidad de la red, realizando registros e informes en forma sistematizada de los comportamientos que suceden en la red, por lo tanto es fundamental basarse en un modelo de gestión que pueda cubrir dichas necesidades para la monitorización

de los equipos con la finalidad de tener conocimiento del estado de los recursos de la red, garantizando la estabilidad de la misma mediante detección, aislamiento y resolución de fallas.

1.2. Objetivos

1.2.1. Objetivo General

Implementar políticas de gestión y administración, para la red de la Universidad Técnica del Norte, haciendo el uso del modelo FCAPS de la ISO.

1.2.2. Objetivos Específicos

- Detallar los fundamentos teóricos del modelo de FCAPs, modelo de políticas, red inalámbrica y red cableada.
- Determinar el estado actual de la red mediante el monitoreo continuo de la red inalámbrica y cableada a través del uso del sistema de gestión DNA que incluyen los equipos de distribución y núcleo.
- Establecer políticas de administración y gestión según el modelo de gestión FCAPS y la implementación de los recursos de la red.
- Implementar políticas de administración y gestión en la red de la Universidad Técnica del Norte según el modelo de gestión FCAPS.
- Verificar el funcionamiento de las políticas que determine una optimización de la gestión de la red.

1.3. Alcance

Mediante el estudio, análisis, levantamiento y planteamiento de información del modelo FCAPS, y el estado actual de la red inalámbrica y cableada de la Universidad técnica

del Norte se logrará determinar los diferentes problemas que hay dentro de la red lo cual permitiría establecer las políticas de gestión y administración para cada área funcional del modelo FCAPS.

El proyecto tiene como finalidad crear políticas de gestión y administración y verificar su correcto funcionamiento tanto para la red inalámbrica como red cableada a través del sistema de gestión DNA, todo esto apoyándonos en el estudio de las áreas funcionales del modelo FCAPS (Fallos, Configuración, Contabilidad, prestaciones y Seguridad) de la ISO, logrando así obtener el correcto funcionamiento de dicha red y la optimización de los recursos existentes, por ende en la Figura 1 se presente el proceso (arquitectura) para la realización del proyecto.

Dentro del modelo de administración en el ámbito de gestión de fallos se deberá detectar las diferentes anomalías de la red como localizar, corregir y diagnosticar problemas tanto para la red inalámbrica como para la cableada de la Universidad Técnica del Norte mediante el servidor DNA el cual notificaran al administrador de la red que tipo de problema está sucediendo y este así podrá brindar una solución eficiente y eficaz, permitiendo obtener una red más confiable y estable tanto para el usuario como para el administrador.

En el ámbito de la gestión de configuraciones se trabajara con el objetivo de realizar un análisis de la situación actual del estado físico y lógico en el que se encuentra la red inalámbrica y la red cableada lo cual permitirá determinar que equipos son de mayor prioridad, obtener registros e informes de cambios de configuraciones y que los cambio de las configuraciones sean de forma activa para así poder tener la supervisión y control de los mismos para una gestión total de la red de la Universidad Técnica del Norte.

La gestión de administración se enfocará en el registro de la utilización de los recursos y servicios prestados por la red a los usuarios ayudando así a definir niveles de tráfico entrante y saliente en puntos críticos, notificación de alertas, el uso total del ancho de banda que se ha

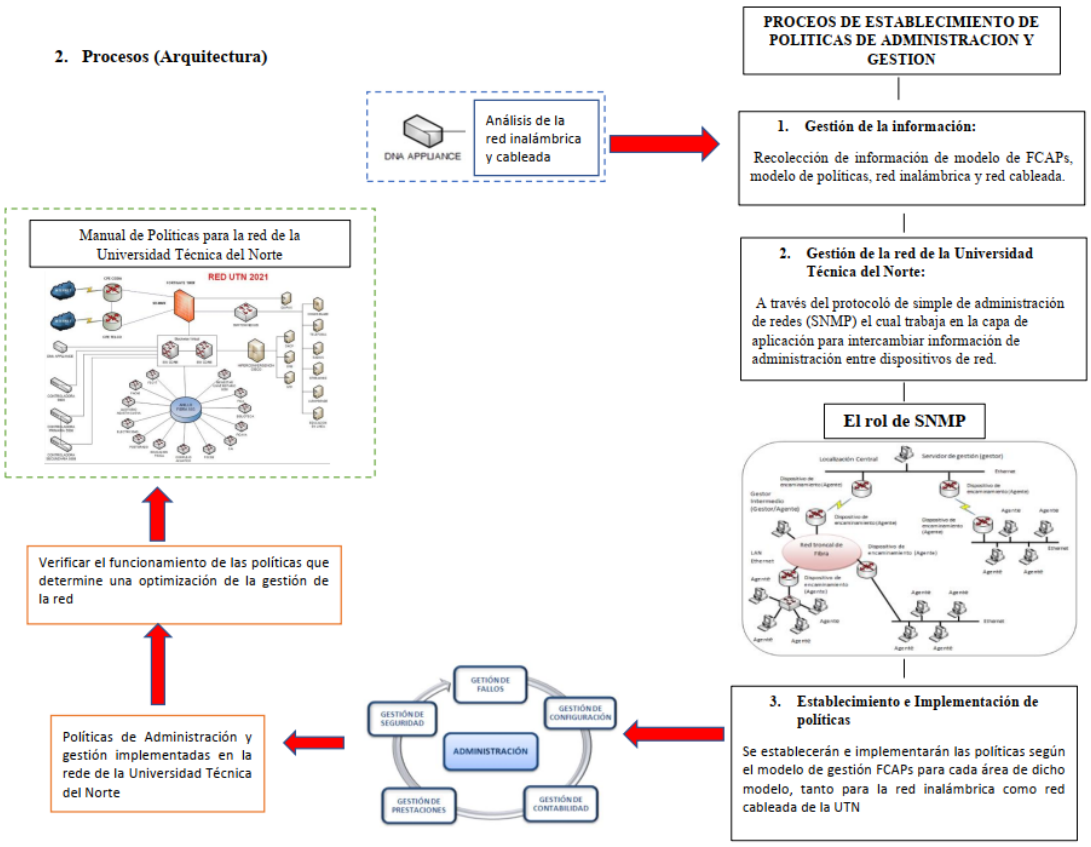
venido utilizando durante cierto tiempo, esto dependiendo de las necesidades a cada punto de acceso y así poder tener un mayor análisis y una mejor administración del consumo de los recursos de la red inalámbrica y cableada de la Universidad Técnica del Norte.

Para llegar a obtener una adecuada administración de la red de la Universidad Técnica del Norte en el ámbito de la gestión de prestaciones, se realizará mediciones del rendimiento de los recursos de la red mediante monitoreos continuos a los equipos de red través del sistema de gestión DNA para la red inalámbrica y la red cableada que incluyen los equipos de Core distribución y acceso logrando así obtener reportes, colección de datos estadísticos e historiales, por ende esto hará que se facilite la disponibilidad de información para que el equipo del DDTI permitiendo mejorar el rendimiento de la red y a través de manuales de procedimientos y configuraciones donde se especifiquen los parámetros de las herramientas (software y hadware), llegar a obtener soluciones a cualquier inconveniente que se presente al instante entonces tomando en cuenta el aumento de equipos en la red y a partir de dichos reportes e información a obtener se partirá para la creación de las políticas de administración y gestión de la red de la Universidad Técnica del Norte.

La gestión de seguridad será la encargada de llevar a cabo y hacer cumplir los controles de acceso, comprobar la identidad de usuarios (autenticación, certificación), protección de la red y la garantía de confidencialidad total para el equipo del DDTI al sistema de gestión de equipos e información, logrando así cumplir el objetivo de administrar y brindar la respectiva seguridad de la red inalámbrica como cableada de la Universidad Técnica del Norte.

Figura 1

Arquitectura



Fuente: Autor propio

1.4. Justificación

La Universidad Técnica del Norte es una institución de educación superior, pública y acreditada que forma profesionales de excelencia, éticos, críticos, humanistas, líderes y emprendedores con responsabilidad social y para ello brindan el uso masivo de tecnólogas de la información y la comunicación (TIC) en distintas áreas, lo cual permite implementar un modelo de gestión de red, ya que es un requerimiento fundamental para el correcto funcionamiento y disponibilidad de la red inalámbrica y cableada de la Universidad Técnica del Norte

Se ha hecho énfasis en conocer el estado actual de los recursos que conforman tanto la red cableada como inalámbrica con la finalidad de prevenir fallos, detectar problemas en

tiempo real y así poder anticiparse, reaccionar a estos imprevistos en el caso de que se produzcan, logrando tener las herramientas necesarias y un equipo totalmente capacitado para atender cualquier inconveniente.

Dentro de la Universidad Técnica del Norte habido un crecimiento exponencial de dicha red, esto conlleva a implementar un modelo de gestión de red ya que el personal del DDTI ha observado fallos en ciertas áreas críticas en la red inalámbrica como cableada, por lo cual se procede a realizar un estudio, monitoreo actual de la red para poder mitigar cualquier fallo que se presente y así obtener una visión en tiempo real del estado de los recursos de la red y mejorar su rendimiento, todo esto fundamentado en el modelo FCAPS de la ISO ya que a partir de dicho modelo se establecerán políticas de administración y gestión para cubrir las necesidad de la red de la Universidad Técnica del Norte.

Con la implementación del modelo de gestión de red, se podrá brindar mejores servicios, en los que los responsables de la gestión de la red inalámbrica y cableada se verán directamente beneficiados porque podrán trabajar de manera eficiente y sin problemas, por lo que los usuarios tendrán un servicio de calidad y presto para cualquier trabajo a realizar.

2. MARCO TEÓRICO

2.1. Redes Cableadas

Las redes cableadas se las identifican por su tipo de medio de transmisión (generalmente basada en Ethernet), dichos cables con conductores (CAT 5) los cuales interconecta computadores y otros dispositivos que forman las redes. Las redes cableadas son mejores cuando se necesita transmitir grandes cantidades de datos a altas velocidad, como contenido multimedia de calidad y de manera fiable.

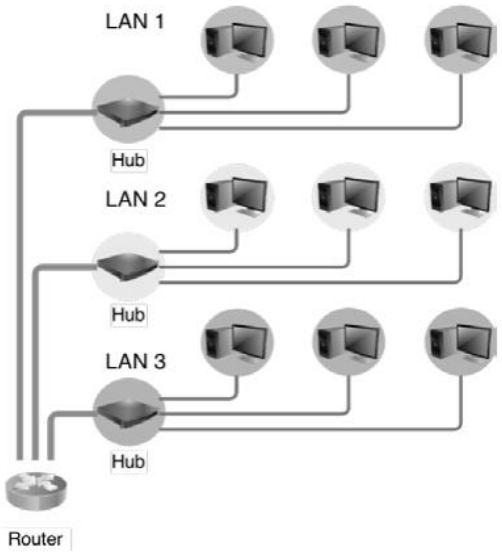
2.1.1. Características

"Las redes LAN ocupan áreas geográficas pequeñas, por ejemplo, un edificio o conjunto de edificios. Generalmente se trata de redes cuyo tendido obedece a la necesidad de compartir recursos, tales como impresoras, scanners y dispositivos de almacenamiento." (Cristina Liberatori, 2018, pág. 30)

La principal característica de una red cableada es que su tendido se realiza sobre un cable del tipo par trenzado, esto puede variar dependiendo del medio de trasmisión que se vaya a utilizar en la comunicación de la red. Una red cableada es caracterizada por interconectar dispositivos tales como computadores personales, repetidores o hubs, puentes y conmutadores o switches tal y como se representa en la Figura *2*. El mantenimiento de las redes cableadas queda a cargo de administradores, ya sean propietarios de las mismas o contratados para tal efecto.(Cristina Liberatori, 2018)

Figura 2

Red LAN cableada.



Nota: A las redes LAN cableadas se las conoce también por su nombre genérico Ethernet. Las redes LAN cableadas alcanzadas altas velocidades en la actualidad. Tomado de (Redes de Datos y sus Protocolos (pág. 31), por Cristina Liberatori 2018)

2.1.2. Desventajas

- El diseño para las redes cableadas es mucho más costoso y necesitan ser físicamente instaladas en postes y paredes. Se debe tener un buen diseño de la red LAN ya que de este dependerá su capacidad y como se lo visualice estéticamente.
- Las redes LAN son más propensas a daños físicos externos ya que un tropezón con el cable, un terremoto o algún daño causado por algún agente externo del ambiente puede llegar a dejar inhabilitada a toda una red.
- Existe la posibilidad que dentro de la red LAN si un equipo principal como un servidor este defectuoso pueda causar una sobrecarga de las demás

computadoras, lo cual puede causar daños y dichos daños se visualizaran en toda la red.

- Las redes LAN tienen un gran problema de incompatibilidad de sistemas ya que a la hora de integrar nuevos equipos y sistemas pueden darse determinados errores que dificulten el trabajo con ellos.
- Las interferencias por los diferentes tipos de cables son un problema que puede darse por emplearse diferentes tipos de cableados estructurados ya que, al conectar entre ellos, puede generarse interferencias que dificulten el acceso y tratamiento de la información.
- Una de las desventajas más comunes de las redes LAN es que al pasar el tiempo el cable se va deteriorando y no sea reutilizable, haciendo imposible que se pueda utilizar para otros fines.

2.2. Redes Inalámbricas

Las redes inalámbricas mencionan un sistema de comunicación que utiliza ondas electromagnéticas para establecer conexiones con dispositivos sin necesidad de ningún tipo de cable. Este tipo de redes brindan ventajas de movilidad a los usuarios ya que a través de su conexión inalámbrica pueden estar conectados en el lugar que sea, todo esto posible mientras estén dentro del rango de la red inalámbrica, también provee la posibilidad de conectar u integrar varios terminales a su vez en una red ya sea domestica o empresarial, teniendo en cuanto que también hace posible la compatibilidad con las redes LAN Ethernet. Antes de describir las características se recuerda que las redes inalámbricas como tales, se encuentran reguladas y trabajan bajo la responsabilidad de organismos internaciones como: ITU, ISO y así junto a la IEEE desarrollaron el estándar IEEE 802.11. Las WLANs crecen exponencialmente y es por ello por lo que deciden expandirse con más normas 802.11 y sus derivados, tal y como se representa en la Figura *3*, ya que prestan mayores beneficios como el

bajo coste de la infraestructura, facilidad de despliegue y compatibilidad con la comunicación con otros equipos y tecnologías. (Ruiz et al., 2018)

Figura 3

Principales normas IEEE 802.11

Standard	Scope
IEEE 802.11a	Physical layer: 5-GHz OFDM at rates from 6 to 54 Mbps
IEEE 802.11b	Physical layer: 2.4-GHz DSSS at 5.5 and 11 Mbps
IEEE 802.11c	Bridge operation at 802.11 MAC layer
IEEE 802.11d	Physical layer: Extend operation of 802.11 WLANs to new regulatory domains (countries)
IEEE 802.11e	MAC: Enhance to improve quality of service and security mechanisms
IEEE 802.11g	Physical layer: Extend 802.11b to data rates >20 Mbps
IEEE 802.11i	MAC: Enhance security and authentication mechanisms
IEEE 802.11n	Physical/MAC: Enhancements to enable higher throughput
IEEE 802.11T	Recommended practice for the evaluation of 802.11 wireless performance
IEEE 802.11ac	Physical/MAC: Enhancements to support 0.5–1 Gbps in 5-GHz band
IEEE 802.11ad	Physical/MAC: Enhancements to support ≥ 1 Gbps in the 60-GHz band

Nota. Las normas IEEE ha crecido con respecto a sus normas 802.11 ya que existe mayor demanda en el mercado y se deben acoplar a dichas necesidad y demandas de acorde a las necesidades de usuarios y a la compatibilidad con otras tecnologías. Tomado de (Data and Computer Communications (pág. 400), por William Stallings, 2014)

2.2.1. Características

Las redes inalámbricas poseen características que otras tecnologías no las poseen y por ello este tipo de tecnologías son mayormente deseas y contratadas en el mercado.

A continuación, se describen alagunas de las características que brindan las redes inalámbricas.(Behrouz A. Forouzan & Firouz Mosharraf, 2012)

- **Atenuación**

Según Andrea et al., (2018), “La señal se dispersa en todas las direcciones provocando que se disminuya la fuerza de las señales electromagnéticas.”

- **Interferencia**

Cuando se trabaja a las mismas bandas de frecuencias existe el riesgo que el receptor no solo reciba la señal del emisor si no de otros emisores que trabajen en las mismas dichas bandas de frecuencias.

- **Propagación Multitrayecto**

Diferentes ondas electromagnéticas pueden reflejarse en obstáculos como paredes, objetos e incluso el aire, provocando así que el receptor reciba más de una señal del emisor a diferentes fases, lo cual hace que la potencia de la señal disminuya o sea menos reconocible para el emisor.

- **Error**

Una característica importante en las redes inalámbricas es la relación señal/ruido ya que aquí se toma en cuenta parámetros como detección, corrección de errores y la retransmisión, entonces dicho de otra manera la SNR no es más que la medición de la relación entro lo bueno y lo malo (señal y ruido).

> Si la SNR es alta, significa que la señal es más fuerte que el ruido (señal no deseada), por lo que podremos convertir la señal en datos reales. Por otro lado, cuando la SNR es baja, significa que la señal está corrompida por el ruido y los datos no pueden recuperarse.(Behrouz A. Forouzan & Firouz Mosharraf, 2012, pág. 482)

- **Traspaso/Roaming**

El roaming se vuelve importante en las WLAN ya que permita que las estaciones móviles se desplacen de una célula a otra.(William Stallings, 2014)

2.2.2. Desventajas

- El funcionamiento de dos o más WLANs en la misma zona hará que haya mayor interferencia entre las LANs.
- Existe mayor riesgo en la perdida de datos ya que toda la información viaja a través de ondas electromagnéticas.
- La velocidad de datos será menor ya que dependerá de la calidad de la señal que emane el dispositivo (AP).
- Las redes WLANs tiene una menor seguridad y por ello son más propensas a ataques de hackers
- Las WLANs son más propensas a las interferencias de otros señales y objetos que se encuentren en el medio ambiente como las paredes.

2.3. Modelo de gestión de red funcional basada en estándar ISO

La gran demanda en el área de las telecomunicaciones ha hecho que cada vez sea más importante utilizar un modelo de gestión de red funcional, lo cual hará que dicha red trabaje de manera más eficiente y eficaz logrando así también obtener robustes en la infraestructura física y lógica tanto para la red inalámbrica y cableada, todo esto permitirá un seguimiento en tiempo real a través de monitoreos en la red, esto llevara a explotar todos los recursos de dicha red para así cumplir con el objetivo principal de brindar un excelente servicio al usuario final que en este caso serían los clientes.(Consultivo, 1993)

Para ello se toma en cuenta el modelo de FCAPS de la ISO como base fundamental que se lo utiliza para comparar las capacidades y características de los sistemas de gestión y supervisión donde los operadores de la red y los proveedores de servicios llegan a comprender el funcionamiento de los sistemas de gestión y monitorización de redes.

La disponibilidad de la red y la capacidad para poder integrar servicios de mayor calidad se lo puede determinar en la organización de dicha red porque así a través de la organización, esto se lleva a cabo ya sea con un modelo o sin un modelo que determinara la calidad de servicio que presta sus usuarios o clientes.

Entonces el modelo FCAPS es un modelo para permitir que los usuarios describan y organicen funciones en las siguientes áreas: gestión de fallas, gestión de la configuración, contabilidad, gestión de prestaciones (rendimiento) y gestión de seguridad.(New et al., 2012)

2.3.1. Fundamentos de Gestión de Red

Dentro de la gestión de red se definen los recursos disponibles, de tal manera que a través de una correcta gestión de red se establezcan actividades de inicialización, monitorización y control, todo ello con la finalidad de evitar llegar a tener fallas de funcionamiento restando disponibilidad en sus prestaciones (rendimiento) y así cumplir con los requisitos del usuario para los cuales se está prestando el servicio. (Manuel Mora, 2014)

La administración y gestión son términos importantes que se emplearan en este proyecto y también son términos relevantes a la hora de monitorizar y control fallos en una red, entonces para ellos se procederá a definir el termino de administración y gestión.

2.3.1.1. Administración de Red

Los administradores de red son los encargados de gestionar el conjunto de acciones que permiten evaluar y mantener en condiciones óptimas las redes de comunicaciones de una organización, a la vez que elabora e implementan estrategias de mejoras, también se incluye el despliegue, mantenimiento y monitoreo del engranaje de la red: switches, routers, cortafuegos, entre otros. Las actividades de administración de una red por lo general incluyen la asignación de direcciones, asignación de protocolos de

ruteo y configuración de tablas de enrutamiento, así como, configuración de autenticación y Autorización de los servicios. (Montes Castañeda & Solano Solano, 2019, pág. 13)

La administración de redes es un conjunto de técnicas tendentes a mantener una red operativa, eficiente, segura, constantemente monitoreada y con una planificación adecuada y propiamente documentada.

Sus objetivos son:

- Mejorar la continuidad en la operación de la red con mecanismos adecuados de control y monitoreo, de resolución de problemas y de suministro de recursos.
- Hacer un uso eficiente de la red y utilizar mejor los recursos, como, por ejemplo, el ancho de banda.
- Reducir costes por medio del control de gastos y de mejores mecanismos de cobro.
- Hacer la red más segura, protegiéndola contra el acceso no Autorizado, haciendo “imposible” que personas ajenas puedan obtener la información que circula por ella.
- Controlar cambios y actualizaciones en la red de modo que ocasionen las menos interrupciones posibles en el servicio a los usuarios. (BRIHUEGA, 2015, pág.136)

2.3.1.2. Gestión de Red

Sosa Sosa, (n.d.) ha afirmado lo siguiente:

La gestión de red es clave en toda organización porque es un conjunto de herramientas integradas las cuales ayudan a la monitorización y control de la red ya que con ello lo que se quiere una planificación, organización, supervisión y control de los elementos de comunicaciones por ende todo ello hará reducir los riegos y costos asociados con el funcionamiento de una red para así poder garantizar un servicio adecuado que sea proporcional a su costo. (pág. 3)

2.3.2. Necesidad de la gestión de red

Según ManageEngine, n.d. menciona lo siguiente:

La necesidad de gestionar una red de manera más optima hoy en día es muy importante, ya que en cualquier empresa o entidad se quiere garantizar la prestación continua de los servicios y poder llegar a obtener un sistema de administración de red solido capaz de administrar redes físicas (alambicas e inalámbricas).

Dentro de las necesidades de la gestión de red en las telecomunicaciones promueven las siguientes razones (Romero, s.f):

- Entornos Heterogéneos: Respecto a la Información que transportan y respecto a la organización.
- Recursos ilimitados para las organizaciones.
- Nuevos retos debido a la gran variedad de nuevas tecnologías y gran número de fabricantes
- Mayor disponibilidad de la red.
- Mayor exigencia por parte de los usuarios: navegación más rápida, segura y multifuncional.
- Reducir costos y fallos en la red

- Monitoreo continuo, prevención y solvencia de los problemas de la red.
- Brindar un servicio de calidad.

2.3.3. Elementos de un sistema de gestión de red

"La gestión de redes tiene tres componentes principales: un centro de gestión, un dispositivo gestionado y un protocolo de gestión de redes. Se especifica en las RFC de Internet y otros documentos, un típico sistema de gestión distribuido que comprende:" (Ding, 2010, pág. 45-45)

Se define a un elemento de red como un nodo de red el cual lleva a un agente SNMP y este se aloja en una red gestionada.

2.3.3.1. Centro de Gestión

Un centro de gestión está conformado por el administrador de la red y sus instalaciones.

2.3.3.2. Dispositivos Gestionados

En el ámbito de los dispositivos gestionados se encuentran todos los equipos que establezcan una comunicación en la red, esto con la finalidad de ser controlados o monitoreados y como ejemplos de dispositivos gestionados se encuentran los puentes, hubs, routers o servidores de red.

2.3.3.3. Gestor

Este gestor es un dispositivo autónomo el cual se maneja a través de un sistema compartido y este recibe notificaciones mediante los agentes. En cualquier caso, la estación de gestión sirve como interfaz entre el administrador de red humano y el sistema de gestión de red.

- Un conjunto de aplicaciones de gestión para el análisis de los datos, recuperación de fallos, etc.
- Una interfaz a través de la cual el gestor de red puede monitorizar y controlar la red.
- La capacidad de traducir los requisitos del administrador de la red en la monitorización y control reales de los elementos remotos de la red.
- Una base de datos de información de gestión de red extraída de las bases de datos de todas las entidades de la red gestionadas. (Stallings, 2004)

2.3.3.4. Agentes

Cuando nos referimos a un agente de gestión nos referimos a un elemento activo en el sistema de gestión de red ya que dichos agentes son módulos de software de administración el cual se lo encuentra en un nodo administrado. Dichos agentes cumplen con diferentes funciones como recolectar información local de gestión como (direcciones IP, número de paquetes de error recibidos por un elemento de red, memoria, rutas, etc.) y luego de haber recolectado información se procede a almacenarla en una base de datos de gestión la cual es trasformada de manera que esta llegue a ser compatible con SNMP para finalmente brindar a las entidades de gestión dentro del sistema de gestión de red (NMS) a través de un protocolo de gestión de red. Otra funcionalidad que tienen estos agentes es que responden a solicitudes de información y en el caso de que se realicen cambios desde la estación gestionada llegaran a brindar a la estación información importante que no se haya solicitado de manera asíncrona. En la actualidad hay exponencial y potencialmente muchos agentes en un sistema de red.

2.3.3.5. Estación de gestión de red o Network Management Station (NMS)

Los dispositivos NMS son conocidos como consolas y dichos dispositivos ejecutan aplicaciones de gestión que supervisan y controlan permanente todos los elementos de la red

administrados. En el aspecto físico los NMS suelen ser ordenadores robustos y semejantes a una estación de trabajo de ingeniería con CPUs rápidas, gran cantidad de memoria y mayor cantidad de espacio en el disco. En cualquier entorno de una red administrada deben estar presente al menos uno o más gestores.

2.3.3.6. Protocolo de gestión de red

La estación de gestión (NMS) y los agentes establecen conexión para poder transmitir la información ya que estos están enlazados por un protocolo de gestión. En la gestión de redes el protocolo utilizado es el TCP/IP ya que este es el Protocolo Simple de Gestión de Red (SNMP), el cual dicho protocolo de gestión es el estándar de facto de la comunidad de Internet.

2.3.3.7. Base de información de Gestión (MIB)

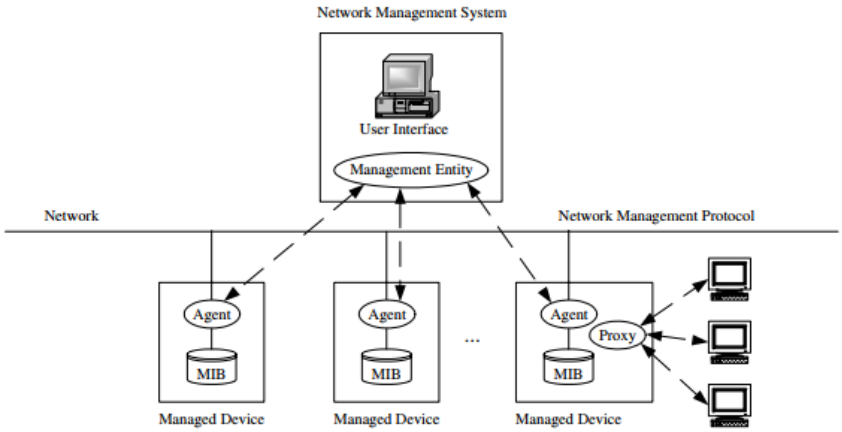
En el modelo de gestión de redes OSI/ISO existe una base de información de gestión conocida como colección de objetos (MIB), la cual es un tipo de base de datos que se utiliza para poder gestionar los dispositivos en una red, de tal manera que funciona como una colección de puntos de acceso para la gestión en el agente. Dentro de la MIB se comprende una colección de objetos en una base de datos (virtual) que se la utiliza para gestionar entidades como routers y switches. (Stallings, 2014; Ding, 2010).

Una MIB suele ser sólo un trozo de papel que dice cosas como "el primer campo es alfanumérico, de 20 caracteres, y contiene el nombre del proveedor" y "el quinto campo es un número entero y contiene el número de paquetes malos recibidos". Todo ello se traduce a traves de un "lenguaje" especial de la ISO llamado ASN.1 (Notación de Sintaxis Abstracta versión 1) para representar todos los campos de la base de datos MIB en un lenguaje muy escueto y críptico que todos los implementadores de MIB entienden.(Goralski, 2017, pág. 716)

Entonces el papel que desempeñara la MIB se lo represeanta en la Figura *4*, ya que se basa al momento de gestionar cada entidad, definira el numero de objetos, nombrara según las reglas establecidad en SMI y asociara un tipo a cada objeto nombrado. En resumen la MIB crea una colección de objetos con nombre, sus tipos y sus relaciones entre sí en una entidad a gestionar.(Behrouz A. Forouzan & Firouz Mosharraf, 2012, pág. 708)

Figura 4

Arquitectura de gestión de redes



Nota: Los elementos más básicos de un modelo de gestión de red se representan gráficamente dentro de la arquitectura básica de gestión de redes. Tomado de Advances in Network Management (p.48), por Ding J, 2010, Taylor & Francis Group

2.3.4. Modelo de gestión FCAPS de la ISO

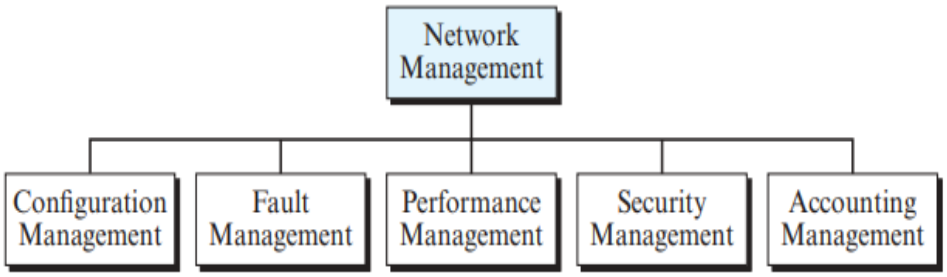
“El modelo ISO (Organización Internacional de Normalización) para clasificar los procesos funcionales que deben realizarse en la gestión de redes informáticas y de telecomunicaciones es el modelo que subyace a todos los protocolos y marcos de gestión de redes.” (Clark, 2003, pág 393)

En la norma ITU-M.3400 se explica sobre la red de gestión de la telecomunicación (RGT), mientras que en las recomendaciones de la serie UIT-T X.700 se requiere una gestión

OSI para varios fines. Los aspectos en los que se requiere gestión se agrupan en cierto número de áreas funcionales donde se definen 5 áreas funciones llamadas SMFA (Systems Managemetn functional Areas), más conocidas como modelo FCAPS (Faul, Configuración, Accuonting, Permormance and Security), dicho modelo se representa en el mapa de la Figura *5*, mediante sus 5 áreas y dentro del modelo funcional se trabaja con el protocolo SNMP(Simple Network Management Protocolo) ya que dicho protocolo hace que se facilite el intercambio de información de gestión entre dispositivos de una red, mientras que el protocolo CMIP es el que brinda un mecanismo de trasporte en la forma de servicios pregunta-respuesta para las 7 capas del modelo OSI.

Figura 5

Áreas de gestión de red o áreas funcionales



Nota: Para este proyecto se implementará el modelo de gestión ya que este modelo viene dado por un esquema de funcionamiento de gestión en las diferentes áreas de aplicabilidad y dentro de estas áreas de gestión de red se encuentran: gestión de configuración, de prestaciones, de fallos, de seguridad y de contabilidad. Tomado de (Computer Networks. A Top-Down Approach (p.702), por Behrouz A. Forouzan & Firouz Mosharraf, 2012, Tata McGraw Hill)

2.3.4.1. Gestión de Fallas

La gestión de fallos es un conjunto de funciones que tiene como objetivo detectar, aislar y corregir los fallos en una red. En el ámbito de la gestión de fallas se incluye el

mantenimiento, aceptación y actuar sobre las notificaciones de detección de errores, localizar y rastrear los fallos mediante una secuencia de pruebas de diagnósticos para así llegar a corregir los fallos e informar al administrador de red en qué condiciones se encuentra dicha red. El protocolo SNMP cumple con la función de notificar al operador si se produce un fallo o un evento dentro de la red. Los fallos son un problema operativo importante y difícil de resolver ya que en una red existe un gran número de componentes implicados, amplia distribución física de los recursos y heterogeneidad de los componentes de hardware y software.(Boston et al., 2009; Ding J, 2010)

Los mensajes sobre los fallos suelen ser transmitidos por los propios componentes o por los usuarios del sistema. Algunas de las fuentes de fallos son las vías de transmisión de datos (por ejemplo, cable transceptor, cable de par trenzado, fibra óptica, líneas alquiladas, canales virtuales), los componentes de la red (por ejemplo, transceptores, repetidores, puentes, acopladores en estrella, ordenadores servidores, terminales de datos), los sistemas finales, el software de los componentes, las descripciones inadecuadas de las interfaces (de forma indirecta) o incluso el funcionamiento incorrecto.(Boston et al., 2009, p. 90)

Existen dos maneras principales para realizar la gestión de fallos:

Gestión de fallos Pasiva. – El protocolo SNMP recoge las alarmas de los dispositivos cuando se detecta algún percance. Para este tipo de fallos solo determinan si un dispositivo que esta monitoreado es lo suficiente apto como para generar un error e informarlo a la herramienta de gestión ya que si el dispositivo que se está monitorizando falla completamente o se bloquea no lanzará una alarma y no se detectará el problema.

Gestión de fallos Activa. – Este tipo de gestión trata los problemas de la red a través de un monitoreo continuo, supervisión activa de los dispositivos mediante herramientas como el PING, para así lograr detectar si el dispositivo esta activo y responde. Cuando el

dispositivo deja de responder se enviará una alarma mediante la monitorización activa donde indicará si el dispositivo no está disponible, lo cual permitirá dar una corrección práctica al problema.

Ding, (2010), en su trabajo presentado menciona 3 pasos básicos con los cuales se trabaja en la gestión de fallos:

- **Detección de fallos**

Detectar la causa de uno o varios fallos en la red es importante ya que es un proceso de adquisición de indicaciones que se presentan en manera de alarmas de (usuarios o de herramientas), mostrando el mal funcionamiento o desorden que presenten los dispositivos que se encuentran en la red.

- **Aislamiento de fallos**

Al aislamiento de fallos se lo conoce también como localización de fallos, correlación de eventos y análisis de la causa raíz. En esta etapa se analizan las indicaciones de los fallos detectados para así lograr determinar el problema que se encontró a través de las alarmas recibidas. Este proceso es importante ya que depende de gran medida la velocidad y precisión del proceso de gestión de fallos.

- **Corrección de averías o fallos**

La corrección de los fallos en una red se define por ser un paso de planificación ya que hace referencia al seguimiento del fallo, observación de síntomas persistentes del fallo, responsabilidad de la reparación del fallo y del control de los procedimientos que utilizan los recursos redundantes todo esto con la finalidad para llegar a sustituir los equipos o instalaciones que han fallado.

2.3.4.2. Gestión de Configuraciones

Para que una red funcione de manera óptima, adecuada y haga lo que se supone que tiene que hacer, debe mantener la información de las configuraciones actualizadas para que así logre realizar el proceso de obtención de datos de la red y luego ajustarla en respuesta a los requisitos cambiantes de dicha red.

La gestión de configuraciones está compuesta por tareas básicas que son las siguientes (Ding, 2010):

- Facilitar la creación de controles.
- Supervisar y hacer cumplir las normas de referencia para hardware y software específicos.
- Almacenar los datos de configuración y mantener un inventario actualizado de todos los componentes de la red.
- Registrar e informar de los cambios en las configuraciones, incluida la identidad del usuario.
- Respaldo mediante copias de seguridad de las configuraciones de red para restáurala en caso de fallos.
- Configuración remota.

"La gestión de la configuración de la red tiene que ocuparse del funcionamiento detallado de la configuración del hardware y de la configuración del software de la red como se detalla a continuación:" (Ding, 2010, pág. 113)

- **Gestión de la configuración del hardware**

La gestión de configuración de hardware es el proceso de crear y mantener un registro actualizado de todos los componentes de la infraestructura, incluida la documentación

relacionada. Su propósito es mostrar los componentes de la infraestructura e ilustrar la ubicación física y los vínculos entre cada elemento, que se denominan elementos de configuración.

- **Gestión de configuración de software**

La gestión de configuración de software incluye procesos a la red, los cuales se mencionan a continuación:

- Identificación de la configuración

La identificación de configuraciones denota un proceso de identificación de los atributos que definen todos los elementos de configuración. Existe una documentación de configuraciones donde se encuentran registrados los atributos mencionados.

- Control de cambios en la configuración

El control de cambios de configuración es el conjunto de procesos y pasos de aprobación necesarios para cambiar los atributos de un elemento de configuración y así poder reajustarlo.

- Administración del estado de configuración

Es la facultad de registrar, informar y reportar las configuraciones asociadas con cada elemento de configuración teniendo en cuenta que esto se debe hacerlo en cualquier momento.

- Autenticación de la configuración

Esta autenticación de configuraciones hace referencia a realizar auditorías de configuración de manera funcional y física de tal manera que esto se produce al momento de entrega o ejecución de un cambio. Para una auditoria de configuración funcional se debe

garantizar que se cumplan con los atributos funcionales y de rendimiento de un elemento de configuración, mientras que para una auditoria de configuración física se debe asegurar que un elemento de configuración se instala de igual manera que los requisitos de la documentación detallada.

2.3.4.3. Gestión de Contabilidad

La gestión de contabilidad se basa en la recopilación de datos estadísticos sobre el procesamiento de información que realizan los usuarios en la red. Y mediante la recolección de datos que realiza la estadística se puede llegar a realizar la correcta facturación de los usuarios y aplicar las cuotas de uso. Una correcta medición de los parámetros de utilización de la red permite regular adecuadamente los recursos individuales o grupales que brinda la red. La correcta regularización de los recursos minimiza los problemas en la red (ya que los recursos de la red se pueden repartir en función de las capacidades de los recursos) lo cual ayuda a maximizar la igualdad del acceso a la red entro los usuarios.

Según Ding, 2010, la gestión de contabilidad desempeña tareas/servicios que realiza el personal contable, a continuación, se mencionan los siguientes:

- Utilización de los recursos de la red
- Análisis de las variaciones
- Análisis de tarifas y volúmenes
- Desarrollo de métricas de negocio
- Modelización de precios
- Rentabilidad del producto
- Análisis coste-beneficio
- Análisis coste-volumen-beneficio
- Análisis de la rentabilidad del cliente

- Información de facturación
- Planificación estratégica
- Asesoramiento en gestión estratégica
- Previsión de ventas y financiera
- Asignación y utilización de recursos
- Regulación de usuarios o grupos
- Ayudar a mantener el rendimiento de la red en un nivel aceptable

Nota: En la red de la Universidad Técnica del Norte no se aplicará el procedimiento de tarifación ya que es una entidad pública y sin fines de lucro que brinda servicios al pueblo, teniendo en cuenta que no se llevara a cabo todas las actividades que se presenten dentro de la gestión de contabilidad.

2.3.4.3.1. Consideraciones

Dentro de esta área de gestión funcional se presentan ciertas consideraciones a tomar en cuenta(Guerrero Pantoja, 2011):

- Identificar y definir los niveles de tráfico entrante y saliente en puntos clave.
- Definir niveles de conectividad ente dispositivos.
- Constatar la capacidad libre que posee un disco duro.
- Los niveles de procesamiento que se muestren por parte del uso del procesador permitirán identificar la cargar procesal a la que está expuesta dicho equipo en la red: niveles que permiten evaluar cambios o revisiones del flujo de trabajo y servicios ejecutado.
- La contabilización de alarmas mediante los registros que los mismos generan permite evaluar cuáles son los eventos más recurrentes y fortalecer las medidas para solventarlos.

- Evaluar los recursos utilizados por parte de los usuarios en función de las estadísticas de interfaces y protocolos permite contabilizar su uso y redistribuir adecuadamente los recursos por bloques.
- Contabilizar las estadísticas entorno a los enlaces que posee la Institución evidencia los niveles de trabajo y periodos de mayor actividad.

Los puntos detallados anteriormente se pueden evidenciar a través de reportes y graficas que permitan al administrador de red contabilizar de manera correcta las medidas a tomarse según las necesidades de la institución.

2.3.4.4. Gestión de Prestaciones

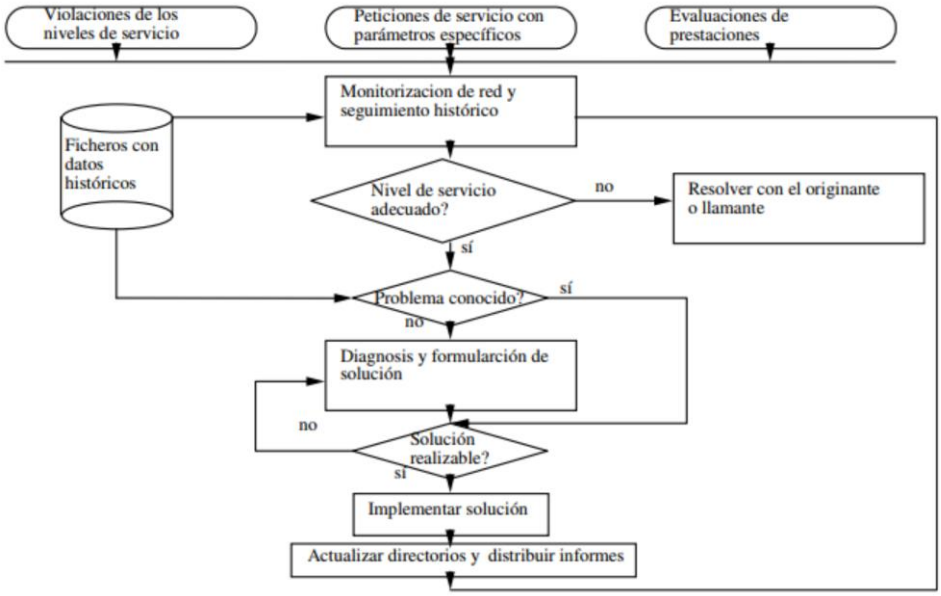
Clark (2003) ha afirmado lo siguiente:

> La gestión del rendimiento es la tarea de gestionar los flujos de tráfico en una red viva: supervisar los flujos de tráfico en los enlaces individuales con respecto a los valores de umbrales críticos y ampliar la capacidad de los enlaces o cambiar la topología añadiendo nuevos enlaces. Es la tarea de garantizar que el rendimiento cumple el objetivo de diseño (por ejemplo, el acuerdo de nivel de servicio). (pág. 394)

Existen indicadores dentro de la gestión de prestaciones que pueden definir los que están orientados a los servicios, disponibilidad, tiempo de respuesta y la fiabilidad. Mientras que en otros indicadores se resaltan la orientación a la eficiencia, como el troughput(canal, flujo) o la utilización, por ello se presenta el proceso de gestión de prestaciones en la Figura 6.

Figura 6

Proceso de gestión de prestaciones.



Nota: En el diagrama se observa el proceso a seguir por una aplicación de gestión de prestaciones hasta encontrar los parámetros de funcionamiento óptimos en la red. Tomado de (Gestión de red (pág. 91), por Barba Martí, 1999)

2.3.4.4.1. Métricas de rendimiento

Según(Clemm, 2006) “Existen varias características de rendimiento las cuales se llegan a medir según las métricas. Las unidades de comunicación dependen de la capa, el tipo de red y el servicio de red en cuestión, a continuación, algunos ejemplos”:

- El número de bytes, octetos, que se trasmiten por segundo dependen de la capa de enlace.
- El número de paquetes que se enrutan por segundo se lo encuentra en la capa de red.
- En la capa de aplicación de un servicio web, el número de solicitudes web que se atienden por segundo.

- En la capa de aplicación de un servicio de voz, el número de llamadas de voz, o intentos de llamada, que se pueden procesar por hora.

La utilización está estrechamente relacionada con el rendimiento. Mientras que el rendimiento es un número absoluto (como el número de bytes por segundo), la utilización es un número relativo que expresa el rendimiento como un porcentaje de la capacidad máxima teórica del sistema subyacente.

2.3.4.4.2. Tareas centrales en la gestión del rendimiento

A continuación, se mencionará dos tareas fundamentales para la gestión del rendimiento:

- **Supervisión (análisis del rendimiento)**

Esta tarea consiste en obtener las tasas de utilización, error de los enlaces, dispositivos actuales en la red, reunir información sobre el tráfico (ya sea sobre tasas de error, rendimiento, pérdidas, utilización, colisiones, volumen, matriz), mientras que para los servicios (protocolos, sobrecarga, matriz, tiempo de respuesta) y también se toma en cuenta a los recursos ya que estos pueden ser la utilización de la CPU, memoria disponible, utilización del disco, puertos.

- **Control (planificación de la capacidad)**

El control propone realizar una línea base de las métricas de utilización para así aislar cualquier problema o anomalía que existente, llegando a tomar acciones para planificar o modificar las configuraciones y capacidades de la red para alcanzar u obtener el rendimiento esperado.

Un punto principal para la gestión del rendimiento es tener la garantía de la calidad del servicio en la red. La gestión del rendimiento toma mayor importancia a medida que

aumenta la relación cliente-servidor en la implantación de redes corporativas o sistemas distribuidos.

2.3.4.5. Gestión Seguridad

La gestión de seguridad hace referencia al conjunto de reglas o funciones que protejan a la red y los sistemas de acceso no Autorizado de personas, actos o influencias, todo esto a través de un análisis de amenazas que incluyen subfunciones, como la creación, la eliminación y el control de los servicios y mecanismos de seguridad; la distribución de información relevante para la seguridad; la notificación de eventos relevantes para la seguridad; el control de la distribución del material de claves criptográficas; y la Autorización del acceso, los derechos y los privilegios de los abonados. Entonces gran parte de la gestión de seguridad se enfoca en proteger los recursos de una empresa y a garantizar que el acceso a la gestión este restringió a los usuarios no Autorizados. La información, las infraestructuras informáticas, los servicios y la producción representan valores que están expuestos a amenazas de ataque o de uso indebido. Las medidas de seguridad que reflejan los resultados de los análisis de las amenazas o de los riesgos de seguridad son necesarias para evitar daños y pérdidas. (Boston et al., 2009; Ding, 2009);

Según Boston et al., (2009); Ding, (2009), existen amenazas típicas que son creadas por:

- Ataques pasivos: escucha de información; producción de un perfil de usuario o un análisis de flujo de tráfico no deseado o robo de información (contraseñas, etc.).
- Ataques activos: enmascaramientos (es decir, usuarios que se hacen pasar por otra persona, o spoofing); manipulación de secuencias de mensajes cambiando la secuencia, repetición inadmisible, dando prioridad o retrasando los

mensajes; modificación de mensajes; manipulación de recursos mediante sobrecarga, reconfiguración, reprogramación, etc. (acceso no Autorizado, virus, troyanos, ataques de denegación de servicio).

- Mal funcionamiento de los recursos.
- Comportamiento defectuoso o inadecuado y funcionamiento de respuesta incorrecta.

Clark, (2003), afirmo Las funciones de gestión de la seguridad incluyen:

- identificación, validación y Autorización de los usuarios de la red y de los operadores de gestión de la red;
- seguridad de los datos;
- confirmación de las acciones de gestión de la red solicitadas, (comandos que crean o pueden crear trastornos importantes en la red o el servicio)
- registro de las acciones de gestión de la red (con fines de recuperación cuando sea necesario, y también para la auditoría de fallos); y
- el mantenimiento de la coherencia de los datos mediante una gestión estricta de los cambios.

2.3.4.5.1. Tareas de la gestión de seguridad

Según (Ding, 2009) "Un ejemplo para un subsistema de gestión de seguridad es que el administrador pueda supervisar a los usuarios que se conectan a una red de manera inapropiada y así poder denegarles el acceso. Entonces existen tareas básicas dentro de un sistema de gestión de seguridad las cuales son:" (pág. 95)

- La información y los dispositivos serán identificados mediante el control de acceso a los recursos de la red por medios físicos y lógicos.

- Implementar un esquema de detección de intrusiones en la red para mejorar la seguridad del perímetro
- Las políticas de cifrado son importantes para proteger la información que sea o este muy vulnerable.
- Tener respuestas automáticamente a las violaciones e intentos de seguridad con operaciones predefinidas a través de las políticas establecidas.

"Las herramientas de gestión, como la clasificación de la información, la evaluación de riesgos y el análisis de riesgos, se utilizan para identificar las amenazas, clasificar los activos y calificar las vulnerabilidades del sistema para poder aplicar un control eficaz."(Ding, 2009, pág. 95)

2.4. Protocolo Simple Gestión de Red (SNMP)

El protocolo simple de gestión de red más conocido como (SNMP) se utiliza en internet ya que utiliza el conjunto de protocolos TCP/IP, este protocolo fue diseñado para que los dispositivos y protocolos de red de internet puedan permitir la gestión remota sobre la red ya sea en el ámbito de la supervisión y control. SNMP es un protocolo que trabaja a nivel de capa aplicación (capa 7), es decir, es transportado por el protocolo de datagramas de usuario UDP en el puerto 161 por defecto.

El protocolo SNMP trabaja bajo el concepto de gestor y agente lo cual quiere decir que un gestor se refiere a un host que controla y supervisa a un conjunto de agentes en este caso a los routers o servidores, es por ello por lo que el protocolo está diseñado a nivel de capa aplicación ya que podrá monitorizar y supervisar en diferentes redes a los diferentes dispositivos de los diferentes fabricantes. En la información que es transportada por SNMP puede ser una orden para establecer un parámetro determinado en el dispositivo remoto, una solicitud con la finalidad de obtener información del estado actual de la red (supervisión de la

red a distancias lejanas) o simplemente una respuesta a una solicitud.(Behrouz A. Forouzan & Firouz Mosharraf et al, 2012)

2.4.1. Componentes de SNMP

SNMP utiliza dos protocolos adicionales para realizar las tareas de gestión, los cuales son: Estructura de a información de gestión (SMI) y Base de información de gestión (MIB). Entonces la corporación de los tres protocolos: SNMP, SMI y MIB hacen posible la gestión en internet. (Behrouz A. Forouzan & Firouz Mosharraf, 2012, pág. 707)

2.4.1.1. Estructura de la información de gestión (SMI)

Las reglas que se definen en el SMI para describir la información de gestión utilizan un subconjunto de ASN.1. Dentro del protocolo SNMP existe un árbol de Estructura de Información de Gestión conocido como (SMI) que está vigente en el RFC 1155, también consta en la norma ISO 10165, donde se denomina Modelo de Información de Gestión (MIM), también consta en las normas UIT-T X.720, X.721 y X.722.(Goralski, 2017)

De acuerdo con Behrouz A. Forouzan & Firouz Mosharraf (2012), “SMI es un protocolo que define las reglas generales para nombrar objetos, definir tipos de objetos (incluyendo rango y longitud) y mostrar cómo codificar objetos y valores. Sin embargo, debemos entender que SMI sólo define las reglas; no define cuántos objetos se gestionan en una entidad ni qué objeto utiliza cada tipo. SMI es una colección de reglas generales para nombrar objetos y listar sus tipos. La asociación de un objeto con el tipo no la hace SMI.” (pág. 708)

El protocolo SMI es una directriz para SNMP, el cual recalca 3 atributos para manejar un objeto: nombre, tipo de datos y método de codificación. A continuación, sus funciones:

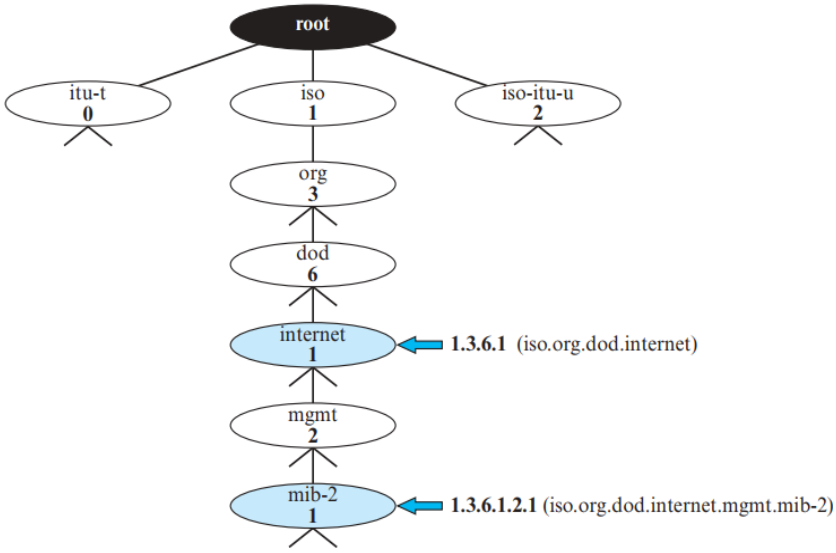
- Nombrar objetos

- Definir el tipo de datos que se puede almacenar en un objeto.
- Visualizar como se codifican los datos para su transmisión por la red.

El Identificador de objeto en SMI se lo visualiza en manera de árbol en la Figura 7, entonces dentro del protocolo SMI cada objeto gestionado (como un enrutador, una variable en un enrutador, un valor, etc.) tenga un nombre único.(Behrouz A. Forouzan & Firouz Mosharraf, 2012)

Figura 7

Identificador de objeto en SMI



Nota. La figura representa el árbol de un Identificador donde para nombrar los objetos de forma global y SMI utiliza un identificador de objeto, que es un identificador jerárquico basado en una estructura de árbol. Tomado de (Computer Networks. A Top-Down Approach (pág. 710), por Behrouz A. Forouzan & Firouz Mosharraf, 2012)

2.4.2. Versión SNMP

"El diseño modular de SNMP se muestra en la consistencia de la arquitectura, la estructura y el marco de las tres versiones; esto ayuda a la evolución gradual de las mejoras del protocolo."(Ding, 2010, pág. 72)

La versión de SNMPv1 era sencilla, fácil de implementar y por ello tenía sus problemas y limitaciones. Ya que existían problemas y limitaciones en SNMPv1 dan paso a la versión de SNMP, SNMPv2 la cual corregía fallos de la versión anterior y sin embargo todavía existían problemas como la deficiencia de seguridad, la privacidad de datos, suplantación de identidad y la divulgación no Autorizada de datos. Entonces tras el planteamiento de dos versiones de SNMP que aun tenían fallos ven la necesidad de desarrollar una versión de SNMPv3 para solucionar las deficiencias en el ámbito de funciones de seguridad, control de acceso, autenticación y el cifrado de los datos de gestión.(Ding, 2010).

2.4.2.1. SNMP versión 1

Ding (2010) ha afirmado lo siguiente:

> En la gestión de redes estándar de internet dentro de los RFCs 1155, 1157 y 1212 se describen al protocolo SNMPv1. Existen tres comunidades en SNMPv1: solo lectura, lectura-escritura y trap.
>
> En SNMPv1 la seguridad se base en las comunidades, lo cual indican que son contraseñas: trabaja de manera que utilizan cadenas de texto plano lo cual permitan a cualquier aplicación basada en SNMP conocer las cadenas para acceder a la información de gestión de un dispositivo. (pág. 73)

2.4.2.2. SNMP versión 2

Ding (2010) afirmo lo siguiente:

> SNMPv2 es una versión mejorar de SNMPv1 y se la encuentra dentro de (RFCs 1901, 1905 a 1909, y 2578 a 2580). Los elementos de SNMPv2, proporciona un marco sobre el que se pueden construir aplicaciones de gestión de redes, como la gestión de

fallos, la supervisión del rendimiento, la contabilidad, etc., que quedan fuera del ámbito de la norma. SNMPv2 proporciona la infraestructura para la gestión de la red.

La esencia de SNMPv2 es un protocolo que se utiliza para intercambiar información de gestión. Cada "jugador" del sistema de gestión de red mantiene una base de datos local de información relevante para la gestión de la red, conocida como MIB. El estándar SNMPv2 define la estructura de esta información y los tipos de datos permitidos; esta definición se conoce como la estructura de la información de gestión (SMI).

SNMPv2 admite tanto una estrategia de gestión de red muy centralizada como una distribuida. Normalmente, SNMPv2 se implementa sobre el protocolo de datagramas de usuario (UDP), que forma parte del conjunto TCP/IP. Dado que los intercambios de SNMPv2 son de naturaleza de pares discretos de solicitud-respuesta, no se requiere una conexión fiable continua. no se requiere una conexión continua y fiable.

2.4.2.3. SNMP versión 3

William Stallings (2007) afirmó lo siguiente:

SNMPv3 se publicó como un conjunto de normas propuestas en enero de 1998 (actualmente RFCs 2570 a 2575). Este conjunto de documentos no proporciona una capacidad completa de SNMP, sino que define una arquitectura general de SNMP y un conjunto de capacidades de seguridad.

SNMPv3 proporciona tres servicios importantes: autenticación, privacidad y control de acceso. Los servicios de seguridad se rigen por la identidad del usuario que solicita el servicio; esta identidad se expresa como una identidad principal, que puede ser un individuo o una aplicación o un grupo de individuos o aplicaciones. (pág. 769-770)

2.5. Plataforma DNA

2.5.1.1. Introducción.

El Centro Cisco DNA (Digital Network Architecture) es un potente controlador de red y panel de administración que, a través de la recopilación continua de datos de una multitud de fuentes de dispositivos y aplicaciones, puede ayudar a crear una red automatizada. Ya que mediante la información que analiza el DNA, se quiere llegar a obtener una red que esté funcionando de forma segura. El Cisco DNA se adapta fácilmente al entorno para apoyar las necesidades de acorde al negocio ya que es un sistema que está en constante aprendizaje.

Cisco DNA Center es utilizado para el aprovisionamiento de una red ya que es el centro de gestión y mando de esta, por lo cual hace que sea fácil de usar para los ingenieros de en redes. El DNA Center brinda la comodidad de automatizar la red ya que se puede gestionar de manera sencilla y eficiente las operaciones, lo cual permitiría disminuir los tiempos de inactividad en dicha red. Cisco DNA Center es una plataforma de hardware y software que proporciona un "panel único" (interfaz única). Se centra en el aseguramiento, el análisis y la automatización.(IPCisco, 2020)

Para las nuevas gestiones de redes el DNA Center utiliza tecnologías como la inteligencia artificial (AI) y el Aprendizaje Automatizado (ML), estos sistemas permiten que la gestión de redes se vuelva proactiva, operaciones más eficaces y las resoluciones de problemas sean más rápidas.

El DNA Center funciona básicamente a través de su interfaz de red el cual se programa y luego envía los datos a Cisco DNA Center Appliance. El DNA Center Appliance es el dispositivo en el que realiza las actividades necesarias, tal como se visualiza en la

Figura ***8*** ya que se puede realizar configuraciones, ajustes, agregación de dispositivos en edificios, etc. Mediante la utilización de este software de automatización puede hacer lo

que necesite en su red. Todas las actividades mencionadas anteriormente pueden visualizarse en el Dashboard del DNA center, el cual es la interfaz gráfica de usuario (GUI), que ve el usuario. El DNA Center utiliza las APIs REST en la interfaz Northbound. Con estas APIs REST, los desarrolladores y usuarios pueden comunicarse con el DNA Center. En la interfaz Southbound, el DNA Center utiliza varios protocolos como RESTCONF, NETCONF, etc. Con esta interfaz, el DNA Center puede comunicarse con los dispositivos que gestiona. En esta interfaz hay tanto dispositivos que soportan protocolos SDN como NETCONF, RESTCONF, etc. como dispositivos tradicionales que soportan SNMP, Telnet, SSH.(Adroit Information Technology Academy (AITA) et al. 2022)

Cisco DNA Center proporciona un panel único para cada tarea de administración fundamental para simplificar el funcionamiento de su red.

- **Diseño (Design):** Para el diseño de una red se utilizará flujos de trabajo intuitivos, de manera que inicialmente se tome en cuenta las ubicaciones de donde se desplegaran los sus dispositivos de red.
- **Política (Policy):** Una prioridad dentro de las políticas es definir perfiles de usuarios y de dispositivos que facilite un acceso altamente seguro y tenga una segmentación de la red adecuada basada a las necesidades del uso de la red. Las políticas de aplicación permitirán que sus aplicaciones criticas brinden un nivel un constante rendimiento, independientemente de la congestión que se encuentre en la red.
- **Aprovisionamiento (Provision):** Utilice la automatización basada en políticas para suministrar servicios a la red en función de la prioridad empresarial y para simplificar la implantación de dispositivos. Las funciones de aprovisionamiento de dispositivos sin intervención y de gestión de imágenes de software reducen el tiempo de instalación o actualización de los

dispositivos de horas a minutos y ponen en línea nuevas oficinas remotas con la facilidad de plug-and-play desde un dispositivo Cisco ya existente.

- **Garantía (Assurance):** Dentro de la garantía se permitirá que cada punto de red se convierta en un sensor el cual permitiría enviar telemetría de flujo continuo sobre el rendimiento de las aplicaciones y la conectividad de los usuarios en tiempo real. Entonces con las características de la visibilidad automática de las turas y la corrección guiada, permitirá resolver las situaciones de riesgo dentro de la red en minutos antes de que se conviertan en problema mayores.
- **Plataforma (Platform):** Tener una plataforma abierta y extensible permite que aplicaciones y procesos de terceros intercambien datos e inteligencia con Cisco DNA center, esto permitira mejorar las operaciones de TI ya que al automatizar los procesos de flujo de trabajo en función de la inteligencia de red proveniente de Cisco DNA Center.(Cisco, 2022, pág. 3)

Figura 8

Representación de las tareas administrativas del Cisco DNA Center

Nota. Cisco DNA Center es un software central de gestión y automatización, una aplicación, que se utiliza como controlador para Cisco DNA. Cisco DNA Center es un

potente controlador de red y panel de administración que le permite hacerse cargo de su red, optimizar su inversión en Cisco y reducir su gasto en TI. Tomado de (Cisco, 2022a)

2.5.1.2. Especificaciones del hardware del dispositivo.

La controladora Cisco DNA suministra el centro de Arquitectura de Red Digital de cisco, de manera que la presenta en forma de aparato físico montado en bastidor. La versión actual que trabaja en la red de la Universidad Técnica del Norte es el: Dispositivo de 44 núcleos: Número de pieza de Cisco DN2-HW-APL. (Cisco, 2022b)

A continuación, mediante la Tabla 1 se presenta las especificaciones de hardware del Core Cisco DNA Center.

Tabla 1

Especificaciones de hardware del dispositivo Cisco DNA Center de 44 núcleos

Rasgo	Descripción
Chasis	Chasis de una unidad de rack (1RU).
Procesadores	Dos procesadores Intel 6238 de 2,1 GHz de 22 núcleo
Memoria	Ocho DIMM registrados (RDIMM) DDR4 de 2933 MHz de 32 GB
Almacenamiento	• 2 x 480 GB in RAID 1 • 2 x 1.9 TB in RAID 1 • 6 x 1.9 TB in RAID 10
Administración de discos (RAID)	• RAID 1 en las ranuras 1 a 4 • RAID 10 en las ranuras 5 a 10
I/O de gestión y red	Conectores compatibles: • Dos puertos Ethernet de 10 Gbps en la NIC Intel X710-DA2

	• Un puerto de gestión RJ-45 de 1 Gbps (Marvell 88E6176) • Dos puertos LOM 10GBase-T (controlador Intel X550 integrado en la placa base). Los siguientes conectores están disponibles, pero no suelen utilizarse en el funcionamiento diario del Cisco DNA Center: • Un puerto serie RS-232 (conector RJ-45) • Un conector VGA (DB-15) • Dos conectores USB 3.0 • Un conector KVM del panel frontal que se utiliza con el cable KVM, que proporciona dos USB 2.0, un VGA (DB-15) y un puerto serie (RS-232) conector RJ-45.
Energía	Dos fuentes de alimentación de CA de 770 W. Redundante como 1+1.
Enfriamiento	Siete módulos de ventiladores intercambiables en caliente para la refrigeración delantera y trasera
Video	Resolución de vídeo VGA de hasta 1920 x 1200, 16 bpp a 60 Hz, y hasta 512 MB de memoria de vídeo (8 MB asignados por defecto).

Fuente: (Cisco, 2022b)

Nota. La tabla presentada anteriormente muestra las especificaciones de hardware que contiene la controladora Cisco DNA Center de 44 núcleos con numero de pieza DN2-HW-APL.

2.5.1.3. Tareas de administración

- **Diseño**

La tarea administrativa de Diseño puede crear una jerarquía de red que represente las ubicaciones geográficas de su red de manera que se presenta en la Figura 9. Su jerarquía de red puede contener sitios, que a su vez contienen edificios y áreas. Puede crear IDs de sitios y edificios para identificar fácilmente dónde aplicar los ajustes de diseño o las configuraciones más adelante. Por defecto, hay un sitio llamado **Global**. (Cisco Systems, 2021, pág. 36)

Cisco Systems, (2021), menciona que en la jerarquía de red existe una jerarquía determina que se menciona a continuación:

- Las áreas o sitios no tienen una dirección física, se podría verlas en las áreas como el más grande elemento. Las áreas tienen edificios y subáreas, por ejemplo, un área llamada Ecuador contiene una subárea llamada Imbabura, y la subárea Imbabura puede contar una subárea llamada Ibarra.
- Los edificios tienen direcciones físicas y contienen planos de planta y piso. Al crear un edificio, se debe especificar una dirección física y las coordenadas de latitud y longitud. Los edificios no pueden contener zonas. Al crear un edificio, puede realizar ajustes en áreas específicas.
- Los pisos están dentro de los edificios y consisten en cubículos, oficinas amuralladas, armarios de cableado, etc. Sólo puede añadir pisos a los edificios.

Los dispositivos no aprovisionados pueden cambiar la jerarquía del sitio y todo esto mientras se conservan las ubicaciones de los APs en el mapa. Se debe tener en cuenta que no puede mover una planta ya existente a un edificio diferente.

Figura 9

Ejemplo del diseño de un plano de planta.

Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Nota. La herramienta de diseño presenta la opción de jerarquía de red, la cual permite estructurar la red de manera jerárquica, visualización de planos por cada planta de edificio, ubicación de Aps, oficinas amuralladas, armarios de cableado, obteniendo así un diseño ordenado de los planos de la red, esto con la finalidad de una mejor interpretación de dichos planos para los administradores de la red. Tomado de (Cisco Systems, 2021)

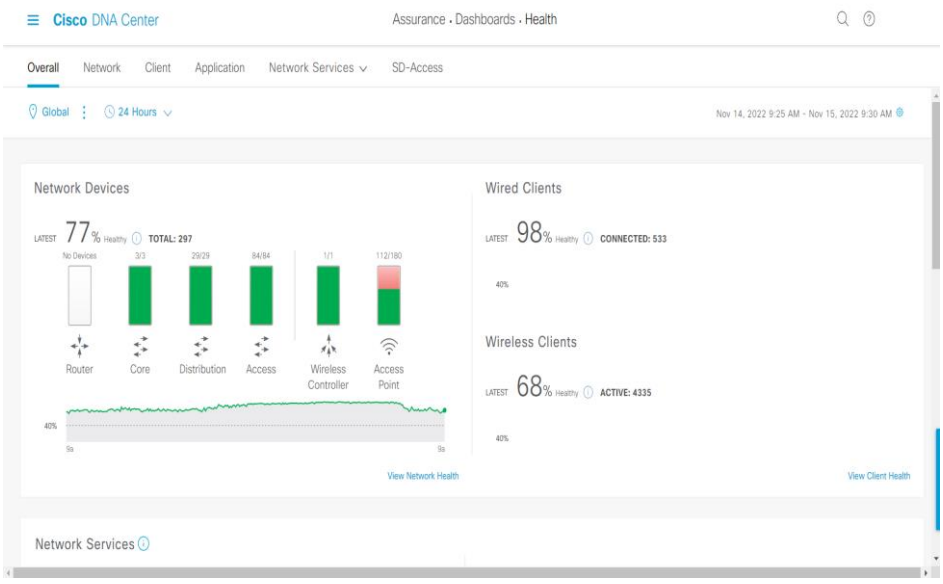
- **Garantía**

Dentro del interfaz del DNA a la Garantía se la como Assurance. Entonces Assurance ofrece una solución integral para garantizar unos niveles de servicio mejores y más constantes para satisfacer las crecientes demandas de las empresas. No sólo se ocupa de la supervisión reactiva de la red y de la resolución de problemas, sino también de los aspectos proactivos y predictivos del funcionamiento de una red y de garantizar un rendimiento óptimo de los clientes, las aplicaciones y los servicios.(Cisco Systems, 2021)

Uno de los ítems que posee Assurance, es el ítem de Salud (Health), dicho item utiliza un procedimiento para obtener una visión global del estado de la red el cual se lo identifica en la Figura 10, para así lograr determinar problemas potenciales existentes que deban ser abordados.

Figura 10

Estado de salud de la red.



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Nota. Una red estar formada por uno o más dispositivos, incluyendo routers, switches, controladoras inalámbricas y puntos de acceso, entonces para el monitoreo continuo de la red

está el panel del estado de la red, el cual brinda una visión general del estado de la red, pero también brinda la posibilidad de visualizar los detalles de un dispositivo en específico para así lograr determinar si existe problemas potenciales que deban resolverse. Tomada de (Cisco Systems, 2021).

Cisco Systems, (2021), en su Guía de usuario Cisco DNA Assurance, versión 2.2.3 propone las siguientes ventajas sobre la tarea administrativa Garantía (Assurence):

- Trata problemas relacionados con la red, clientes y aplicaciones, todo esto es proporcionado mediante información procesable. Existen problemas que consisten en la correlación básica y avanzada de múltiples piezas de información, eliminando así el ruido blanco y los falsos positivos, como, por ejemplo.
- Para un gran número de problemas Garantía (Assurance) brinda soluciones guiada por el sistema y también autoguiadas, permitiendo ofrecer un enfoque guiado por el sistema, en el que se correlacionan múltiples indicadores clave de rendimiento (KPI) y los resultados de las pruebas y los sensores se utilizan para determinar la causa raíz de un problema, para así ofrecer posibles acciones para resolver los problemas.
- Proporciona puntajes de salud detallados para la red y sus dispositivos, clientes, aplicaciones y servicios. La experiencia del cliente está asegurada tanto en términos de acceso (onboarding) como de conectividad.

➢ **Disposición**

Dentro de la tarea administrativa Disposición (Provision) se encuentra la función de **Inventario** tal y como consta en la

Figura *11*, la cual cumple la función de guardar y recuperar en su base de datos detalles como las direcciones IPs de los hosts, las direcciones MAC y los puntos de conexión a la red sobre los dispositivos en su base de datos. La función control de dispositivos también trabaja junto a la función de inventario, esto con la finalidad de configurar los ajustes de red necesarios en los dispositivos y teniendo en cuento si los ajustes ya no se los ha realizados en los dispositivos. (Cisco Systems, 202, pág 54)

Cisco Systems (2021), menciona en su Guía de Usuario que el inventario utiliza los siguientes protocolos, según sea necesario:

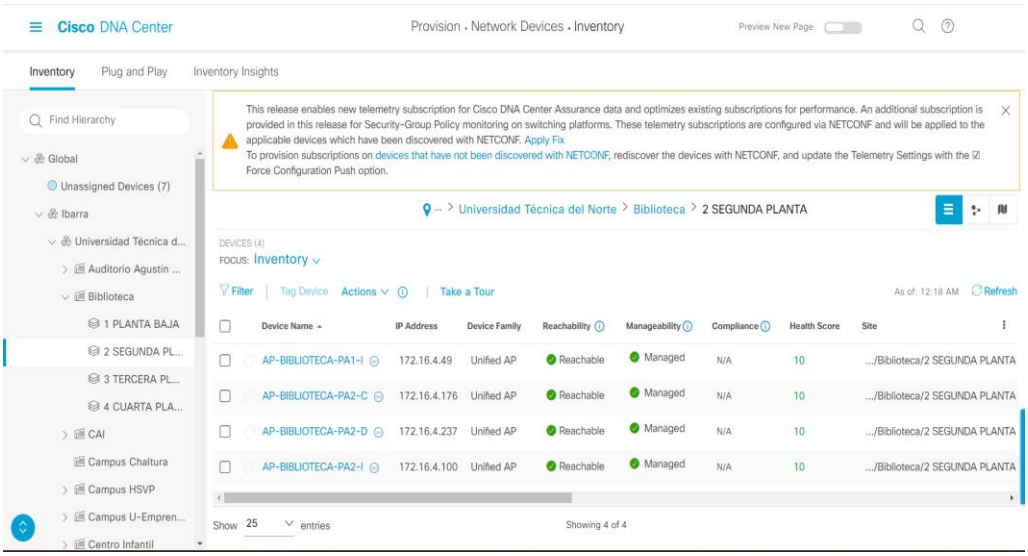
- El protocolo de descubrimiento de la capa de enlace (LLDP)
- IP Device Tracking (IPDT) o Switch Integrated Security Features (SISF)IPDT o SISF deben estar activados en el dispositivo).
- LLDP Media End-point Discovery. (Este protocolo se utiliza para descubrir teléfonos IP y algunos servidores).
- Protocolo de configuración de red (NETCONF).

La función inventario mantiene en un sondeo a intervalos regulares a los dispositivos. Existe un intervalo ya determinado, el cual es cada seis horas, pero este puede cambiar a otros valores y según sea necesario el entorno de su red. Se debe tener en cuenta que un cambio de configuraciones en los dispositivos activara una trampa SNMP, que a su vez activara la resincronización del dispositivo. El sondeo se lo realiza a cada dispositivo, enlace, host e

interfaz. Solo aparecen los dispositivos que han estado activos durante menos de un día. Esto evita que se muestren datos antiguos de los dispositivos, en caso de que los haya.

Figura 11

Panel principal de la función de inventario



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Nota. La función inventario permita sondear todos los dispositivos posibles en la red de manera jerárquica, o sea tal y como se encuentran ubicados físicamente en la red, también permite la opción de guardar y recuperar direcciones IPs, direcciones MAC y puntos de conexión a la red dentro de la base de datos. Tomado de (Cisco Systems, 2021)

- **Herramientas**

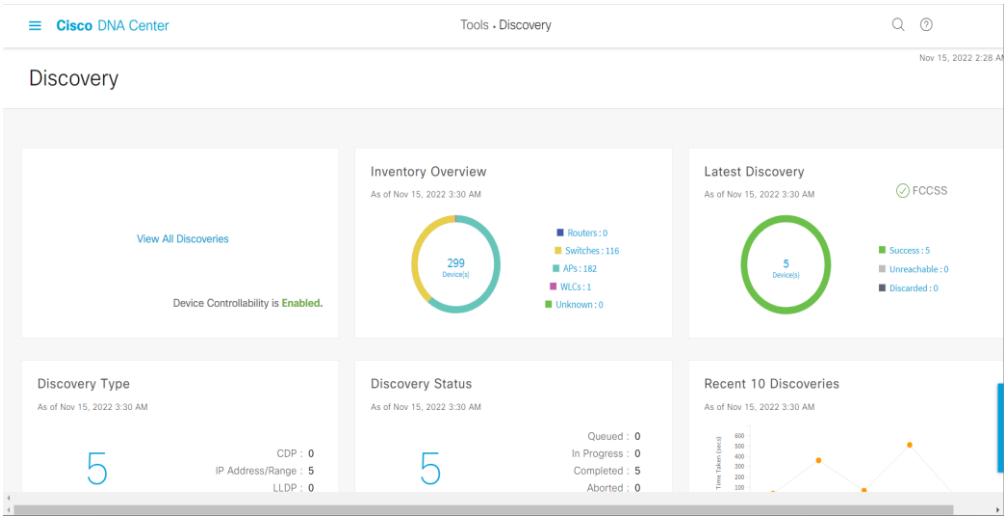
“Descubrir dispositivos (Discovery), es una de las funciones que se encuentra presenta en el ítem de Herramientas, esta función de Descubrir dispositivos escanea a los dispositivos de la red y envía el listado de los dispositivos encontrados al inventario, como se visualiza en la Figura 12.”(Cisco Systems, 2021, pág. 16)

Cisco Systems, (2021), en su Guía de Usuario describe tres formas de descubrir dispositivos:

- Utilizar el Protocolo de Descubrimiento de Cisco (CDP) y proporcionar una dirección IP inicial.
- Especificar un rango de direcciones IP. (Se admite un rango máximo de 4096 dispositivos).
- Utilizar el Protocolo de Descubrimiento de la Capa de Enlace (LLDP) y proporcionar una dirección IP semilla.

Figura 12

Ventana principal de la función Descubrimientos (Discovery)



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

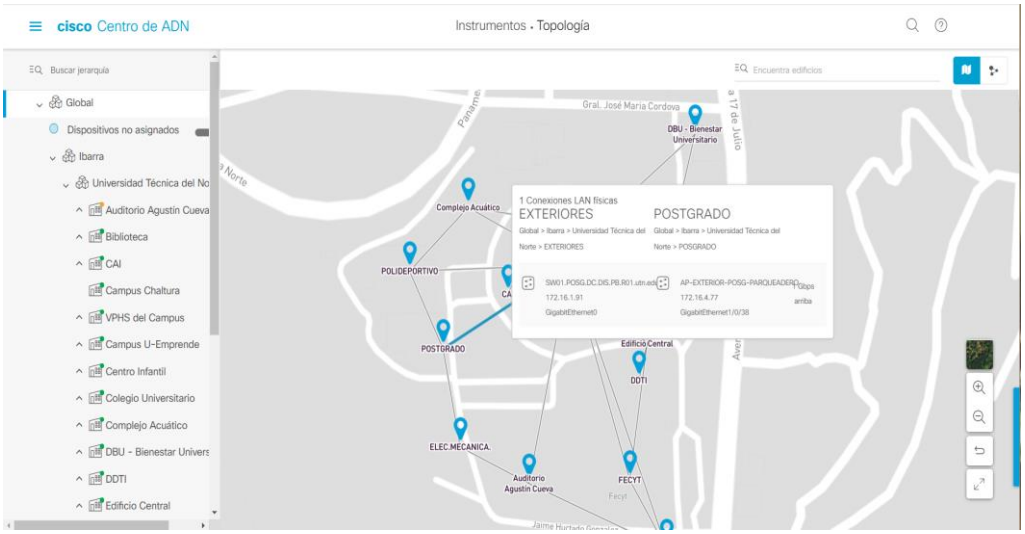
Nota. La función descubrimiento permite obtener una descripción general del inventario, reporte de últimos descubrimientos, el tipo de descubrimientos, los estados de los

descubrimientos y el número de los descubrimientos recientes. Tomando de (Cisco Systems, 2021)

También posee la función de **Topología** el ítem de Herramientas, el cual ayudara a visualizar los enlaces de la red. En la función topología, realizando clic en cualquiera de los enlaces conectados, se podrá visualizar en la Figura 13, que aparecen ciertas características como: la dirección de la ruta, los dispositivos a lo largo de la misma y cada equipo con sus respetivas direcciones IPs.

Figura 13

Panel principal de la función Topología



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

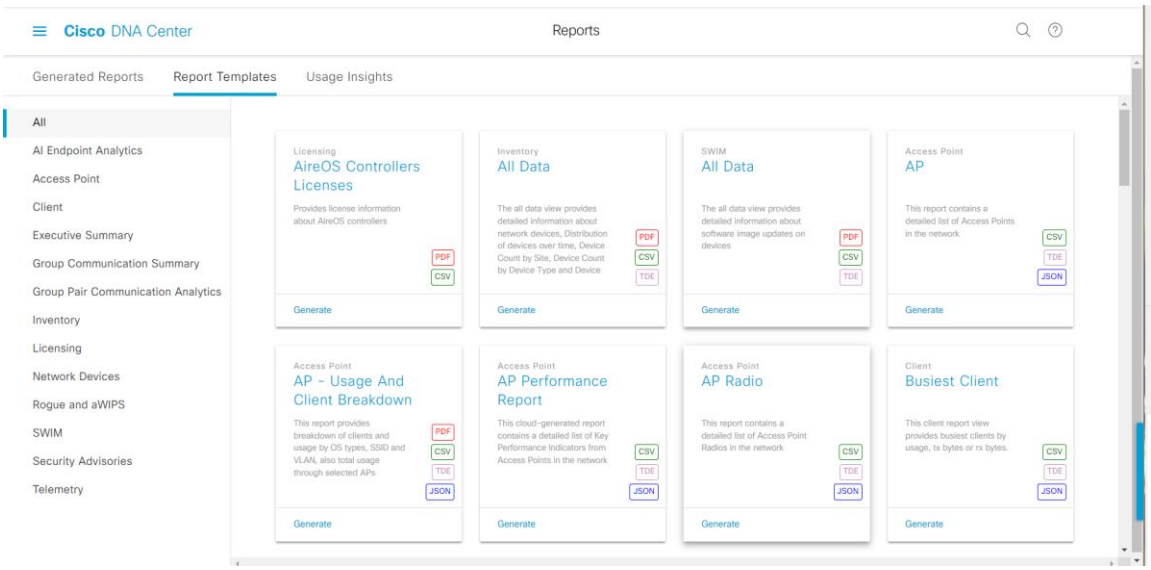
Nota. Cuando se inicia un rastreo de ruta, el equipo Cisco DNA Center revisa y recopila la topología de red y los datos de enrutamiento de los dispositivos descubiertos. A continuación, utiliza estos datos para calcular una ruta entre los dos hosts o interfaces de capa 3, y muestra la ruta en una topología de trazado de ruta. La topología incluye la dirección de la ruta y los dispositivos a lo largo de la ruta, incluyendo sus direcciones IP. Tomando de (Cisco Systems, 2021).

- **Reportes**

El ítem **Reportes** puede utilizar los datos de la función de informes para obtener información sobre su red y su funcionamiento, de acuerdo como se visualiza en la Figura 14 en el panel principal de **Reportes**. Al informar estos datos en una variedad de formatos y ofrecer opciones de configuración y programación flexibles, los datos y los informes se pueden adaptar fácilmente para satisfacer sus necesidades operativas.

Figura 14

Ventana de Reportes



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Nota. A través de la generación de Reportes se visualiza varios ámbitos de la red y mediante las Plantillas de Informes (Report Templates) se generan informes sobre acciones específicas de ciertos elementos de la red.

3. Capitulo III

3.1. Estructura jerárquica actual del Departamento de Desarrollo Tecnológico e Informático (DDTI)

A continuación, en la Figura 15 se visualiza la estructura organizacional del Departamento de Desarrollo Tecnológico e Informático (DDTI) de la UTN el cual posee 3 áreas enfocadas al ámbito tecnológico.

Figura 15

Organigrama del DDTI

Fuente: Departamento de Desarrollo de Tecnológico e Informático

La Tabla 2 presenta la estructura jerárquica del Departamento de Desarrollo y Tecnología en el área de las Redes y Comunicaciones.

Tabla 2

Estructura jerárquica del DDTI

Representante	Cargo
Ing. Jorge Caraguay Msc	Dirección DDTI
Ing. Vinicio Guerra	Analista de Redes y Comunicaciones
Ing. Estefanía Torres	Analista de Redes y Comunicaciones
Ing. Edison Carrión	Asistente de Redes y Comunicaciones

Fuente: Departamento de Desarrollo de Tecnología e Informática

3.2. Situación Actual de la Red de la Universidad Técnica del Norte

En este capítulo se describe de manera estructural las dependencias internas de la Universidad Técnica del Norte. La topología de la red de la Universidad Técnica del Norte funciona a través de un modelo de arquitectura jerárquica el cual consta de tres capas identificadas, Core, Distribución y Acceso. La Universidad Técnica del Norte cuenta con un rango de direccionamiento IP, en IPv4 dispone del rango 172.16.X.X/12 clase B.

Los elementos de la Capa de Core se encuentran ubicados en el Data Center del Edificio central de la Universidad Técnica del Norte, aquí se encuentran dos routers, donde el principal router de borde es el equipo de CEDIA marca Nokia 7705 SAR8 y el segundo router de borde es Cisco 3750 siendo el equipo de backup, ambos equipos están enlazados al Firewall FORTIGATE 1800F lo cual forma una SD-WAN.

Otro equipo que consta en la capa de Core es el Switch Catalys 9300 que está conectado al Firewall FORTIGATE 1800F y proporciona la conectividad a los servidores de la DMZ.

En la Capa Distribución se encuentran dos equipos de conmutación, un switch Cisco (9407), el cual brinda la propagación de VLANs a lo largo de la capa de acceso, y este, a su vez está conectado a un switch Cisco (9407) y estos dos equipos se encuentran configurados en virtual stackwise, también se encuentran las dos controladoras inalámbricas, la primera

marca cisco 9800 y la otra controladora serie 5520. En el ámbito del Software la UTN cuenta con la infraestructura como servicio (SaaS e IaaS, contratados), por ende, se tiene el servicio de Office 365 el cual tiene su principal servicio de correo institucional y la nube de Oracle, donde está alojado el sitio web y el sistema integrado de la Universidad.

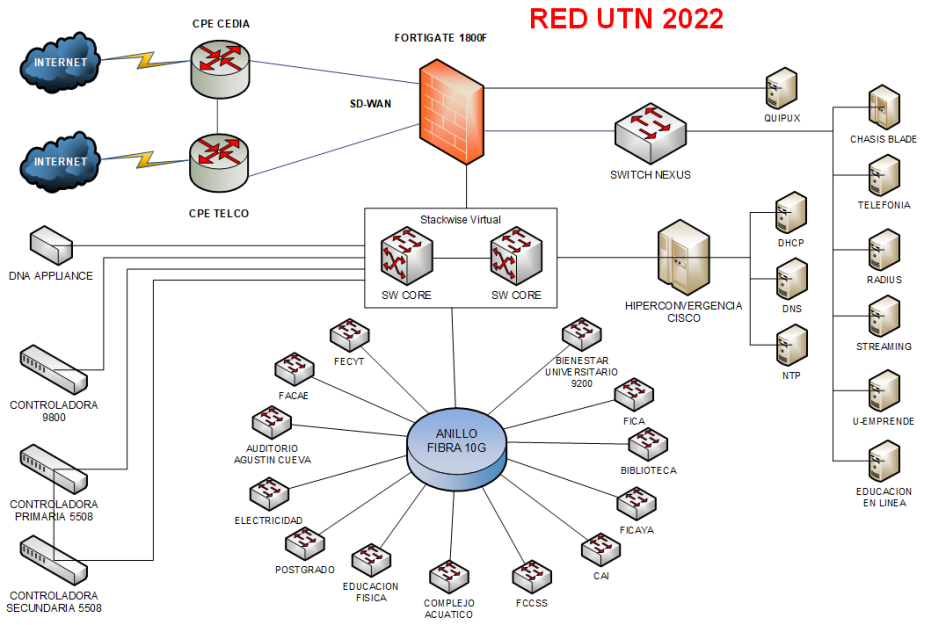
El software de gestión Cisco DNA center trabaja en la capa de Distribución, el cual será el cerebro de la red, permitiendo centralizar la gestión de los dispositivos físicos como los switches, las controladoras y Access Point que conforman la capa de Core, Distribución y Acceso, que forman parte la red de la Universidad Técnica del Norte. Cisco DNA center a través de su interfaz gráfica permitirá configurar y monitorear todos los equipos antes mencionados, todo aquello se lo puede realizar mediante las APIs que posee, lo cual permite programar a los dispositivos en función de las necesidades por parte del administrador de red.

La capa de acceso se divide en las distintas Facultades FICA, FICAYA, FACAE, FCSS, FECYT, POSTGRADO y las dependencias que son el edificio central, auditorio Agustín Cueva, Electricidad, Educación Física, Complejo Acuático, CAI, Biblioteca, todo esto a través de un anillo de fibra monomodo G652D a 10Gbps.

La Universidad Técnica del Norte consta de una topología física y en base a la Figura 16, se describió de manera estructural como se encuentra la red de la Universidad Técnica del Norte.

Figura 16

Topología física de la Universidad Técnica del Norte



Fuente: Departamento de Desarrollo de Tecnológico e Informático

Nota. La red de la Universidad Técnica del Norte presenta su arquitectura de manera jerárquica la cual consta de 3 capas que son Core, distribución y acceso.

3.2.1. Descripción de la red por Facultad.

La información presentada a continuación se basa de acorde a trabajos realizados anteriormente dentro de la Universidad Técnica del Norte y a previas inspecciones dentro de cada facultad para constatar o actualizar la información de la situación actual de la red cableada.

3.2.1.1. FICA

3.2.1.1.1.Situación Actual de la red cableada

La información recopilada en la Facultad (FICA) se lo realiza con la finalidad de determinar su situación actual, esto con el fin de verificar si el equipamiento y/o infraestructura es la adecuada, se encuentra en óptimas condiciones y así poder tomar en cuenta la información para dicho trabajo a realizar.

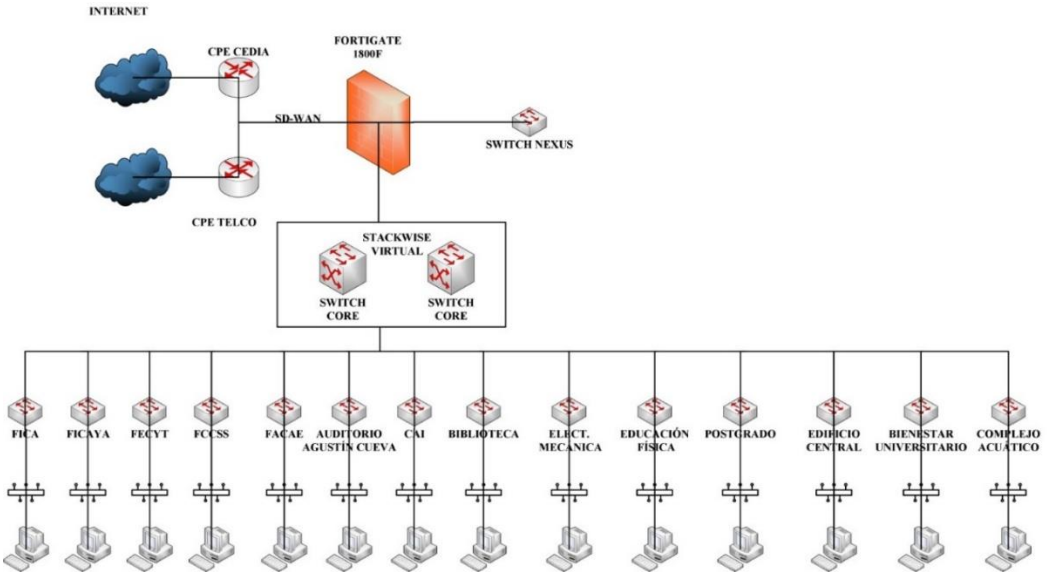
La red de la Facultad de Ingeniera en Ciencias Aplicadas cuenta con el cableado estructurado UTP Categoría 5e, no certificado. Su recorrido horizontal se realiza sobre la estructura del falso techo, en bandejas metálicas con mallazos transversales. Las rutas verticales no cuentan con acceso suficiente (como bandejas antiestáticas) para protegerlas de fenómenos externos como la humedad, la temperatura o el ruido provocado por el campo electromagnético de la red inalámbrica. En algunas zonas, el cableado supera el número estándar de curvas de ≥ 90° (máximo 3 en 90 m de longitud).

3.2.1.1.2. Red externa

El gabinete de comunicaciones que se encuentra en la Facultad está configurado de manera que es el punto de principal de redundancia del anillo de fibra óptica de toda la Universidad de tal manera como se visualiza en la Figura 17. Entonces, si se presentan inconvenientes (cortes en el medio de transmisión o fallos de hardware) en la red principal de la Universidad, el equipo de la red FICA se convierte inmediatamente en el enlace de comunicación entre las 87 divisiones del DDTI y el resto de las entidades de la red (departamentos, auditorios, departamentos, etc.) a través del anillo secundario de fibra óptica.(*Informe Diseño Cableado Estructurado*, 2017)

Figura 17

Topología de red externa.



Fuente: Elaboración Autor

3.2.1.1.3. Red Interna

Las Comunicación y demás servicios de red que brinda la Universidad, se realizan a través del hardware de networking, el cual se encuentra en un gabinete ubicado en la Carrera de Ingeniería en Electrónica y Redes de comunicación, en el primer piso de la Facultad.

Desde el DDTI se brinda los servicios de la UTN, mediante un cable de fibra óptica de 62.5/125 μm de 6 hilos, estos vienen en una bandeja específica para el arreglo, organización y distribución de cada hilo hacia un switch compatible con la tecnología de alta disponibilidad y capacidad de procesamiento, a través de pigtails tipo LC. Los puertos de conexión RJ45 del switch de CORE se distribuyen mediante patch panels horizontales instalados en el rack empleando patch cords UTP Categoría 6.

3.2.1.1.4. Arquitectura de Red

Según el Informe Diseño Cableado Estructurado (2017), “en el Centro de Datos de la Facultad consta de los siguientes espacios de telecomunicaciones:”

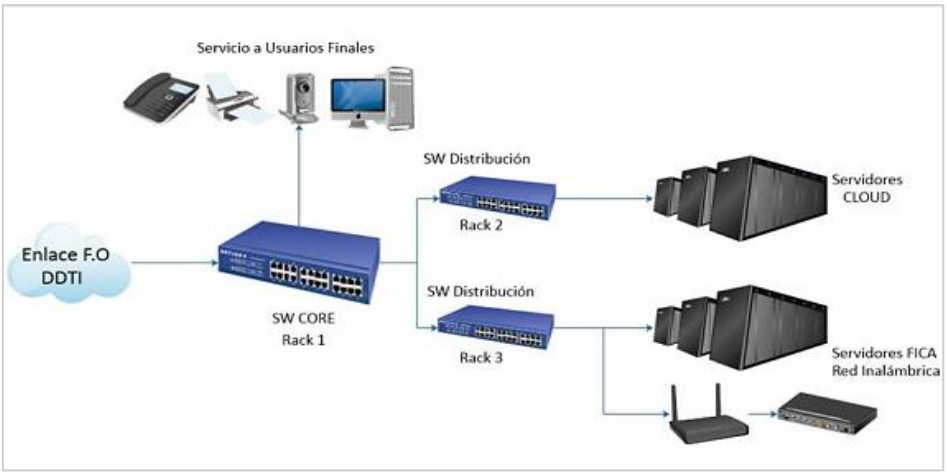
- *Cuarto de entrada:* Zona de acometidas eléctricas del CDP y bandeja ODF ubicada en rack #1.

- *Área de Distribución Principal:* Switch CORE de alta disponibilidad, instalado en el rack #1.
- *Área de Distribución Horizontal:* Representada por los patch panels de conexión cruzada para el cableado horizontal instalados en el rack #1.
- *Área de Distribución de Zona:* Puntos de consolidación y/o futuras instalaciones de mutoas.
- Área de Distribución de Equipos: Switchs de distribución de cableado horizontal de cada planta y racks de servidores #2 y #3.
- Área de Trabajo: Puntos de red (rosetas y faceplate) terminales de usuario para conexiones RJ45 del cableado estructurado.

La Figura 18 muestra las conexiones de red y sus jerarquizaciones físicas dentro de la Facultad.

Figura 18

Conexión de red y jerarquizaciones



Fuente: Información DDTI de la UTN, adaptado de (*Informe Diseño Cableado Estructurado*, 2017)

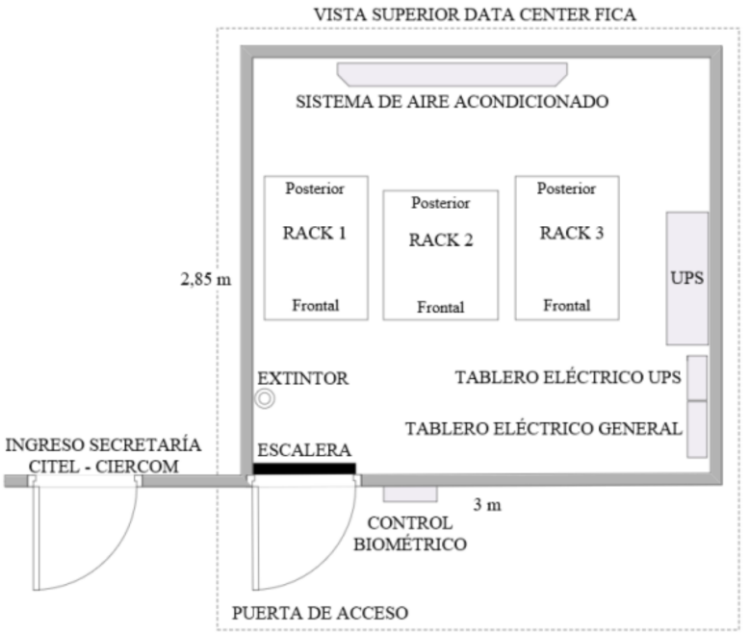
Nota. El Data Center que se encuentra en la Facultad contiene equipamiento TIC (de servicio y de red) distribuido por toda la infraestructura del edificio, en espacios improvisados y convencionales, lo cual permite tener una administración pertinente del mismo.

3.2.1.1.5. Ubicación del Data Center

Dentro de la oficina de la carrera de Ingeniera en Telecomunicación (CITEL) está ubicado el Data Center, este se encuentra en la planta baja de la Facultad FICA. El Data Center de la FICA se representa en la Figura 19 de tal manera se presenta un diagrama de infraestructura y además sus dimensiones físicas son: 2.85m de longitud por 3m de ancho, dando un área total de 8.55m2.(Narváez Manosalvas, 2016)

Figura 19

Infraestructura del Data center FICA



Fuente: Información DDTI de la UTN, adaptado de (Nicolalde Quilca, 2021)

Nota. El Data Center de la FICA cuenta con los siguientes apartados: sistema eléctrico, sistema de control de acceso, sistema de aire acondicionado, sistema de seguridad y sistema de telecomunicaciones.

3.2.1.1.6.Sistema de Telecomunicaciones

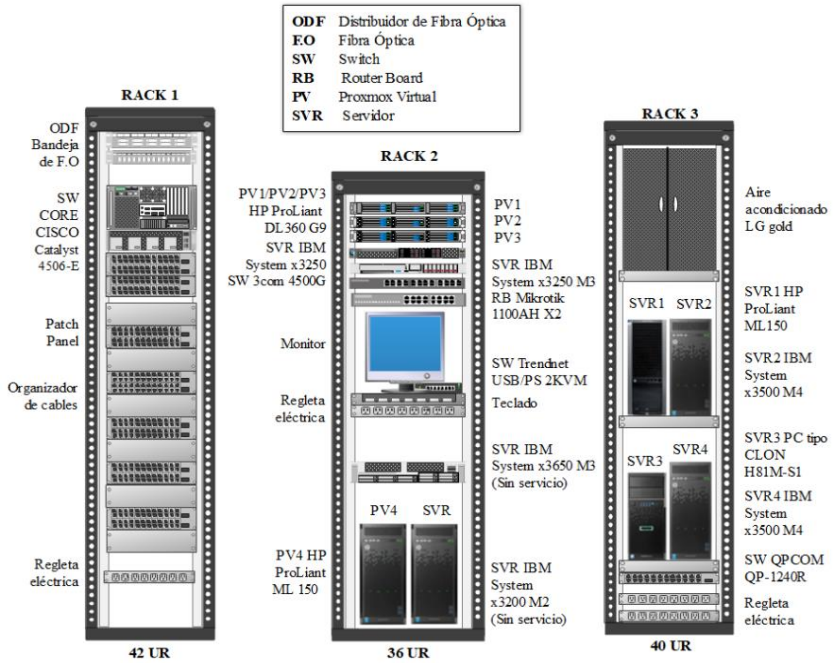
El Data Center de la Faculta de Ingeniera en Ciencias Aplicadas cumple con el objetivo de alojar a los Equipos TIC, pero también cumple con la funcionalidad de ser una red de redundancia para el anillo de fibra de la Universidad Técnica del Norte. El Data center cuenta con un total de 3 Racks, que a continuación se detallan en la Figura 20, los equipos con los que cuenta cada uno de los Racks.

Dentro del Rack 1 se encuentra un switch de capa tres, equipo que es utilizado como borde para la conexión del data center con el edificio central y hacia internet, esto a través de dos cables de fibra óptica. En el Rack 2 cuanta con cuatro servidores denominados Promox Virtual (PV), pero únicamente 3 (PV1, PV2, PV3) brindan la infraestructura fica para virtualizar equipos, Promox es el software que hace posible los procesos. Dentro del mismo

rack se encuentra un servidor Radius, en donde 3 servidores perteneces a la Carrera de Ingeniera en Sistemas Computacionales (CISIC), un switch 3Com 4500G administrable y un router Mikrotik que permite la administración de la red inalámbrica. Para el caso del Rack 3, se encuentran alojado un switch QPcom y 4 servidores, dichos servidores son dedicados para servicios administrativos y educativos dirigidos a docentes y estudiantes, estos servidores son: Opina, Reactivos, Biométricos y Revista Universitaria. (Nicolalde Quilca, 2021)

Figura 20

Data Center – FICA



Fuente: Información DDTI de la UTN, adaptado de (Nicolalde Quilca, 2021)

3.2.1.1.7.Equipos TIC y demás hardware de conexión disponible

- **Racks**

Las características del rack de telecomunicaciones que se encuentra en la Facultad tienen las siguientes características:

- Gabinete marca BEAUCOUP; de color negro; metálico; de 2 m de altura; 0,6 m de ancho y 0,8 m de profundidad; con rack interno de 4 postes con capacidad máxima de 42 UR, bien definidas y numeradas en su totalidad.
- La estructura presenta posee cuatro ruedas inferiores con sistema de bloqueo, para facilidad de su desplazamiento.

➢ **Topología Física**

El Data Center que en encuentra en la Facultad FICA, tal y como se muestra en la Figura 21 posee conexión a internet y servicios, esto a través de un enlace de fibra óptica que viene directamente desde el Departamento de Desarrollo de Tecnóloga e Información (DDTI) y todo esto conecta al switch de marca Cisco, modelo Catalyst 4506E, el cual es un switch de alta disponibilidad.

Además, existen 3 switches de 24 puertos: de la marca 3COM y uno de la marca Cisco Linksys, modelo SR224G. Dado que la red implementada en la FICA es segmentada físicamente en tres partes y cada uno de los segmentos se menciona a continuación:

El primer segmento consta con el switch de core Catalyst 4506-E que va desde el puerto 28 hasta el switch 3Com 3226. Esta conexión permita el acceso a varios servidores como: Opina, Biométrico, Reactivos y Revista Universitaria.

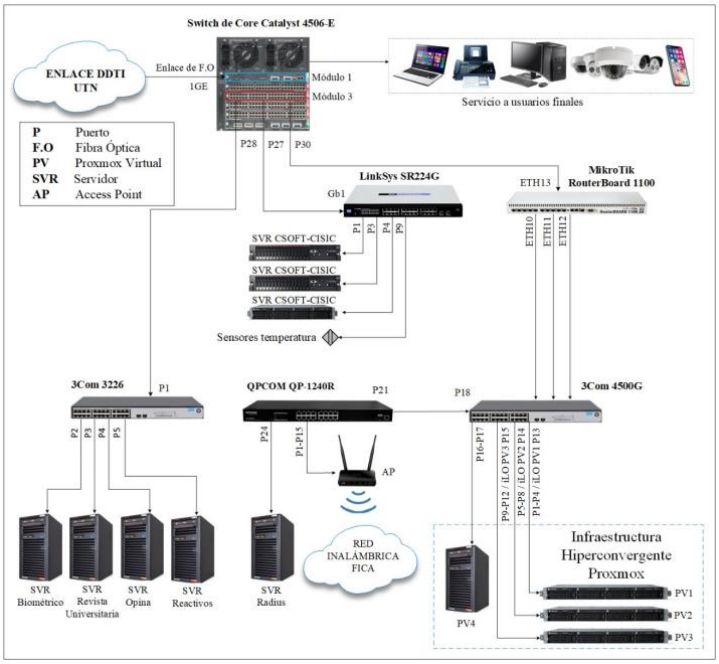
En el segundo segmento está el switch de core Catalyst 4506-E que conecta en el puerto 27 con un switch LinkSys SR224G, el objetico de esta conexión es permitir la comunicación de los tres servidores que administra la Carrera de Ingeniera en Sistemas Computacionales (CISIC).

Mientras que el tercer segmento brinda una conexión a la red inalámbrica que posee la FICA y a la infraestructura virtualizada Promox, este se encuentra conectado en el puerto 30 del switch Catalyst 4506-E y conecta a un equpo Mikrotik RouterBoard 1100, dicho equipo

mencionado se encarga del enrutamiento, también conecta a un switch 3COm 4500G en el cual se encuentran enlazados: un switch QPCom QP-1240R y a la infraestructura hiperconvergente de Proxmox; el primero tiene la función de mantener conectados a los puntos de acceso (A.P.) que se ubican en toda la FICA, además este switch permite la comunicación con el servidor Radius, por otro lado la infraestructura de Proxmox se administra a través de los servidores PV1, PV2 y PV3.(Guerrero Ipiales, 2019)

Figura 21

Topología física del Data Center



Fuente: Información DDTI de la UTN, adaptado de (Nicolalde Quilca, 2021)

- **Servidores**

La Facultad cuenta con varios equipos TIC que cumplen con la función de servidores (Tabla 3), distribuidos por todo el edificio.

Tabla 3

Servidores de la Facultad

Servicio	Tipo	Estado	Marca

Reactivos Moodle	Torre	Activo	IBM x3500 M4
Gestor de encuestas Opina	Torre	Activo	Hp ProLiant ML150
Repositorio Digital Dspace	Torre	Activo	IBM x3500 M4
LDPA	Torre	Activo	IBM System x3200 M2
Control de Acceso	Torre	Activo	HP Proliant ML370
Sin Servicio	Torre	Activo	HP Proliant ML150 G5
Nube de la FICA	Torre	Activo	HP Proliant G9
Nube de la FICA	Rack	Activo	HP Proliant G9
Nube de la FICA	Rack	Activo	HP Proliant G9
Proyecto de CISIC	Rack	Activo	IBM System x3250
Proyecto de CISIC	Rack	Activo	IBM System x3250
Proyecto de CISIC	Rack	Activo	HP System x3650 M3

Fuente: Información DDTI de la UTN, adaptado de (*Informe Diseño Cableado Estructurado*, 2017)

3.2.1.1.8.Equipos Activos de Red

En la Tabla 4 se presenta los equipos de red en la Facultad FICA con su respectiva ubicación, nombre y modelo.

Tabla 4

Ubicación actual de los equipos activos de red en la Facultad – FICA

N^o	Dependencia	Ubicación	Nombre	Marca	Modelo
1	FICA	Datacenter	SW01.FICA.DC.DIS.PB.R01	Cisco	C9300-48UXM-E
2		Datacenter	SW02.FICA.DC.DIS.PB.R01	Cisco	WS-C4510R+E
3		Laboratorio I	SW01.FICA.LAB1.ACC.PA1.R01	Cisco	WS-C2960-48TC-L
3		Laboratorio II	SW01.FICA.LAB2.ACC.PA1.R02	Cisco	WS-C2960-48TC-L
4		Laboratorio III	SW01.FICA.LAB3.ACC.PA1.R03	Cisco	WS-C2960-48TC-L
5		Laboratorio III	SW02.FICA.LAB3.ACC.PA1.R03	Cisco	WS-C2960-24TC-L
6		Laboratorio MAC	SW-LABMAC	Cisco	WS-C2960-48TC-L
7		Laboratorio Cisco	SW01.FICA.LABCISCO.ACC.PA5.R05	Cisco	WS-C2960-48TC-L
8		Laboratorio Cisco	SW02.FICA.LABCISCO.ACC.PA5.R05	Cisco	WS-C2960-48TC-L
9		Sala de Investigación	SW01.FICA.CUBI.ACC.PA5.R06	Cisco	WS-C2960-48TC-L
10		Sala de Profesores	SW01.FICA.ASOPROF.ACC.PA5.R07	Cisco	WS-C2960-24TC-L
11		Laboratorio 6	SW02.FICA.LAB5.ACC.PA3.R08	Cisco	WS-C2950-24
12		Switches Servidores	SW_01_FICA	3COM	SuperStack 3226
13		Laboratorio 5	SW01.FICA.LAB5.ACC.PA3.R08	Cisco	WS-C2950-24
14		Electricidad	SW01.ELECT.DC.DIS.PB.R01	Cisco	C9200L-48P-4X-E
15		Laboratorio 7	SW-LAB7	Cisco	WS-C2950-24

Fuente: Departamento de Desarrollo de Tecnológico e Informático

3.2.1.1.9.Levantamiento de Información

- **Planta Baja FICA**

Mediante la información obtenida de (Documento), se recolecta la información sobre las salidas de telecomunicaciones, tal y como se muestra en la Tabla 5 con sus respectivas aplicaciones, las áreas de trabajo y cuarto de equipos.

Tabla 5

Salidas de telecomunicaciones de la planta baja

Dependencias	Puntos de red	Biométricos	Cámaras	AP	Data center
Secretaria CIELE	8				
Sala de Profesores	4	1			

Secretaria CIERCOM	6	1			1
Secretario-Abogado	2				
Secretaria CISIC	6				
Secretaria CIME	6				
Secretaria decanato	4				
Decanato	4				
Secretaria Subdecanato	4				
Subdecanato	4				
Sala de Grados	2				
Secretaria CIAUT	6				
Pasillos	2	1	4	3	
TOTAL	58	3	4	3	1

Fuente: Información DDTI de la UTN, adaptado de (*Informe Diseño Cableado Estructurado*, 2017)

En el Data Center que se está ubicado en la planta baja de la Facultad FICA se encuentran puntos de red, cámaras y biométricos que están directamente conectados al Rack del Data Center a través del cableado horizontal. Los APs que están conectados a la red WIFI FICA bajan directamente a un Rack que está en el Data Center. Existe un Rack principal en el Data Center, al cual se conectan los Racks de cada piso, cuenta con las conexiones de fibra que se dirigen hacia las otras facultades, también hay dos armarios que contienen servidores y todos los Racks de cada piso se conectan al Data Center con cableado vertical.(Jácome Chávez, 2019)

- **Segunda Planta FICA**

La Tabla 6 representa las dependencias existentes, los puntos de red, biométricos, cámaras, APs y Racks.

Tabla 6

Información sobre Segunda planta FICA

Dependencias	Puntos de red	Biométricos	Cámaras	Aps	Racks
Laboratorio 1 Informática	46		1		1
Laboratorio 2 Informática	46		1		1
Centro de computo	22		2	1	
Jefe de laboratorio	2				
Laboratorio 3 Informática		1	1		1
Laboratorio 4 Redes		1	1		1
Laboratorio de fibra	4				
Auditorio	4		1		
Pasillos		1	3	1	
TOTAL	124	3	10	2	4

Fuente: Información DDTI de la UTN, adaptado de (*Informe Diseño Cableado Estructurado*, 2017)

En el segundo piso existen 4 Racks, cada Rack por cada laboratorio donde se conectan a los puntos de red de cada laboratorio. En este piso hay un cableado horizontal, donde las cámaras y los biométricos están conectados a los racks más cercanos.

- **Laboratorio 1**

El Laboratorio 1 se encuentra en la segunda planta de la FICA, los equipos de la Tabla 7 de telecomunicaciones existentes en dicha planta y se detallan en la Tabla 8 y su mapeo de puertos.

Tabla 7

Equipos Lab. 1- FICA

Equipos de Telecomunicaciones	Marca	Nombre	Dirección IP	Cantidad
Rack de pared de 19”	Panduit	-----	-----	1
Patch Panel de 48 Puertos Cat 6	NewLink	-----	-----	1
Switch de 48 puertos	WS-C2960-48TC-L	SW01.FICA.LAB1.ACC.PA1.R01	172.17.X.X	1

Fuente: Información DDTI de la UTN, adaptado de (Vallejos Garzón, 2019)

Tabla 8

Mapeo de la red Lab.1 - FICA

Switch Catalyst 2960 Laboratorio 1							Equipo Conectado	
Modo VLAN	**VAN**	**Descripción**	**Puerto**	**Estado**	**Patch Panel**	**Punto Red/N^o**	**Nombre**	**IP**
access	x	Laboratorios	Fa0/1	Disponible	1	Si/1	-	-
access	x	Laboratorios	Fa0/2	Activado	2	Si/2	PCFICA-312	172.17.X.X
access	x	Laboratorios	Fa0/3	Activado	3	Si/3	PCFICA-311	172.17.X.X
access	x	Laboratorios	Fa0/4	Disponible	4	Si/4		-
access	x	Laboratorios	Fa0/5	Activado	5	Si/5	PCFICA-313	172.17.X.X
access	x	Laboratorios	Fa0/6	Activado	6	Si/6	PCFICA-319	172.17.X.X
access	x	Laboratorios	Fa0/7	Activado	7	Si/7	PCFICA-318	172.17.X.X
access	x	Laboratorios	Fa0/8	Activado	8	Si/8	PCFICA-317	172.17.X.X
access	x	Laboratorios	Fa0/9	Disponible	9	Si/9	-	-
access	x	Laboratorios	Fa0/10	Disponible	10	Si/10	-	-
access	x	Laboratorios	Fa0/11	Activado	11	Si/11	PCFICA-325	172.17.X.X

access	x	Laboratorios	Fa0/12	Activado	12	Si/12	PCFICA-324	172.17.X.X
access	x	Laboratorios	Fa0/13	Disponible	13	Si/13	-	-
access	x	Laboratorios	Fa0/14	Activado	14	Si/14	PCFICA-331	172.17.X.X
access	x	Laboratorios	Fa0/15	Activado	15	Si/15	PCFICA-330	172.17.X.X
access	x	Laboratorios	Fa0/16	Disponible	16	Si/16	-	-
access	x	Laboratorios	Fa0/17	Activado	17	Si/17	PCFICA-329	172.17.X.X
access	x	Laboratorios	Fa0/18	Activado	18	Si/18	PCFICA-337	172.17.X.X
access	x	Laboratorios	Fa0/19	Disponible	19	Si/19		-
access	x	Laboratorios	Fa0/20	Disponible	20	Si/20		-
access	x	Laboratorios	Fa0/21	Activado	21	Si/21	PCFICA-336	172.17.X.X
access	x	Laboratorios	Fa0/22	Activado	22	Si/22	PC5PPOIQ9	172.17.X.X
access	x	Laboratorios	Fa0/23	Disponible	23	Si/23	-	-
access	x	Laboratorios	Fa0/24	Disponible	24	Si/24	-	-
access	x	Laboratorios	Fa0/25	Disponible	25	Si/25	-	-
access	x	Laboratorios	Fa0/26	Activado	26	Si/26	PCFICA-314	172.17.X.X
access	x	Laboratorios	Fa0/27	Activado	27	Si/27	PCFICA-315	172.17.X.X
access	x	Laboratorios	Fa0/28	Disponible	28	Si/28	-	-
access	x	Laboratorios	Fa0/29	Disponible	29	Si/29	-	-
access	x	Laboratorios	Fa0/30	Activado	30	Si/30	PCFICA-322	172.17.X.X
access	x	Laboratorios	Fa0/31	Activado	31	Si/31	PCFICA-320	172.17.X.X
access	x	Laboratorios	Fa0/32	Activado	32	Si/32	PCFICA-321	172.17.X.X
access	x	Laboratorios	Fa0/33	Disponible	33	Si/33	-	-
access	x	Laboratorios	Fa0/34	Disponible	34	Si/34	-	-
access	x	Laboratorios	Fa0/35	Disponible	35	Si/35	-	-
access	x	Laboratorios	Fa0/36	Activado	36	Si/36	PCFICA-326	172.17.X.X
access	x	Laboratorios	Fa0/37	Activado	37	Si/37	PCFICA-328	172.17.X.X
access	x	Laboratorios	Fa0/38	Activado	38	Si/38	PCFICA-334	172.17.X.X
access	x	Laboratorios	Fa0/39	Activado	39	Si/39	PCFICA-332	172.17.X.X

access	x	Laboratorios	Fa0/40	Disponible	40	Si/40	-	-
access	x	Laboratorios	Fa0/41	Activado	41	Si/41	PCFICA-333	172.17.X.X
access	x	Laboratorios	Fa0/42	Activado	42	Si/42	PCFICA-340	172.17.X.X
access	x	Laboratorios	Fa0/43	Activado	43	Si/43	PCFICA-338	172.17.X.X
access	x	Laboratorios	Fa0/44	Activado	44	Si/44	PCFICA-339	172.17.X.X
access	x	Laboratorios	Fa0/45	Disponible	45	Si/45	-	-
access	x	Laboratorios	Fa0/46	Disponible	46	Si/46	-	-
access	x	Laboratorios	Fa0/47	Disponible	47	Si/47	-	-
access	x	Administrativos	Fa0/48	Disponible	48	Si/48	-	-
trunk			G1/0					
			G2/0					

Fuente: Información DDTI de la UTN, adaptado de (Vallejos Garzón, 2019)

- **Laboratorio 2**

Los equipos de telecomunicaciones se presentan en la Tabla 9 y el mapeo de puertos como se visualiza en la Tabla 10, se encuentran en el laboratorio 2 el cual está ubicado en la planta 2 de la facultad FICA.

Tabla 9

Equipos Lab.2 – FICA

Equipos de Telecomunicaciones	**Marca**	**Nombre**	**Dirección IP**	**Cantidad**
Rack de pared de 19”	Panduit	-----	-----	1
Patch Panel de 48 Puertos Cat 6	NewLink	-----	-----	1
Switch de 48 puertos	WS-C2960-48TC-L	SW01.FICA.LAB2.ACC.PA1.R02	172.17.X.X	1

Fuente: Información DDTI de la UTN, adaptado de (Vallejos Garzón, 2019)

Tabla 10

Mapeo de la red Lab.2 – FICA

Switch Catalyst 2960 Laboratorio 2					Equipo Conectado		
Modo VLAN	**VAN**	**Descripción**	**Puerto**	**Estado**	**Patch Panel**	**Nombre**	**IP**
access	x	Laboratorios	Fa0/1	Disponible	1	-	-
access	x	Laboratorios	Fa0/2	Disponible	2	PCFICA-184	172.17.X.X
access	x	Laboratorios	Fa0/3	Activado	3	PCFICA-183	172.17.X.X
access	x	Laboratorios	Fa0/4	Activado	4	-	-
access	x	Laboratorios	Fa0/5	Disponible	5	-	-
access	x	Laboratorios	Fa0/6	Disponible	6	PCFICA-190	172.17.X.X
access	x	Laboratorios	Fa0/7	Activado	7	PCFICA-188	172.17.X.X
access	x	Laboratorios	Fa0/8	Activado	8	PCFICA-189	172.17.X.X
access	x	Laboratorios	Fa0/9	Activado	9	PCFICA-189	172.17.X.X
access	x	Laboratorios	Fa0/10	Activado	10	PCFICA-190	172.17.X.X
access	x	Laboratorios	Fa0/11	Activado	11	PCFICA-196	172.17.X.X
access	x	Laboratorios	Fa0/12	Activado	12	PCFICA-195	172.17.X.X
access	x	Laboratorios	Fa0/13	Disponible	13	-	-
access	x	Laboratorios	Fa0/14	Activado	14	PCFICA-199	172.17.X.X
access	x	Laboratorios	Fa0/15	Activado	15	PCFICA-243	172.17.X.X
access	x	Laboratorios	Fa0/16	Disponible	16	-	-
access	x	Laboratorios	Fa0/17	Activado	17	PCFICA-262	172.17.X.X
access	x	Laboratorios	Fa0/18	Disponible	18	-	-
access	x	Laboratorios	Fa0/19	Disponible	19	-	-
access	x	Laboratorios	Fa0/20	Disponible	20	-	-
access	x	Laboratorios	Fa0/21	Disponible	21	-	-
access	x	Laboratorios	Fa0/22	Activado	22	PCFICA-181	172.17.X.X
access	x	Laboratorios	Fa0/23	Disponible	23	-	-
access	x	Laboratorios	Fa0/24	Disponible	24	-	-

access	x	Laboratorios	Fa0/25	Disponible	25	-	-
access	x	Laboratorios	Fa0/26	Disponible	26	-	-
access	x	Laboratorios	Fa0/27	Activado	27	PCFICA-182	172.17.X.X
access	x	Laboratorios	Fa0/28	Disponible	28	-	-
access	x	Laboratorios	Fa0/29	Disponible	29	-	-
access	x	Laboratorios	Fa0/30	Activado	30	-	-
access	x	Laboratorios	Fa0/31	Disponible	31	-	-
access	x	Laboratorios	Fa0/32	Disponible	32	-	-
access	x	Laboratorios	Fa0/33	Activado	33	PCFICA-187	172.17.X.X
access	x	Laboratorios	Fa0/34	Activado	34	PCFICA-193	172.17.X.X
access	x	Laboratorios	Fa0/35	Activado	35	PCFICA-192	172.17.X.X
access	x	Laboratorios	Fa0/36	Disponible	36	-	-
access	x	Laboratorios	Fa0/37	Activado	37	PCFICA-191	172.17.X.X
access	x	Laboratorios	Fa0/38	Disponible	38	-	-
access	x	Laboratorios	Fa0/39	Activado	39	PCFICA-198	172.17.X.X
access	x	Laboratorios	Fa0/40	Activado	40	PCFICA-200	172.17.X.X
access	x	Laboratorios	Fa0/41	Activado	41	-	-
access	x	Laboratorios	Fa0/42	Disponible	42	-	-
access	x	Laboratorios	Fa0/43	Disponible	43	-	-
access	x	Laboratorios	Fa0/44	Disponible	44	-	-
access	x	Laboratorios	Fa0/45	Disponible	45	-	-
access	x	Laboratorios	Fa0/46	Disponible	46	-	-
access	x	Laboratorios	Fa0/47	Disponible	47	-	-
access	x	Administrativos	Fa0/48	Activado	48	-	-
trunk			G1/0				
			G2/0				

Fuente: Información DDTI de la UTN, adaptado de (Vallejos Garzón, 2019)

- **Laboratorio 3**

Los equipos de telecomunicaciones que se presentan en la Tabla 11 y su mapeo de puertos como se visualiza en la Tabla 12 se encuentran en el laboratorio 2 el cual está ubicado en la planta 2 de la facultad FICA.

Tabla 11

Equipos Lab.3 – FICA

Equipos de Telecomunicaciones	Marca	Nombre	Dirección IP	Cantidad
Rack de pared de 19”	Panduit	-----	-----	1
Patch Panel de 24 Puertos Cat 6	NewLink	-----	-----	1
Switch de 48 puertos	WS-C2960-48TC-L	SW01.FICA.LAB2.ACC.PA1.R02	172.17.X.X	1
Switch de 48 puertos	WS-C2960-48TC-L	SW01.FICA.LAB3.ACC.PA1.R03	172.17.X.X	1

Fuente: Información DDTI de la UTN, adaptado de (Espinosa Padilla, 2017)

Tabla 12

Mapeo de red Lab.3 -FICA

Switch Catalyst 2960 Laboratorio 3							Equipo Conectado	
Modo VLAN	**VAN**	**Descripción**	**Puerto**	**Punto Red/*N°***	**Estado**	**Patch Panel**	**Nombre**	**IP**
access	x	Laboratorios	Fa0/1	Si/A01	Activado	A01	PCFICA-390	-
access	x	Laboratorios	Fa0/2	Si/A02	Disponible	A02	-	-
access	x	Laboratorios	Fa0/3	Si/A03	Activado	A03	PCFICA-388	172.17.X.X
access	x	Laboratorios	Fa0/4	Si/A04	Activado	A04	PCFICA-389	172.17.X.X
access	x	Laboratorios	Fa0/5	Si/A05	Disponible	A05	-	-
access	x	Laboratorios	Fa0/6	Si/A06	Activado	A06	PCFICA-382	172.17.X.X
access	x	Laboratorios	Fa0/7	Si/A07	Activado	A07	PCFICA-383	172.17.X.X

access	x	Laboratorios	Fa0/8	Si/A08	Activado	A08	PCFICA-384	172.17.X.X
access	x	Laboratorios	Fa0/9	Si/A09	Activado	A09	PCFICA-378	172.17.X.X
access	x	Laboratorios	Fa0/10	Si/A10	Activado	A10	PCFICA-376	172.17.X.X
access	x	Laboratorios	Fa0/11	Si/A11	Activado	A11	PCFICA-377	172.17.X.X
access	x	Laboratorios	Fa0/12	Si/A12	Activado	A12	PCFICA-372	172.17.X.X
access	x	Laboratorios	Fa0/13	Si/A13	Activado	A13	PCFICA-371	172.17.X.X
access	x	Laboratorios	Fa0/14	Si/A14	Disponible	A14	-	-
access	x	Laboratorios	Fa0/15	Si/A15	Disponible	A15	-	-
access	x	Laboratorios	Fa0/16	Si/A16	Activado	A16	PCFICA-370	172.17.X.X
access	x	Laboratorios	Fa0/17	Si/A17	Disponible	A17	-	-
access	x	Laboratorios	Fa0/18	Si/A18	Activado	A18	PCFICA-366	172.17.X.X
access	x	Laboratorios	Fa0/19	Si/A19	Activado	A19	PCFICA-364	172.17.X.X
access	x	Laboratorios	Fa0/20	Si/A20	Activado	A20	PCFICA-365	172.17.X.X
access	x	Laboratorios	Fa0/21	Si/A21	Disponible	A21	-	-
access	x	Laboratorios	Fa0/22	Si/A22	Activado	A22	PCFICA-365	172.17.X.X
access	x	Laboratorios	Fa0/23	Si/A23	Activado	A23	PCFICA-361	172.17.X.X
access	x	Laboratorios	Fa0/24	Si/A24	Activado	A24	PCFICA-364	172.17.X.X
access	x	Laboratorios	Fa0/25	Si/B01	Disponible	B01	-	-
access	x	Laboratorios	Fa0/26	Si/B02	Activado	B02	PCFICA-369	172.17.X.X
access	x	Laboratorios	Fa0/27	Si/B03	Activado	B03	PCFICA-367	172.17.X.X
access	x	Laboratorios	Fa0/28	Si/B04	Activado	B04	PCFICA-368	172.17.X.X
access	x	Laboratorios	Fa0/29	Si/B05	Disponible	B05	-	-
access	x	Laboratorios	Fa0/30	Si/B06	Disponible	B06	-	-
access	x	Laboratorios	Fa0/31	Si/B07	Activado	B07	PCFICA-375	172.17.X.X
access	x	Laboratorios	Fa0/32	Si/B08	Activado	B08	PCFICA-373	172.17.X.X
access	x	Laboratorios	Fa0/33	Si/B09	Activado	B09	PCFICA-374	172.17.X.X
access	x	Laboratorios	Fa0/34	Si/B10	Activado	B10	PCFICA-379	172.17.X.X
access	x	Laboratorios	Fa0/35	Si/B11	Activado	B11	PCFICA-381	172.17.X.X
access	x	Laboratorios	Fa0/36	Si/B12	Activado	B12	PCFICA-380	172.17.X.X

access	x	Laboratorios	Fa0/37	Si/B13	Disponible	B13	-	-
access	x	Laboratorios	Fa0/38	Si/B14	Activado	B14	PCFICA-386	172.17.X.X
access	x	Laboratorios	Fa0/39	Si/B15	Activado	B15	PCFICA-387	172.17.X.X
access	x	Laboratorios	Fa0/40	Si/B16	Activado	B16	PCFICA-385	172.17.X.X
access	x	Laboratorios	Fa0/41	Si/B17	Disponible	B17	-	-
access	x	Laboratorios	Fa0/42	NO	Disponible	-	-	-
access	x	Laboratorios	Fa0/43	Si/B19	Disponible	B19	-	-
access	x	Laboratorios	Fa0/44	NO	Disponible	-	-	-
access	x	Laboratorios	Fa0/45	NO	Disponible	-	-	-
access	x	Laboratorios	Fa0/46	NO	Disponible	-	-	-
access	x	Laboratorios	Fa0/47	NO	Disponible	-	-	-
access	x	Administrativos	Fa0/48	NO	Disponibel	-	-	-
trunk			G1/0	-				
			G2/0			A01		

Fuente: Información DDTI de la UTN, adaptado de (Vallejos Garzón, 2019)

- **Laboratorio 4**

Los equipos de telecomunicaciones que se presentan en la Tabla 13 y su mapeo de puertos como se visualiza en la Tabla 14, se encuentran en el laboratorio 2 el cual está ubicado en la planta 2 de la facultad FICA.

Tabla 13

Equipos Lab.4 – FICA

Equipos de Telecomunicaciones	Marca	Nombre	Dirección IP	Cantidad
Rack de 19” de ancho – 24UR	-----	-----	-----	1
Patch Panel de 24 Puertos Cat 6	-----	-----	-----	3

Switch de 48 puertos	WS-C2960-48TC-L	SW02.FICA.LAB3.ACC.PA1.R03	172.17.X.X	1
Switch de 48 puertos	WS-C2960-48TC-L	SW01.FICA.LAB3.ACC.PA1.R03	172.17.X.X	1

Fuente: Información DDTI de la UTN, adaptado de (Vallejos Garzón, 2019)

Tabla 14

Mapeo de red Lab.4 – FICA

		Switch Catalyst 2960 Laboratorio 4					**Equipo Conectado**	
Modo VLAN	**VAN**	**Descripción**	**Puerto**	**Punto Red/*N°***	**Estado**	**Patch Panel**	**Nombre**	**IP**
access	x	Laboratorios	Fa0/1	Si/A01	Disponible	A01	-	-
access	x	Laboratorios	Fa0/2	Si/A02	Disponible	A02	-	-
access	x	Laboratorios	Fa0/3	Si/A03	Disponible	A03	-	-
access	x	Laboratorios	Fa0/4	Si/A04	Disponible	A04	-	-
access	x	Laboratorios	Fa0/5	Si/A05	Activado	A05	PCFICA-350	172.17.X.X
access	x	Laboratorios	Fa0/6	Si/A06	Activado	A06	PCFICA-352	172.17.X.X
access	x	Laboratorios	Fa0/7	Si/A07	Disponible	A07	-	-
access	x	Laboratorios	Fa0/8	Si/A08	Activado	A08	PCFICA-351	172.17.X.X
access	x	Laboratorios	Fa0/9	Si/A09	Disponible	A09	-	-
access	x	Laboratorios	Fa0/10	Si/A10	Activado	A10	PCFICA-357	172.17.X.X
access	x	Laboratorios	Fa0/11	Si/A11	Activado	A11	PCFICA-356	172.17.X.X
access	x	Laboratorios	Fa0/12	Si/A12	Disponible	A12	-	-
access	x	Laboratorios	Fa0/13	Si/A13	Activado	A13	PCFICA-343	172.17.X.X
access	x	Laboratorios	Fa0/14	Si/A14	Activado	A14	PCFICA-181	172.17.X.X
access	x	Laboratorios	Fa0/15	Si/A15	Activado	A15	PCFICA-341	172.17.X.X
access	x	Laboratorios	Fa0/16	Si/A16	Disponible	A16	-	-
access	x	Laboratorios	Fa0/17	Si/A17	Activado	A17	PCFICA-347	172.17.X.X
access	x	Laboratorios	Fa0/18	Si/A18	Activado	A18	PCFICA-346	172.17.X.X
access	x	Laboratorios	Fa0/19	Si/A19	Disponible	A19	-	-

access	x	Laboratorios	Fa0/20	Si/A20	Disponible	A20	-	-
access	x	Laboratorios	Fa0/21	Si/A21	Disponible	A21	-	-
access	x	Laboratorios	Fa0/22	NO	Disponible	-	-	-
access	x	Laboratorios	Fa0/23	Si/A23	Disponible	A23	-	-
access	x	Laboratorios	Fa0/24	Si/A24	Disponible	A24	-	-
access	x	Laboratorios	Fa0/25	Si/B01	Disponible	B01	-	-
access	x	Laboratorios	Fa0/26	Si/B02	Disponible	B02	-	-
access	x	Laboratorios	Fa0/27	Si/B03	Activado	B03	PCFICA-344	172.17.X.X
access	x	Laboratorios	Fa0/28	Si/B04	Activado	B04	PCFICA-343	172.17.X.X
access	x	Laboratorios	Fa0/29	Si/B05	Activado	B05	PCFICA-345	172.17.X.X
access	x	Laboratorios	Fa0/30	Si/B06	Activado	B06	PCFICA-348	172.17.X.X
access	x	Laboratorios	Fa0/31	Si/B07	Activado	B07	-	-
access	x	Laboratorios	Fa0/32	Si/B08	Disponible	B08	-	-
access	x	Laboratorios	Fa0/33	Si/B09	Activado	B09	PCFICA-349	172.17.X.X
access	x	Laboratorios	Fa0/34	Si/B10	Disponible	B10	-	-
access	x	Laboratorios	Fa0/35	Si/B11	Activado	B11	PCFICA-353	172.17.X.X
access	x	Laboratorios	Fa0/36	Si/B12	Activado	B12	PCFICA-355	172.17.X.X
access	x	Laboratorios	Fa0/37	Si/B13	Disponible	B13	-	-
access	x	Laboratorios	Fa0/38	Si/B14	Activado	B14	PCFICA-354	172.17.X.X
access	x	Laboratorios	Fa0/39	Si/B15	Activado	B15	PCFICA-360	172.17.X.X
access	x	Laboratorios	Fa0/40	Si/B16	Activado	B16	PCFICA-198	172.17.X.X
access	x	Laboratorios	Fa0/41	Si/B17	Disponible	B17	-	-
access	x	Laboratorios	Fa0/42	Si/B18	Disponible	B18	-	-
access	x	Laboratorios	Fa0/43	Si/B19	Disponible	B19	-	-
access	x	Laboratorios	Fa0/44	NO	Disponible	-	-	-
access	x	Laboratorios	Fa0/45	NO	Disponible	-	-	-
access	x	Laboratorios	Fa0/46	NO	Disponible	-	-	-
access	x	Laboratorios	Fa0/47	NO	Disponible	-	-	-
access	x	Administrativos	Fa0/48	NO	Disponible	-	-	-

trunk	G1/0	-	
	G2/0		A01

Fuente: Información DDTI de la UTN, adaptado de (Vallejos Garzón, 2019)

- **Tercera Planta FICA**

La Tabla 15 presentada a continuación, demuestra las dependencias existentes, los puntos de red, biométricos, cámaras, APs y Racks

Tabla 15

Información sobre tercera planta - FICA

Dependencias	Puntos de red	Biométricos	Cámaras	Ap	Racks
Laboratorio 5 Software-Base de Datos	25	1	1		1
Laboratorio 6 Software-Multimedia	25	1	1		1
Laboratorio 7 Informática					
Pasillo	2		5	5	
TOTAL	33	6	7	5	2

Fuente: Información DDTI de la UTN, adaptado de (*Informe Diseño Cableado Estructurado*, 2017)

El tercer piso cuenta con cableado vertical y dos Racks en cada laboratorio, ya que a ellos se encuentran conectados los puntos de red de cada laboratorio, las cámaras y los biométricos.

- **Laboratorio 5**

El laboratorio 5 se encuentra en el segundo piso de la FICA, en el cual se ubica un switch WS-C2950-24 y su mapeo de puerto como se muestra en la Tabla 16.

Tabla 16

Mapeo de la red Lab.5 - FICA

		Switch Catalyst 2960 Laboratorio 5					Equipo Conectado	
Modo VLAN	**VAN**	**Descripción**	**Puerto**	**Punto Red/*Nº***	**Estado**	**Patch Panel**	**Nombre**	**IP**
access	x	Laboratorios	Fa0/1	NO	Disponible	NO	PCFICA-311	172.17.X.X
access	x	Laboratorios	Fa0/2	NO	Disponible	NO	PCFICA-312	172.17.X.X
access	x	Laboratorios	Fa0/3	NO	Disponible	NO	PCFICA-313	172.17.X.X
access	x	Laboratorios	Fa0/4	NO	Disponible	NO	PCFICA-314	172.17.X.X
access	x	Laboratorios	Fa0/5	NO	Activado	NO	PCFICA-315	172.17.X.X
access	x	Laboratorios	Fa0/6	NO	Activado	NO	PCFICA-316	172.17.X.X
access	x	Laboratorios	Fa0/7	NO	Activado	NO	PCFICA-317	172.17.X.X
access	x	Laboratorios	Fa0/8	NO	Activado	NO	PCFICA-318	172.17.X.X
access	x	Laboratorios	Fa0/9	NO	Activado	NO	-	-
access	x	Laboratorios	Fa0/10	NO	Activado	NO	-	-
access	x	Laboratorios	Fa0/11	NO	Activado	NO	-	-
access	x	Laboratorios	Fa0/12	NO	Activado	NO	-	-
access	x	Laboratorios	Fa0/13	NO	Activado	NO	PCFICA-319	172.17.X.X
access	x	Laboratorios	Fa0/14	NO	Activado	NO	PCFICA-320	172.17.X.X
access	x	Laboratorios	Fa0/15	NO	Activado	NO	PCFICA-321	172.17.X.X
access	x	Laboratorios	Fa0/16	NO	Activado	NO	PCFICA-322	172.17.X.X
access	x	Laboratorios	Fa0/17	NO	Activado	NO	PCFICA-323	172.17.X.X
access	x	Laboratorios	Fa0/18	NO	Activado	NO	PCFICA-324	172.17.X.X
access	x	Laboratorios	Fa0/19	NO	Activado	NO	PCFICA-325	172.17.X.X
access	x	Laboratorios	Fa0/20	NO	Activado	NO	PCFICA-326	172.17.X.X

access	x	Laboratorios	Fa0/21	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/22	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/23	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/24	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/1	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/2	NO	Activado	NO	PCFICA-327	172.17.X.X
access	x	Laboratorios	Fa0/3	NO	Activado	NO	PCFICA-328	172.17.X.X
access	x	Laboratorios	Fa0/4	NO	Activado	NO	PCFICA-329	172.17.X.X
access	x	Laboratorios	Fa0/5	NO	Activado	NO	PCFICA-330	172.17.X.X
access	x	Laboratorios	Fa0/6	NO	Activado	NO	PCFICA-331	172.17.X.X
access	x	Laboratorios	Fa0/7	NO	Activado	NO	PCFICA-332	172.17.X.X
access	x	Laboratorios	Fa0/8	NO	Activado	NO	PCFICA-333	172.17.X.X
access	x	Laboratorios	Fa0/9	NO	Activado	NO	PCFICA-334	172.17.X.X
access	x	Laboratorios	Fa0/10	NO	Activado	NO	PCFICA-335	172.17.X.X
access	x	Laboratorios	Fa0/11	NO	Activado	NO	PCFICA-336	172.17.X.X
access	x	Laboratorios	Fa0/12	NO	Activado	NO	PCFICA-337	172.17.X.X
access	x	Laboratorios	Fa0/13	NO	Activado	NO	PCFICA-338	172.17.X.X
access	x	Laboratorios	Fa0/14	NO	Activado	NO	PCFICA-339	172.17.X.X
access	x	Laboratorios	Fa0/15	NO	Activado	NO	PCFICA-340	172.17.X.X
access	x	Laboratorios	Fa0/16	NO	Activado	NO	-	-
access	x	Laboratorios	Fa0/17	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/18	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/19	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/20	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/21	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/22	NO	Disponible	NO	-	-
access	x	Laboratorios	Fa0/23	NO	Disponible	NO	-	-
access	x	Administrativos	Fa0/24	NO	Disponible	NO	-	-

trunk	G1/0 G2/0	-

Fuente: Información DDTI de la UTN, adaptado de (Vallejos Garzón, 2019)

- **Cuarta Planta FICA**

La Tabla 17 muestra las dependencias existentes, los puntos de red, biométricos, cámaras, APs y Racks.

Tabla 17

Información sobre Segunda planta FICA

Dependencias	Puntos de red	Biométricos	Cámaras	Aps	Racks
Pasillo y aulas		10	5	4	
TOTAL	0	10	5	4	

Fuente: Información DDTI de la UTN, adaptado de (*Informe Diseño Cableado Estructurado*, 2017)

- **Quinta Planta FICA**

La Tabla 18 demuestra las dependencias existentes, los puntos de red, biométricos, cámaras, APs y Racks.

Tabla 18

Quinto piso de la Facultad FICA

Dependencias	Puntos de red	Biométricos	Cámaras	Aps	Racks
Laboratorio 8 software-programación		1	1		1
Laboratorio 9 software-sistemas operativo			1		

Pasillos y aulas	52		3	2	
TOTAL	52	1	5	5	3

Fuente: Información DDTI de la UTN, adaptado de (*Informe Diseño Cableado Estructurado*, 2017)

- **Laboratorio 9**

El laboratorio 9 que corresponde a software-sistemas operativos se encuentra en el quinto piso de la FICA, en el cual se encuentran los equipos que se detallan en la Tabla 19 y su mapeo de puerto como se muestra en la Tabla 20.

Tabla 19

Equipo Lab.9 – FICA

Equipos de Telecomunicaciones	**Marca**	**Nombre**	**Dirección IP**	**Cantidad**
Rack de 19" de ancho – 36UR	Pandiut	-----	-----	1
Patch Panel de 24 Puertos Cat 6	Newlink	-----	-----	3
Switch de 48 puertos	WS-C2960	-----	172.17.X.X	1
Switch de 48 puertos	WS-C2960	-----	172.17.X.X	1

Fuente: Información DDTI de la UTN, adaptado de (Vallejos Garzón, 2019)

Tabla 20

Mapeo de red Lab.9 - FICA

		Switch Catalyst 2960 Laboratorio 9					**Equipo Conectado**	
Modo VLAN	**VAN**	**Descripción**	**Puerto**	**Punto Red/*N°***	**Estado**	**Patch Panel**	**Nombre**	**IP**
access	x	Laboratorios	Fa0/1	NO	Disponible	A01	PCFICA-311	172.17.X.X
access	x	Laboratorios	Fa0/2	NO	Disponible	A02	PCFICA-312	172.17.X.X
access	x	Laboratorios	Fa0/3	NO	Disponible	A03	PCFICA-313	172.17.X.X

access	x	Laboratorios	Fa0/4	NO	Disponible	A04	PCFICA-314	172.17.X.X
access	x	Laboratorios	Fa0/5	NO	Activado	A05	PCFICA-315	172.17.X.X
access	x	Laboratorios	Fa0/6	NO	Activado	A06	PCFICA-316	172.17.X.X
access	x	Laboratorios	Fa0/7	NO	Activado	A07	PCFICA-317	172.17.X.X
access	x	Laboratorios	Fa0/8	NO	Activado	A08	PCFICA-318	172.17.X.X
access	x	Laboratorios	Fa0/9	NO	Activado	A09	-	-
access	x	Laboratorios	Fa0/10	NO	Activado	A10	-	-
access	x	Laboratorios	Fa0/11	NO	Activado	A11	-	-
access	x	Laboratorios	Fa0/12	NO	Activado	A12	-	-
access	x	Laboratorios	Fa0/13	NO	Activado	A13	PCFICA-319	172.17.X.X
access	x	Laboratorios	Fa0/14	NO	Activado	A14	PCFICA-320	172.17.X.X
access	x	Laboratorios	Fa0/15	NO	Activado	A15	PCFICA-321	172.17.X.X
access	x	Laboratorios	Fa0/16	NO	Activado	A16	PCFICA-322	172.17.X.X
access	x	Laboratorios	Fa0/17	NO	Activado	A17	PCFICA-323	172.17.X.X
access	x	Laboratorios	Fa0/18	NO	Activado	A18	PCFICA-324	172.17.X.X
access	x	Laboratorios	Fa0/19	NO	Activado	A19	PCFICA-325	172.17.X.X
access	x	Laboratorios	Fa0/20	NO	Activado	A20	PCFICA-326	172.17.X.X
access	x	Laboratorios	Fa0/21	NO	Disponible	A21	-	-
access	x	Laboratorios	Fa0/22	NO	Disponible	A22	-	-
access	x	Laboratorios	Fa0/23	NO	Disponible	A23	-	-
access	x	Laboratorios	Fa0/24	NO	Disponible	A24	-	-
access	x	Laboratorios	Fa0/1	NO	Disponible	A25	-	-
access	x	Laboratorios	Fa0/2	NO	Activado	A26	PCFICA-327	172.17.X.X
access	x	Laboratorios	Fa0/3	NO	Activado	A27	PCFICA-328	172.17.X.X
access	x	Laboratorios	Fa0/4	NO	Activado	A28	PCFICA-329	172.17.X.X
access	x	Laboratorios	Fa0/5	NO	Activado	A29	PCFICA-330	172.17.X.X
access	x	Laboratorios	Fa0/6	NO	Activado	A30	PCFICA-331	172.17.X.X
access	x	Laboratorios	Fa0/7	NO	Activado	A31	PCFICA-332	172.17.X.X
access	x	Laboratorios	Fa0/8	NO	Activado	A32	PCFICA-333	172.17.X.X
access	x	Laboratorios	Fa0/9	NO	Activado	A33	PCFICA-334	172.17.X.X

access	x	Laboratorios	Fa0/10	NO	Activado	A34	PCFICA-335	172.17.X.X
access	x	Laboratorios	Fa0/11	NO	Activado	A35	PCFICA-336	172.17.X.X
access	x	Laboratorios	Fa0/12	NO	Activado	A36	PCFICA-337	172.17.X.X
access	x	Laboratorios	Fa0/13	NO	Activado	A37	PCFICA-338	172.17.X.X
access	x	Laboratorios	Fa0/14	NO	Activado	A38	PCFICA-339	172.17.X.X
access	x	Laboratorios	Fa0/15	NO	Activado	A39	PCFICA-340	172.17.X.X
access	x	Laboratorios	Fa0/16	NO	Activado	A40	-	-
access	x	Laboratorios	Fa0/17	NO	Disponible	A41	-	-
access	x	Laboratorios	Fa0/18	NO	Disponible	A42	-	-
access	x	Laboratorios	Fa0/19	NO	Disponible	A43	-	-
access	x	Laboratorios	Fa0/20	NO	Disponible	A44	-	-
access	x	Laboratorios	Fa0/21	NO	Disponible	A45	-	-
access	x	Laboratorios	Fa0/22	NO	Disponible	A46	-	-
access	x	Laboratorios	Fa0/23	NO	Disponible	A47	-	-
access	x	Administrativos	Fa0/24	NO	Disponible	A48	-	-
trunk			G1/0	-				
			G2/0					

Fuente: Información DDTI de la UTN, adaptado de (Vallejos Garzón, 2019)

En el quinto piso, el laboratorio y los cubículos cuentan con sus propis Racks, puntos de red, cámaras y biométricos, los cuales están dirigidos a los Racks más cercanos, este piso tiene un cableado horizontal, canaletas por techo y de pared.

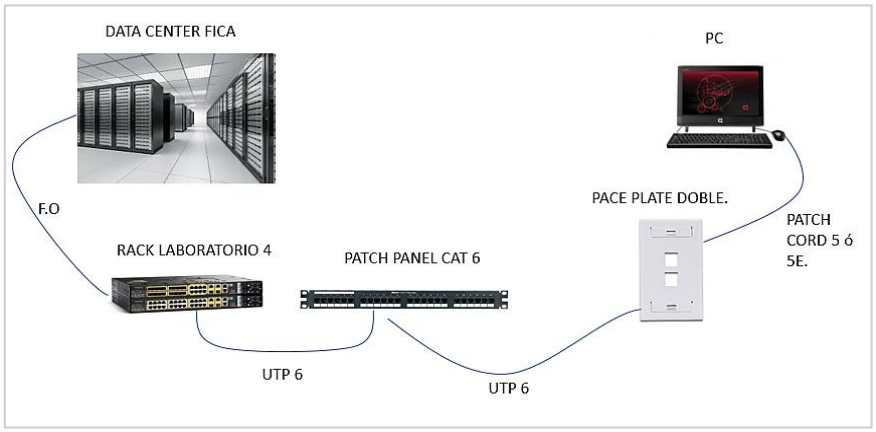
3.2.1.1.10. Revisión de Etiquetamiento y Recorridos

Para la revisión de Etiquetamiento y Recorridos se tomó al Rack del laboratorio 4 y se obtuvieron los siguientes resultados que se detallan en la Figura 22: se cuenta con dos switches Catalyst 2960, 3 regletas de patch panel (PPA, PPB, PPC) y una regleta de tomas eléctricas. Son 43 puntos de red dentro del laboratorio, los cuales estad distribuidos en dos grupos. Un grupo es llamado PPA, el cual cuenta con 24 puertos de red y el segundo grupo se

denomina PPB, contiene 19 puntos de red. Ambos puntos de red se encuentran conectados al switch Catalyt 296 de 48 puertos que se encuentra en el rack del laboratorio. Para el grupo llamado PPC no se lo toma en cuenta ya que no es utilizado dentro del laboratorio donde se encuentra el Rack.

Figura 22

Diagrama de Conexión de los puntos de red del Laboratorio 4



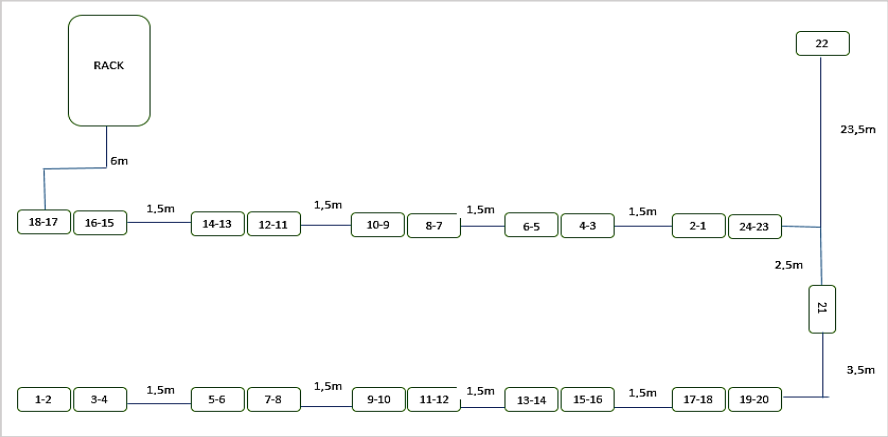
Fuente: Información DDTI de la UTN, adaptado de (*Informe Diseño Cableado Estructurado*, 2017)

Mediante el uso de la herramienta tester se logró encontrar los puntos de red de extremo a extremo y su respectiva conectividad, tomando en cuenta que existe un etiquetamiento tanto en patch panel como en faceplate.

En la Figura 23 se detalla los recorridos y distancias de cada uno de los puntos de red. Del Rack a los puntos de red N° 18-17, hay una distancia de 6metros y entre cada 4 puntos de red hay una separación de 1, 5 metros.

Figura 23

Distancias de los Puntos de Red en Laboratorio 4



Fuente: Información DDTI de la UTN, adaptado de (*Informe Diseño Cableado Estructurado*, 2017)

El cable de las paredes laterales que va desde el rack hasta la salida de trabajo cuenta con patch cord de cable de categoría 6, este va desde la salida de telecomunicaciones hasta el switch del computador.

La conexión que va desde el rack hasta la salida de telecomunicaciones se encuentra en buen estado y esta utiliza canaleta plástica con un grosor de 6cm para el enrutamiento, por ello se detalla en la Tabla 21 las características de cada uno de los puntos de red.

Tabla 21

Características de cada uno de los puntos de red del Laboratorio 4

Punto de Red	Etiqueta Patch Panel	Etiqueta Faceplate	Categoría Cable Cableado horizontal	Distancia(metros) desde el rack hasta la salida de trabajo	Tipo de Canaleta.	Patch Cord en Área de Trabajo.

PPA1	Si	Si	6	24	Plástica 6cm.	5e
PPA2	Si	Si	6	24	Plástica 6cm.	5e
PPA3	Si	Si	6	24	Plástica 6cm.	5e
PPA4	Si	Si	6	24	Plástica 6cm.	5e
PPA5	Si	Si	6	23	Plástica 6cm.	5e
PPA6	Si	Si	6	23	Plástica 6cm.	5e
PPA7	Si	Si	6	22,5	Plástica 6cm.	5e
PPA8	Si	Si	6	22,5	Plástica 6cm.	5e
PPA9	Si	Si	6	21	Plástica 6cm.	5e
PPA10	Si	Si	6	21	Plástica 6cm.	5e
PPA11	Si	Si	6	21,5	Plástica 6cm.	5e
PPA12	Si	Si	6	21,5	Plástica 6cm.	5e
PPA13	Si	Si	6	19,5	Plástica 6cm.	5e
PPA14	Si	Si	6	19,5	Plástica 6cm.	5e
PPA15	Si	Si	6	19	Plástica 6cm.	5e
PPA16	Si	Si	6	19	Plástica 6cm.	5e
PPA17	Si	Si	6	17,5	Plástica 6cm.	5e
PPA18	Si	Si	6	17,5	Plástica 6cm.	5e
PPA19	Si	Si	6	17	Plástica 6cm.	5e
PPA20	Si	Si	6	17	Plástica 6cm.	5e
PPA21	Si	Si	6	14,5	Plástica 6cm.	5e
PPA22	Si	Si	6	18	Plástica 6cm.	5e
PPA23	Si	Si	6	12	Plástica 6cm.	5e
PPA24	Si	Si	6	12	Plástica 6cm.	5e
PPB1	Si	Si	6	12	Plástica 6cm.	6
PPB2	Si	Si	6	12	Plástica 6cm.	5e
PPB3	Si	Si	6	10,5	Plástica 6cm.	5e

PPB4	Si	Si	6	10,5	Plástica 6cm.	6
PPB5	Si	Si	6	10	Plástica 6cm.	6
PPB6	Si	Si	6	10	Plástica 6cm.	6
PPB7	Si	Si	6	9	Plástica 6cm.	6
PPB8	Si	Si	6	9	Plástica 6cm.	5e
PPB9	Si	Si	6	9	Plástica 6cm.	5e
PPB10	Si	Si	6	9	Plástica 6cm.	6
PPB11	Si	Si	6	7,5	Plástica 6cm.	5e
PPB12	Si	Si	6	7,5	Plástica 6cm.	5e
PPB13	Si	Si	6	7	Plástica 6cm.	6
PPB14	Si	Si	6	7	Plástica 6cm.	6
PPB15	Si	Si	6	6	Plástica 6cm.	6
PPB16	Si	Si	6	6	Plástica 6cm.	6
PPB17	Si	Si	6	6	Plástica 6cm.	5e
PPB18	Si	Si	6	6	Plástica 6cm.	5e

Fuente: Información DDTI de la UTN, adaptado de (*Informe Diseño Cableado Estructurado*, 2017)

Nota. En la tabla ilustrada anteriormente se presenta un resumen de las características de cada uno de los puntos de red del Laboratorio 4.

3.2.1.2. FICAYA

3.2.1.2.1. Equipos Activos de la Red

En la **Tabla *22*** se visualizan los equipos activos que se encuentran en la facultad FICAYA y dentro de dicha tabla se detalla su ubicación, el nombre, la marca, el modelo y los puertos de cada equipo, esto con la finalidad de tener un registro de los equipos en la facultad mencionada.

Tabla 22

Equipos activos de la red que se encuentran en la red

Nº	Dependencia	Ubicación	Nombre	Marca	Modelo	# Puertos
1		Datacenter	SW01.FICA.DC.DIS.PB.R01	Cisco	C9300-48UXM-E	
2		Datacenter	SW02.FICA.DC.DIS.PB.R01	Cisco	WS-C4510R+E	
3		Laboratorio I	SW01.FICA.LAB1.ACC.PA1.R01	Cisco	WS-C2960-48TC-L	48
4		Laboratorio II	SW01.FICA.LAB2.ACC.PA1.R02	Cisco	WS-C2960-48TC-L	48
5		Laboratorio III	SW01.FICA.LAB3.ACC.PA1.R03	Cisco	WS-C2960-48TC-L	48
6		Laboratorio III	SW02.FICA.LAB3.ACC.PA1.R03	Cisco	WS-C2960-24TC-L	24
7		Laboratorio MAC	SW-LABMAC	Cisco	WS-C2960-48TC-L	48
8	**FICA**	Laboratorio Cisco	SW01.FICA.LABCISCO.ACC.PA5.R05	Cisco	WS-C2960-48TC-L	48
9		Laboratorio Cisco	SW02.FICA.LABCISCO.ACC.PA5.R05	Cisco	WS-C2960-48TC-L	48
10		Sala de Investigación	SW01.FICA.CUBI.ACC.PA5.R06	Cisco	WS-C2960-48TC-L	48
11		Sala de Profesores	SW01.FICA.ASOPROF.ACC.PA5.R07	Cisco	WS-C2960-24TC-L	24
12		Laboratorio 6	SW02.FICA.LAB5.ACC.PA3.R08	Cisco	WS-C2950-24	
13		Switches Servidores	SW_01_FICA	3COM	SuperStack 3226	
14		Laboratorio 5	SW01.FICA.LAB5.ACC.PA3.R08	Cisco	WS-C2950-24	
15		Electricidad	SW01.ELECT.DC.DIS.PB.R01	Cisco	C9200L-48P-4X-E	
16		Laboratorio 7	SW-LAB7	Cisco	WS-C2950-24	

Fuente: Departamento de Desarrollo de Tecnológico e Informático.

3.2.1.2.2. Recopilación de información sobre cableado estructurado y puntos de red en cada planta.

La facultad FICAYA consta de un cableado estructurado CAT 6ª, dicho cable se describe dentro del estándar TIA e ISO EN para clase Ea y categoría 6A, y permite trabajar a velocidades de hasta 10Gbps dentro de un entorno Ethernet, pudiendo también llevar otras señales como servicios básicos de telefonía, TokenRing y ATM. Diseñado para transmisión a frecuencias de hasta 500MHz. El sistema completo de cableado UTP Cat6A incluye el cable LSHF, módulos hembra, paneles de 24, paneles de ordenación y latiguillos de varias medidas y colores. Con relleno central en forma de estrella para mantener y aumentar el rendimiento del cable.(Cervi, 2018)

3.2.1.3. FECYT

3.2.1.3.1. Elementos de red por planta

- **Planta Baja**

Se encuentra el Data Center.

Existen puntos de red que no se encuentran en uso y en los laboratorios 1 y 2 de computación existía un router para que haya más puntos de red para los computadores de esa oficina. Solo el laboratorio 1 tiene un etiquetado de cada punto de res a un área de trabajo. También se encuentra el Laboratorio de inglés y diseño, con su respectivo cableado, también existen 4 cámaras habilitadas en esta planta. (Escobar César, 2017)

- **Segunda Planta**

Existen 3 cámaras habilitadas y un switch Cisco Catalyst 9300 en el cual se conectan 4 APs en funcionamiento.

- **Tercera Planta**

Existe un switch Cisco Catalyst 9300 de cual se conectan 4 APs funcionales y 3 cámaras en funcionamiento.

- **Cuarta Planta**

Existe un switch Cisco Catalyst 9300 de cual se conectan 4 APs funcionales y posee 3 cámaras en funcionamiento

- **Quinta Planta**

Se halla un Rack y existe un switch Cisco Catalyst 9300 de cual se conectan 4 APs funcionales.

3.2.1.3.2. Equipos activos de la red

A continuación, en la Tabla 23 se visualizan los equipos activos que se encuentran en la facultad FECYT y dentro de dicha tabla se detalla su ubicación, el nombre, la marca, el modelo y los puertos de cada equipo, esto con la finalidad de tener un registro de los equipos en la facultad mencionada.

Tabla 23

Equipos activos de la red que se encuentran en la red

Nº	Dependencia	Ubicación	Nombre	Marca	Modelo	# Puertos
1	FECYT	Cuarto de Equipos	SW01.FECYT.DC.DIS.PB.R01	Cisco	C9300-48UXM-E	
2		Cuarto de Equipos	SW03.FECYT.DC.ACC.PB.R0	Cisco	WS-C2960-48TC-L	48
3		Cuarto de Equipos	SW04.FECYT.DC.ACC.PB.R01	Cisco	WS-C2960-48TC-L	48
4		Cuarto de Equipos	SW02.FECYT.DC.ACC.PB.R01	Cisco	WS-C2960-24TC-L	24
5		Laboratorio 1	SW05.FECYT.LAB1.PB	Cisco	WS-C2960-48TC-L	48
6		Laboratorio 2	SW06.FECYT.LAB2.PB	Cisco	WS-C2960-48TC-L	48
7		Laboratorio MAC	SW07.FECYT.LABMAC.PB	Cisco	WS-C2960-48TC-L	48
8		Cubículos Docentes 1	SW-CUBICULOS-FECYT-1	3COM	Switch 4400 SE	
9		Cubículos Docentes 2	SW-CUBICULOS-FECYT-2	3COM	Switch 4400 SE	
10		Ultimo Piso	SW01.FECYT.PA5.R5	Cisco	WS-C2960X-48TS-L	
11		Psicología	SW01.FECYT.PB.PSICO.R6	Cisco	WS-C2960-48TC-L	48

Fuente: Departamento de Desarrollo de Tecnológico e Informático

3.2.1.4. FCCSS

3.2.1.4.1.Equipos activos de la red

En la siguiente Tabla 24 se visualizan los equipos activos que se encuentran en la facultad FCCSS y dentro de dicha tabla se detalla su ubicación, el nombre, la marca, el modelo y los puertos de cada equipo, esto con la finalidad de tener un registro de los equipos en la facultad mencionada.

Tabla 24

Ubicación actual de los equipos activos de red en la Facultad - FCCSS

Nº	Dependencia	Ubicación	Nombre	Equipo	Modelo	# Puerto
1	**FCCSS**	Cuarto de Equipos	SW01.FCCSS.DC.DIS.PB.R01	Cisco	C9300-48UXM-E	48
2		Cuarto de Equipos	SW02.FCCSS.DC.ACC.PB.R01	Cisco	WS-C3850-48T-S	
3		Cuarto de Equipos	SW03.FCCSS.DC.ACC.PB.R01	Cisco	WS-C2960X-48TS-LL	
4		Planta Alta 4	SW04.FCCSS.PASILLO.PA4.R02	Cisco	WS-C2960X-48TS-L	48
5		Planta Alta 4	SW05.FCCSS.LAB1.PA4.R03	Cisco	WS-C2960X-48TS-L	48
6		Planta Alta 4	SW06.FCCSS.LAB2.PA4.R04	Cisco	WS-C2960X-48TS-L	48

Fuente: Departamento de Desarrollo de Tecnología e Innovación

3.2.1.5. FACAE

3.2.1.5.1. Situación Actual de la red cableada

La facultad FACAE consta de un cableado estructurado CAT 6ª, dicho cable se describe dentro del estándar TIA e ISO EN para clase E y categoría 6A, y permite trabajar a velocidades de hasta 10Gbps dentro de un entorno Ethernet, pudiendo también llevar otras señales como servicios básicos de telefonía, TokenRing y ATM. Diseñado para transmisión a frecuencias de hasta 500MHz. El sistema completo de cableado UTP Cat6A incluye el cable LSHF, módulos hembra, paneles de 24, paneles de ordenación y latiguillos de varias medidas y colores. Con relleno central en forma de estrella para mantener y aumentar el rendimiento del cable.(Cervi, 2018)

La Facultad de Ciencias Administrativas y Económicas tiene una infraestructura civil que se encuentra distribuida de la siguiente manera:

- Planta Baja: Oficinas Administrativas y Laboratorios de Computación
- Primer Piso: Aulas de aprendizaje
- Segundo Piso: Aulas de aprendizaje
- Tercer piso: Aulas de aprendizaje

- **Establecimiento de los puntos de red por zonas**

La siguiente Tabla 25 muestra los equipos en la planta baja y por área en la facultad FACAE

Tabla 25

Puntos de red por zonas

Planta Baja						
Área	**# PCs**	**Puntos de Red**	**Telefonos IPs**	**Cámaras**	**APs**	**# Racks**
Laboratorio de Imagen	21	21		1		
Laboratorio de Audiovisuales	35	35		1		
Laboratorio 1 de Computación	41	41		1		
Laboratorio 2 de Computación	33	33		1		1
Laboratorio 3 de Computación						
Sub-Decanato		1				
Secretaria-Sub-Decanato		1	1			
Cubículos (112)		4				

Secretaria Ing. Comercial	2	1	
Auditorio	1		
Coordinación Contabilidad	3	1	
Cubículos (103)	5		
Secretaria Mercadotecnia	3	1	
Secretaria Gastronomía	1	1	
Coordinación Gastronomía Y Derecho	2	1	
Departamento Investigadores Turismo	4		
Decanato Secretaria	5	1	1
Decanato Secretaria Abogado			
Investigadores Ing. Comercial	3		
Investigadores Gastronomía	1		

Investigadores	3				
Contabilidad					
Grupo	1			1	
Potencia					
Sala				1	
Profesores					
Investigadores	1				
Mercadotecnia					
Y					
Contabilidad					
Laboratorio	5		1		
Publicidad					
Oficina					
Laboratorios					
Data Center					1
Pasillos	3	1		1	
Parte Exterior			1	4	
Primer Piso					
Pasillos	3			2	
Segundo Piso					
Pasillos	3			2	
Tercer Piso					
Pasillos	2			2	

Fuente: Información DDTI de la UTN, adaptado de (Carrera et al., 2017)

3.2.1.5.2.Equipos activos de red

En la Tabla 26 se visualizan los equipos activos que se encuentran en la facultad FACAE y dentro de dicha tabla se detalla su ubicación, el nombre, la marca, el modelo y los

puertos de cada equipo, esto con la finalidad de tener un registro de los equipos en la facultad mencionada.

Tabla 26

Equipos activos dentro de la Facultad - FACAE

Nº	Dependencia	Ubicación	Nombre	Marca	Modelo	# Puertos
1	FACAE	Cuarto de Equipos	SW01.FACAE.DC.DIS.PB.R01	Cisco	C9300-48UXM-E	
2		Cuarto de Equipos	SW02.FACAE.DC.ACC.PB.R01	Cisco	9200L-48T-4X-E	
3		Cuarto de Equipos	SW03.FACAE.DC.ACC.PB.R01	Cisco	9200L-48T-4X-E	
4		Cuarto de Equipos	SW04.FACAE.DC.ACC.PB.R01	Cisco	9200L-48T-4X-E	
5		Cuarto de Equipos	SW05.FACAE.DC.ACC.PB.R01	Cisco	9200L-48T-4X-E	
6		Cuarto de Equipos	SW06.FACAE.DC.ACC.PB.R01	Cisco	9200L-48P-4X-E	
7		Ultimo Piso	SW01.FACAE.DC.ACC.PA4.R01	Cisco	WS-C2960X-48TS-L	48

Fuente: Departamento de Desarrollo de Tecnológico e Informático

3.2.1.6. POSGRADO

3.2.1.6.1.Equipos activos de red

A continuación, en la Tabla 27 se visualizan los equipos activos que se encuentran en la facultad Posgrado y dentro de dicha tabla se detalla su ubicación, el nombre, la marca, el modelo y los puertos de cada equipo, esto con la finalidad de tener un registro de los equipos en la facultad mencionada.

Tabla 27

Ubicación actual de los equipos de red en el edificio de Posgrado

Nº	Dependencia	Ubicación	Nombre	Modelo	Marca	# Puertos
58	Posgrado	Cuarto de Equipos	SW01.POSG.DC.DIS.PB.R01	Cisco	C9300-48P-E	
59		Cuarto de Equipos	SW02.POSG.DC.ACC.PB.R01	Cisco	WS-C4503R+E	
60		Cuarto de Equipos	SW03.POSG.DC.ACC.PB.R01	Cisco	WS-C2960-24TC-L	24
61		Cuarto de Equipos	SW04.POSG.DC.ACC.PB.R01	Cisco	WS-C2960-24TC-L	42
62		Cuarto de Equipos	SW05.POSG.DC.ACC.PB.R01	Cisco	WS-C2960S-48TS-S	48
63		Cuarto de Equipos	SW06.POSG.DC.ACC.PB.R01	Cisco	WS-C2960S-48TS-S	48
64		Primer Piso	SW01.POSG.ACC.PA1.R02	Cisco	WS-C2960S-48TD-L	48

65	Primer Piso	SW02.POSG.ACC.PA1.R02	Cisco	WS-C2960S-48TS-S	48
66	Primer Piso	SW03.POSG.ACC.PA1.R02	Cisco	WS-C2960S-48TS-S	48
67	Tercer Piso	SW01-POSG-PA3	Cisco	SG-200-26	48

Fuente: Departamento de Desarrollo de Tecnológico e Informático

3.2.2. Descripción de la red en otras dependencias

3.2.2.1. Edificio Central

3.2.2.1.1. Situación actual de la red cableada

El edificio central de la Universidad Técnica del Norte cuenta con cinco plantes actualmente y se encuentra distribuido por diferentes instancias de gestión.

3.2.2.1.2. Equipos de comunicación por Planta

- **Planta Baja**

En esta planta se encuentran las oficinas de las siguientes dependencias:

- Departamento Financiero
- Departamento de Vinculación
- Coordinación de Transporte
- Departamento de Sistemas (Data Center Universitario)
- Gestión de Talento Humano Informática
- Jefatura de adquisiciones
- Instituto de alto rendimiento
- Oficina del estudiante

En esta planta se encuentran dos racks de comunicación que están ubicados de la siguiente manera que a continuación se detallan en la Tabla 28, los cables de conexión, puntos de red están distribuidos en un techo falso, mismo el cual se encuentra en bandejas ya que estas conducen todo el sistema de cableado a cada una de las oficinas.

Tabla 28

Ubicación de equipos de comunicación en la Planta Baja

Ubicación	Racks	APs
Bloque Izquierdo	Rack B	
Bloque Derecho	Rack A	
Departamento Vinculación		Access Point 1
Departamento Financiero		Access Point 2
Almacenamiento y Bodega		Access Point 3

Fuente: Información DDTI de la UTN, adaptado de (Quilca Fernández et al., 2017)

- **Segunda Planta**

A continuación, se mencionan a las dependencias que se encuentran en esta Planta:

- Vicerrectorado Administrativo
- Vicerrectorado Académico
- Relaciones Publicas
- Rectorado
- Sala de Reuniones
- Archivos

En la Tabla 29 se describen los elementos de comunicación de la segunda planta

Tabla 29

Equipos de comunicación en la Segunda Planta

Ubicación	Racks	APs
Bloque Izquierdo	Rack C (Switchs)	
Bloque Derecho	Rack D (Switchs)	
Vicerrector académico	Access Point 1	
Pasillo	Access Point 2	

Fuente: Información DDTI de la UTN, adaptado de (Quilca Fernández et al., 2017)

- **Tercera Planta**

A continuación, en la se

Tabla ***30*** detallan las dependencias que existen en dicha planta:

- Sala José Martí
- Planeamiento Integral y Evaluación
- Cubículos de investigadores
- Sala Francisco de Orellana
- Comisión General de Evaluación Interna
- CUICYT

Tabla 30

Equipamiento de comunicación en la Tercera Planta

Ubicación	Racks	APs
Bloque Izquierdo	Rack E	
Vicerrectorado		Access Point 1
Pasillo		Access Point 2

Fuente: Información DDTI de la UTN, adaptado de (Quilca Fernández et al., 2017)

Cuarta Planta

En esta Planta se encuentra las siguientes dependencias:

- Radio y Televisión
- Dirección de Comunicación Organizacional
- Sala Simón Bolívar
- Procuraduría
- Departamento de mantenimiento y Construcciones

En la siguiente Tabla 31 se muestran los equipos de comunicación que se encuentran alojados en la cuarta planta del Edificio Central.

Tabla 31

Equipos de comunicación ubicados en la Cuarta Planta

Ubicación	Racks	APs
Bloque Izquierdo	Rack F (Switchs)	
Vicerrectorado		Access Point 1
Pasillo		Access Point 2

Fuente: Información DDTI de la UTN, adaptado de (Quilca Fernández et al., 2017)

- **Quinta Planta**

En la Quinta Planta se encuentran las siguientes dependencias, tal y como se visualizan en la Tabla 32:

- Dos Bodegas Vacías
- Secretaria del Departamento Financiero
- Talento Humano

Tabla 32

Equipos de comunicación ubicados en la Quinta Planta

Ubicación	Racks	APs
Bloque Izquierdo	Rack C (Switchs)	
Vicerrectorado		Access Point 1
Pasillo		Access Point 2

Fuente: Información DDTI de la UTN, adaptado de (Quilca Fernández et al., 2017)

3.2.2.1.3.Distribución actual de los puntos de red y equipos receptores

En la Tabla 33 se visualiza la distribución de los puntos de red en el Edificio Central.

Tabla 33

Distribución de los puntos de red en el Edificio Central

Pisos	Puntos de Red
Planta Baja	59
Segunda Planta	46
Tercera Planta	59
Cuarta Planta	36
Quinta Planta	23
Total	223

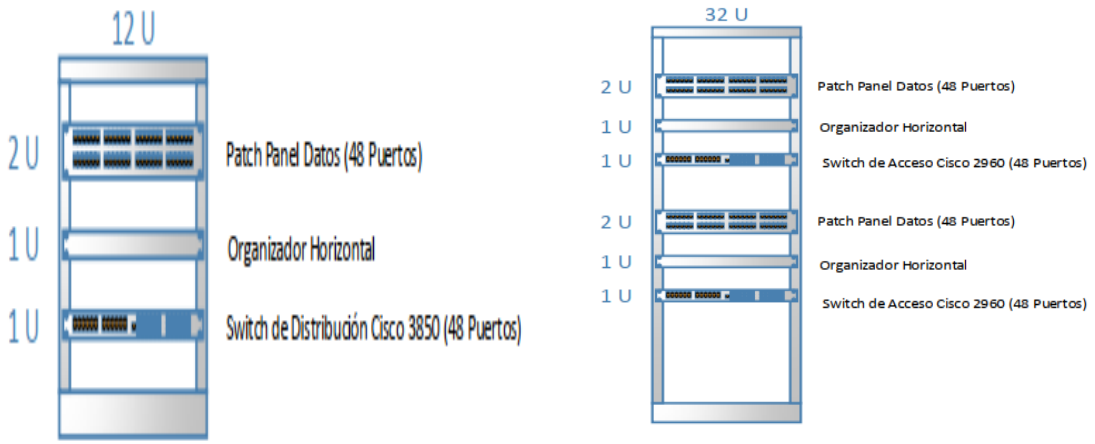
Fuente: Información DDTI de la UTN, adaptado de (Quilca Fernández et al., 2017)

Se obtiene un total de 223 puntos de red, tanto para vos y datos. Existen dos racks en cada piso, tal y como se visualiza en la

Figura ***24***.

Figura 24

Switchs distribución del Rack



Fuente: Información DDTI de la UTN, adaptado de la chica de DISEÑO DEL SISTEMA DE CABLEADO ESTRUCTURADO CAT. 6ª PARA EL EDIFICIO CENTRAL DE LA UNIVERSIDAD TECNICA DEL NORTE (p.44), por Quilca Fernández et al., 2017)

Nota. Los racks se encuentran conectados mediante fibra óptica al rack principal, el cual se encuentra ubicado en el DDTI dentro del Edificio Central.

3.2.2.1.4.

3.2.2.1.5.Equipos de conectividad

En la Tabla 34 se detallan los equipos existentes actualmente en el Edificio Central, mencionando la ubicación, el nombre del dispositivo, la marca, el modelo y el número de puertos.

Tabla 34

Ubicación actual de los equipos de red en el Edificio Central

Nº	Dependencia	Ubicación	Nombre - Nuevo	Marca	Modelo	# Puertos
1	EDIFICIO CENTRAL	Datacenter	SW.CENTRAL.DC.COR.PB.RDC	Cisco	C9407R	
2		Datacenter	SW-Nexus	Nexus	Nexus 5548	
3		Datacenter Chasis Blade	SW-Afrodita	Cisco	WS-CBS3020-HPQ	
4		Datacenter Chasis Blade	SW-Apolo	Cisco	WS-CBS3020-HPQ	
5		Planta Baja	SW01.CENTRAL.BODEGA.ACC.PB.R02	Cisco	WS-C2960-48TC-L	48
6		Planta Alta 1	SW01.CENTRAL.RECT.ACC.PA1.R03	Cisco	WS-C2960-48TC-L	48
7		Planta Alta1	SW02.CENTRAL.RECT.ACC.PA1.R03	Cisco	WS-C2960-24TC-L	24
8		Auditorio José Martí	SW01.CENTRAL.AUDIJM.ACC.PA2.R04	Cisco	WS-C2960-48TC-L	48
9		Auditorio José Martí	SW02.CENTRAL.AUDIJM.ACC.PA2.R04	Cisco	WS-C2960-48TC-L	48
10		Canal Universitario	SW01.CENTRAL.UTV.ACC.PA4.R05	Cisco	WS-C2960-48TC-L	48
11		Planta Alta 4	SW01.CENTRAL.TERRAZA.DIS.PA5.R06	Cisco	WS-C3850-48T	48
12		Planta Alta 4	SW02.CENTRAL.TERRAZA.ACC.PA5.R06	Cisco	WS-C2960X-48TS-L	48
13		Planta Alta 4	SW03.CENTRAL.TERRAZA.ACC.PA5.R06	Cisco	WS-C2960-48TC-L	48
14		Canal Universitario	SW02.CENTRAL.UTV.ACC.PA4.R5	Cisco	WS-C2960-48TC-L	48
15		Entrada Principal	SW-ACCESO	Cisco	WS-C2960X-24PS-L	24

Fuente: Departamento de Desarrollo de Tecnológico e Informático.

3.2.2.1.6. Distribución de los racks y sus componentes

En la siguiente Tabla 35 se detalla la Ubicación y distribución de los Racks con su respectivo Patch Panel y equipo.

Tabla 35

Locación y distribución de los racks y sus componentes.

Pisos	Rack	Patch Panel	Equipo
Planta Baja	32U	48 Puertos	2 Switches de 48 puertos
Segunda Planta	32U	48 Puertos	2 Switches de 48 puertos
Tercera Planta	32U	48 Puertos	2 Switches de 48 puertos
Cuarta Planta	32U	48 Puertos	2 Switches de 48 puertos
Quinta Planta	32U		2 Switches de 48 puertos
Total	223		

Fuente: Información DDTI de la UTN, adaptado de (Quilca Fernández et al., 2017)

3.2.2.2. U. EMPRENDE, CAI

El edificio de la U. EMPRENDE, CAI presenta los siguientes equipos de telecomunicaciones y se lo presenta a través de la Tabla 36.

Tabla 36

Equipos de Telecomunicaciones – U. EMPRENDE, CAI

N°	Dependencia	Ubicación	Nombre	Marca	Modelo	# Puertos
1	CAI	Planta Baja	SW01.CAI.DIS.PB.R01	Cisco	C9300-48P	
2		Planta Baja	SW02.CAI.ACC.PB.R01	Cisco	WS-C3850-48T-S	48
3		Planta Baja	SW03.CAI.ACC.PB.R01	Cisco	WS-C2960X-48TS-L	48
4		Segundo Piso	SW01.CAI.ACC.PA2.R02	Cisco	WS-C2960X-48TS-L	48
5		Segundo Piso	CAI-SW2-R2	Cisco Linksys	SRW2048	
6		Segundo Piso	SW02.CAI.ACC.PA2.R02	Cisco	WS-C2960-48TC-L	48
7		Cuarto Piso	SW01.CAI.ACC.PA4.R03	Cisco	C9200L-48P-4X	
8		Quinto Piso	SW01.CAI.ACC.PA5.R04	Cisco	WS-C3750X-24	

Fuente: Departamento de Desarrollo de Tecnológico e Informático

3.2.2.3. Biblioteca

3.2.2.3.1.Situación actual de la red cableada

- **Equipos activos de la red en la BIBLIOTECA**

La Tabla 37 identifica los equipos activos que se encuentran en la facultad FICAYA y dentro de dicha tabla se detalla su ubicación, el nombre, la marca, el modelo y los puertos de cada equipo, esto con la finalidad de tener un registro de los equipos en la facultad mencionada.

Tabla 37

Equipos de Telecomunicaciones – BIBLIOTECA

N°	Dependencia	Ubicación	Nombre	Marca	Modelo	# Puertos
1	Biblioteca	Cuarto de equipos	SW01.BIBLIO.DIS.PB.R01	Cisco		
2		Cuarto de equipos	SW02.BIBLIO.ACC.PB.R01	Cisco	WS-C2960X-48TS-L	48
3		Cuarto de equipos	SW03BIBLIO	Cisco	SG-300-52	48
4		Cuarto de equipos	SW04BIBLIO	Cisco	SG-200-18	48
5		Hemeroteca	Benedetti	3COM	3C16792A	
6		IC3	SW05BIBLIO	Cisco	SG 200-50	48
7		IC3	SW06BIBLIO	Cisco	SG 200-50	48
8		Cuarto de equipos	SW-Camaras	Cisco	WS-C2960-48TS-LL	48

Fuente: Departamento de Desarrollo de Tecnológico e Informático

3.2.2.3.2.Infraestructura por planta

- **Planta Baja**

Para la infraestructura de la planta baja se muestra la Tabla 38, donde se detallan las dependencias que existen.

Tabla 38

Infraestructura Planta Baja

INFRAESTRUCTURA PLANTA BAJA	
PLANTA BAJA	Sala entrada
	Área para no videntes
	Sala locker
	Estación de tesis
	Sala de libros
	Área estudiantil 1
	Área estudiantil 2(máquinas de búsqueda de libros)
	Copiadora
	Sala de telecomunicaciones

Fuente: Información DDTI de la UTN, adaptado de (Guerrero Ipiales, 2019)

- **Segunda Planta**

Para la infraestructura de la segunda planta se muestra la Tabla 39, donde se detallan las dependencias que existen

Tabla 39

Infraestructura Segunda Planta

INFRAESTRUCTURA SEGUNDA PLANTA	
SEGUNDA PLANTA	Sala hemeroteca
	Área estudiantil 1(oficinas de atención)
	Área estudiantil 2
	Área estudiantil 3
	Oficina dirección

Fuente: Información DDTI de la UTN, adaptado de (Guerrero Ipiales, 2019)

- **Tercera Planta**

Para la infraestructura de la tercera planta se muestra la Tabla 40, donde se detallan las dependencias que existen.

Tabla 40

Infraestructura Tercera Planta

INFRAESTRUCTURA TERCER PISO	
TERCER PISO	Área estudiantil
	Videoteca
	Área de procesos técnicos
	Área de informática

Fuente: Información DDTI de la UTN, adaptado de (Guerrero Ipiales, 2019)

- **Cuarta Planta**

Para la infraestructura de la cuarta planta se muestra la Tabla 41, donde se detallan las dependencias que existen.

Tabla 41

Infraestructura Cuarta Planta

INFRAESTRUCTURA CUARTO PISO	
CUARTO PISO	Centro de entrenamiento y certificación internacional

Fuente: Información DDTI de la UTN, adaptado de (Guerrero Ipiales, 2019)

3.2.2.3.3. Disponibilidad de puntos de red

A continuación, se detallan los números de números de puntos de red disponibles en cada Panta del edificio de la Biblioteca.

En la Tabla 42 se describen los números de puntos de red que existen y se encuentran disponibles.

Tabla 42

Puntos de red disponibles en la planta baja de la Biblioteca

PUNTOS DE RED PLANTA BAJA					
Localización	**Puntos de red**	**Cámaras**	**Biométricos**	**Alarma**	**Climatización**
Sala entrada	2	1	1	1	1
Área para no videntes					
Sala locker		1			
Estación de tesis	1	1	1		
Sala de libros	2	8			
Área estudiantil 1	6	3			
Área estudiantil 2 (máquinas de búsqueda de libros)	1	4			
Copiadora					
Sala de telecomunicaciones					
TOTAL PUNTOS	12	18	2	1	1

Fuente: Información DDTI de la UTN, adaptado de (Guerrero Ipiales, 2019)

En la Tabla 43 se describen los números de puntos de red que existen y se encuentran disponibles.

Tabla 43

Puntos de red disponibles en la Segunda Planta de la Biblioteca

PUNTOS DE RED PRIMER PISO					
Localización	**Puntos de red**	**Cámaras**	**Biométricos**	**Sensores**	**Alarma**
Sala hemeroteca	8	2			
Área estudiantil 1 (oficinas de atención)	1	5			
Área estudiantil 2	1	2			
Área estudiantil 3		2			
Oficina dirección	1				
TOTAL PUNTOS	11	11	0	0	0

Fuente: Información DDTI de la UTN, adaptado de (Guerrero Ipiales, 2019)

En la Tabla 44 se describen los números de puntos de red que existen y se encuentran disponibles.

Tabla 44

Puntos de red disponibles en la Tercera Planta de la Biblioteca

PUNTOS DE RED TERCER PISO					
Localización	**Puntos de red**	**Cámaras**	**Biométricos**	**Sensores**	**Alarma**
Área estudiantil		2			
Videoteca	2	2			

Área de procesos técnicos	4				
Área de informática	2				
TOTAL PUNTOS	6	4	0	0	0

Fuente: Información DDTI de la UTN, adaptado de (Guerrero Ipiales, 2019)

En la

se describen los números de puntos de red que existen y se encuentran disponibles.

PUNTOS DE RED CUARTO PISO

Localización	Puntos de red	Cámaras	Biométricos	Sensores	Alarma
Centro de entrenamiento y certificación internacional (oficinas en construcción)	38	1	1		
TOTAL PUNTOS	38	1	1	0	0

Tabla 45

Puntos de red disponibles en la Cuarta Planta de la Biblioteca

PUNTOS DE RED CUARTO PISO

Localización	Puntos de red	Cámaras	Biométricos	Sensores	Alarma

Centro de entrenamiento y certificación internacional (oficinas en construcción)	38	1	1		
TOTAL PUNTOS	38	1	1	0	0

Fuente: Información DDTI de la UTN, adaptado de (Quilca Fernández et al., 2017)

- **Racks de comunicación y etiquetado.**

En la inspección realizada se visualizó lo elementos anclados al armario, también se comprobó que dichos elementos poseen una conexión regular, tanto eléctrica como de datos. El primer rack está ubicado detrás del stand de libros en la planta baja, este cuenta con un switch el cual brinda puntos de red a las diferentes áreas de la Biblioteca. Los switchs tienen una comunicación a través de fibra óptica desde el Data Center Principal. Toda la información presentada anteriormente fue tomada y modificada de: (Bonilla Fonte et al., 2017)

3.2.2.4. Bienestar Universitario

3.2.2.4.1. Equipos Activos de red

En la Tabla 46 se presentan los equipos de telecomunicaciones activos que se encuentran en el Departamento de Bienestar Universitario.

Tabla 46

Equipos de Telecomunicaciones - BIENESTAR UNIVERSITARIO

N°	**Dependencias**	**Ubicación**	**Nombre**	**Modelo**	**Marca**	**# Puertos**
1	**Bienestar Universitario**	Planta Baja	SW01.DBU.DIS.PB.R01	Cisco	C9300-48P	48
2		Planta Baja	SW02.DBU.ACC.PB.R01	Cisco	WS-C2960X-48TS-LL	48
3		Planta Baja	SW03.DBU.ACC.PB.R01	Cisco	WS-C2960X-48TS-LL	

5	Planta Alta 2	SW01.DBU.ACC.PA2.R02	Cisco	WS-C2960X-48TS-LL	48
6	Planta Alta 2	SW02.DBU.ACC.PA2.R02	Cisco	WS-C2960X-48TS-LL	48
7	Planta Alta 2	SW-ODIN	3COM	SS3 SW 4400 SE	
8	Planta Alta 4	SW01.DBU.ACC.PA4.R03	Cisco	WS-C2960X-48TS-L	48
9	Garita	SW01.DBU.ACC.GARITA.R04	Cisco	WS-C2960-24TC-L	

Fuente: Departamento de Desarrollo de Tecnológico e Informático

3.2.2.5. Complejo Acuático

3.2.2.5.1.Equipos Activos de red

En la Tabla 47 se presentan los equipos de telecomunicaciones activos que se encuentran en la dependencia Complejo Acuático.

Tabla 47

Equipos de Telecomunicaciones – COMPLEJO ACUATICO

Nº	Dependencia	Ubicación	Nombre	Marca	Modelo	# Puertos
1	Complejo Acuático	Clubes UTN	SW01.CLUB.ACC.PA1.R01	Cisco	C9300-48P-E	48
2			SW02.CLUB.ACC.PA1.R01	Cisco	WS-C2960X-48TS-L	
3		Gimnasio	SW-Gimnasio	3COM	SS3 SW 4400 SE	
4		Piscina	SW-Metallica	3COM	SS3 SW 4200	

Fuente: Departamento de Desarrollo de Tecnológico e Informático

3.2.2.6. Auditorio Agustín Cueva

3.2.2.6.1.Equipos Activos de red

La Tabla 48 presenta a los equipos de telecomunicaciones activos en el Auditorio Agustín Cueva.

Tabla 48

Equipos de Telecomunicaciones – AUDITORIO AGUSTIN CUEVA

Nº	Dependencia	Ubicación	Nombre	Marca	Modelo	# Puertos
1	**Auditorio Agustín Cueva**	Planta Alta 1	SW01.AUDIAC.DIS.PB.R01	Cisco	C9200L-48P-4X	48
2			SW02.AUDIAC.ACC.PB.R01	Cisco	WS-C2960X-48TS-L	

Fuente: Departamento de Desarrollo de Tecnológico e Informático

3.2.2.7. Polideportivo

3.2.2.7.1. Equipos Activos de red

En la Tabla 49 se presentan los equipos de telecomunicaciones activos que se encuentran la dependencia del Polideportivo.

Tabla 49

Equipos de Telecomunicaciones – POLIDEPORTIVO

Nº	Dependencia	Ubicación	Nombre	Modelo	Marca	# Puerto
1	**IEF**	Inst. Educación Física	SW01.IEF.DC.DIS.PA.R01	Cisco	C9200L-48P-4X-E	24
2		Inst. Educación Física	SW02.IEF.DC.ACC.PA.R01	Cisco	WS-C2960S-24TS-S	

Fuente: Departamento de Desarrollo de Tecnológico e Informático

3.2.2.8. Electricidad y Mecánica

3.2.2.8.1. Equipos Activos de red

En la Tabla 50 se presentan los equipos de telecomunicaciones activos que se encuentran en la dependencia de Electricidad y Mecánica.

Tabla 50

Equipos de Telecomunicaciones – ELECTRICIDAD Y MECANICA

Nº	Dependencia	Ubicación	Nombre	Modelo	Marca

1	**Electricidad y Mecánica**	Cuarto de Equipos	SW01.ELECT.DC.DIS.PB.R01	Cisco	C9200L-48P-4X

Fuente: Departamento de Desarrollo de Tecnológico e Informático

3.3. Situación actual del anillo de fibra óptica de la Universidad Técnica del Norte.

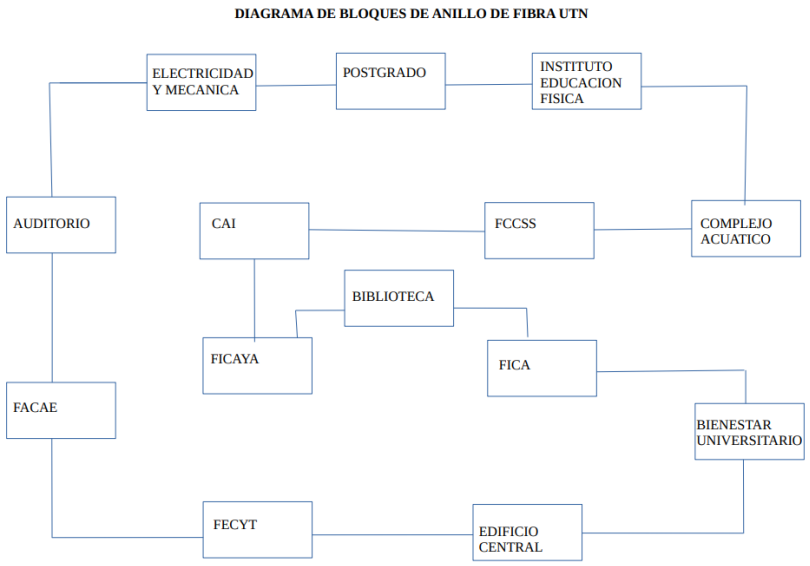
La información que se presenta a continuación fue brindad por el personal del DDTI de la Universidad Técnica del Norte. El anillo de fibra que se extiende a lo largo de las facultados es un tipo de fibra Monomodo G652D con una velocidad de transmisión de 10Gbps, y las diferentes facultades están interconectadas mediante enlaces de fibra óptica sin redundancia con una capacidad de canal de 1 Gbps, dicho anillo de fibra óptica es soterrado y aéreo.

- **Diagrama de bloques del anillo de fibra de la red de la Universidad Técnica del Norte.**

La Figura 25 representa el diagrama de bloques del anillo de fibra óptica que se encuentra en el Campus de la Universidad Técnica del Norte.

Figura 25

Diagrama de bloques de anillo de fibra UTN



Fuente: Departamento de Desarrollo de Tecnológico e Informático

A continuación, en la Figura 26 se presenta el anillo de fibra óptica de la Universidad Técnica del Norte a nivel físico.

Figura 26

Anillo de fibra óptica a nivel físico

Fuente: Adaptado de Cisco DNA Center del del DDTI de la UTN

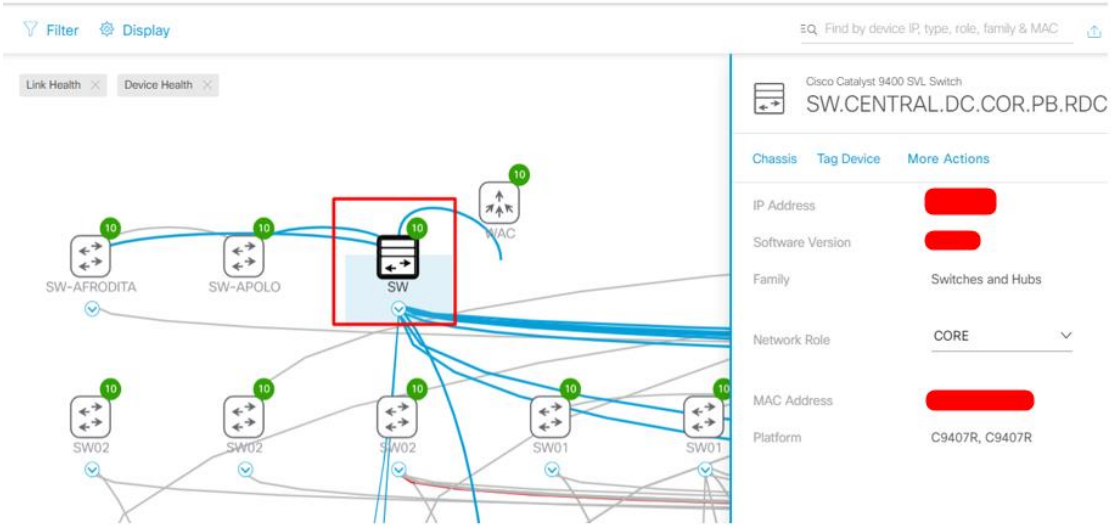
3.3.1.1. Descripción de la distribución de Subredes (VLANS) de la Universidad Técnica del Norte.

La red interna de la Universidad se divide en 45 VLNs que se encuentran administradas uno de los Switch Cisco (9407) que se encuentran en configuración stackwise, donde el acceso se lo realiza por SSH, en la Tabla 51 se presenta las VLANs que se encuentran activas dentro de la red de la Universidad Técnica del Norte.

A continuación, en la Figura 27 se evidencia mediante el software de gestión DNA Center el stackwise configurado en los switchs Cisco 9407.

Figura 27

Configuración Stackwise en switchs



Fuente: Adaptado de Cisco DNA Center del DDTI de la UTN

A través de comandos ejecutados dentro del dispositivo se verifica y valida el estado de stackwise para garantizar que este configurado correctamente. El comando **show switch detail** proporciona información sobre el hardware de la pila, el estado del puerto y los detalles del vecino. También identifica cuál es el conmutador activo y en espera actual, así como cualquier conmutador miembro. Una vez configurado StackWise Virtual, un conmutador desempeña el papel activo y el otro el papel de reserva. Ambos conmutadores de la pila se asocian a una dirección IP de gestión primaria, tal como se visualiza en la Figura 28

Figura 28

Comando show switch

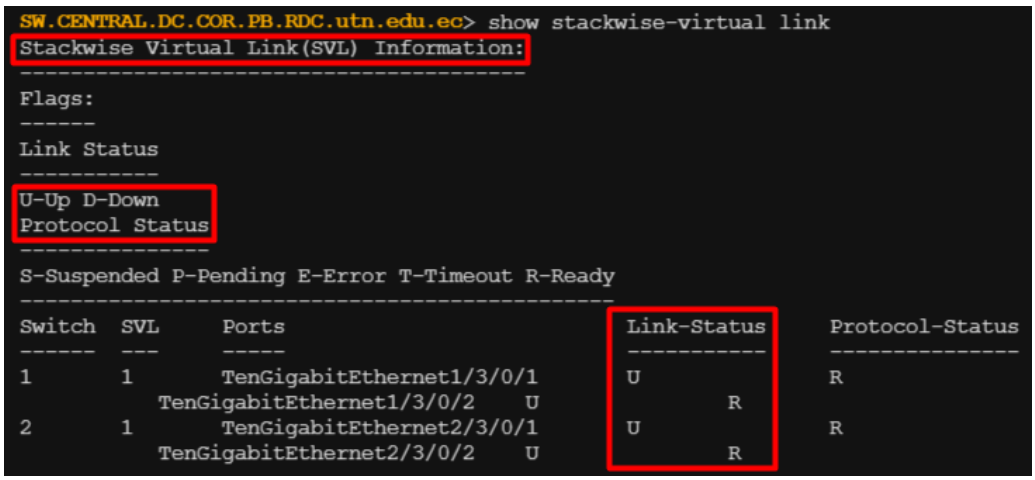
```
SW.CENTRAL.DC.COR.PB.RDC.utn.edu.ec> show switch
Switch/Stack Mac Address : 40f0.7845.efd8 - Local Mac Address
Mac persistency wait time: Indefinite
                                                     H/W   Current
Switch#   Role    Mac Address     Priority Version  State
-----------------------------------------------------------------
*1       Active   40f0.7845.efd8     15     V02     Ready
 2       Standby  a03d.6ee9.d248     14     V02     Ready
```

Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

En la Figura 29 se evidencia que el estado del link de los puertos SVL esté en estado "U" (Activo) y el estado del protocolo debe ser "R" (Preparado).

Figura 29

Estado del link de los puertos SVL



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Las VLANs que se encuentran dentro de la universidad fueron creadas de acuerdo con las necesidades ya la funcionalidad de cada dependencia.

Tabla 51

Distribución de Subredes (VLANS)

N°	DESCRIPCION	VLAN	DIRECCION IP	MASCARA DE SUBRED	GAREWAY
1	EQUIPOS-ACTIVOS	1	172.16.X.X	255.255.255.0	172.16.X.X
2	DMZ	2	10.24.8.X	255.255.255.0	10.24.X.X
		3	172.16.X.X	255.255.255.0	172.16.X.X
3	CORE-FIREWALL	4	172.16.X.X	255.255.255.0	172.16.X.X
4	EQUIPOS WIRELESS	5	172.16.X.X	255.255.255.0	172.16.X.X
5	CCTV	6	172.16.X.X	255.255.255.0	172.16.X.X

6	RELJOS-BIOMETRICOS	7	172.16.X.X	255.255.255.0	172.16.X.X
7	TELEFONIA-IP-ELASTIX	8	172.16.X.X	255.255.255.0	172.16.X.X
8	AUTORIDADES	12	172.16.X.X	255.255.255.0	172.16.X.X
9	DDTI	14	172.16.X.X	255.255.255.0	172.16.X.X
10	FINANCIERO	16	172.16.X.X	255.255.255.0	172.16.X.X
11	COMUNICACION-ORGANIZACIONAL	18	172.16.X.X	255.255.255.0	172.16.X.X
12	ADMINISTRATIVOS	20	172.16.X.X	255.255.255.0	172.16.X.X
13	ADQUISICIONES	22	172.16.X.X	255.255.255.0	172.16.X.X
14	U-EMPRENDE	24	172.16.X.X	255.255.255.0	172.16.X.X
15	AGUSTIN-CUEVA	26	172.16.X.X	255.255.255.0	172.16.X.X
16	BIENESTAR-DOCENTES	28	172.16.X.X	255.255.255.0	172.16.X.X
17	BIENESTAR-ADMINISTRATIVOS	30	172.16.X.X	255.255.255.0	172.16.X.X
18	CLUBES-UTN	32	172.16.X.X	255.255.255.0	172.16.X.X
19	NATIVA	39	----------	----------	----------
20	FICA-LABORATORIOS	40	172.17.X.X	255.255.254.0	17.17.X.X
21	FICA-WIRELESS	42	172.17.X.X	255.255.255.0	17.17.X.X
22	FICA-ADMINISTRATIVOS	44	172.16.X.X	255.255.255.0	17.16.X.X
23	FICAYA-LABORATORIOS	48	172.17.X.X	255.255.254.0	17.17.X.X

24	FICAYA-ADMINISTRATIVOS	52	172.16.X.X	255.255.255.0	17.16.X.X
25	FECYT-LABORATORIOS	56	172.17.X.X	255.255.254.0	17.17.X.X
26	FECYT-ADMINISTRATIVOS	60	172.16.X.X	255.255.255.0	17.16.X.X
27	FACAE-LABORATORIOS	64	172.17.X.X	255.255.254.0	17.17.X.X
28	FACAE-ADMINISTRATIVOS	68	172.16.X.X	255.255.255.0	17.16.X.X
29	FCCSS-LABORATORIOS	72	172.17.X.X	255.255.254.0	17.17.X.X
30	FCCSS-ADMINISTRATIVOS	76	172.16.X.X	255.255.254.0	17.16.X.X
31	POSTGRADO-LABORATORIOS	80	172.16.X.X	255.255.255.0	17.16.X.X
32	POSTGRADO-ADMINISTRATIVOS	84	172.16.X.X	255.255.255.0	17.16.X.X
33	CAI-LABORATORIOS	88	172.17.X.X	255.255.254.0	17.17.X.X
34	CAI-ADMINISTRATIVOS	92	172.16.X.X	255.255.255.0	17.16.X.X
35	BIBLIOTECA-LABORATORIOS	96	172.17.X.X	255.255.254.0	17.17.X.X
36	BIBLIOTECA-DOCENTES	98	172.16.X.X	255.255.255.0	17.16.X.X
37	BIBLIOTECA-ADMINISTRATIVOS	100	172.16.X.X	255.255.254.0	17.16.X.X

38	COLEGIO-LABORATORIOS	104	172.17.X.X	255.255.254.0	17.17.X.X
39	COLEGIO-ADMINISTRATIVOS	108	172.16.X.X	255.255.255.0	17.16.X.X
40	AHSVP	110	172.16.X.X	255.255.255.0	17.16.X.X
41	WIRELESS-DOCENTES	112	172.18.X.X	255.255.248.0	17.18.X.X
42	WIRELESS-ADMINISTRATIVOS	120	172.19.X.X	255.255.254.0	17.19.X.X
43	EDUROAM	128	172.20.X.X	255.255.224.0	17.20.X.X
44	WIRELESS-EVENTOS1	160	172.21.X.X	255.255.248.0	17.21.X.X
45	WIRELESS-EVENTOS2	168	172.22.X.X	255.255.248.0	17.22.X.X

Fuente: Departamento de Desarrollo Tecnología e Información.

3.3.1.1.1.Descripción de Switches (Conmutadores) de la Universidad Técnica del Norte.

En la Tabla 52 se describen las características generalas de los switchs que se encuentran monitoreados por el software de gestión Cisco DNA Center dentro de la red de la Universidad técnica del Norte.

Tabla 52

Características de los Switchs de la UTN

Switch	Características generales	Memoria	Protocolos de administración remota
Cisco Catalyst C9407R	Configurable a nivel capa 2 y capa 3 Forwarding Access Control List (ACL) Quality of Service (QoS)	16 GB of DDR4 2400MT/s RAM	SNMPv1, v2, and v3 (IPv4 & IPv6) Remote monitoring (RMON)

	240 puertos y 480 Gbps por slot	Soporta M2 SATA :240, 480, 960 GB 16GB of internal embedded USB (eUSB) flash	Secure Shell Version 2 (SSHv2) Telnet
Cisco Nexus 5548	16 puertos 10 Gigabit Ethernet 12 puertos 10G BASE-T Layer 3 daughter card Low-latency		SNMPv1, v2 y v3 Remote monitoring (RMON) Secure Shell Version 2 (SSHv2) Telnet
Cisco WS-CBS3020-HPQ	16 puertos 1 Gbps velocidad de transferencia de datos Gigabit Ethernet protocolo de enlace capa 2	Ram: 128 Mb Ddr Sdram Flash Memory: 32 Mb Flash	SNMP v1, v2c, and v3, Rmon 1, Rmon 2, Rmon 3, Rmon 9, Telnet.
Cisco WS-C2960-48TC-L	48 puertos Ethernet 10/100 Throughput 6.5 Mpps 255 Vlans máximas activas.	DRAM 128 MB Flash memory 64 MB	RMON, SNMP
Cisco WS-C3850-48T	Switch Administrable capa L3 48 puertos Gigabit 10/100/1000 Soporta hasta 40G wireless bandwidth por switch Soporta hasta 50 APs y 2000 clientes por cada switch Soporta Cisco Aironet 1040/1140/1260/1600/2600/3500/3600	DRAM 4 GB (8 GB on 48-port Flash 2 GB (4 GB on 12-port and 24-port SFP+ models, 8 GB on 48-port SFP+ model)	Remote Switch Port Analyzer (RSPAN) traffic management, monitoring, and analysis, the Embedded RMON, SSH, SNMPv3

	Wireless controller intregrado 64 WLAN por switch		
Cisco WS-C2960X-48TS-L	48 puertos Ethernet 10/100/1000 Gigabit 80Gbps Bandwidth 108Gbps Forwarding Bandwidth 216Gbps Switching Bandwidth	RAM 512MB Flash Memory 128MB	SSH, SSL, SCP Y SNMPv3 crypto
Cisco C9300-48UXM-E	Switch - 48 puertos capa 3 580 Gbps de capacidad de Switching 480 Gbps bandwidth 431.54 Mpps de Forwarding rate Protocolos de enrutamiento (OSPF, IS-IS, RIP-1, RIP-2, IGMP, OSPFv3)	RAM 8 GB Flash Memory 16 GB	SNMP 1, RMON 1, RMON 2, SNMP 3, SNMP 2c, CLI, NETCONF, RESTCON
Cisco WS C4510R+E	10 slots total 48 Gbps full duplex por slot		SNMP V1 SNMP V2c RMON RMON II
Cisco WS-C2950-24	Administración de redes mayor a 250 usuarios. 4.8 Gbps maximum forwarding bandwidth ConFigurable up to 8000 MAC addresses	16 MB DRAM 8 MB Flash memory	SSHv2 SNMPv1, v2, and v3 (non-cryptographic) RMON Cisco Discovery Protocol (CDP)

3COM SuperStack 3226	Admite hasta 255 VLAN y enlace troncal basado en estándares IEEE 802.3ad Latencia <12 µs		SNMP RMON SSH v1 SSH v2
3COM Switch 4400 SE	24 o 48 puertos 10BASE-T/100BASE-TX de negociación automática configurados como Auto MDIX		SNMP Protocol (RFC 1157) MIB-II (RFC 1213) Bridge MIB (RFC 1493) RMON MIB II (RFC2021)
Cisco SG-200-26	Switch - 24 puertos 10Base-T/100Base-TX/1000Base-T - RJ-45 y 2 x SFP (mini-GBIC) Capacidad de conmutación: 38,69 Mbps Rendimiento de reenvío (tamaño de paquete de 64 bytes): 52 Gbps Capa 2 switching	RAM 128 MB Flash Memory 16 MB	SNMP, RMON, HTTP, TFTP
Cisco WS-C3750X-24	24 puertos x 10Base-T/100Base-TX/1000Base-T - RJ-45 Switch capa 3	DRAM Memory 256 MB Flash Memory 128 MB Flash	SNMP 1, SNMP 2, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, TFTP, SSH, CLI

Fuente: Elaboración Autor

3.4. Situación actual de la red inalámbrica de la UTN

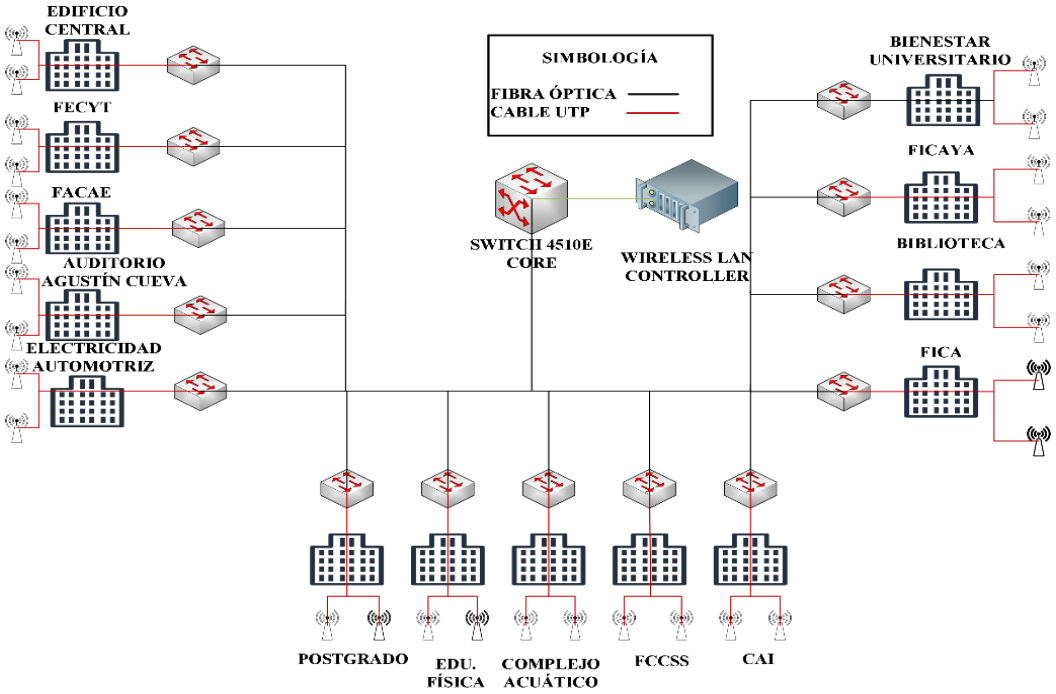
La Universidad Técnica Del Norte cuenta con una red inalámbrica distribuida tanto en los interiores de cada edificio y en los exteriores, proporcionando accesibilidad a todos los usuarios que conforman la universidad, a continuación, se procede a detallar la información relacionada a la red inalámbrica

3.4.1.1. Análisis físico de la red inalámbrico

En la Figura 30 se muestra la topología física de la red inalámbrica, donde se puede observar la distribución de los equipos de red inalámbrica, aquí se tiene como servidor principal al Wireless LAN Controller que se conecta al switch 9704 CORE PRINCIPAL y ambos equipos están conectados al software de gestión Cisco DNA Center el cual brinda un constante monitore de los recursos, y por ende estos equipos distribuye los enlaces físicos por fibra óptica a los Switches de cada edificio y posteriormente con cable UTP a cada AP.

Figura 30

Topología física de la red inalámbrica



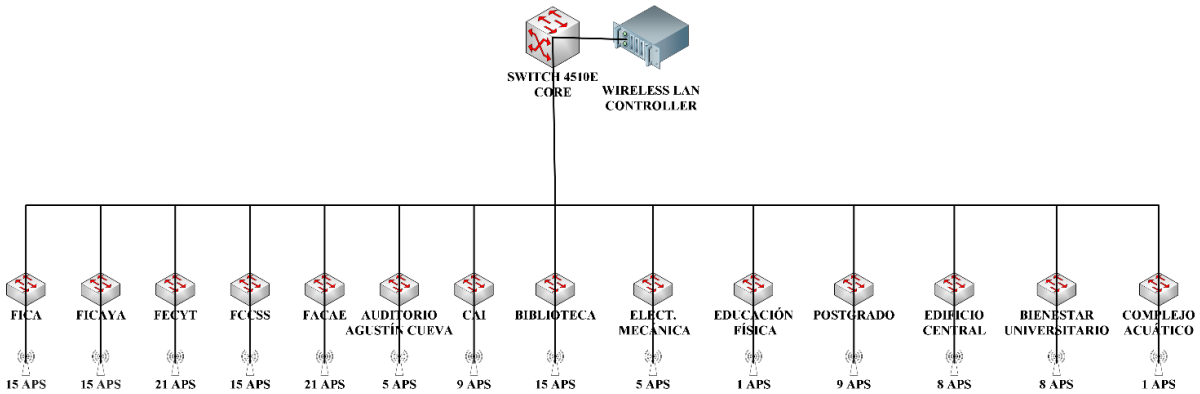
Fuente: Elaboración Autor

3.4.1.2. Equipos utilizados en la red inalámbrica de la UTN

En la Figura 31 se muestra la topología actual de la red inalámbrica, donde se muestra la cantidad de Access Ponts por edificio que conforma la Universidad, además de la VLAN y el direccionamiento IPv4 asignado para la red inalámbrica.

Figura 31

Topología actual de la red inalámbrica de la UTN.



Fuente: Elaboración Autor

La universidad técnica del norte posee 148 Access Point entre internos y externos que conforman la red inalámbrica de la universidad, a continuación, se detalla la ubicación, marcado o modelo, nombre y la ubicación por edificios.

3.4.1.2.1.APS INTERNOS

FICA

A continuación, en la Tabla 53 se detalla la información de cada uno de los equipos de red instalados en el edificio FICA.

Tabla 53

Equipos de red planta baja FICA

Ubicación	Dirección ip	Marca /modelo	Nombre
Planta baja	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICA-PBI

	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICA-PBC
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICA-PBD
Segunda planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICA-PA1-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICA-PA1-C
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICA-PA1-D
Tercera planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICA-PA2-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICA-PA2-C
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICA-PA2-D
Cuarta planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICA-PA3-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICA-PA3-C
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICA-PA3-D
Quinta planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICA-PA4-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICA-PA4-C
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICA-PA4-D

Fuente: Elaboración Autor

FICAYA

A continuación, en la Tabla 54 se detalla la información de cada uno de los equipos de red instalados en el edificio FICAYA.

Tabla 54

Equipos de red planta baja FICAYA

Ubicación	Dirección ip	Marca /modelo	Descripción
Planta baja	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICAYA-PB-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICAYA-PB-C
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICAYA-PB-D
Segunda planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICAYA-PA2-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICAYA-PA2-C

	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICAYA-PA2-D
Tercera planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICAYA-PA3-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICAYA-PA3-C
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICAYA-PA3-D
Cuarta planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICAYA-PA4-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICAYA-PA4-C
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICAYA-PA4-D
Planta Quinta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICAYA-PA5-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICAYA-PA5-C
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICAYA-PA5-D

Fuente: Elaboración Autor

FECYT

A continuación, en la Tabla 55 se detalla la información de cada uno de los equipos de red instalados en el edificio FECYT.

Tabla 55

Equipos de red planta baja FECYT

Ubicación	Dirección ip	Marca /modelo	descripción
Planta baja	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PBI-1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PBD-1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PBI-2
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PBD-2
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PBI-3
Segunda planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PA2-D1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PA2-I1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PA2-D2

	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PA2-I2
Tercera planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PA3-D1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PA3-I1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PA3-D2
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PA3-I2
Cuarta planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PA4-D1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PA4-I1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PA4-D2
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PA4-I2
Tercera planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PA5-D1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PA5-I1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PA5-D2
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PA5-I2

Fuente: Elaboración Autor

FCCSS

A continuación, en la Tabla 56 se detalla la información de cada uno de los equipos de red instalados en edificio FCCSS.

Tabla 56

Equipos de red planta baja FCCSS

Ubicación	Dirección ip	Marca /modelo	descripción
Planta baja	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FCCSS-PBI-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FCCSS-PBD-C
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FCCSS-PBI-D
Segunda planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FCCSS-PA2-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FCCSS-PA2-D

	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FCCSS-PA2-C
Tercera planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FCCSS-PA3-D
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FCCSS-PA3-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FCCSS-PA3-C
Cuarta planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FCCSS-PA4-D
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FCCSS-PA4-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FCCSS-PA4-C
Quinta planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FCCSS-PA5-D
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FCCSS-PA5-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FCCSS-PA5-C

Fuente: Elaboración Autor

FACAE

A continuación, en la Tabla 57 se detalla la información de cada uno de los equipos de red instalados en edificio FACEA.

Tabla 57

Equipos de red planta baja FACAE

Ubicación	Dirección ip	Marca /modelo	descripción
Planta baja	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE-PBI-I1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE-PBI-I2
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE-PBI-D1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE-PBI-D2
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE-PBI-C
Segunda planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE -PA2-I1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE -PA2-I2
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE -PA2-D1

	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE -PA2-D2
Tercera planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE-PA3-D1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE-PA3-D2
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE-PA3-I1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE-PA3-I2
Cuarta planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE-PA4-I1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE-PA4-I2
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE-PA4-D1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE-PA4-D2
Quinta planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE-PA5-I1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE-PA5-I2
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE-PA5-D1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE-PA5-D2

Fuente: Elaboración Autor

AUDITORIO AGUSTÍN CUEVA

A continuación, en la Tabla 58 se detalla la información de cada uno de los equipos de red instalados en el AUDITORIO AGUSTÍN CUEVA.

Tabla 58

Equipos de red Auditorio Agustín Cueva.

Ubicación	Dirección ip	Marca /modelo	descripción
Planta baja	172.16.X.X	Cisco 3700I Series Unified Access Points	AP-AUDITORIO-PBI-I
	172.16.X.X	Cisco 3700I Series Unified Access Points	AP-AUDITORIO-PBI-D

Fuente: Elaboración Autor

BIBLIOTECA

A continuación, en la Tabla 59 se detalla la información de cada uno de los equipos de red instalados en la BIBLIOTECA.

Tabla 59

Equipos de red en la Biblioteca.

Ubicación	Dirección ip	Marca /modelo	descripción
Planta baja	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- BIBLIOTECA -PBI-I1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- BIBLIOTECA -PBI-I2
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- BIBLIOTECA -PBI-D
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- BIBLIOTECA -PBI-C
Segunda planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- BIBLIOTECA -PA2-I1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- BIBLIOTECA -PA2-I2
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- BIBLIOTECA -PA2-D
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- BIBLIOTECA -PA2-C
Tercera planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- BIBLIOTECA -PA3-D
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- BIBLIOTECA -PA3-C
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- BIBLIOTECA -PA3-I1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- BIBLIOTECA -PA3-I2
Cuarta planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- BIBLIOTECA-PA4-I1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- BIBLIOTECA-PA4-I2
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- BIBLIOTECA-PA4-D
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- BIBLIOTECA-PA4-C

Fuente: Elaboración Autor

LABORATORIOS ELECTRICIDAD Y MECÁNICA

A continuación, en la Tabla 60 se detalla la información de cada uno de los equipos de red instalados en el LAB.ELETRICIDAD.

Tabla 60

Equipos de red en Lab. Electricidad

Ubicación	Dirección ip	Marca /modelo	descripción
Planta baja lab. Electricidad	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-ELECTRICIDAD-PB-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-ELECTRICIDAD-PB-D
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-ELECTRICIDAD-PB-C
Planta baja Lab. Mecánica	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-MECANICA-I
Planta alta lab. Elec-mecanica	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-MECANICA-D

Fuente: Elaboración Autor

POLIDEPORTIVO

A continuación, en la Tabla 61 se detalla la información de cada uno de los equipos de red instalados en el POLIDEPORTIVO.

Tabla 61

Equipos de red en el Polideportivo.

Ubicación	Dirección ip	Marca /modelo	descripción
Planta baja	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- POLIDEPORTIVO-PB-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- POLIDEPORTIVO-PB-D
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- POLIDEPORTIVO-PB-C

Fuente: Elaboración Autor

POSTGRADO

A continuación, en la Tabla 62 se detalla la información de cada uno de los equipos de red instalados en POSTGRADO.

Tabla 62

Equipos de red en Postgrado

Ubicación	Dirección ip	Marca /modelo	descripción
Segunda planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- POSTGRADO-PA2-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- POSTGRADO-PA2-D
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- POSTGRADO-PA2-C
Tercera planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- POSTGRADO-PA3-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- POSTGRADO-PA3-D
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- POSTGRADO-PA3-C
Cuarta planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- POSTGRADO-PA4-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- POSTGRADO-PA4-D
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- POSTGRADO-PA4-C

Fuente: Elaboración Autor

CAI

A continuación, en la Tabla 63 se detalla la información de cada uno de los equipos de red instalados en la CAI.

Tabla 63

Equipos de red en el CAI

Ubicación	Dirección ip	Marca /modelo	descripción
Planta baja	172.16.X.X	Air-CAP1262N-A-K9	AP- CAI-PBI-I
	172.16.X.X	Air-CAP1262N-A-K9	AP- CAI-PBI-D
Segunda planta	172.16.X.X	Air-CAP1262N-A-K9	AP- CAI-PA1-I
	172.16.X.X	Air-CAP1262N-A-K9	AP- CAI-PA1-D
Tercera planta	172.16.X.X	Air-CAP1262N-A-K9	AP- CAI -PA2-I

Cuarta planta	172.16.X.X	Air-CAP1262N-A-K9	AP- CAI-PA3-I
	172.16.X.X	Air-CAP1262N-A-K9	AP- CAI-PA3-D
Quinta planta	172.16.X.X	Air-CAP1262N-A-K9	AP- CAI-PA4-I
	172.16.X.X	Air-CAP1262N-A-K9	AP- CAI-PA4-D

Fuente: Elaboración Autor

GIMNASIO

A continuación, en la Tabla 64 se detalla la información de cada uno de los equipos de red instalados en la GIMNASIO.

Tabla 64

Equipos de red en el Gimnasio

Ubicación	Dirección ip	Marca /modelo	descripción
Planta baja	172.16.X.X	Air-CAP1262N-A-K9	AP- GIMNASIO-PA1-I

Fuente: Elaboración Autor

COMPLEJO ACUÁTICO

A continuación, en la Tabla 65 se detalla la información de cada uno de los equipos de red instalados en la COMPLEJO ACUÁTICO.

Tabla 65

Equipos de red en el Complejo Acuático

Ubicación	Dirección ip	Marca /modelo	descripción
Planta baja	172.16.X.X	Air-CAP1262N-A-K9	AP- PISCINA-INTERIOR

Fuente: Elaboración Autor

EDIFICIO CENTRAL

A continuación, en la Tabla 66 se detalla la información de cada uno de los equipos de red instalados en EDIFICIO CENTRAL.

Tabla 66

Equipos de red en el Edificio Central

Ubicación	Dirección ip	Marca /modelo	descripción
Planta baja	172.16.X.X	Air-CAP1262N-A-K9	AP- CENTRAL-PB-I-V
	172.16.X.X	Air-CAP1262N-A-K9	AP- CENTRAL-PB-I-AB
Segunda planta	172.16.X.X	Air-CAP1262N-A-K9	AP- CENTRAL-PA1-VAC
	172.16.X.X	Air-CAP1262N-A-K9	AP- CENTRAL-PA1-VAD
Tercera planta	172.16.X.X	Air-CAP1262N-A-K9	AP- CENTRAL-PA2-I-JM
	172.16.X.X	Air-CAP1262N-A-K9	AP- CENTRAL-PA2-I-P
Cuarta planta	172.16.X.X	Air-CAP1262N-A-K9	AP- CENTRAL-PA3-I
	172.16.X.X	Air-CAP1262N-A-K9	AP- CENTRAL-PA3-D

Fuente: Elaboración Autor

3.4.1.2.2.APS EXTERNOS

A continuación, en la Tabla 67 se detalla cada uno de los puntos de acceso exteriores y su ubicación.

Tabla 67

Ubicación de APs en accesos exteriores

Ubicación	Dirección ip	Marca /modelo	descripción
Exteriores laterales del Polideportivo	172.16.X.X	Cisco 1562E Unified Access Point	AP-EXTERIOR-POL-1
	172.16.X.X	Cisco 1562E Unified Access Point	AP-EXTERIOR-POL-2
Terraza sur edificio central	172.16.X.X	Cisco 1562E Unified Access Point	AP-EXTERIOR-CENTRAL-POSTERIOR
Exterior Postgrado	172.16.X.X	Cisco 1562E Unified Access Point	AP-EXTERIOR-POSG-PARQUEADERO
Terraza norte Fica planta 1	172.16.X.X	Cisco 1562E Unified Access Point	AP-EXTERIOR-FICA
Terraza este Facae frente parque	172.16.X.X	Cisco 1562E Unified Access Point	AP-EXTERIOR-FACAE-PARQUE
Terraza oeste Fecyt frente parque	172.16.X.X	Cisco 1562E Unified Access Point	AP-EXTERIOR-FECYT-PARQUE
Terraza norte edificio central	172.16.X.X	Cisco 1562E Unified Access Point	AP-EXTERIOR-CENTRAL-PARQUEADERO
Exteriores de Auditorio Agustín cueva	172.16.X.X	Cisco 1562E Unified Access Point	AP-EXTERIOR-AUDIAC-PLAZA
	172.16.X.X	Cisco 1562E Unified Access Point	AP-EXTERIOR-AUDIAC-CANCHA2
	172.16.X.X	Cisco 1562E Unified Access Point	AP-EXTERIOR-AUDIAC-CANCHA1
Exterior complejo acuático	172.16.X.X	Cisco 1562E Unified Access Point	AP-EXTERIOR-PISCINA

Fuente: Elaboración Autor

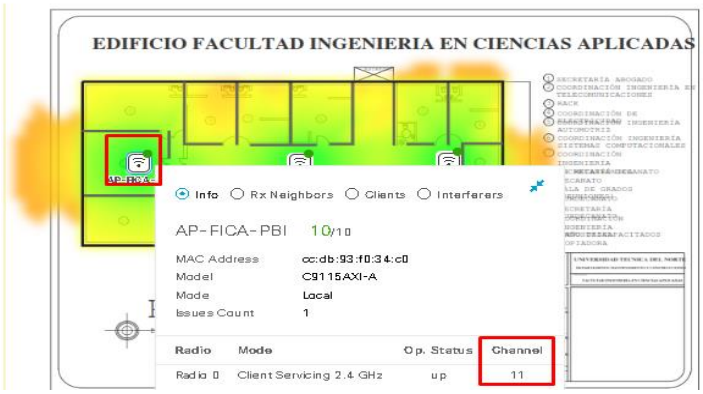
3.4.1.3. Distribución de canales IEEE 802.11 b/g/a

La distribución de canales para los estándares IEEE 802.11 b/g/a utilizados en las redes inalámbricas de la Universidad, se distribuyen de tal manera que reduzca la interferencia al ocupar la misma frecuencia de propagación 2.4 GHz y 5 GHz, para el estándar IEEE 802.11 b/g se tiene 11 canales de los cuales se utiliza el canal 1, canal 6 y canal 11, lo cual se configura en cada AP que se encuentran en la misma planta para evitar interferencia como se muestra en las Figura 32, Figura 33, Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Figura *34*.

Figura 32

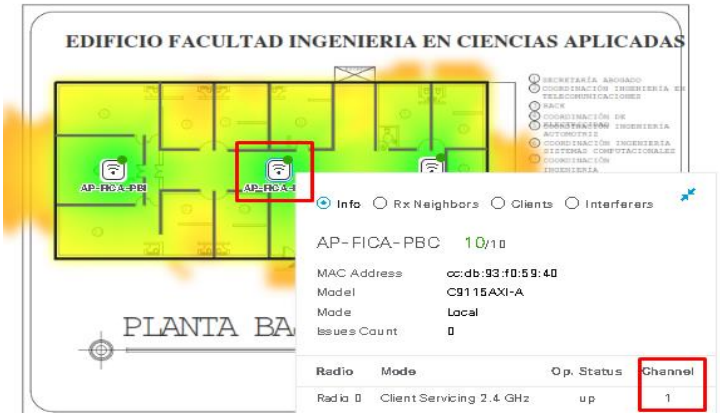
Distribución de canales, canal 11



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Figura 33

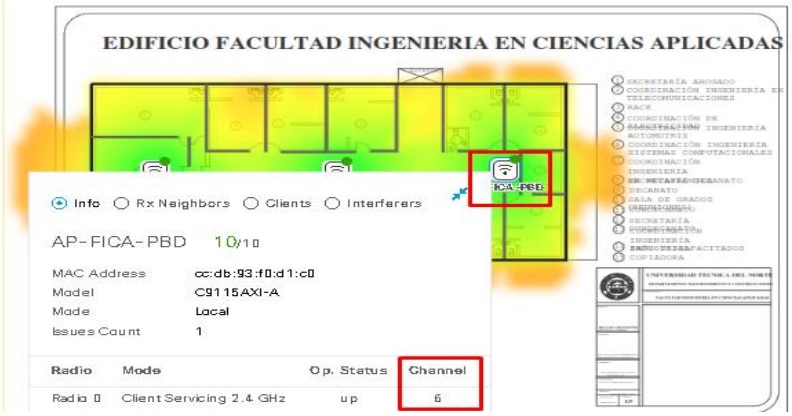
Distribución de canales, canal 1



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Figura 34

Distribución de canales, canal 6



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Para el estándar IEEE 802.11a que posee 25 canales de 20 MHz los cuales se los distribuye evitando utilizar el mismo canal en las mismas plantas, esta configuración se realiza de manera automática en cada AP, a continuación, en las Figura 35, Figura 36 Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Figura *37*, se muestra una distribución de canales 5GHz.

Figura 35

Distribución de canales 5GHz

Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Figura 36

Distribución de canales 5GHz

Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Figura 37

Distribución de canales 5GHz

Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Para la red inalámbrica para la frecuencia de 2.4 GHz y 5 GHz se maneja velocidad de datos dependientes del estándar IEEE 802.11 que se establezca entre la estación y el AP, a continuación, en la Figura 38 se muestra las velocidades de datos que se manejan por frecuencia y los anchos de banda.

Figura 38

Velocidades de datos y anchos de banda

Profile Name	Type	5Ghz Data Rates	2.4Ghz Data Rates	Channel Width
HIGH	2.4 GHz,5 GHz	12,18,24,36,48,54	9,12,18,24,36,48,54	20 MHz
LOW	2.4 GHz,5 GHz	6,9,12,18,24,36,48,54	1,2,5.5,6,9,11,12,18,24,36,48,54	20 MHz
TYPICAL	2.4 GHz,5 GHz	6,9,12,18,24,36,48,54	9,12,18,24,36,48,54	20 MHz

Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

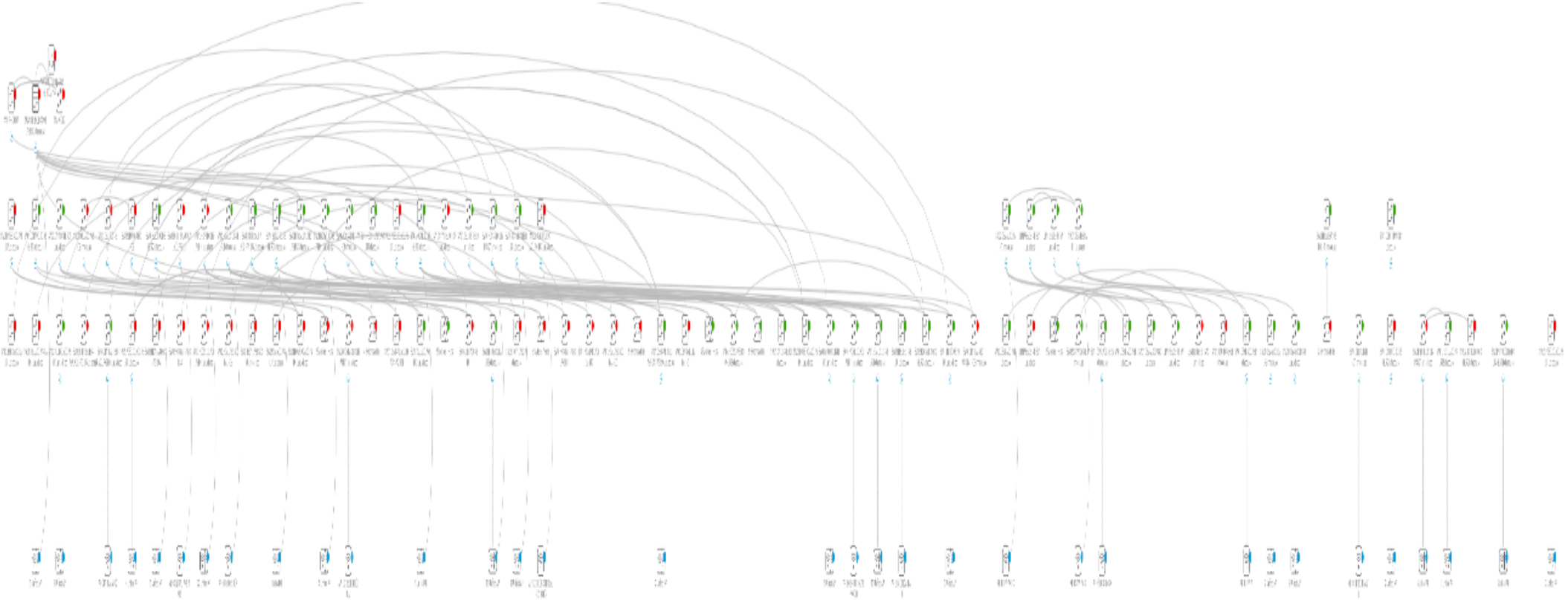
3.5. Situación actual de la red por DNA

El Centro Cisco DNA (Digital Network Architecture) al ser una herramienta de administración de red permite observar las diferentes topologías de red de toda la UTN donde se muestra cada uno de los equipos de red CISCO que se encuentran distribuidos en la red

cableada e inalámbrica, a continuación, en la Figura 39 se muestra la topología general de la universidad vista desde DNA.

Figura 39

Topología general de la universidad vista desde DNA



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

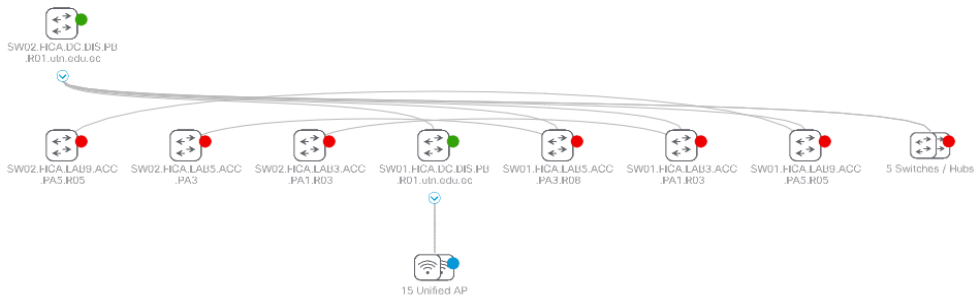
3.5.1. Estado actual de la conexión de red por DNA en cada Facultad

3.5.1.1. FICA

En la Figura 40 se muestra la topología de equipos de red pertenecientes a la facultad FICA visualizadas por DNA.

Figura 40

Estado actual de conexión de red FICA



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Para las conexiones de los equipos de red utilizados en la topología correspondiente a la FICA mediante medio cableado. Donde se tiene a un switch Cisco Catalyst 4500 Series principal donde se conectan doce switches Cisco Catalyst que se distribuyen en toda la facultad dando acceso a la red a todos los equipos de red, los cuales se pueden observar en la Figura.

Conexión de la red por plantas

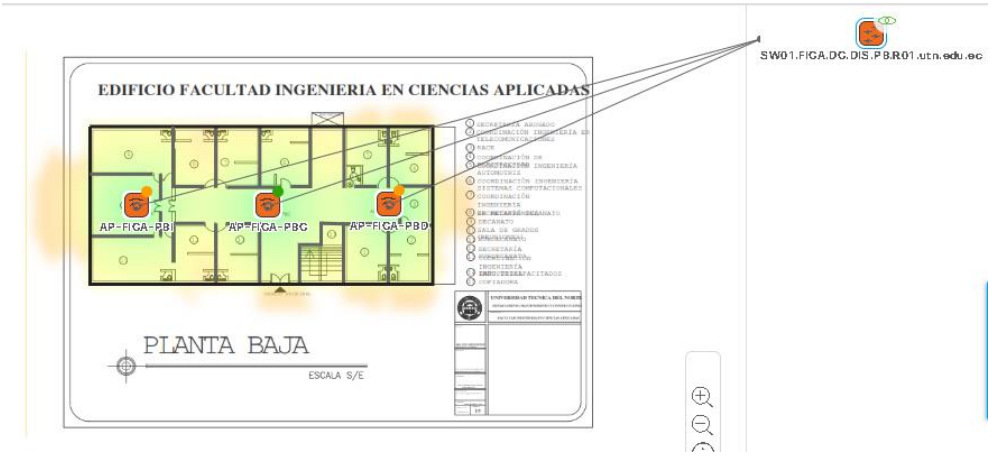
En el siguiente apartado se detalla las conexiones de los equipos de red utilizados en la topología para cada planta correspondiente a la FICA.

Planta baja FICA

Para planta baja se tiene un switch Cisco Catalyst 9300 de cual se conectan el AP-FICA-PBI, AP-FICA-PBA y AP-FICA-PBD como se muestra en la Figura 41.

Figura 41

Equipos en la planta Baja-FICA



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 68 se detalla la información de cada uno de los equipos de red instalados en la planta baja FICA.

Tabla 68

Equipos de red por DNA

Ubicación	Dirección ip	Marca /modelo	descripción
Planta baja	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.FICA.DC.DIS.PB.R01.utn.edu.ec
Planta baja	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICA-PBI
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICA-PBC

	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICA-PBD

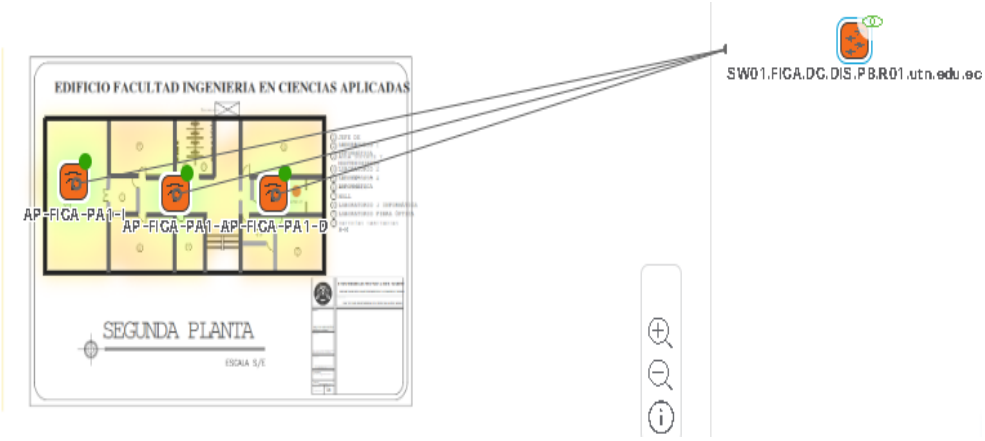
Fuente: Elaboración Autor

Segunda planta FICA

Para la segunda planta se tiene un switch Cisco Catalyst 9300 de cual se conectan el AP-FICA-PA1-I, AP-FICA-PA1-C y AP-FICA-PA1-D como se muestra en la Figura 42.

Figura 42

Equipos en la Segunda planta-FICA



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN.

A continuación, en la Tabla 69 se detalla la información de cada uno de los equipos de red instalados en la segunda planta FICA.

Tabla 69

Equipos de red por DNA

Ubicación	Dirección ip	Marca /modelo	descripción
Planta baja	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.FICA.DC.DIS.PB.R01.utn.edu.ec

Segunda planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICA-PA1-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICA-PA1-C
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICA-PA1-D

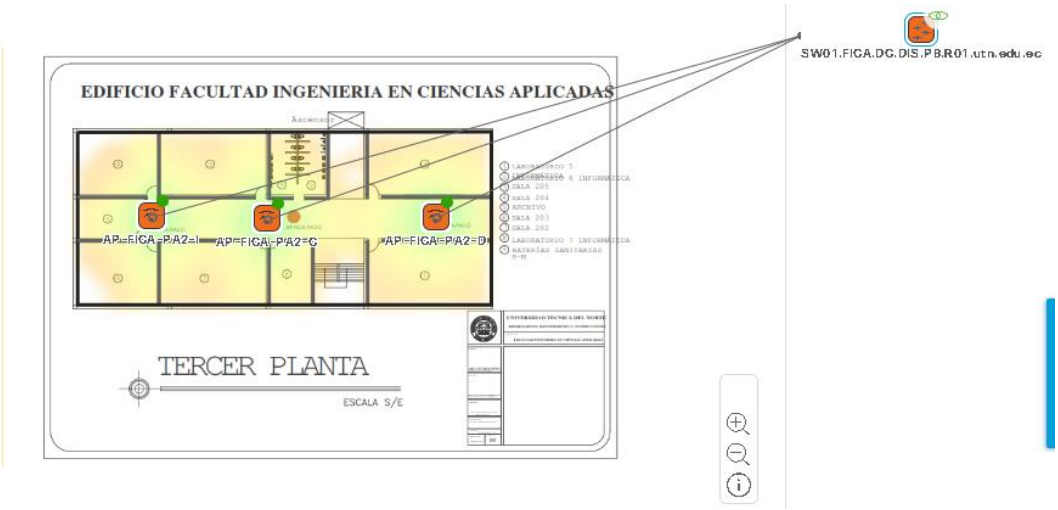
Fuente: Elaboración Autor

Tercer planta FICA

Para la tercera planta se tiene un switch Cisco Catalyst 9300 de cual se conectan el AP-FICA-PA2-I, AP-FICA-PA2-C y AP-FICA-PA2-D como se muestra en la Figura 43.

Figura 43

Equipos en la Tercera planta-FICA



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 70 se detalla la información de cada uno de los equipos de red instalados en la tercera planta FICA.

Tabla 70

Equipos de red por DNA

Ubicación	Dirección ip	Marca /modelo	descripción
Planta baja	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.FICA.DC.DIS.PB.R01.utn.edu.ec
Tercera planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICA-PA2-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICA-PA2-C
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICA-PA2-D

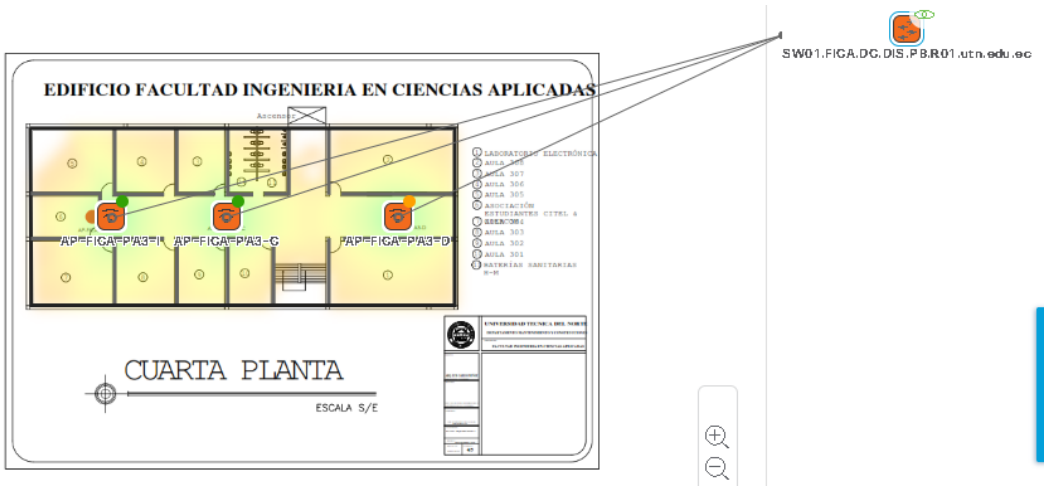
Fuente: Elaboración Autor

Cuarta planta FICA

Para cuarta planta se tiene un switch Cisco Catalyst 9300 de cual se conectan el AP-FICA-PA3-I, AP-FICA-PA3-C y AP-FICA-PA3-D como se muestra en la Figura 44.

Figura 44

Equipos en la Cuarta planta-FICA



Fuente: Adaptado de Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 71 se detalla la información de cada uno de los equipos de red instalados en la cuarta planta FICA.

Tabla 71

Equipos de red por DNA

Ubicación	Dirección ip	Marca /modelo	descripción
Planta baja	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.FICA.DC.DIS.PB.R01.utn.edu.ec
Cuarta planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICA-PA3-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICA-PA3-C
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICA-PA3-D

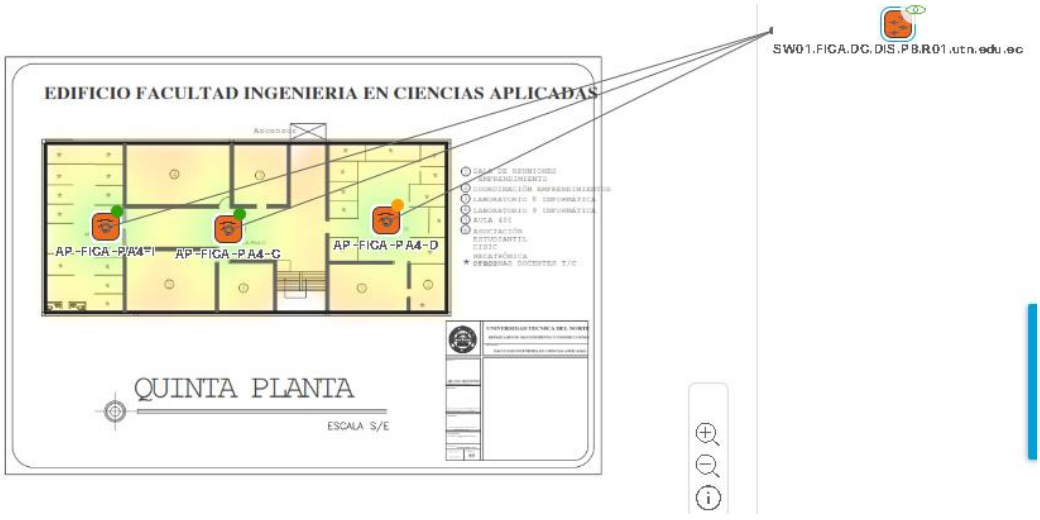
Fuente: Elaboración Autor

Quinta planta FICA

Para la quinta planta se tiene un switch Cisco Catalyst 9300 de cual se conectan el AP-FICA-PA4-I, AP-FICA-PA4-C y AP-FICA-PA4-D como se muestra en la Figura 45.

Figura 45

Equipos en la Quinta planta-FICA



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 72 se detalla la información de cada uno de los equipos de red instalados en la cuarta planta FICA.

Tabla 72

Equipos de red por DNA

Ubicación	Dirección IP	Marca /modelo	descripción
Planta baja	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.FICA.DC.DIS.PB.R01.utn.edu.ec
Quinta planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICA-PA4-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICA-PA4-C
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICA-PA4-D

Fuente: Elaboración Autor

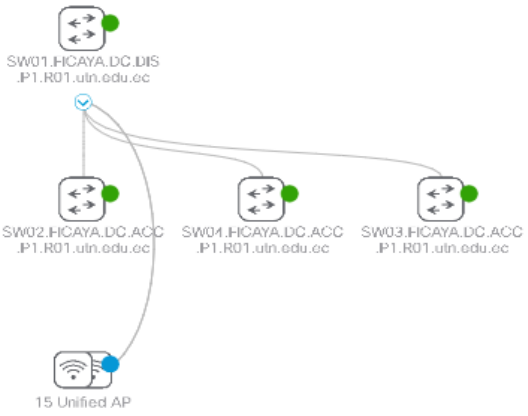
3.5.1.2. FICAYA

Para las conexiones de los equipos de red utilizados en la topología correspondiente a la FICAYA mediante medio cableado. Donde se tiene a un switch Cisco Catalyst 9300 Series principal donde se conectan tres switches Cisco Catalyst 9200 Series.

A continuación, en la Figura 46 se muestra la topología de equipos de red pertenecientes a la facultad FICAYA visualizadas por DNA.

Figura 46

Estado actual de conexión de red FICAYA



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Conexión de red por plantas

A continuación, se detalla las conexiones de red por cada planta.

Planta baja FICAYA

Para planta baja se tiene un switch Cisco Catalyst 9300 Series de cual se conectan el AP-FICAYA-PB-I, AP-FICAYA-PB-C y AP-FICAYA-PB-D como se muestra en la Figura 47.

Figura 47

Equipos en la planta Baja-FICAYA

Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 73 se detalla la información de cada uno de los equipos de red instalados en la planta baja FICAYA.

Tabla 73

Equipos de red por DNA

Ubicación	Dirección IP	Marca /modelo	Descripción
Planta baja	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.FICAYA.DC.DIS.P1.R01.utn.edu.ec
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICAYA-PB-I

172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICAYA-PB-C
172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICAYA-PB-D

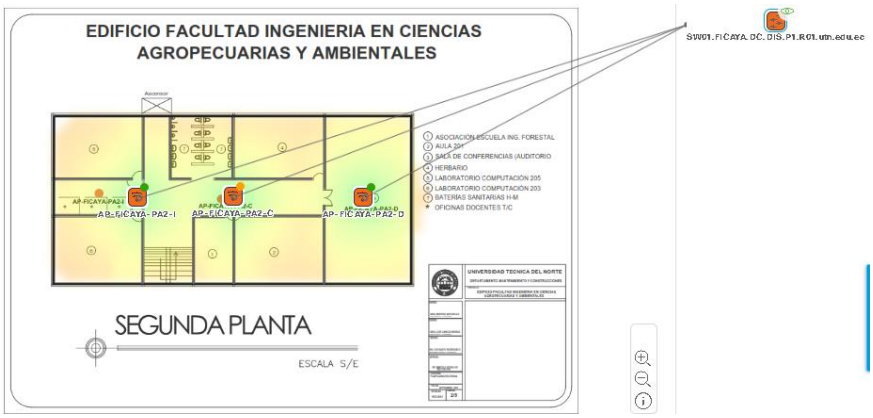
Fuente: Elaboración Autor

Segunda planta FICAYA

Para la segunda planta se tiene un switch Cisco Catalyst 9300 de cual se conectan el AP-FICAYA-PA2-I, AP-FICAYA-PA2-C y AP-FICAYA-PA2-D como se muestra en la Figura 48.

Figura 48

Equipos en la Segunda planta-FICAYA



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 74 se detalla la información de cada uno de los equipos de red instalados en la segunda planta FICAYA.

Tabla 74

Equipos de red por DNA

Ubicación	Dirección ip	Marca /modelo	descripción
Planta baja	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.FICAYA.DC.DIS.P1.R01.utn.edu.ec

Segunda planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICAYA-PA2-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICAYA-PA2-C
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICAYA-PA2-D

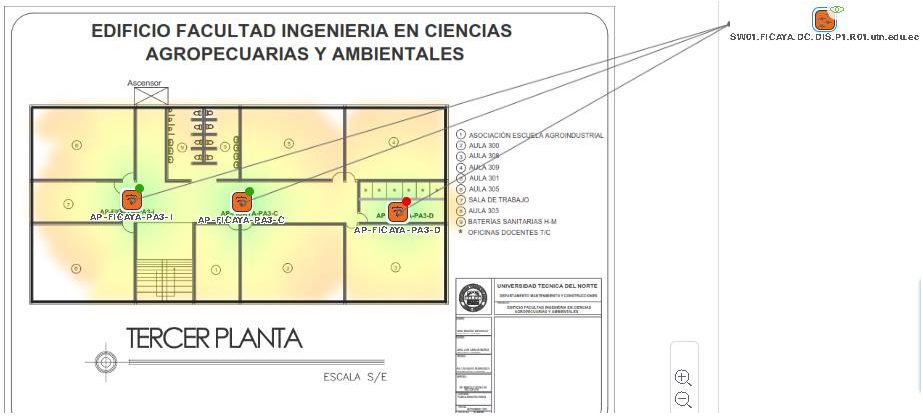
Fuente: Elaboración Autor

Tercera planta FICAYA

Para la tercera planta se tiene un switch Cisco Catalyst 9300 de cual se conectan el AP-FICAYA-PA3-I, AP-FICAYA-PA3-C y AP-FICAYA-PA3-D como se muestra en la Figura 49.

Figura 49

Equipos en la Tercera planta-FICAYA



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 75 se detalla la información de cada uno de los equipos de red instalados en la tercera planta FICAYA.

Tabla 75

Equipos de red por DNA

Ubicación	Dirección ip	Marca /modelo	descripción

Planta baja	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.FICAYA.DC.DIS.P1.R01.utn.edu.ec
Tercera planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICAYA-PA3-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICAYA-PA3-C
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICAYA-PA3-D

Fuente: Elaboración Autor

Cuarta planta FICAYA

Para cuarta planta se tiene un switch Cisco Catalyst 9300 de cual se conectan el AP-FICAYA-PA4-I, AP-FICAYA-PA4-C y AP-FICAYA-PA4-D como se muestra en la Figura 50.

Figura 50

Equipos en la Cuarta planta-FICAYA

Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 76 se detalla la información de cada uno de los equipos de red instalados en la cuarta planta FICAYA.

Tabla 76

Equipos de red por DNA

Ubicación	Dirección ip	Marca /modelo	descripción

Planta baja	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.FICAYA.DC.DIS.P1.R01.utn.edu.ec
Cuarta planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICAYA-PA4-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICAYA-PA4-C
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICAYA-PA4-D

Fuente: Elaboración Autor

Quinta planta FICAYA

Para la quinta planta se tiene un switch Cisco Catalyst 9300 de cual se conectan el AP-FICAYA-PA5-I, AP-FICAYA-PA5-C y AP-FICAYA-PA5-D como se muestra en la Figura 51.

Figura 51

Equipos en la Quina planta-FICAYA

Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 77 se detalla la información de cada uno de los equipos de red instalados en la cuarta planta FICAYA.

Tabla 77

Equipos de red por DNA

Ubicación	Dirección IP	Marca /modelo	descripción
Planta baja	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.FICAYA.DC.DIS.P1.R01.utn.edu.ec
Planta Quinta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICAYA-PA5-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICAYA-PA5-C
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FICAYA-PA5-D

Fuente: Elaboración Autor

3.5.1.3. FECYT

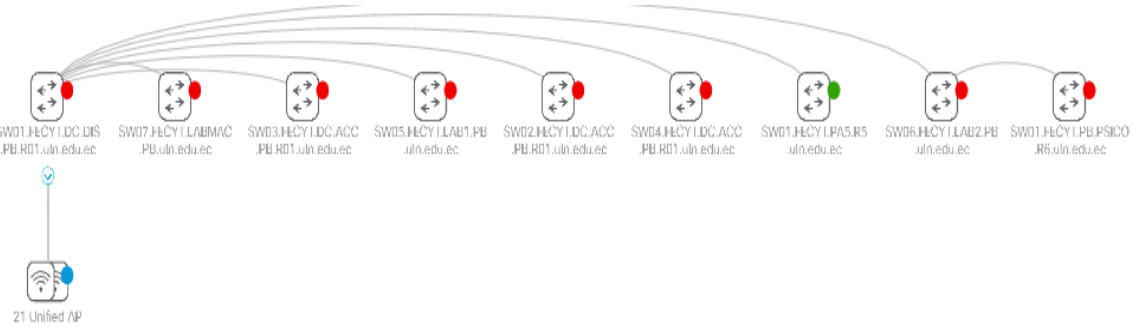
Conexión de la red

Para las conexiones de los equipos de red utilizados en la topología correspondiente a la FECYT mediante enlaces físicos. Donde se tiene a un switch Cisco Catalyst 9300 Series principal donde se conectan ocho switches Cisco Catalyst 2960 Series como se muestra en la Figura 52.

A continuación, se muestra la topología de equipos de red pertenecientes a la facultad FECYT visualizadas por DNA.

Figura 52

Estado actual de conexión de red FECYT



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Conexión de red por plantas

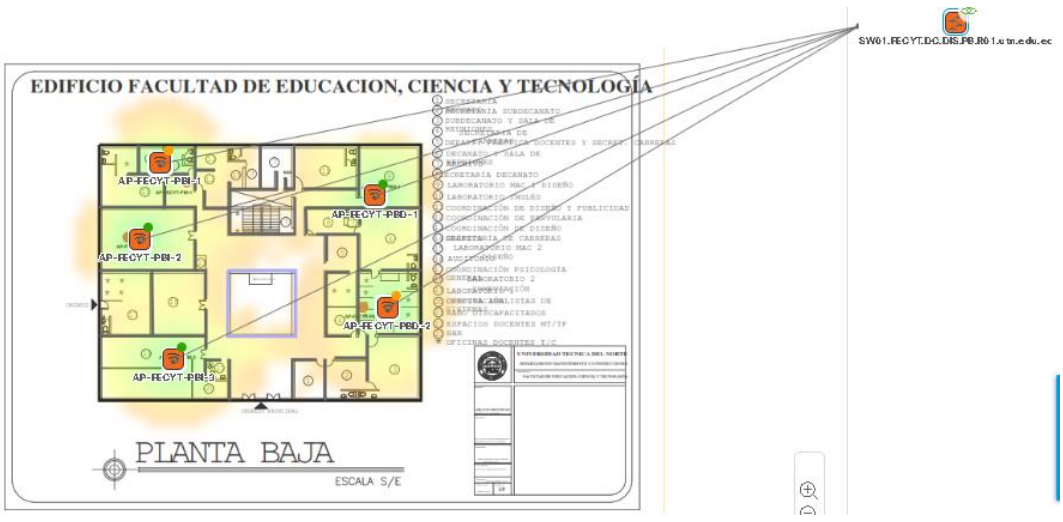
A continuación, se detalla las conexiones de red por cada planta.

Planta baja FECYT

Para planta baja se tiene un switch Cisco Catalyst 9300 Series de cual se conectan el AP-FECYT-PBI-1, AP-FECYT-PBD-1, AP-FECYT-PBI-2, AP-FECYT-PBD-2 y AP-FECYT-PBI-3 como se muestra en la Figura 53.

Figura 53

Equipos en la planta Baja-FECYT



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 78 se detalla la información de cada uno de los equipos de red instalados en la planta baja FECYT.

Tabla 78

Equipos de red por DNA

Ubicación	Dirección IP	Marca /modelo	descripción
	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.FECYT.DC.DIS.PB.R01.utn.edu.ec
Planta baja			
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PBI-1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PBD-1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PBI-2
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PBD-2
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PBI-3

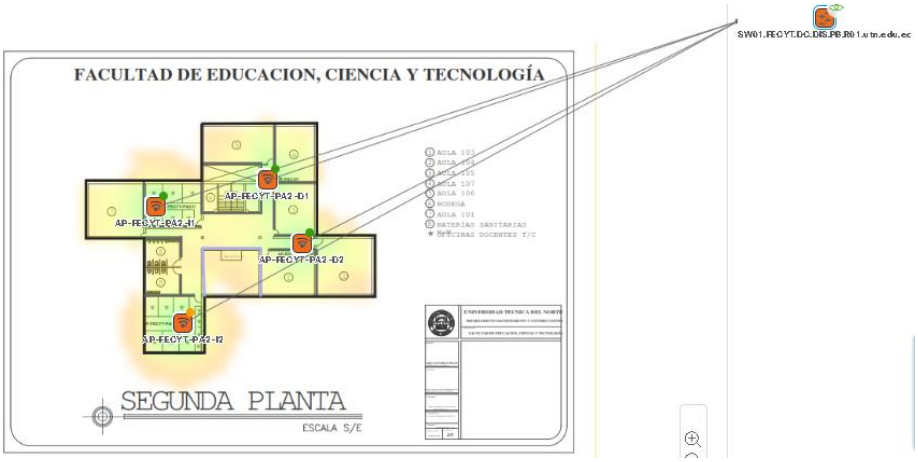
Fuente: Elaboración Autor

Segunda planta FECYT

Para la segunda planta se tiene un switch Cisco Catalyst 9300 de cual se conectan el AP-FECYT-PA2-D1, AP-FECYT-PA2-I1, AP-FECYT-PA2-D2 y AP-FECYT-PA2-I2 como se muestra en la Figura 54.

Figura 54

Equipos en la Segunda planta-FECYT



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 79 se detalla la información de cada uno de los equipos de red instalados en la segunda planta FECYT.

Tabla 79

Equipos de red por DNA

Ubicación	Dirección ip	Marca /modelo	descripción
Planta baja	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.FICAYA.DC.DIS.P1.R01.utn.edu.ec
Segunda planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PA2-D1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PA2-I1

172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PA2-D2
172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PA2-I2

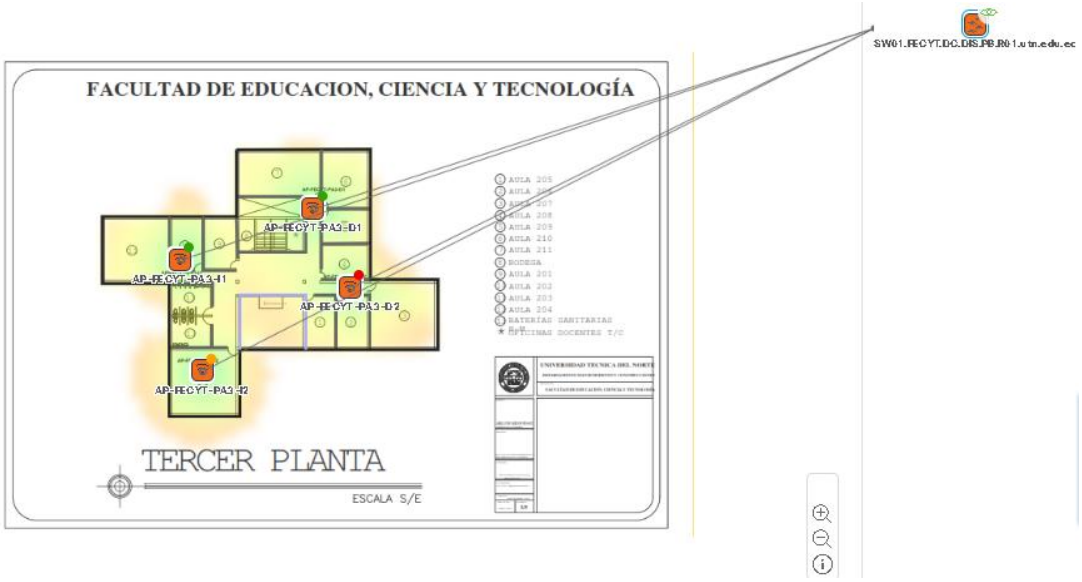
Fuente: Elaboración Autor

Tercera planta FECYT

Para la tercera planta se tiene un switch Cisco Catalyst 9300 de cual se conectan el AP-FECYT-PA3-D1, AP-FECYT-PA3-I1, AP-FECYT-PA3-D2 y AP-FECYT-PA3-I2 como se muestra en la Figura 55.

Figura 55

Equipos en la Tercera planta-FECYT



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 80 se detalla la información de cada uno de los equipos de red instalados en la tercera planta FECYT.

Tabla 80

Equipos de red por DNA

Ubicación	Dirección ip	Marca /modelo	descripción
Planta baja	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.FECYT.DC.DIS.PB.R01.utn.edu.ec
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PA3-D1
Tercera planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PA3-I1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PA3-D2
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PA3-I2

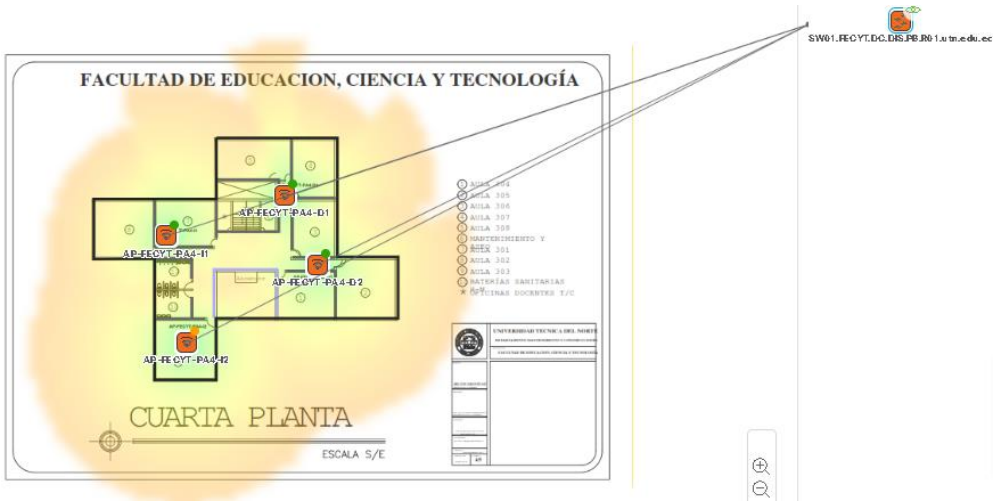
Fuente: Elaboración Autor

Cuarta planta FECYT

Para cuarta planta se tiene un switch Cisco Catalyst 9300 de cual se conectan el AP-FECYT-PA4-I, AP-FECYT-PA4-C y AP-FECYT-PA4-D como se muestra en la Figura 56.

Figura 56

Equipos en la Cuarta planta-FECYT



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 81 se detalla la información de cada uno de los equipos de red instalados en la cuarta planta FECYT.

Tabla 81

Equipos de red por DNA

Ubicación	Dirección ip	Marca /modelo	descripción
Planta baja	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.FECYT.DC.DIS.PB.R01.utn.edu.ec
Cuarta planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PA4-D1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PA4-I1

172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PA4-D2
172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PA4-I2

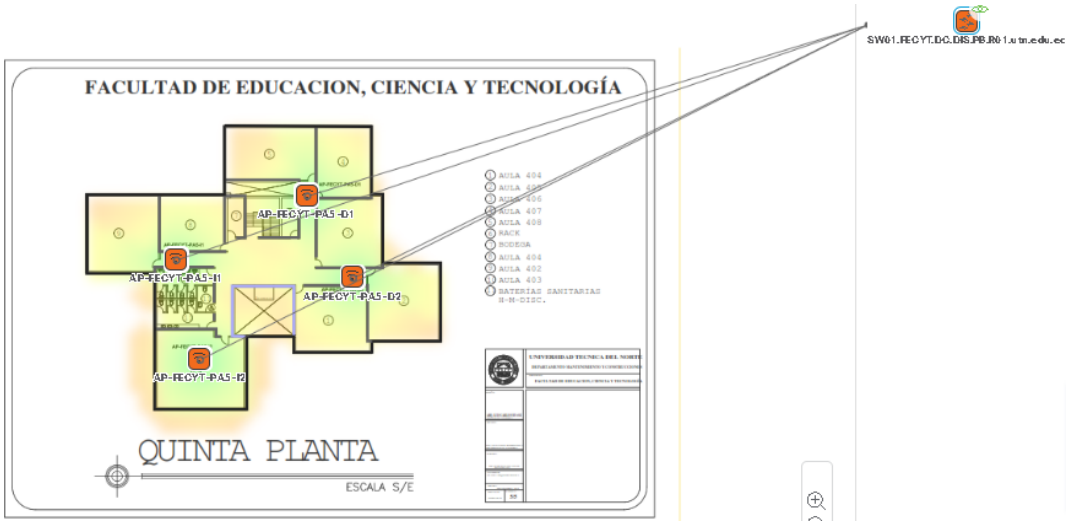
Fuente: Elaboración Autor

Quinta planta FECYT

Para la quinta planta se tiene un switch Cisco Catalyst 9300 de cual se conectan por medio cableado a AP-FECYT-PA5-D1, AP-FECYT-PA5-I1, AP-FECYT-PA5-D2 y AP-FECYT-PA5-I2 como se muestra en la Figura 57.

Figura 57

Equipos en la Quinta planta-FECYT



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 82 se detalla la información de cada uno de los equipos de red instalados en la cuarta planta FECYT.

Tabla 82

Equipos de red por DNA

Ubicación	Dirección ip	Marca /modelo	descripción
Planta baja	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.FECYT.DC.DIS.PB.R01.utn.edu.ec
Tercera planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PA5-D1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PA5-I1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PA5-D2
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FECYT-PA5-I2

Fuente: Elaboración Autor

3.5.1.4. FCCSS

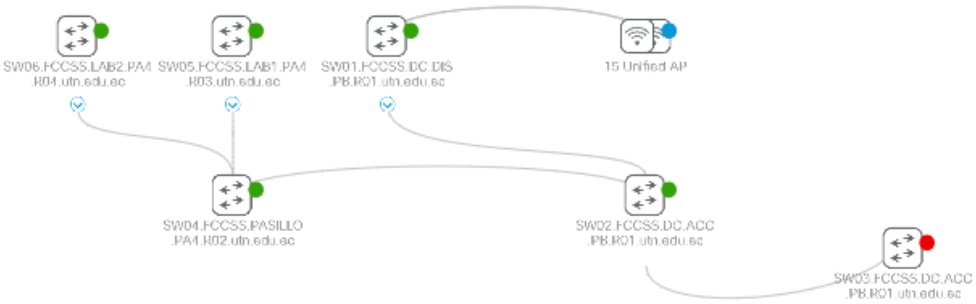
Conexión de la red

Para las conexiones de los equipos de red utilizados en la topología correspondiente a la FCCSS mediante enlaces físicos. Donde se tiene a un switch Cisco Catalyst 9300 Series principal donde se conectan ocho switches Cisco Catalyst 2960 Series como se muestra en la Figura 58.

A continuación, se muestra la topología de equipos de red pertenecientes a la facultad FCCSS visualizadas por DNA.

Figura 58

Estado actual de conexión de red FCCSS



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Conexión de red por plantas

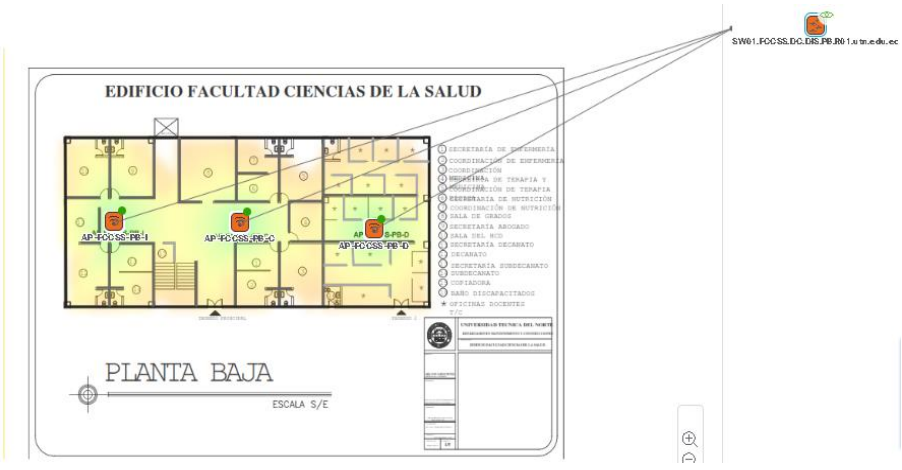
A continuación, se detalla las conexiones de red por cada planta.

Planta baja FCCSS

Para planta baja se tiene un switch Cisco Catalyst 9300 Series de cual se conectan el AP-FCCSS-PBI-I, AP-FCCSS-PBD-C y AP-FCCSS-PBI-D, como se muestra en la Figura 59.

Figura 59

Equipos en la Planta Baja-FCCSS



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 83 se detalla la información de cada uno de los equipos de red instalados en la planta baja FCCSS.

Tabla 83

Equipos de red por DNA

Ubicación	Dirección IP	Marca /modelo	Descripción
Planta baja	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.FCCSS.DC.DIS.PB.R01.utn.edu.ec
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FCCSS-PBI-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FCCSS-PBD-C
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FCCSS-PBI-D

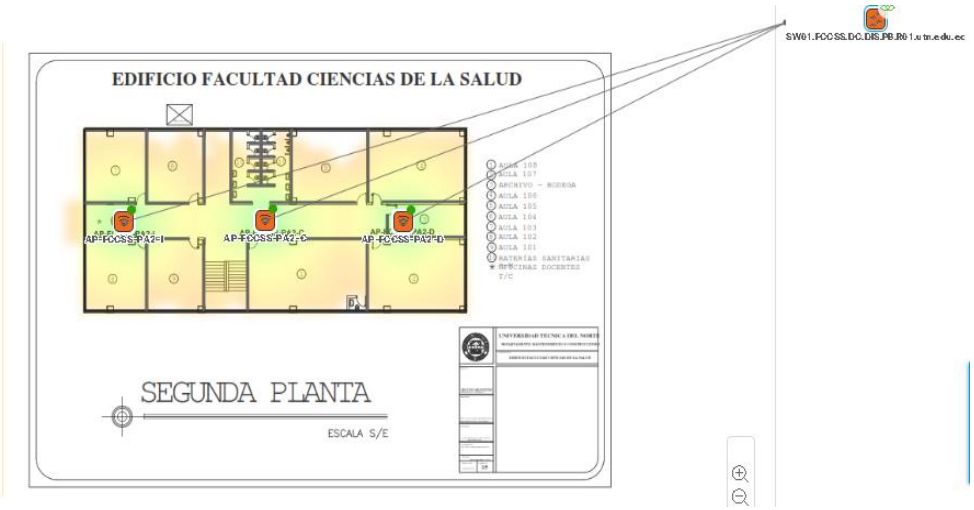
Fuente: Elaboración Autor

Segunda planta FCCSS

Para la segunda planta se tiene un switch Cisco Catalyst 9300 de cual se conectan el AP-FCCSS-PA2-I, AP-FCCSS-PA2-C y AP-FCCSS-PA2-D como se muestra en la Figura 60.

Figura 60

Equipos en la Segunda planta-FCCSS



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 84 se detalla la información de cada uno de los equipos de red instalados en la segunda planta FCCSS.

Tabla 84

Equipos de red por DNA

Ubicación	Dirección ip	Marca /modelo	descripción
Planta baja	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.FCCSS.DC.DIS.PB.R01.utn.edu.ec
Segunda planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FCCSS-PA2-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FCCSS-PA2-D
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FCCSS-PA2-C

Fuente: Elaboración Autor

Tercera planta FCCSS

Para la tercera planta se tiene un switch Cisco Catalyst 9300 de cual se conectan el AP-FCCSS-PA3-D, AP-FCCSS-PA3-I y AP-FCCSS-PA3-C como se muestra en la Figura 61.

Figura 61

Equipos en la Tercera planta-FCCSS

Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 85 se detalla la información de cada uno de los equipos de red instalados en la tercera planta FCCSS.

Tabla 85

Equipos de red por DNA

Ubicación	Dirección IP	Marca /modelo	descripción
Planta baja	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.FCCSS.DC.DIS.PB.R01.utn.edu.ec

	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FCCSS-PA3-D
Tercera planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FCCSS-PA3-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FCCSS-PA3-C

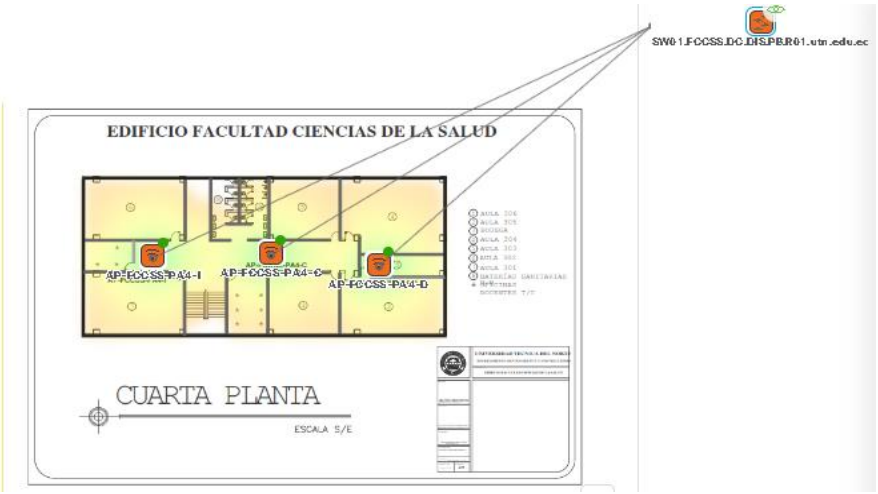
Fuente: Elaboración Autor

Cuarta planta FCCSS

Para cuarta planta se tiene un switch Cisco Catalyst 9300 de cual se conectan el AP-FCCSS-PA4-I, AP-FCCSS-PA4-C y AP-FCCSS-PA4-D como se muestra en la Figura 62.

Figura 62

Equipos en la Cuarta planta-FCCSS



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 86 se detalla la información de cada uno de los equipos de red instalados en la cuarta planta FCCSS.

Tabla 86

Equipos de red por DNA

Ubicación	Dirección ip	Marca /modelo	descripción
Planta baja	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.FCCSS.DC.DIS.PB.R01.utn.edu.ec
Cuarta planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FCCSS-PA4-D
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FCCSS-PA4-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FCCSS-PA4-C

Fuente: Elaboración Autor

Quinta planta FCCSS

Para la quinta planta se tiene un switch Cisco Catalyst 9300 de cual se conectan por medio cableado a AP-FCCSS-PA5-D, AP-FCCSS-PA5-I y AP-FCCSS-PA5-C como se muestra en la Figura 63.

Figura 63

Equipos en la Tercera planta-FCCSS

Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 87 se detalla la información de cada uno de los equipos de red instalados en la cuarta planta FCCSS.

Tabla 87

Equipos de red por DNA

Ubicación	Dirección ip	Marca /modelo	descripción
Planta baja	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.FCCSS.DC.DIS.PB.R01.utn.edu.ec
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FCCSS-PA5-D
Quinta planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FCCSS-PA5-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FCCSS-PA5-C

Fuente: Elaboración Autor

3.5.1.5. FACAE

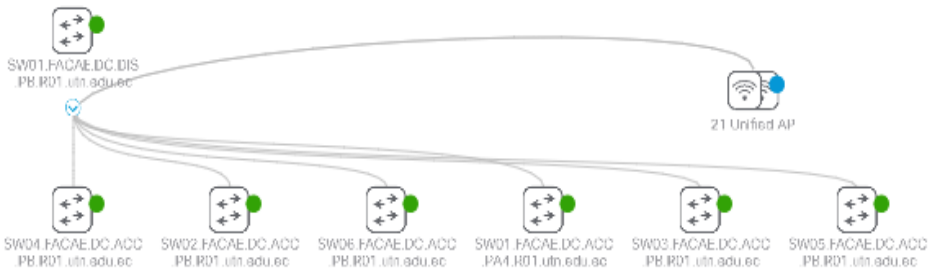
Conexión de la red

Para las conexiones de los equipos de red utilizados en la topología correspondiente a la FACAE mediante enlaces físicos. Donde se tiene a un switch Cisco Catalyst 9300 Series principal donde se conectan Seis Cisco Catalyst 9200 Series Switches y veintiún Cisco Catalyst 9115AXI Series Unified Access Points como se muestra en la Figura 64.

A continuación, se muestra la topología de equipos de red pertenecientes a la facultad FACAE visualizadas por DNA.

Figura 64

Estado actual de conexión de red FCCSS



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Conexión de red por plantas

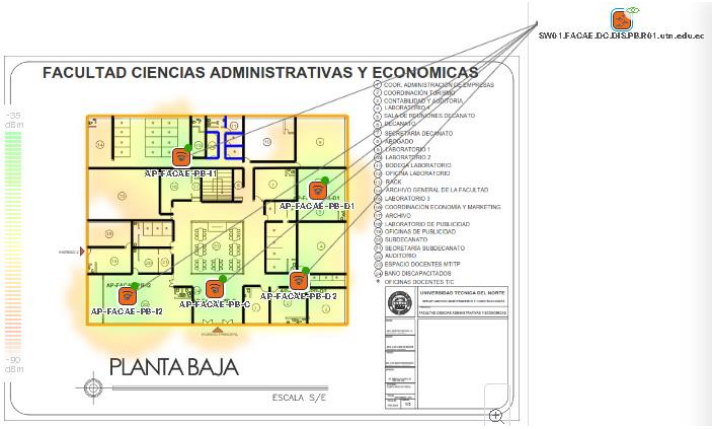
A continuación, se detalla las conexiones de red por cada planta.

Planta baja FACAE

Para planta baja se tiene un switch Cisco Catalyst 9300 Series de cual se conectan el AP-FACAE-PBI-I1, AP-FACAE-PBI-I1, AP-FACAE-PBI-D1, AP-FACAE-PBI-D2 y AP-FACAE-PBI-C, como se muestra en la Figura 65.

Figura 65

Equipos en la Planta Baja-FICAYA



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 88 se detalla la información de cada uno de los equipos de red instalados en la planta baja FACAE.

Tabla 88

Equipos de red por DNA

Ubicación	Dirección ip	Marca /modelo	descripción
Planta baja	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.FACAE.DC.DIS.PB.R01.utn.edu.ec
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE-PBI-I1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE-PBI-I2
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE-PBI-D1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE-PBI-D2
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE-PBI-C

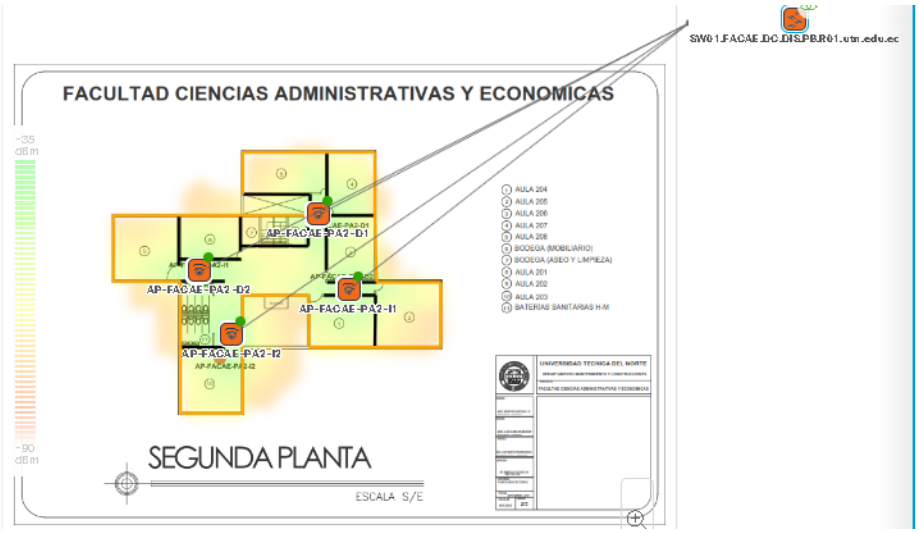
Fuente: Elaboración Autor

Segunda planta FACAE

Para la segunda planta se tiene un switch Cisco Catalyst 9300 de cual se conectan el AP-FACAE -PA2-I1, AP-FACAE -PA2-I2, AP-FACAE -PA2-D1 y AP-FACAE -PA2-D2 como se muestra en la Figura 66.

Figura 66

Equipos en la Segunda planta-FACAE



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 89 se detalla la información de cada uno de los equipos de red instalados en la segunda planta FACAE.

Tabla 89

Equipos de red por DNA

Ubicación	Dirección ip	Marca /modelo	descripción
Planta baja	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.FACAE.DC.DIS.PB.R01.utn.edu.ec
Segunda planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE -PA2-I1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE -PA2-I2
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE -PA2-D1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE -PA2-D2

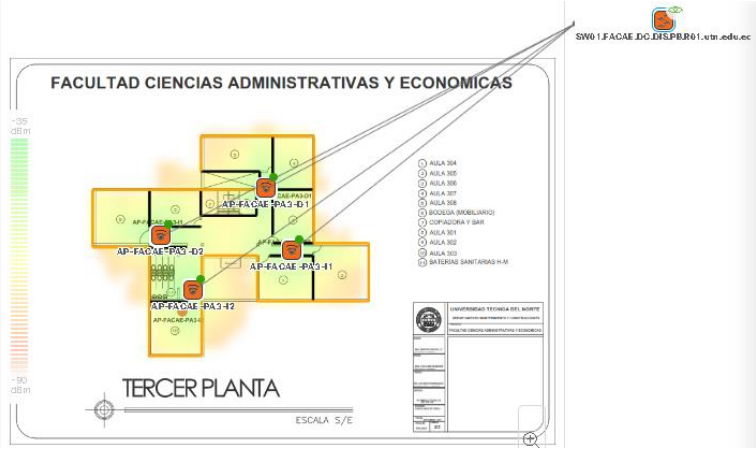
Fuente: Elaboración Autor

Tercera planta FACAE

Para la tercera planta se tiene un switch Cisco Catalyst 9300 de cual se conectan el AP-FACAE-PA3-D1, AP-FACAE-PA3-D2, AP-FACAE-PA3-I1 y AP-FACAE-PA3-I2 como se muestra en la Figura 67.

Figura 67

Equipos en la Tercera planta-FICAYA



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 90 se detalla la información de cada uno de los equipos de red instalados en la tercera planta FACAE.

Tabla 90

Equipos de red por DNA

Ubicación	Dirección IP	Marca /modelo	descripción
Planta baja	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.FACAE.DC.DIS.PB.R01.utn.edu.ec
Tercera planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE-PA3-D1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE-PA3-D2
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE-PA3-I1

	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE-PA3-I2

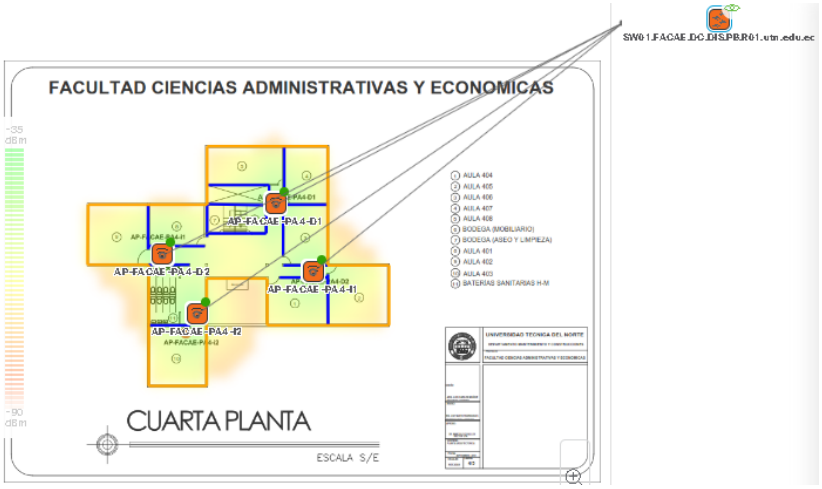
Fuente: Elaboración Autor

Cuarta planta FACAE

Para cuarta planta se tiene un switch Cisco Catalyst 9300 de cual se conectan el AP-FACAE-PA4-I1, AP-FACAE-PA4-I2, AP-FACAE-PA4-D1 y AP-FACAE-PA4-D2 como se muestra en la Figura 68.

Figura 68

Equipos en la Cuarta planta-FICAYA



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 91 se detalla la información de cada uno de los equipos de red instalados en la cuarta planta FACAE.

Tabla 91

Equipos de red por DNA

Ubicación	Dirección IP	Marca /modelo	descripción
Planta baja	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.FACAE.DC.DIS.PB.R01.utn.edu.ec

Cuarta planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE-PA4-I1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE-PA4-I2
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE-PA4-D1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE-PA4-D2

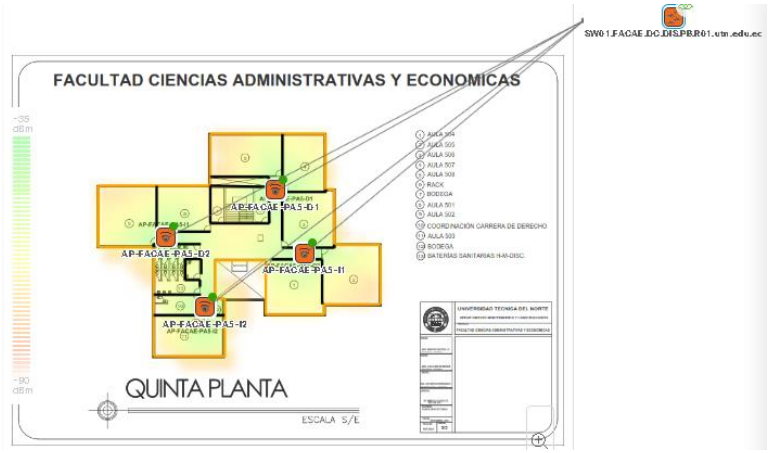
Fuente: Elaboración Autor

Quinta planta FACAE

Para la quinta planta se tiene un switch Cisco Catalyst 9300 de cual se conectan por medio cableado a AP-FACAE-PA5-I1, AP-FACAE-PA5-I2, AP-FACAE-PA5-D1 y AP-FACAE-PA5-D2 como se muestra en la Figura 69.

Figura 69

Equipos en la Quinta planta-FICAYA



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 92 se detalla la información de cada uno de los equipos de red instalados en la cuarta planta FACAE.

Tabla 92

Equipos de red por DNA

Ubicación	Dirección ip	Marca /modelo	descripción
Planta baja	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.FACAE.DC.DIS.PB.R01.utn.edu.ec
Tercera planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE-PA5-I1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE-PA5-I2
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE-PA5-D1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-FACAE-PA5-D2

Fuente: Elaboración Autor

3.5.1.6. AUDITORIO AGUSTÍN CUEVA

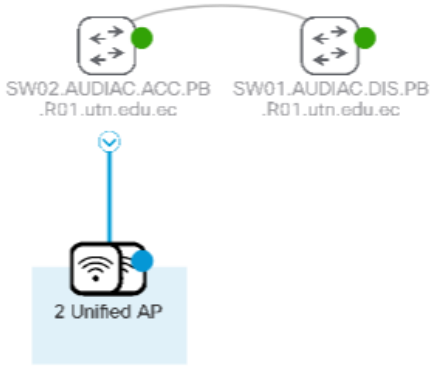
Conexión de la red

Para las conexiones de los equipos de red utilizados en la topología correspondiente a el AUDITORIO AGUSTÍN mediante enlaces físicos. Donde se tiene a un switch Cisco Catalyst 2960-X/XR Series Switches principal donde se conecta un Cisco Catalyst 9200 Series Switches y dos Cisco 3700I Series Unified Access Points como se muestra en la Figura 70.

A continuación, se muestra la topología de equipos de red pertenecientes a el AUDITORIO AGUSTÍN visualizadas por DNA.

Figura 70

Estado actual de conexión de red Auditorio Agustín Cueva



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

3.5.1.7. BIBLIOTECA

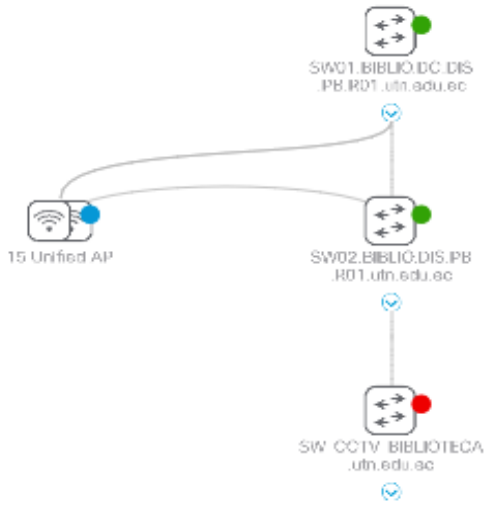
Conexión de la red

Para las conexiones de los equipos de red utilizados en la topología correspondiente a la BIBLIOTECA mediante enlaces físicos. Donde se tiene a un switch switch Cisco Catalyst 9300 Series Switches principal donde se conecta un Cisco Catalyst 9200 Series Switches y un Cisco Catalyst 2960-X/XR Series Switches y quince Cisco Catalyst 9115AXI Unified Access Pointcomo se muestra en la Figura 71.

A continuación, se muestra la topología de equipos de red pertenecientes a la BIBLIOTECA visualizadas por DNA.

Figura 71

Estado actual de conexión de red de la Biblioteca



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Conexión de red por plantas

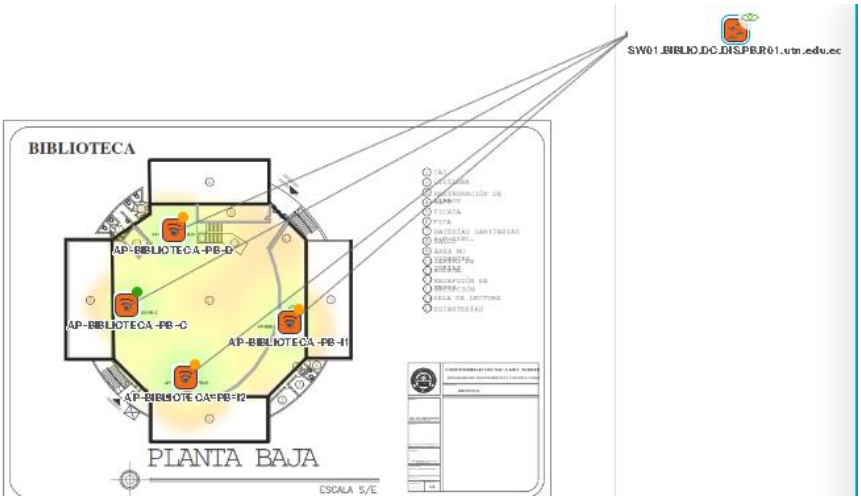
A continuación, se detalla las conexiones de red por cada planta.

Planta baja BIBLIOTECA

Para planta baja se tiene un switch Cisco Catalyst 9300 Series de cual se conectan el AP-BIBLIOTECA-PBI-I1, AP- BIBLIOTECA -PBI-I2, AP- BIBLIOTECA -PBI-D y AP-BIBLIOTECA -PBI-C, como se muestra en la Figura 72.

Figura 72

Equipos en la planta Baja-FICAYA



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 93 se detalla la información de cada uno de los equipos de red instalados en la planta baja BIBLIOTECA.

Tabla 93

Equipos de red por DNA

Ubicación	Dirección IP	Marca /modelo	Descripción
Planta baja	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.BIBLIO.DC.DIS.PB.R01.utn.edu.ec
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- BIBLIOTECA -PBI-I1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- BIBLIOTECA -PBI-I2
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- BIBLIOTECA -PBI-D
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- BIBLIOTECA -PBI-C

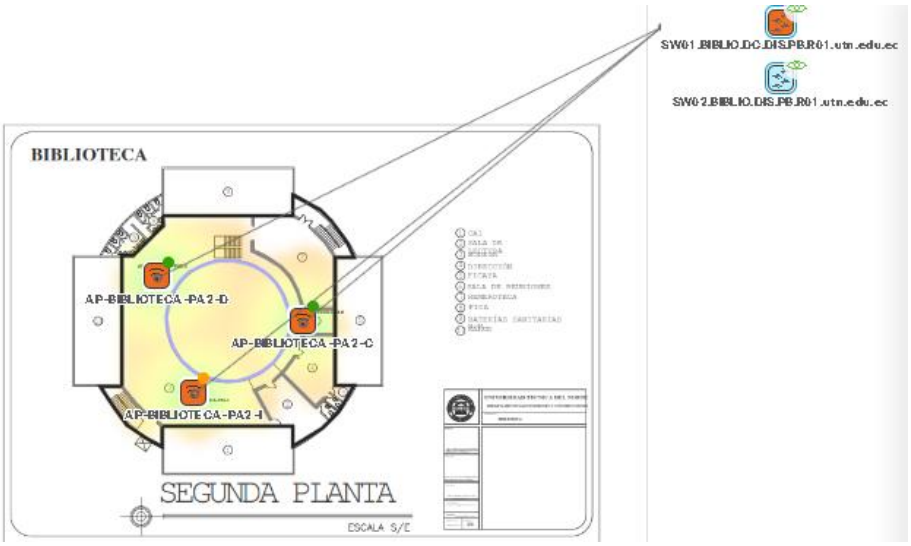
Fuente: Elaboración Autor

Segunda planta BLIOTECA

Para la segunda planta se tiene un switch Cisco Catalyst 9300 de cual se conectan el AP- BIBLIOTECA-PA2-I1, AP- BIBLIOTECA-PA2-I2, AP- BIBLIOTECA -PA2-D y AP-BIBLIOTECA -PA2-C, además se conecta Cisco Catalyst 2960-X/XR Series Switche un como se muestra en la Figura 73.

Figura 73

Equipos en la Segunda planta-Biblioteca



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 94 se detalla la información de cada uno de los equipos de red instalados en la segunda planta BIBLIOTECA.

Tabla 94

Equipos de red por DNA

Ubicación	Dirección ip	Marca /modelo	descripción
Planta baja	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.BIBLIO.DC.DIS.PB.R01.utn.edu.ec

	172.16.X.X	Cisco Catalyst 2960-X/XR Series Switches	SW02.BIBLIO.DIS.PB.R01.utn.edu.ec
Segunda planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- BIBLIOTECA -PA2-I1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- BIBLIOTECA -PA2-I2
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- BIBLIOTECA -PA2-D
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- BIBLIOTECA -PA2-C

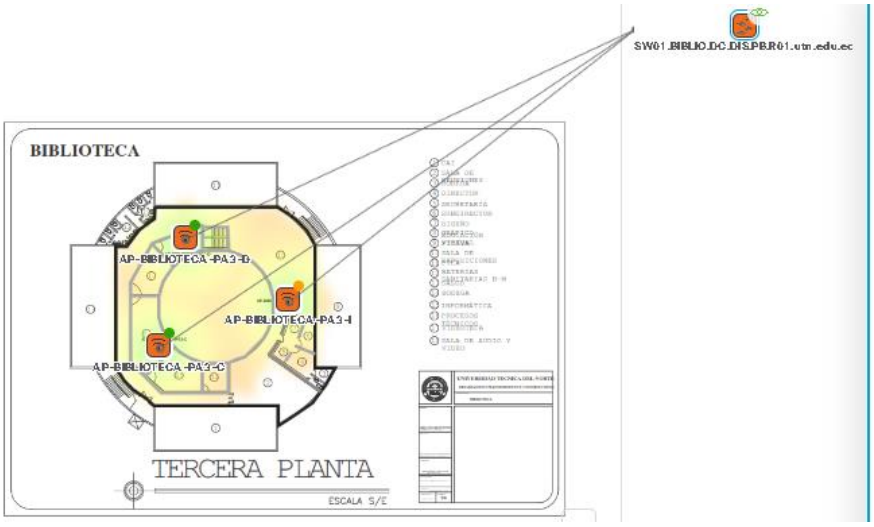
Fuente: Elaboración Autor

Tercera planta BIBLIOTECA

Para la tercera planta se tiene un switch Cisco Catalyst 9300 de cual se conectan el AP- BIBLIOTECA -PA3-I1, AP- BIBLIOTECA -PA3-I2, AP- BIBLIOTECA-PA3-D y AP-BIBLIOTECA-PA3-C como se muestra en la Figura 74.

Figura 74

Equipos en la Tercera planta-FICAYA



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 95 se detalla la información de cada uno de los equipos de red instalados en la tercera planta BIBLIOTECA.

Tabla 95

Equipos de red por DNA

Ubicación	Dirección IP	Marca /modelo	descripción
Planta baja	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.BIBLIO.DC.DIS.PB.R01.utn.edu.ec
Tercera planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- BIBLIOTECA -PA3-D
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- BIBLIOTECA -PA3-C
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- BIBLIOTECA -PA3-I1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- BIBLIOTECA -PA3-I2

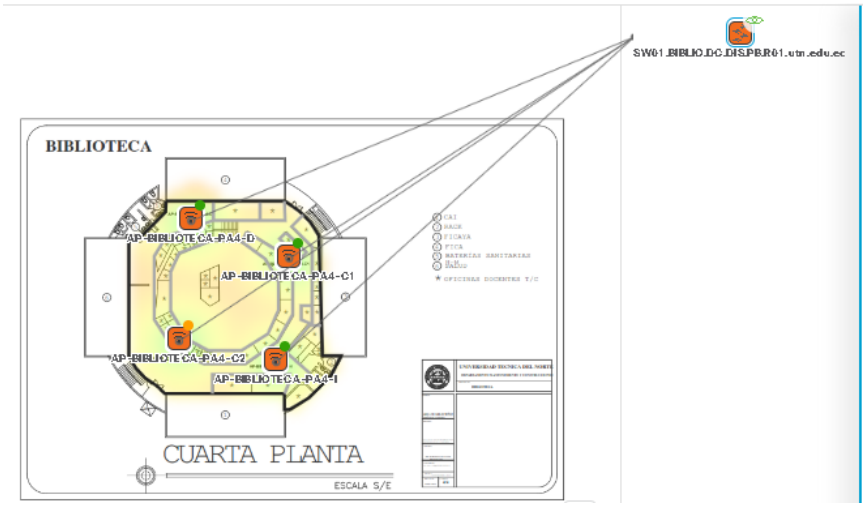
Fuente: Elaboración Autor

Cuarta planta BIBLIOTECA

Para cuarta planta se tiene un switch Cisco Catalyst 9300 de cual se conectan el AP-BIBLIOTECA-PA4-C1, AP- BIBLIOTECA -PA4-C2, AP- BIBLIOTECA -PA4-C y AP-BIBLIOTECA -PA4-D como se muestra en la Figura 75.

Figura 75

Equipos en la Cuarta planta-Biblioteca



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 96 se detalla la información de cada uno de los equipos de red instalados en la cuarta planta BIBLIOTECA.

Tabla 96

Equipos de red por DNA

Ubicación	Dirección IP	Marca /modelo	descripción
Planta baja	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.BLIBLIO.DC.DIS.PB.R01.utn.edu.ec
Cuarta planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- BIBLIOTECA-PA4-C1
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- BIBLIOTECA-PA4-C2
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- BIBLIOTECA-PA4-D
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- BIBLIOTECA-PA4-C

Fuente: Elaboración Autor

3.5.1.8. EDIFICIO CENTRAL

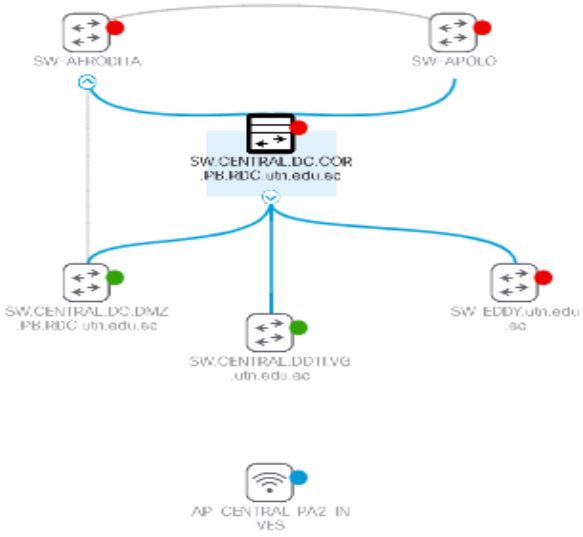
Conexión de la red

Para las conexiones de los equipos de red utilizados en la topología correspondiente a el EDIFICIO CENTRAL donde se encuentra el data center compuestos por un Cisco Catalyst 9400 Series Switches, dos Cisco Catalyst Blade Switch 3000 Series como core, un Cisco Catalyst 9300 Series Switches para distribución y dos Cisco Catalyst 2960-X/XR Series Switches para acceso.

A continuación, en la Figura 76 se muestra la topología de equipos de red pertenecientes a el EDIFICO CENTRAL DATA CENTER visualizadas por DNA.

Figura 76

Estado actual de conexión de red en el Edificio Central



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

3.5.1.9. LABORATORIOS ELECTRICIDAD Y MECÁNICA

Conexión de la red

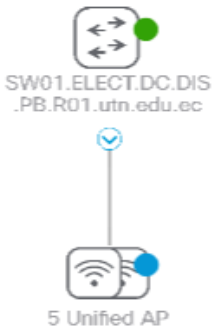
Para las conexiones de los equipos de red utilizados en la topología correspondiente a la LAB ELEC-MECANICA mediante enlaces físicos. Donde se tiene a un switch switch

Cisco Catalyst 9200 Series Switches principal donde se conectan cinco Cisco Catalyst 9115AXI Unified Access Pointcomo se muestra en la Figura 77.

A continuación, se muestra la topología de equipos de red pertenecientes a la LAB ELEC-MECANICA visualizadas por DNA.

Figura 77

Estado actual de conexión de red en los Labs. de Electricidad y Mecánica



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Conexión de red por plantas

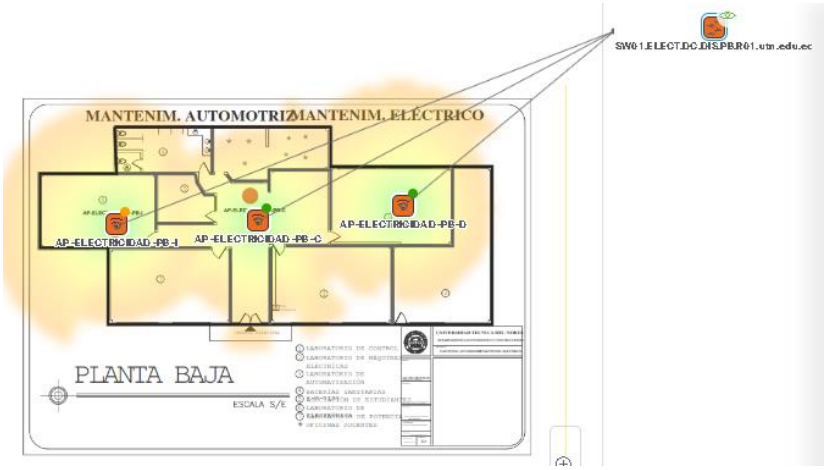
A continuación, se detalla las conexiones de red por cada planta.

Planta baja LAB ELEC-MECANICA

Para planta baja se tiene un switch Cisco Catalyst 9200 Series de cual se conectan el AP-ELECTRICIDAD-PB-I, AP- ELECTRICIDAD -PB-D y AP- ELECTRICIDAD-PB-D, como se muestra en la Figura 78.

Figura 78

Equipos en la Segunda planta-Mantenim. Automotriz y Eléctrico



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 97 se detalla la información de cada uno de los equipos de red instalados en la planta baja LAB.ELETRICIDAD.

Tabla 97

Equipos de red por DNA

Ubicación	Dirección IP	Marca /modelo	descripción
Planta baja	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.ELECT.DC.DIS.PB.R01.utn.edu.ec
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-ELECTRICIDAD-PB-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-ELECTRICIDAD-PB-D
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-ELECTRICIDAD-PB-C

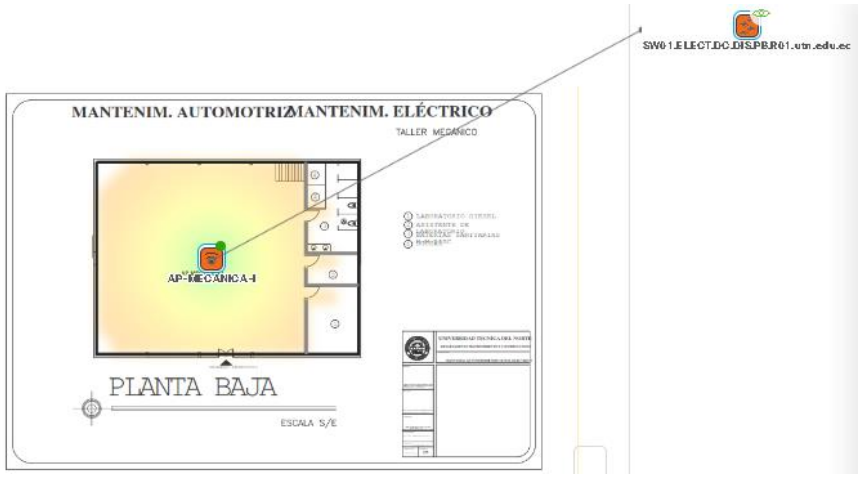
Fuente: Elaboración Autor

Planta baja LAB. MECÁNICA AUTOMOTRIZ

Para la planta baja del lab. mecánica se tiene un switch Cisco Catalyst 9200 de cual se conecta a el AP-MECANICA-I, como se muestra en la Figura 79.

Figura 79

Equipos en la Segunda planta-Mantenimiento Automotriz y Eléctrico



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 98 se detalla la información de cada uno de los equipos de red instalados en la segunda planta LAB. MECANICA.

Tabla 98

Equipos de red por DNA

Ubicación	Dirección ip	Marca /modelo	descripción
Planta baja Lab. Mecánica	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.ELECT.DC.DIS.PB.R01.utn.edu.ec
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-MECANICA-I

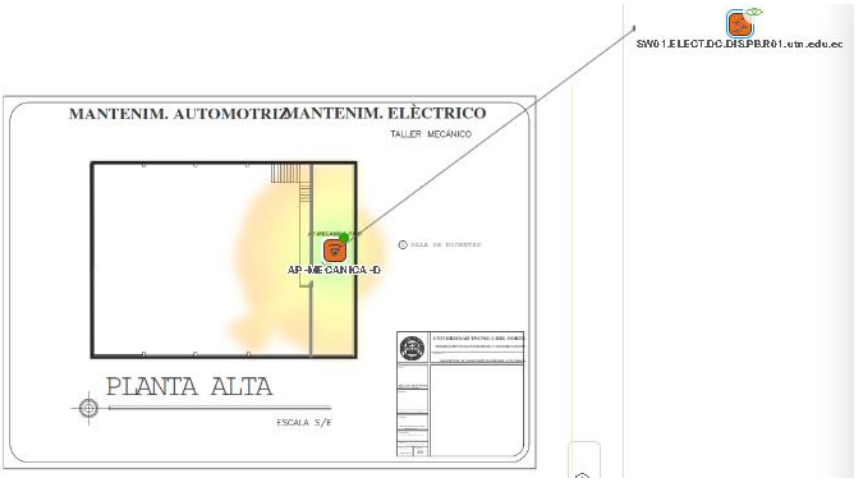
Fuente: Elaboración Autor

Planta alta LAB. ELEC-MECÁNICA

Para la tercera planta se tiene un switch Cisco Catalyst 9200 de cual se conectan a el AP-MECANICA-D como se muestra en la Figura 80.

Figura 80

Equipos en la Segunda planta- Mantenim Automotriz y Eléctrico



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 99 se detalla la información de cada uno de los equipos de red instalados en la planta alta del LAB. ELECT-MECANICA.

Tabla 99

Equipos de red por DNA

Ubicación	Dirección ip	Marca /modelo	descripción
Planta alta lab. Elec-mecanica	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.ELECT.DC.DIS.PB.R01.utn.edu.ec
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP-MECANICA-D

Fuente: Elaboración Autor

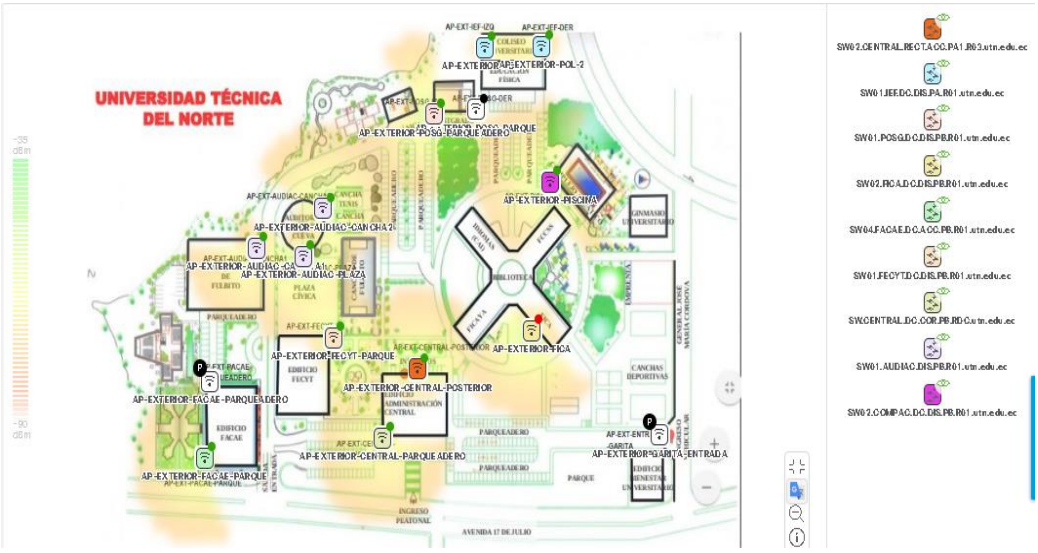
3.5.1.10.EXTERIORES

Conexión de la red

Para las conexiones de los equipos de red utilizados en la topología correspondiente a la EXTERIORES mediante enlaces físicos en varios puntos alrededor del campus universitario como muestra en la Figura 81.

Figura 81

Conexiones de los equipos de red en los exteriores de la UTN



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, se detalla cada uno de los puntos de acceso exteriores y su enlace físico a los conmutadores.

Para los APS AP-EXTERIOR-POL-1 y AP-EXTERIOR-POL-2 (Cisco 1562E Unified Access Point) se conectan mediante enlace físico al switch SW02.CENTRAL.RECT.ACC.PA1.R03.utn.edu.ec (Cisco Catalyst 2960 Series Switches), como se muestra en la Figura 82.

Figura 82

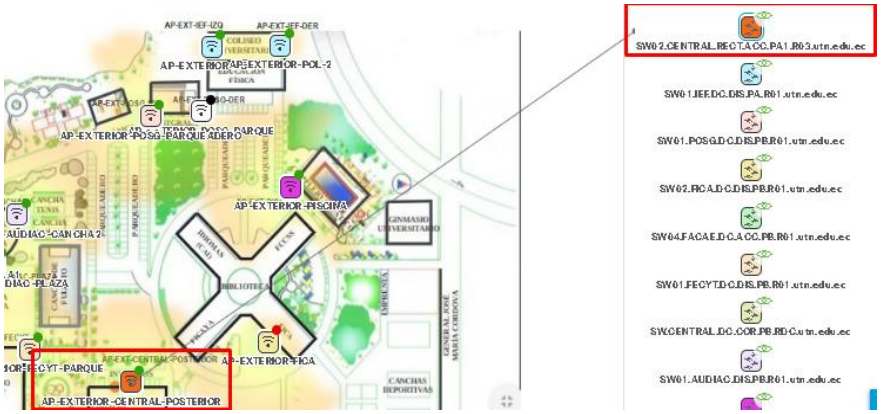
APS AP-EXTERIOR-POL-1 y AP-EXTERIOR-POL-2

Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Para el AP-EXTERIOR-CENTRAL-POSTERIOR (Cisco 1562E Unified Access Point) se encuentra conectado mediante un enlace físico a SW02.CENTRAL.RECT.ACC.PA1.R03.utn.edu.ec(Cisco Catalyst 2960 Series Switches), como se muestra en la Figura 83.

Figura 83

AP-EXTERIOR-CENTRAL-POSTERIOR

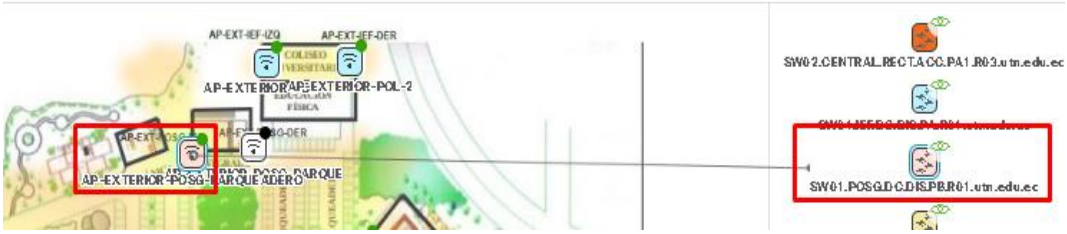


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Para el AP-EXTERIOR-POSG-PARQUEADERO (Cisco 1562E Unified Access Point) se encuentra conectado mediante enlace físico al switch SW01.POSG.DC.DIS.PB.R01.utn.edu.ec (Cisco Catalyst 9300 Series Switches), como se muestra en la Figura 84.

Figura 84

AP-EXTERIOR-POSG-PARQUEADERO

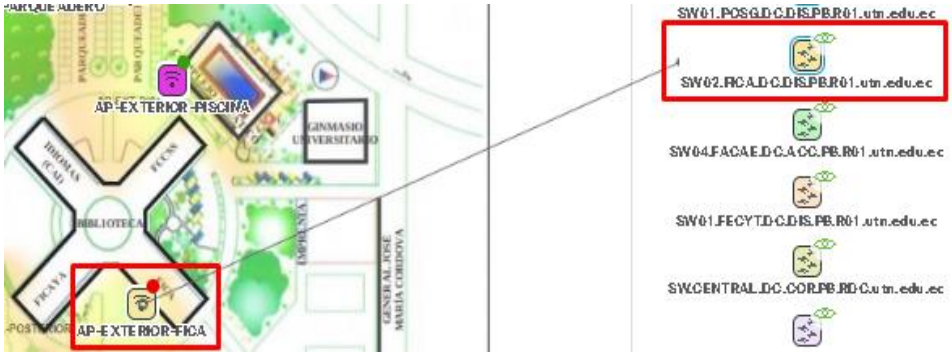


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Para el AP-EXTERIOR-FICA (Cisco 1562E Unified Access Point) se encuentra conectado mediante enlace físico al switch SW02.FICA.DC.DIS.PB.R01.utn.edu.ec (Cisco Catalyst 4500 Series Switches), como se muestra en la Figura 85.

Figura 85

AP-EXTERIOR-FICA

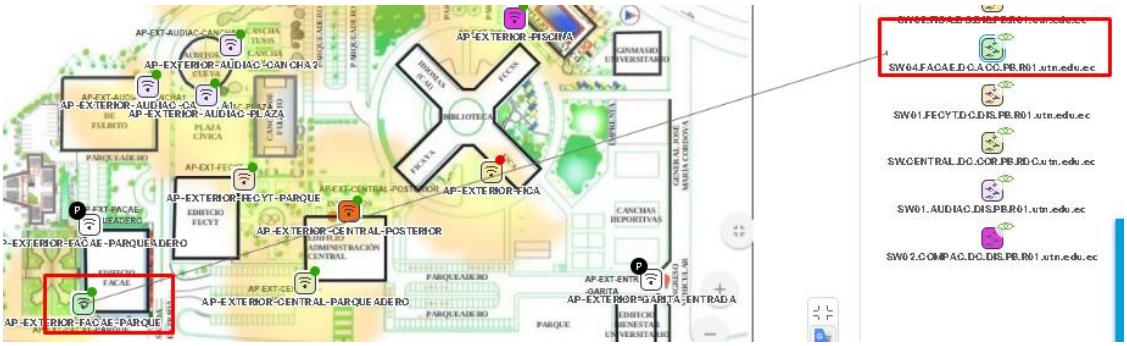


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Para el AP-EXTERIOR-FACAE-PARQUE (Cisco 1562E Unified Access Point) se encuentra conectado mediante enlace físico al switch SW04.FACAE.DC.ACC.PB.R01.utn.edu.ec (Cisco Catalyst 9200 Series Switches), como se muestra en la Figura 86.

Figura 86

AP-EXTERIOR-FACAE-PARQUE

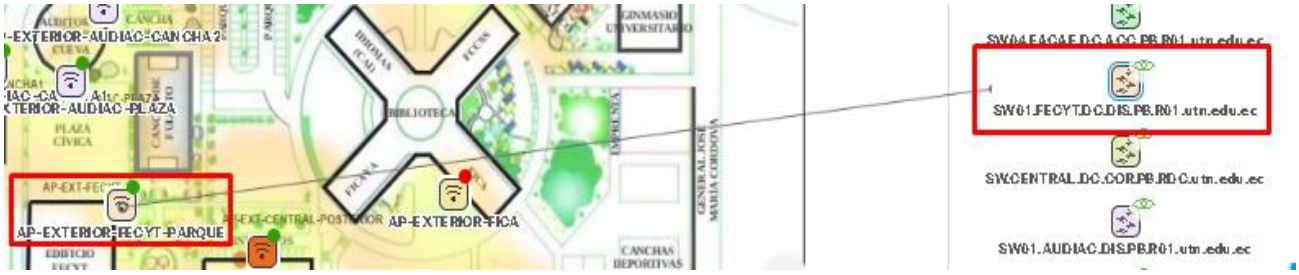


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Para el AP-EXTERIOR-FECYT-PARQUE (Cisco 1562E Unified Access Point) se encuentra conectado mediante enlace físico al switch SW01.FECYT.DC.DIS.PB.R01.utn.edu.ec (Cisco Catalyst 9300 Series Switches), como se muestra en la Figura 87.

Figura 87

AP-EXTERIOR-FECYT-PARQUE



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Para el AP-EXTERIOR-CENTRAL-PARQUEADERO (Cisco 1562E Unified Access Point) se encuentra conectado mediante enlace físico al switch SW.CENTRAL.DC.COR.PB.RDC.utn.edu.ec (Cisco Catalyst 9400 Series Switches), como se muestra en la Figura 88.

Figura 88

AP-EXTERIOR-CENTRAL-PARQUEADERO

Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Para los AP-EXTERIOR-AUDIAC-PLAZA, AP-EXTERIOR-AUDIAC-CANCHA2 y AP-EXTERIOR-AUDIAC-CANCHA1 (Cisco 1562E Unified Access Point) se encuentra conectado mediante enlace físico al switch SW01.AUDIAC.DIS.PB.R01.utn.edu.ec (Cisco Catalyst 9200 Series Switches), como se muestra en la Figura 89.

Figura 89

AP-EXTERIOR-AUDIAC-PLAZA

Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Para el AP-EXTERIOR-PISCINA (Cisco 1562E Unified Access Point) se encuentra conectado mediante enlace físico al switch SW02.COMPAC.DC.DIS.PB.R01.utn.edu.ec (Cisco Catalyst 2960-X/XR Series Switches), como se muestra en la Figura 90.

Figura 90

AP-EXTERIOR-PISCINA

Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

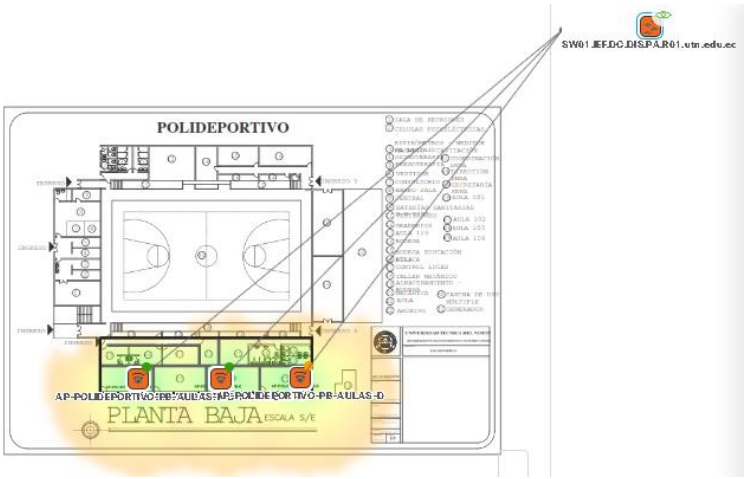
3.5.1.11.POLIDEPORTIVO

Conexión de la red

Para las conexiones de los equipos de red utilizados en la topología correspondiente a el POLIDEPORTIVO mediante enlaces físicos. Donde se tiene a un switch switch Cisco Catalyst 9200 Series Switches principal donde se conectan tres Cisco Catalyst 9115AXI Unified Access Pointcomo se muestra en la Figura 91.

Figura 91

Equipos de la red en el Polideportivo



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

3.5.1.12.POSGRADO

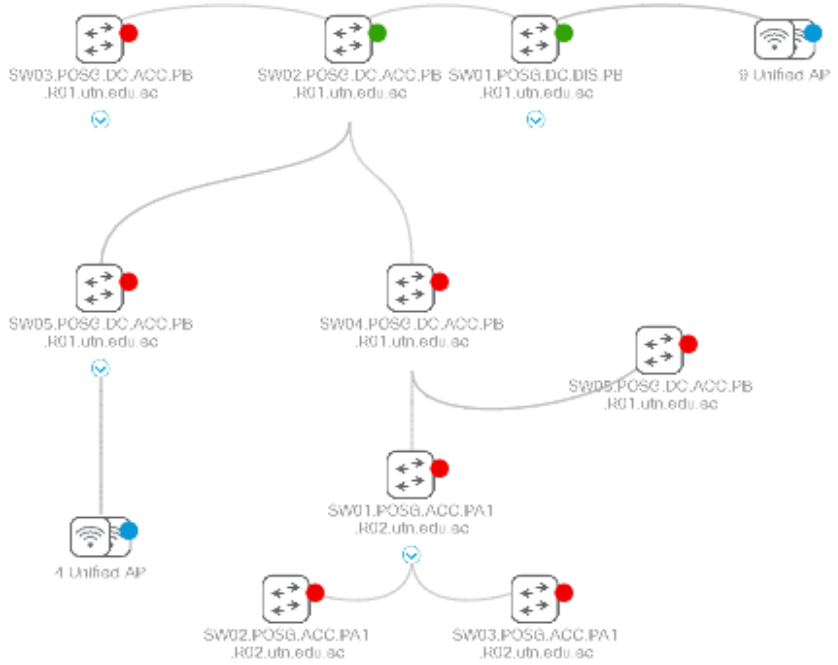
Conexión de la red

Para las conexiones de los equipos de red utilizados en la topología correspondiente a la POSTGRADO mediante enlaces físicos. Donde se tiene a un switch de distribución Cisco Catalyst 2960 Series Switches donde se conectan ocho equipos de conmutación entre Cisco Catalyst 9300 Series Switches, Cisco Catalyst 2960 Series Switches, Cisco Catalyst 4500 Series Switches y Catalyst 2960-X/XR Series Switches y trece Cisco Catalyst 9115AXI Unified Access Pointcomo se muestra en la Figura 92.

A continuación, se muestra la topología de equipos de red pertenecientes a la POSTGRADOS visualizadas por DNA.

Figura 92

Estado actual de conexión de red Posgrado



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Conexión de red por plantas

A continuación, se detalla las conexiones de red por cada planta.

Planta baja POSTGRADO

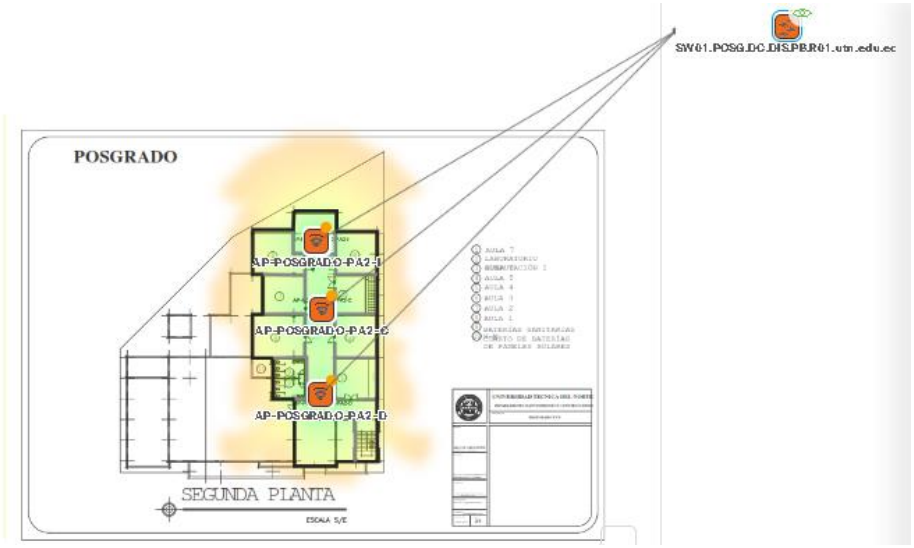
Para planta baja no se tiene equipos implementados.

Segunda planta POSTGRADO

Para la segunda planta se tiene un switch Cisco Catalyst 9300 de cual se conectan el AP- POSTGRADO-PA2-I, AP- POSTGRADO-PA2-C y AP- POSTGRADO-PA2-D como se muestra en la Figura 93.

Figura 93

Equipos en la Segunda planta-Postgrado



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 100 se detalla la información de cada uno de los equipos de red instalados en la segunda planta POSTGRADO.

Tabla 100

Equipos de red por DNA

Ubicación	Dirección ip	Marca /modelo	descripción
Planta baja	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.POSG.DC.DIS.PB.R01.utn.edu.ec
Segunda planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- POSTGRADO-PA2-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- POSTGRADO-PA2-D
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- POSTGRADO-PA2-C

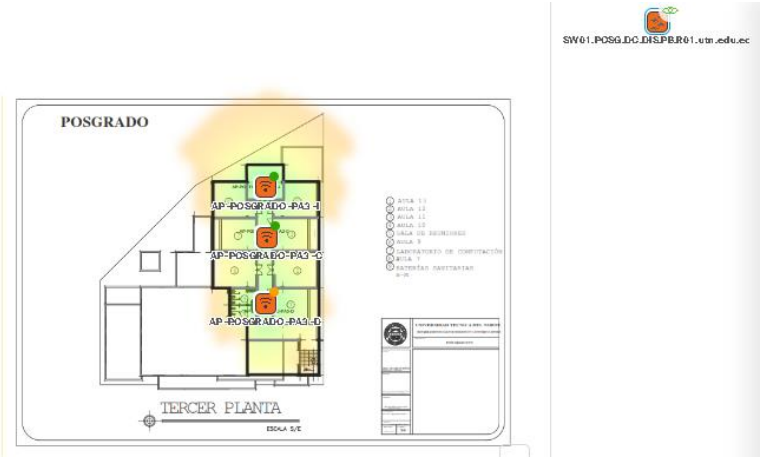
Fuente: Elaboración Autor

Tercera planta POSTGRADO

Para la tercera planta se tiene un switch Cisco Catalyst 9300 de cual se conectan el AP- POSTGRADO-PA3-I, AP- POSTGRADO-PA3-C y AP- POSTGRADO-PA3-D como se muestra en la Figura 94.

Figura 94

Equipos en la Segunda planta-Postgrado



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 101 se detalla la información de cada uno de los equipos de red instalados en la tercera planta POSTGRADO.

Tabla 101

Equipos de red por DNA

Ubicación	Dirección ip	Marca /modelo	descripción
Planta baja	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.POSG.DC.DIS.PB.R01.utn.edu.ec
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- POSTGRADO-PA3-I
Tercera planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- POSTGRADO-PA3-D
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- POSTGRADO-PA3-C

Fuente: Elaboración Autor

Cuarta planta POSTGRADO

Para la cuarta planta se tiene un switch Cisco Catalyst 9300 de cual se conectan el AP- POSTGRADO-PA4-I, AP- POSTGRADO-PA4-C y AP- POSTGRADO-PA4-D como se muestra en la Figura 95.

Figura 95

Equipos en la Cuarta planta-Postgrado

Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 102 se detalla la información de cada uno de los equipos de red instalados en la cuarta planta POSTGRADO.

Tabla 102

Equipos de red por DNA

Ubicación	Dirección IP	Marca /modelo	descripción
Planta baja	172.16.X.X	Cisco Catalyst 9300 Series Switches	SW01.POSG.DC.DIS.PB.R01.utn.edu.ec
Cuarta planta	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- POSTGRADO-PA4-I
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- POSTGRADO-PA4-D
	172.16.X.X	Cisco Catalyst 9115AXI Unified Access Point	AP- POSTGRADO-PA4-C

Fuente: Elaboración Autor

3.5.1.13.CAI

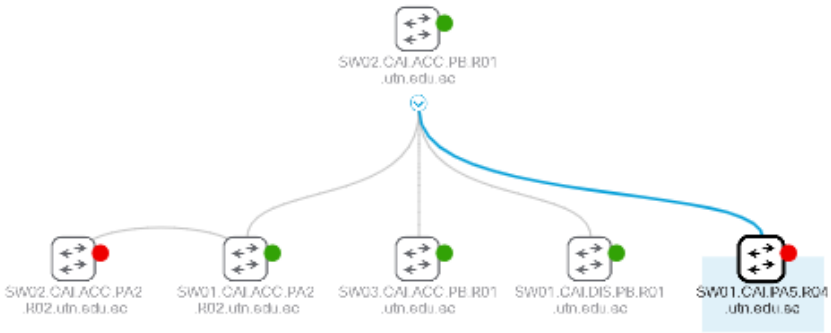
Conexión de la red

Para las conexiones de los equipos de red utilizados en la topología correspondiente a el CAI mediante enlaces físicos. Donde se tiene a un switch de distribución Cisco Catalyst 3850 Series Ethernet Stackable Switch donde se conectan cinco equipos de conmutación un Cisco Catalyst 9200 Series Switches, tres Cisco Catalyst 2960-X/XR Series Switches y un Cisco Catalyst 3750 Series Switches, como se muestra en la Figura 96.

A continuación, se muestra la topología de equipos de red pertenecientes a CAI visualizadas por DNA.

Figura 96

Estado actual de conexión de red CAI



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

3.5.2. Equipamiento del DNA

Como se explicó anteriormente el software de gestión Cisco DNA Center posee en su interfaz a todos los equipos cisco que se encuentren en la red, entonces para equipos como Conmutadores y Access Point es necesario habilitar el protocolo SNMP para poder ser monitoreados por dicho software antes mencionado.

3.5.2.1. Equipamiento del DNA en Conmutadores

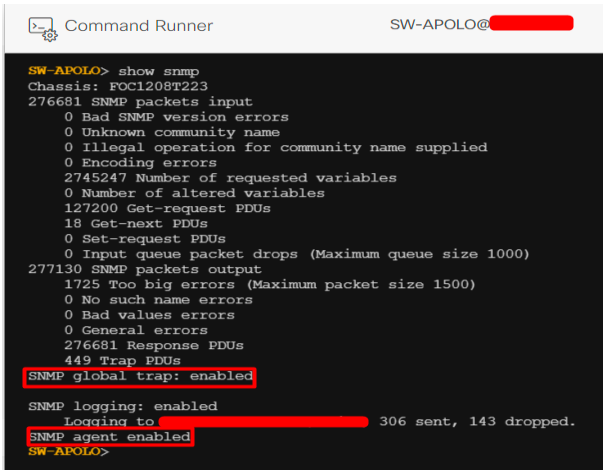
En el siguiente ítem se procede a explicar el procedimiento de equipamiento de los servicios DNA para gestión telemétrica de los conmutadores.

El software DNA Center permite monitorear la red a través del protocolo SNMP y sus respectivas versiones SNMPv1, SNMPv2 y SNMPv3. La versión del del protocolo configurada en este tipo de equipos es la versión V2C, la cual es una subversión de SNMPv2. La versión del protocolo SNMP a configurar dentro del dispositivo gestionado dependerá del administrador de la red, pero comúnmente se configura la versión V2C ya que tiene mejores características que su primera versión y posee una configuración más simple. La configuración de SNMPv3 agrega cifrado y autenticación, que se pueden usar juntos o por separado por ende la configuración es más compleja que simplemente definir una cadena comunitaria.

Es necesario tener el conocimiento que el dispositivo agregado al software de gestión tenga habilitado el protocolo SNMP, mediante el comando *show snmp*, podemos visualizar en la Figura 97 si el protocolo de gestión se encuentra habilitado.

Figura 97

Protocolo de gestión SNMP habilitado

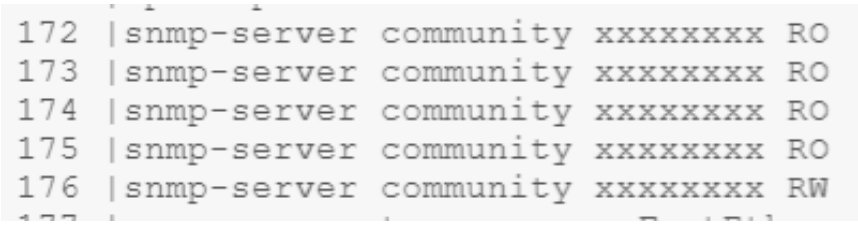


Fuente: Adaptado de Cisco DNA Center del DDTI de la UTN

También se debe tener en cuenta la configuración de la cadena comunidad, donde RO corresponda a la función Read-Only y RW que indica Read-Write, mientras que la cada XXXXXX corresponde al nombre de la comunidad de gestión y por motivos de seguridad por parte del administrado posee esa nomenclatura establecida, tal y como se evidencia en la Figura 98.

Figura 98

Configuración de la cadena comunidad para el protocolo SNMP

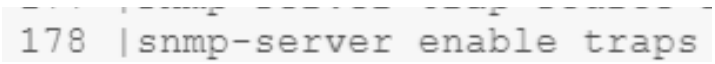


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

También se realiza la configuración de los snmp traps, de tal manera como se visualiza en la Figura 99, ya que estos mensajes son enviados por agentes, sin petición alguna por la estación del administrador y esto sucede cuando un ocurre un imprevisto.

Figura 99

Configuración de los snmp traps



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Las capturas de las configuraciones establecidas son del equipo SW-APOLO que se encuentra en la capa de Core y está ubicado físicamente en el Edificio Central dentro del Data Center en la Universidad Técnica del Norte

Cabe mencionar que dentro de las configuraciones dentro del software de gestión Cisco DNA Center para la recopilación de los parámetros de los recursos de los equipos de conmutación se debe activar las métricas del recopilador SNMP y así seleccionar los

parámetros con los cuales va a funcionar el equipo de conmutación, por ende, en el ANEXO A se detalla la activación de métricas de SNMP COLLECTOR.

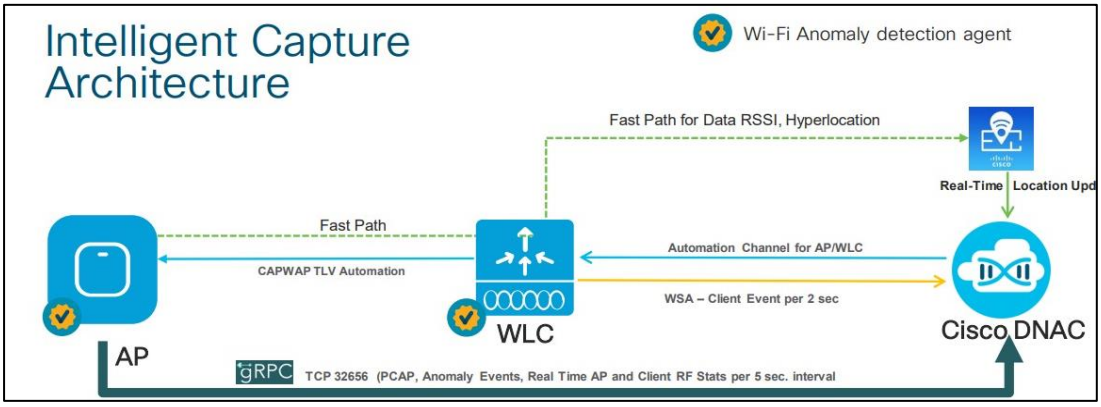
Dentro del ANEXO B se detallan las configuraciones realizadas en los equipos de conmutación, donde se habilitan todos los servicios de SNMP.

3.5.2.2. Equipamientos del DNA en APs

En el siguiente apartado se procede a explicar el procedimiento de equipamiento de los servicios DNA para la gestión telemática de los Access Point. Para poseer una mejor idea de cómo es el funcionamiento entre los AP, el Wireless Controler y Cisco DNA Center se muestra en la Figura 100 la arquitectura de comunicación entre los diferentes equipos que conforman la red inalámbrica.

Figura 100

Arquitectura de funcionamiento entre AP, WLC y DNA



Fuente: Extraído de (Cisco, 2019) Cisco DNA Assurance

El AP Envíe los datos de telemetría directamente al servidor donde se encuentra alojado el software Cisco DNA Center utilizando el canal GRPC.

Estos datos de telemetría contienen estadísticas de RF del cliente en tiempo real y estadísticas AP, PCAP basado en anomalías, eventos de anomalía, datos del espectro.

Una vez entendido como se realiza la comunicación entre los equipos que conforman la red inalámbrica, se procede a explicar el equipamiento y activación de los servicios de telemetría, Para ello lo primero que se realiza es añadir el nuevo equipo al Cisco DNA Center, a continuación, se muestran el proceso a seguir.

- Design > Network Hierarchy.
- En el panel izquierdo, haga clic en la planta del edificio.
- En la barra de herramientas del mapa, haga clic en Añadir/Editar.
- Asegúrese de que el conmutador APs está activado en la barra de herramientas del mapa.
- En el panel izquierdo del mapa, haga clic en Añadir AP.
- En el panel deslizante Agregar AP, marque las casillas de verificación de los puntos de acceso para seleccionar los AP en bloque y haga clic en Agregar Seleccionado. También puede hacer clic en Añadir junto a un punto de acceso.

Utilice el panel deslizante Editar AP para configurar detalles del AP como:

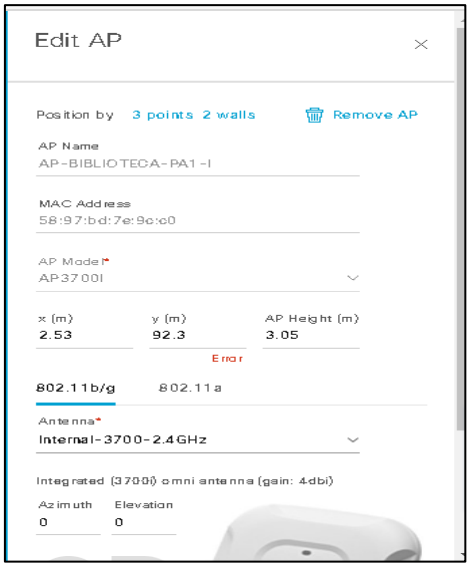
a) **Associated**
b) **Name**.
c) **MAC Address.**
d) **Model.**
e) **Admin/Mode.**
f) **Type Radio**
g) **OP/Admim(Operational status and AP mode.)**
h) **Channel**
i) **Antenna name.**
j) **Azimuth**: dirección de la antena.

k) **Elevation:** elevación en grados.

A continuación, en la Figura 101 se muestra la ventana de visualización de configuraciones después de agregar un AP.

Figura 101

Configuraciones para añadir AP



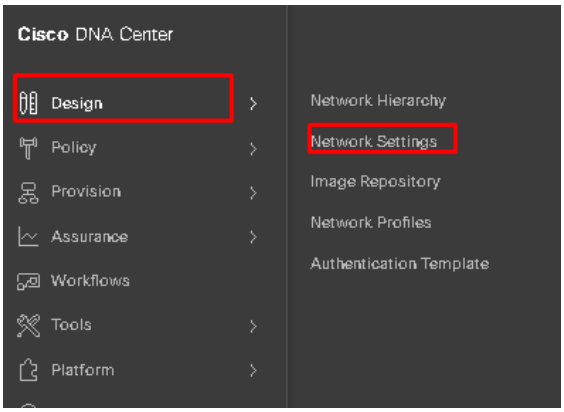
Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

La configuración de servicio de telemetría como Syslog, SNMPTraps, servidores colectores de NetFlow y Recopilación de datos de clientes, a continuación, se muestra el proceso de configuración:

- ✓ Design > Network Settings > Telemetry. Como se muestra en la siguiente Figura 102.

Figura 102

Ingreso a configuraciones deservicios de telemetría



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

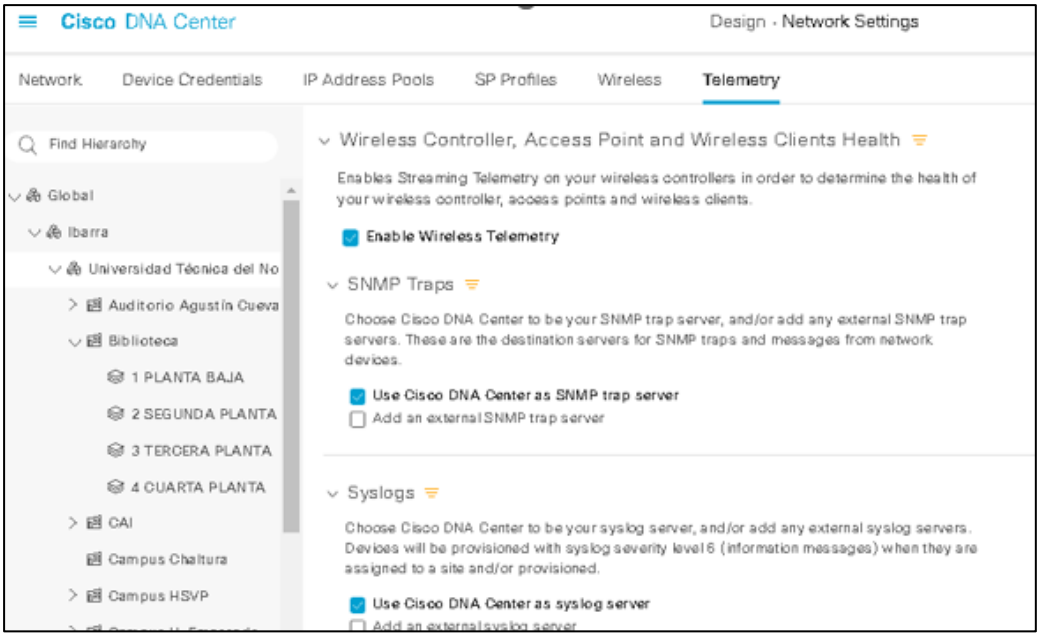
- ✓ Marque la casilla Cisco DNA Center como servidor de traps SNMP.
- ✓ Marque la casilla Agregar un servidor de traps SNMP externo e introduzca la dirección IP del servidor de traps SNMP externo.
- ✓ El servidor seleccionado recopila trampas y mensajes SNMP de los dispositivos de red.
- ✓ Expanda el área Syslogs si no está visible y realice una de las siguientes acciones:
- ✓ Marque la casilla de verificación Utilizar Cisco DNA Center como servidor syslog.
- ✓ Marque la casilla Agregar un servidor syslog externo e introduzca la dirección IP del servidor syslog externo.
- ✓ Expanda el área NetFlow si no está visible y realice una de las siguientes acciones:
- ✓ Seleccione la casilla de verificación Utilizar Cisco DNA Center como servidor de recopilación de NetFlow.

- ✓ La configuración de NetFlow en las interfaces del dispositivo sólo se completa cuando habilita la telemetría de aplicaciones en el
- ✓ dispositivo. Seleccione el recopilador NetFlow a nivel de sitio para configurar el servidor de destino de NetFlow en el dispositivo.
- ✓ Expanda el área Recopilación de datos de clientes cableados y marque la casilla de verificación Supervisar clientes cableados.
- ✓ Expanda el área Salud de la controladora inalámbrica, el punto de acceso y los clientes inalámbricos y active la casilla Activar telemetría inalámbrica.
- ✓ Haga clic en Guardar.

A continuación, en la Figura 103 se muestra la ventana de visualización de configuración de servicios telemetría

Figura 103

Configuración de telemetría



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

3.5.3. Descripción de los servidores en uso dentro de la red de la Universidad Técnica del Norte.

- **Servidor DHCP**

El servidor DHCP proporciona una configuración automática de red TCP/IP segura y evita conflictos de direcciones repetidas para los clientes que desean formar parte de la red. Utiliza un modelo cliente-servidor en el que el servidor DHCP mantiene una administración centralizada con un pool de direcciones IP que pueden ser asignadas. Los clientes podrán solicitar al servidor una dirección IP y así poder integrarse en la red. (Stallings, 2004)

En la Figura 104 se presenta las características del Servidor DHCP que se encuentra en funcionamiento en la red de la Universidad Técnica del Norte.

Figura 104

Características lógicas y físicas del servidor DHCP

```
**************SERVIDOR DHCP**************
        #####           srv_dhcp.utn.edu.ec
       #######          ------------------------
       ##O#O##          OS: AlmaLinux 8.7 (Stone Smilodon) x86_64
       #######          Host: VMware7,1 None
     ###########        Kernel: 4.18.0-425.13.1.el8_7.x86_64
    #############       Uptime: 12 days, 4 hours, 20 mins
   ###############      Packages: 611 (rpm)
   ################     Shell: bash 4.4.20
  ##################    Resolution: 1024x768
####################    CPU: Intel Xeon Silver 4214R (2) @ 2.399GHz
####################    GPU: 00:0f.0 VMware SVGA II Adapter
  ##################    Memory: 453MiB / 1784MiB
```

Fuente: Departamento de Desarrollo de Tecnológico e Informático

- **Servidor DNS CACHE**

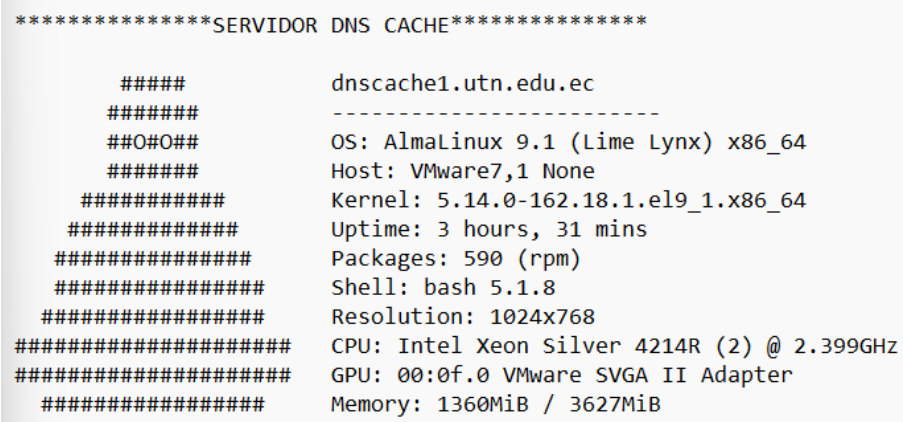
Un servidor DNS caché almacena localmente las búsquedas que los clientes de la red realizan a un servidor de nombres de dominio (DNS SERVER) que se encuentran en internet. Guardando los dominios consultados, lo cual permite que se resuelvan en menor tiempo y

aumentar la velocidad de respuesta a los clientes de la red que realizan las búsquedas. (Stallings, 2004)

En la Figura 105 se presenta las características del Servidor DNS CACHE que se encuentra en funcionamiento en la red de la Universidad Técnica del Norte

Figura 105

Características lógicas y físicas del servidor DNS CACHE



Fuente: Departamento de Desarrollo de Tecnológico e Informático

- **Servidor NTP**

Un servidor NTP es un servidor con la capacidad de suministrar la hora de forma exacta a otros equipos a través del enrutamiento de paquetes en redes con latencia variable, utiliza para ello el protocolo NTP (Network Time Protocolo) a través del protocolo de capa transporte UDP con el puerto 123. (Stallings, 2004)

En la se Figura 106 presenta las características del Servidor NTP que se encuentra en funcionamiento en la red de la Universidad Técnica del Norte.

Figura 106

Características lógicas y físicas del servidor NTP

```
**************SERVIDOR NTP************************

       #####
      #######          ----------------------
      ##O#O##          OS: AlmaLinux 8.7 (Stone Smilodon) x86_64
      #######          Host: VMware7,1 None
    ###########        Kernel: 4.18.0-425.13.1.el8_7.x86_64
   #############       Uptime: 12 days, 7 hours, 54 mins
  ###############      Packages: 545 (rpm)
  ################     Shell: bash 4.4.20
 ##################    Resolution: 1024x768
####################   Terminal: /dev/pts/1
####################   CPU: Intel Xeon Silver 4214R (2) @ 2.399GHz
 ##################    GPU: 00:0f.0 VMware SVGA II Adapter
                       Memory: 289MiB / 1784MiB
```

Fuente: Departamento de Desarrollo de Tecnológico e Informático

- **Servidor Radius**

Es un servidor cliente servidor el cual proporciona una autenticación para clientes donde se tiene un nombre de usuario/contraseña o certificado digital para autenticarnos en la red. (BRIHUEGA, 2015)

En la Figura 107 se presenta las características del Servidor Radius que se encuentra en funcionamiento en la red de la Universidad Técnica del Norte.

Figura 107

Características lógicas y físicas del servidor NTP

```
**************SERVIDOR RADIUS**************

                ..                    srv_eduroam.utn.edu.ec
              .PLTJ.                  --------------------------
             <><><><>                 OS: CentOS Linux 7 (Core) x86_64
    KKSSV' 4KKK LJ KKKL.'VSSKK        Host: ProLiant ML110 G5 NA
    KKV' 4KKKKK LJ KKKKAL 'VKK        Kernel: 3.10.0-1160.83.1.el7.x86_64
    V' ' 'VKKKK LJ KKKKV' ' 'V        Uptime: 27 days, 3 hours, 4 mins
    .4MA.' 'VKK LJ KKV' '.4Mb.        Packages: 414 (rpm)
  . KKKKKA.' 'V LJ V' '.4KKKKK .      Shell: bash 4.2.46
 .4D KKKKKKKA.'' LJ ''.4KKKKKKK FA.   CPU: Intel Pentium Dual E2160 (2) @ 1.800GHz
<QDD ++++++++++++  ++++++++++++ GFD>   Memory: 361MiB / 989MiB
 'VD KKKKKKKK'.. LJ ..'KKKKKKKK FV
   ' VKKKKK'. .4 LJ K. .'KKKKKV '
      'VK'. .4KK LJ KKA. .'KV'
    A. . .4KKKK LJ KKKKA. . .4
    KKA. 'KKKKK LJ KKKKK' .4KK
    KKSSA. VKKK LJ KKKV .4SSKK
             <><><><>
              'MKKM'
                ''
```

Fuente: Departamento de Desarrollo de Tecnológico e Informático

- **Servidor Telefonía**

Servidor de telefonía que provee los servicios de llamada a través de la red de datos, permitiendo emitir y recibir, llamadas contestador automático, registro de llamadas en la nube entre otros servicios.

En la

Figura ***108*** se presenta las características del Servidor Telefonía que se encuentra en funcionamiento en la red de la Universidad Técnica del Norte.

Figura 108

Características lógicas y físicas del servidor de Telefonía

```
**************SERVIDOR TELEFONIA***************

        #####           srv-issabel
       #######          ----------------
       ##O#O##          OS: Issabel 4 x86_64
       #######          Host: VMware Virtual Platform None
     ###########        Kernel: 3.10.0-1062.el7.x86_64
    #############       Uptime: 3 days, 21 hours, 48 mins
   ###############      Packages: 867 (rpm)
   ################     Shell: bash 4.2.46
  ##################    CPU: Intel Xeon Silver 4214R (2) @ 2.399GHz
####################    GPU: 00:0f.0 VMware SVGA II Adapter
####################    Memory: 485MiB / 16046MiB
  ##################
```

Fuente: Departamento de Desarrollo de Tecnológico e Informático

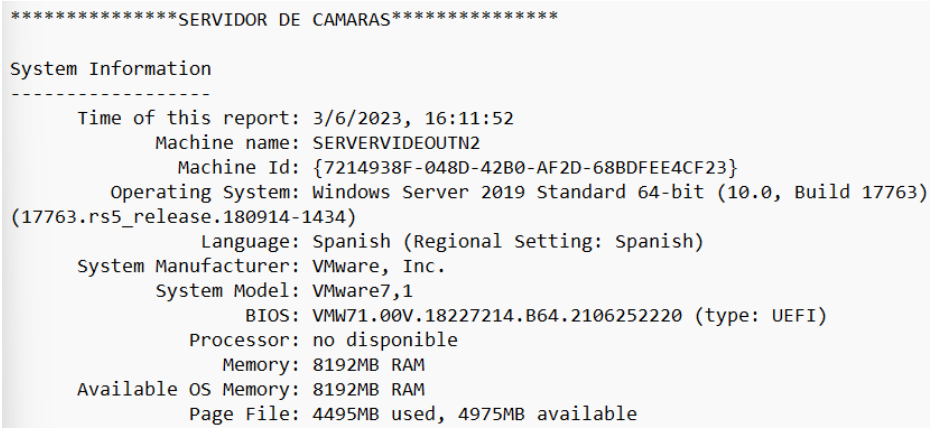
- **Servidor de Cámaras**

El servidor de cámaras permite la captura de imagen y audio por medio de cámaras y micrófonos que comprimen la información y la envía al servidor de videovigilancia por la red, permitiendo descomprimir, visualizarlos y automatizar.

En la Figura 109 se presenta las características del Servidor Telefonía que se encuentra en funcionamiento en la red de la Universidad Técnica del Norte.

Figura 109

Características lógicas y físicas del Servidor de Cámaras



Fuente: Departamento de Desarrollo de Tecnológico e Informático

3.6. Requerimientos

A continuación, en la Tabla 103 se presentan los detalles de los requerimientos que se reflejaran en el establecimiento de políticas.

Tabla 103

Requerimientos de las Políticas

Tabla de Requerimientos					
#	**Requerimiento**	**Prioridad**			**Relación**
		Alta	**Media**	**Baja**	
Requerimientos Operacionales del sistema de Gestión					
Req1	Disponibilidad de información actualizada sobre la red de la Universidad Técnica del Norte.	X			
Req2	El sistema de gestión de red debe permanecer operativo 24/7.	**X**			
Req3	El sistema de gestión debe permitir la adquisición y visualización de datos en	**X**			

	tiempo real sobre los equipos cisco que se encuentran en la red.				
Req4	Base de datos disponible y actualizada constantemente con la información de la red.	**X**			
Req5	El sistema debe determinar de la gravedad del fallo ocurrido para resolver en los tiempos establecidos.	**X**			
Req6	Asignación mediante identificativos de colores y numéricos para determinar el nivel de prioridad del fallo.	**X**			
Req7	Notificaciones de fallos mediante herramientas de mensajería.	**X**			
Req8	Soporte para modelos de gestión de redes	X			
Req9	Back ups con disponibilidad full-time para los administradores de red.	X			
Req10	Destinar ubicación y recurrencia para la generación de reportes mediante el software de gestión.	X			
Req11	Los niveles de usuario solo podrán ser editados por el administrador de la red, a la hora de dar acceso a usuarios ajenos.	X			
Req12	Registro de log para todos los usuarios que poseen acceso al sistema de gestión de red	**X**			
Req13	Registro de configuraciones realizadas en el sistema de gestión de red.	**X**			
Req16	Monitoreo y visualización de parámetros de rendimiento y estadísticos de la red inalámbrica y cableada.	**X**			
Requerimientos para la red Inalámbrica					
Req15	Configuraciones adecuadas para cada equipo de red inalámbrico.	**X**			
Req16	Soporte para modelo de gestión de red.				

Req17	Disponibilidad de acceso en todo el campus universitario.	**X**			
Req18	Establecimiento de umbrales óptimos para precautelar el buen funcionamiento de la red inalámbrica.	**X**			
Req19	Generación de reportes donde se detalle los datos relacionados con los recursos de la red.	**X**			
Req20	Base de datos actualizada donde se detalle la ubicación física de los APs.	**X**			
Req21	El acceso a la red se realiza mediante un acceso único de autenticación.	**X**			
Req22	Notificación continua al gestor del estado de los recursos de los equipos.	**X**			
Req23	Distribución adecuada de los recursos de los equipos de red.				
Requerimientos para la red Cableada					
Req24	Establecimiento de conexiones seguras a nivel físico.	**X**			
Req25	Establecimiento de umbrales óptimos para precautelar el buen funcionamiento de la red cableada	**X**			
Req26	Reportes o informes generados que determinen el estado de los dispositivos gestionados.	**X**			
Req27	Disponibilidad de más de un software de gestión para el monitoreo de la red cableada	**X**			
Req28	Manuales sobre configuración y uso de equipos. Llevar inventarios.	**X**			

Req29	Monitoreo de equipos para su respectivo establecimiento de conexión.	**X**			
Req30	Soporte para modelo de gestión de red.	**X**			
Req31	Visualización de scripts sobre las configuraciones realizadas en los equipos de conmutación.	**X**			

Fuente: Elaboración Autor

3.7. Establecimiento de Políticas de Gestión y Administración para la red de la Universidad Técnica del Norte

Se realiza un análisis de la situación actual en la que se encuentra la red inalámbrica y cableada de la UTN, donde a partir de esta información obtenida se determina las políticas de gestión, las cuales cubran todas las áreas funcionales del modelo de gestión FCAPS de la ISO.

Se implementa el modelo de gestión FCAPS de la ISO para determinar en qué áreas se va a trabajar y así poder determinar las políticas.

3.7.1.1. Desarrollo de Políticas

Después del levantamiento de información sobre el estado actual de la red Inalámbrica y Cableada de la Universidad Técnica del Norte se procede a determinar las políticas de gestión y administración.

UNIVERSIDAD TÉCNICA DEL NORTE		
POLÍTICAS DE ADMINITRACIÓN Y GESTIÓN PARA LA RED IMABLAMBRICA Y CABLEADA DE LA UTN		
	Elaborado por:	Axel Almeida
	Revisado por:	Ing. Vinicio Guerra, Administrador de red
	Aprobado por:	Ing. Jorge Caraguay, Director de DDTI
	Versión:	1.0
	Fecha:	22/03/2023

I. PROPÓSITO

El presente documento tiene como principal objetivo presentar políticas de administración y gestión sobre la red de la Universidad Técnica del Norte, mismas que deberán ser cumplidas por el personal encargado de la administración de la red, todo ello con la finalidad de mantener en óptimas condiciones los recursos de la red y un eficiente servicio de conectividad a través de la red inalámbrica y cableada de la Universidad Técnica del Norte.

II. CONCEPTOS PREVIOS

- **Políticas de Administración y Gestión de red**

Las políticas de administración y gestión de red son un conjunto de directrices y procedimientos que establecen las reglas y prácticas para la gestión de una red. Estas políticas son importantes para garantizar la eficiencia, la seguridad y la disponibilidad de los recursos de la red.

- **Gestión de red**

La gestión de red consiste en planificar, organizar, supervisar y controlar los recursos de la red, esto con el objetivo de garantizar un nivel de servicio optimo a los usuarios.

III. NIVELES ORGANIZACIONALES

a) Director. – Autoridad que posee el nivel superior dentro del Departamento de Desarrollo Tecnología e Informático de la UTN.

b) Analista de red. – Persona encarga de administrar los recursos de la red de la UTN. Bajo su responsabilidad y administración le compete la aceptación de las políticas de administración y gestión.

c) Asistente de red. – Persona encargada de brindar soporte técnico y ayuda al analista de la red al momento de ocurra alguna eventualidad en la red.

IV. GENERALIDADES

a) Las políticas establecidas en este documento deberán ser cumplidas por el administrador de la red, en cuanto al uso del sistema de gestión de red.

b) Las políticas establecidas en este documento serán actualizadas en caso de ser necesario, siempre y cuando se acople a las áreas funcionales del modelo de gestión ISO/OSI.

V. VIGENCIA

Las políticas presentadas en el documento entraran en vigor desde el instante que se dé la aprobación por parte del Administrador de la red de la UTN.

Las reglas estarán prestas y sujetas a modificaciones que el Administrador de red considere acorde a su necesidad.

VI. REFERENCIA

Ya que la Universidad Técnica del Norte no posee aun un formato para establecer políticas de administración y gestión de red, se toma como referencia la tesis realizada en el GAD de Ibarra por Viviana Ayala, en el año 2015 y también a la tesis realizada en la Universidad Técnica del Norte por Jessica Báez, en el año 2017.

VII. ESTRUCTURA DE LAS POLITICAS

1. Política de Administración y Gestión de la red.

1.1. Objetivo de las políticas de administración y gestión de red.

1.2. Compromiso de las Autoridades

2. Gestión de Fallos

2.1. Manejo y documentación de Fallos

3. Gestión de Configuraciones

3.1**.** Ingreso de equipos

3.2. Ingreso de equipos

3.3. Configuración de equipos

4. Gestión de Prestaciones

4.1. Parámetros de Monitoreo

5. Gestión de Contabilidad

5.1. Reportes de rendimiento

5.2. Monitoreo de trafico de red

6. Gestión de Seguridad

6.1. Acceso al equipo de gestión.

VIII. GLOSARIO DE TÉRMINOS

SNMP: Simple Network Management Protocol. Este protocolo hace referencia a la capa aplicación, el cual pertenece a la familia de protocolo TCP/IP, dicho protocolo permite el intercambio de información de administración entre los dispositivos de red.

DDTI: Departamento de Desarrollo de Tecnológico e Informático de las TIC´s en la UTN.

Syslog: Es el protocolo de registro del sistema (Syslog), es una forma en que los dispositivos de red pueden usar un formato de mensaje estándar para comunicarse con un servidor de registro.

API: Interfaz de programación de aplicaciones

KPI: Indicador Clave de Desempeño. Son las métricas del rendimiento que funcionan en el DNA Center para cierta información específica.

DNA: Digital Network Architecture, e**s** un software central de gestión y automatización, una aplicación que se utiliza como controlador para Cisco DNA

CPU: Es la Central Processing Unit o Unidad de Proceso Central, es decir, el cerebro de cualquier dispositivo desde la que se controlan y originan todos los comandos directores, que generan las funciones en la CPU.

Agente: Es el software que se encuentra en el dispositivo gestionado, este tiene acceso a la información de gestión e interactúa con el mánager para atender solicitudes y generar eventos.

Gestor: Es el software que se encuentra en la central de gestión y es el responsable de realizar la supervisión, control constante de los dispositivos gestionados.

Fallo: Son sucesos que interfieren en el correcto funcionamiento de la red, y por consiguiente disminuyen significativamente su rendimiento

Reporte: Es un documento en el que se recogen todas las métricas que resumen el funcionamiento de tus perfiles en el periodo de tiempo que quieras

WLC: Wireless LAN Controller que en español significa controladora de red inalámbrica

phpIPAM: Aplicación web de código abierto para la gestión de direcciones IP (IPAM). Su objetivo es proporcionar una gestión de direcciones IP ligera, moderna y útil.

Dispositivo de red: Es cualquier hardware que conecte diferentes recursos de red.

POLÍTICAS DE GESTIÓN Y ADMINISTRACIÓN DE RED

	UNIVERSIDAD TÉCNICA DEL NORTE	
	Dominio	1. Política de Administración y Gestión de la red.
	Control	1.1. Objetivo de las políticas de administración y gestión de red.
	Encargado	Administrador de la red

Art. 1. Difundir la información correspondiente sobre el funcionamiento del sistema de gestión, así como sus respectivos lineamientos que deben seguir y utilizar los responsables de la administración de la red de la Universidad Técnica del Norte, para así

evitar cualquier eventualidad o fallo, lo cual permitirá mantener el buen funcionamiento de la red y un correcto uso de los recursos de la misma para la solución de problemas.

	UNIVERSIDAD TÉCNICA DEL NORTE	
	Dominio	1. Política de Administración y Gestión de la red.
	Control	1.2. Compromiso de las Autoridades
	Encargado	Administrador de la red
Art. 2. El DDTI, como corresponsables de la elaboración de las políticas de Administración y Gestión para la red de la Universidad Técnica del Norte, asume el compromiso de dar revisión constante y socialización de los lineamientos descritos en este documento.		

POLÍTICAS DE GESTIÓN DE FALLOS

	UNIVERSIDAD TÉCNICA DEL NORTE	
	Dominio	2. Política de Administración y Gestión de la red.
	Control	2.1. Manejo y documentación de Fallos
	Encargado	Administrador de la red
Art. 3. Al momento que el Software de gestión emita notificaciones de los fallos en el entorno de la red, a través de mensajes emitidos por la aplicación designada, deberán llegar directamente al administrador de la red, el cual deberá aislar y diagnosticar el problema detectado para luego proceder a resolverlo.		

Art. 4. Los problemas que se presenten dentro de la red deberán ser solucionados por el administrador de la red o el personal encargado, en el menor tiempo posible.

Art. 5. El administrador deberá realizar monitoreos constantes a los niveles de umbrales que se presentan en el Software de Gestión, ya que brinda información de la gravedad a través de la puntuación de salud. La salud se mide en una escala de 1 a 10, donde 10 es la mejor puntuación. Una puntuación de 0 indica que no se han podido obtener datos.

De acuerdo con el tipo de fallo notificado y al diagnóstico realizado, se implanta un nivel de prioridades, según el fallo detectado.

Tipo de Fallo	Prioridad	Tiempo de solución
Dispositivo fuera de servicio	Prioridad 1/ Cuestiones críticas	Verificación del dispositivo y su servicio de 1 minuto. Si el dispositivo no puede ser habilitado con su respectivo servicio, lo más pronto posible, se dará el tiempo aproximadamente de 1 hora para poder solucionarlo.

Alerta en dispositivos parcialmente caídos	Prioridad 2/ Advertencias	Verificación del dispositivo y su servicio de 1 minuto. Si el dispositivo no puede ser habilitado con su respectivo servicio, lo más pronto posible, se dará el tiempo aproximadamente de 2 a 4 horas para poder solucionarlo.
Dispositivo Funcionando	Prioridad 3/ Sin errores ni advertencias – Notificación de Información	Monitoreo constante de dispositivos y sus servicios para visualizar su correcto funcionamiento.
Dispositivo sin respuesta	Prioridad 4/ No hay datos disponibles	Verificación del dispositivo y su servicio de 1 minuto. Si el dispositivo no puede ser habilitado con su respectivo servicio, lo más pronto posible, se dará el tiempo aproximadamente de 48 horas para poder solucionarlo.

Art. 6. En caso de que exista un nuevo fallo dentro de la red y no se pueda llegar a brindar una solución pronta y eficiente, se requerirá el uso de nuevos y diferentes mecanismos por parte del administrador ya que es importante documentar la falla junto con

su solución correspondiente para que en el futuro se puedan resolver eficazmente las fallas en la red.
Para la realización de los artículos establecidos en la política número dos, se presentan los manuales de gestión de fallos, que se encuentran en el ítem 5.2.2 para la red cableada y 5.3.2 para la red inalámbrica. Se presenta el procedimiento a seguir para la detección y aislamiento de fallos.

POLÍTICAS DE GESTIÓN DE CONFIGURACIONES

	UNIVERSIDAD TÉCNICA DEL NORTE	
	Dominio	3. Política de Administración y Gestión de la red.
	Control	3.1.Ingreso de equipos
	Encargado	Administrador de la red
Art. 7. Previo al ingreso de un equipo a la red, el administrador deberá monitorear y analizar el estado de la red en el que se encuentra, posterior a ello deberá ingresar a la base de datos la información básica del dispositivo, dado que se pueda localizar de manera óptima.		

	UNIVERSIDAD TÉCNICA DEL NORTE	
	Dominio	3. Política de Administración y Gestión de la red.
	Control	3.2.Ingreso de equipos
	Encargado	Administrador de la red
Art. 8. El ingreso de equipos en la base de datos de la Universidad Técnica del Norte será de acuerdo con la nomenclatura determinada en dicha Institución.		

	UNIVERSIDAD TÉCNICA DEL NORTE	
	Dominio	3. Política de Administración y Gestión de la red.
	Control	3.3. Configuración de Equipos
	Encargado	Administrador de la red

Art. 9. Los equipos que se integren a la red de la Universidad Técnica del Norte deberán contar con una configuración básica, la cual que permita administrar dicho dispositivo acorde a las necesidades de la red.

Art. 10. Una vez que el equipo o los equipos formen parte de la red, deberá ser configurado a través de la sintaxis, para que el equipo soporte el protocolo SNMP o alguna de sus versiones y así permitir una gestión remota total sobre el dispositivo por parte del administrador de la red.

Art. 11. El administrador de red deberá llevar documentación o notas de las configuraciones que se realicen en los dispositivos y sus servicios que prestan, esto con la finalidad de tener disponibilidad de la información sobre las configuraciones que existen en los equipos de la red.

Art. 12. Al momento de realizar cambios a nivel de infraestructura se realizará la respectiva actualización de la información en la base de datos.

Art. 13. Al momento de realizar cambios en los equipos, dispositivos de red o en la configuración de ellos, se realizará una actualización en la base de datos, donde se almacena la información, con la finalidad de mantener un correcto funcionamiento de la red y sus recursos.

Art. 14. El administrador de la red deberá realizar un respaldo (Backup) cada 3 meses o cada que se realice modificaciones dentro de servidores y sus servicios, funcionamiento de equipos y actualización del mapa topológico de la red.

Para la realización de los artículos establecidos en la política número tres, se presentan los manuales de gestión de configuraciones en el ítem 5.2.1. para la red cableada y 5.3.1. para la red inalámbrica. Dentro de este documento se incluyen los formatos necesarios para el registro de equipos, así como las configuraciones recomendadas para su correcto funcionamiento

POLÍTICAS DE GESTIÓN DE PRESTACIÓN

	UNIVERSIDAD TÉCNICA DEL NORTE	
	Dominio	4. Política de Administración y Gestión de la red.
	Control	4.1. Parámetros de Monitoreo
	Encargado	Administrador de la red
Art. 15. Con la ayuda software de gestión el administrador de la red deberá conocer los parámetros de monitoreo, lo cual permitirá determinar el estado funcional actual de la red y sus dispositivos. **Art. 16.** El software de gestión permite dar un total seguimiento a los procesos de funcionamiento de los recursos activos de la red, ya que dentro de sus funcionalidades permite obtener información de estado, de manera diaria, por horas y mensual		
Para la realización de los artículos establecidos en la política número cuatro, se presentan los manuales de gestión de prestaciones, se presentan los parámetros de monitoreo y chequeo de los recursos de los dispositivos, los cuales viene dados en el manual de gestión de prestaciones ubicado en el ítem 5.2.4 para la red cableada y 5.3.4 para la red inalámbrica.		

POLÍTICAS DE GESTIÓN DE CONTABILIDAD

	UNIVERSIDAD TÉCNICA DEL NORTE	
	Dominio	5. Política de Administración y Gestión de la red.
	Control	5.1. Reportes.
	Encargado	Administrador de la red

Art. 17. El administrador de la red deberá generar y descargar los reportes que serán guardados de manera virtual dentro de una carpeta creada por el administrador y se lo hará al finalizar cada mes.

Art. 18. El personal administrativo del DDTI para el caso de la red se analizará la posibilidad de administrar de manera más optima las redes que se encuentran trabajando en la Universidad Técnica del Norte

	UNIVERSIDAD TÉCNICA DEL NORTE	
	Dominio	5. Política de Administración y Gestión de la red.
	Control	5.2. Monitoreo de trafico de red
	Encargado	Administrador de la red

Art. 19. Mediante el software de gestión el administrador de la red podrá visualizar reportes, gráficos estadísticos de la salud de la red, listado de los dispositivos de red, con la finalidad de mostrar el estado actual de la red y el correcto funcionamiento de esta.

Para la realización de los artículos establecidos en la política número cinco, se presentan los manuales de gestión de contabilidad para la obtención de reportes y el respectivo

monitoreo de trafico de red, en el ítem 5.2.3 para la red cableada y 5.3.3 para la red inalámbrica.

POLÍTICAS DE GESTIÓN DE SEGURIDAD

	UNIVERSIDAD TÉCNICA DEL NORTE	
	Dominio	6. Política de Administración y Gestión de la red.
	Control	6.1. Acceso al equipo de gestión.
	Encargado	Administrador de la red
Art. 20. El acceso a los dispositivos que brindan un monitoreo constante para la red de la Universidad Técnica del Norte se dará exclusivamente a través del acceso único, Autorización y confidencialidad al personal a cargo de la administración de dicha red. **Art. 21.** Al momento que un usuario desee conectarse a la red de la Universidad Técnica del Norte deberá ser autenticado su acceso, la cual permite conectar tu dispositivo a la red. **Art. 22.** El software de gestión posee 3 tipo de niveles de usuario, los cuales son: administrador, write y monitor, estos niveles de usuarios tendrán acceso remoto a cada nivel dependiendo del proceso o la tarea que se le asigne a cada usuario por parte del personal administrativo de la red.		
Para cumplir con los requisitos de la política número cinco, se ponen a disposición los manuales de gestión de seguridad, los cuales detallan los procedimientos necesarios. Además, se proporciona acceso al equipo de gestión de seguridad a través del manual correspondiente, que se encuentra ubicado en el ítem 5.2.5 para la red cableada y 5.3.5 para la red inalámbrica.		

4. IMPLEMENTACIÓN

4.1. Implementación del modelo de Gestión FCAPS para la Red de la Universidad Técnica del Norte.

El presente capitulo se describe el desarrollo a detalle de la implementación de las cinco áreas funcionales del modelo FCAPS de la ISO, tanto para la red inalámbrica como cableada de la Universidad Técnica del Norte, para llevar a cabo el monitoreo constante de la red, se utiliza el software de gestión Cisco DNA Center junto con sus herramientas complementarias. Tomando en cuenta que en ciertos ámbitos del modelo funcional FCAPS de la ISO, la implementación será la misma para la red inalámbrica y cableada, se la colocará dentro de la implementación en la red cableada.

4.1.1. Implementación del Modelo de Gestión FCAPS en la red Cableada.

El análisis de la situación actual de la red cableada realizado en el Capítulo III, logra determinar las áreas críticas, permitiendo al administrador tener un control de la red, todo esto a través de procesos como identificación de los dispositivos conectado a la LAN, recolección de datos de los dispositivos para conocer su funcionamiento dentro de la red.

4.1.1.1. Implementación de políticas en la gestión de Configuración

4.1.1.1.1.Ingreso de equipos a la base de datos

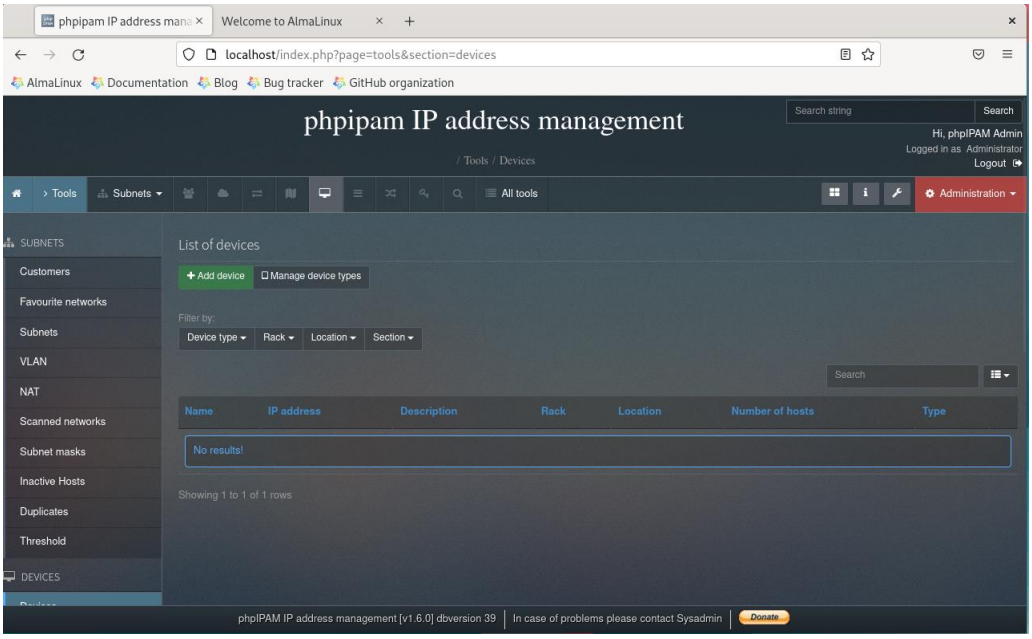
Para la gestión de configuraciones se realiza el registro de las configuraciones e inventario de los equipos que ingresaran al software de gestión, para ello, mediante un dialogo con el Analista y el Asistente de la red de la UTN, se propone la idea de migrar la base de datos actual de los equipos, hacia el programa phpIPAM ya que este es una aplicación de gestión de direcciones IP web de código abierto, la cual posee algunas características como: Gestión de direcciones IP (IPv4/IPv6), Calculadora para IPv4 e IPv6,

búsqueda de base de datos IP, notificaciones por correo electrónico y la administración de dispositivos/tipos de dispositivos, dichas características que brinda de la aplicación ayudaran a cumplir con los ***Artículos* 7, 8, 11, 12 y 13** establecidos dentro de las políticas en el ámbito de gestión de configuraciones.

A continuación, en la Figura 110 se presenta el interfaz del programa phpIPAM ya instalado, en el ANEXO K se detalla el proceso de instalación del distro de Linux elegido y un manual de manejo del programa phpIPAM.

Figura 110

Interfaz del programa phpIPAM.



Fuente: Elaboración Autor

Nota: Mediante el dialogo establecido con personal del DDTI, se acordó la incorporación de los siguientes dispositivos para la red cableada: switches, APs, servidores, firewall, y para Wireless estará la Wireless LAN Controller. Además, se deberán agregar las direcciones IPv4 públicas y privadas correspondientes en la base de datos de phpipam con el objetivo de mantenerla actualizada.

4.1.1.1.2. Registro de equipos y sus configuraciones en el DNA Center

Para la implantación de la gestión de configuraciones se toma en cuenta a los ***Art.9 y Art.10,*** ya que para la implementación de este ámbito hace énfasis en el ***Req.29*** planteado, por lo cual todo dispositivo a ingresar al software de gestión DNA Center deberá poseer una configuración básica y soportar un modelo de gestión de red, se trabajará con el principal software de gestión, que es el Cisco DNA Center y en caso de ser necesario se utilizara cierta información del software de gestión Zabbix.

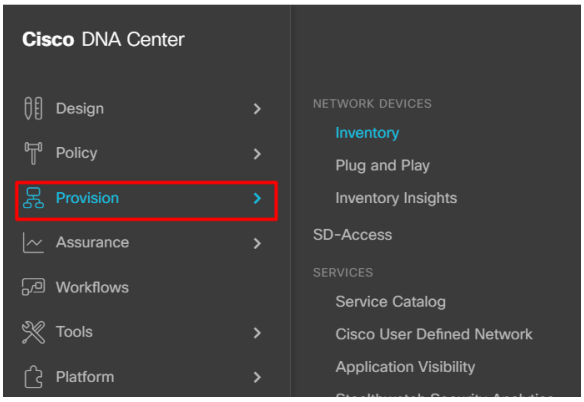
- **Agregar un equipo a Cisco DNA Center**

Al agregar dispositivos a un sitio, Cisco DNA Center se configura como el servidor de Syslog y SNMP Trap. Como primer paso vamos a la pestaña **Provision,** luego en la sección de **NETWROK DEVICES** seleccionamos la opción **Inventory,** tal y como se ilustran en la Figura 111 y Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Figura *112*.

Figura 111

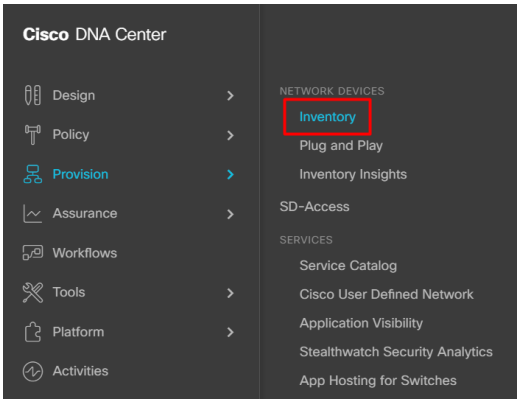
*Selección de la pestaña **Provision***



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Figura 112

Selección de la opción ***Inventory***

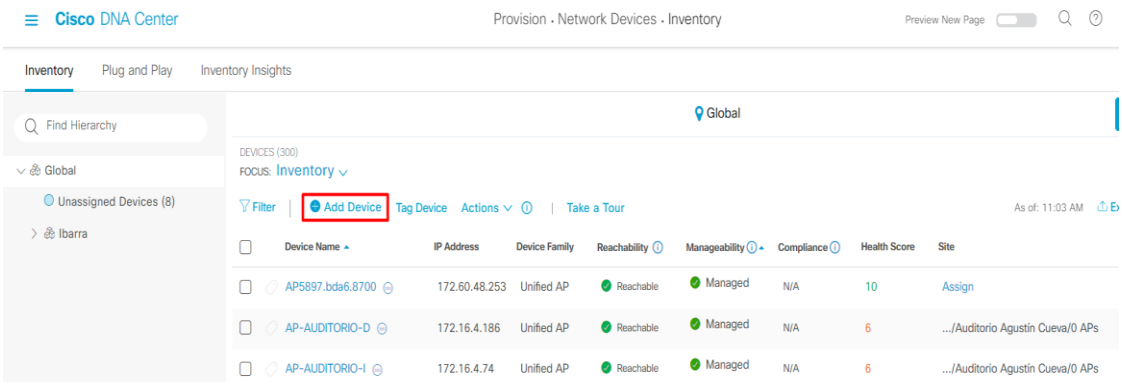


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Aparecerá el icono de **Add Device** que se muestra en la Figura 113, enmarcado en el cuadro rojo

Figura 113

Agregar dispositivo

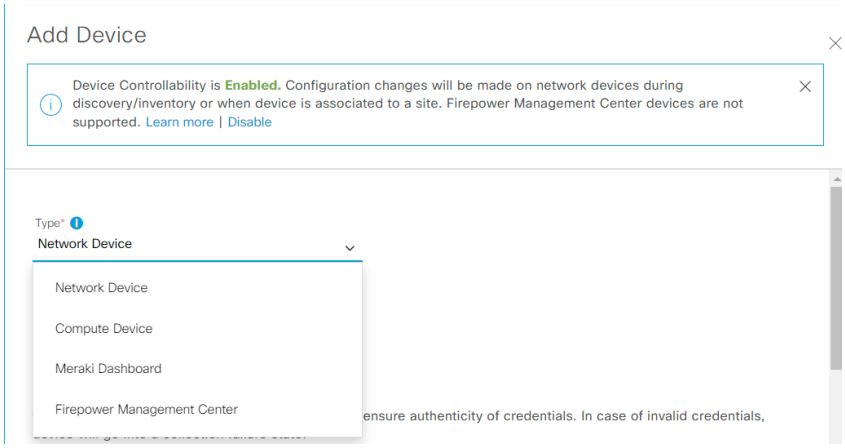


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Como siguiente paso se procede a selección el tipo de equipo que se vaya a agregar, tal y como se indica en la Figura 114, este ya sea dispositivo de red, dispositivo de cómputo, tablero Meraki, Centro de gestión de potencia de fuego.

Figura 114

Agregar un dispositivo de red.

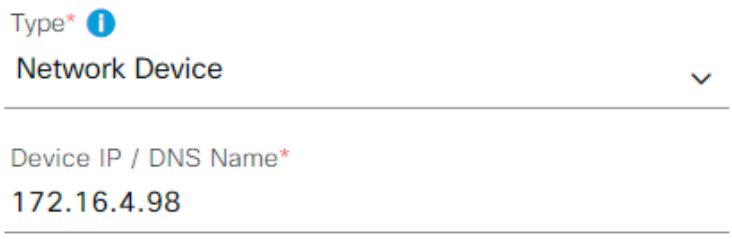


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

En este caso será un dispositivo de red que se agregará, con su respectiva dirección IP tal y como se muestra en la Figura 115.

Figura 115

Asignación de IP al dispositivo de red.

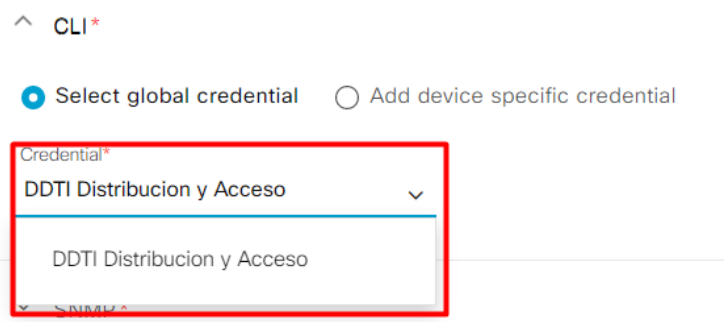


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Expanda el área de las credenciales y configure las credenciales que desee utilizar, para este caso se selecciona las credenciales de DDTI de distribución y acceso, tal y como se muestra en la Figura 116.

Figura 116

Selección de credenciales al dispositivo de red.



Fuente: Adaptado de Cisco DNA Center

Después de haber seleccionado las credenciales con las cuales se va a trabajar, se procede a configurar los siguientes protocolos, tal y como se muestra en la Figura 117.

Figura 117

Configuración de protocolos

Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

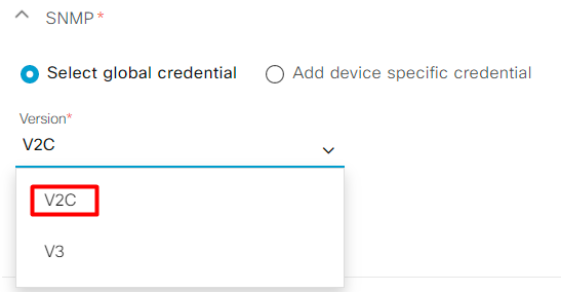
Para la configuración del protocolo SNMP, como primer paso se selecciona la versión de SNMP, para este caso se selecciona la V2C, mientras que para las credenciales se escogerá el modo write o read, esta selección se la hará de acuerdo con el administrador de la red y el rol que se le vaya a proporcionar al dispositivo, estos dos pasos se detallan en la Figura 118 y

Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Figura *119*.

Figura 118

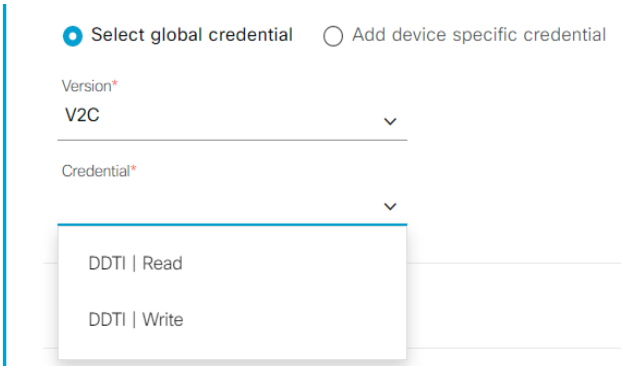
Selección de la versión del protocolo SNMP



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Figura 119

Selección de credenciales globales

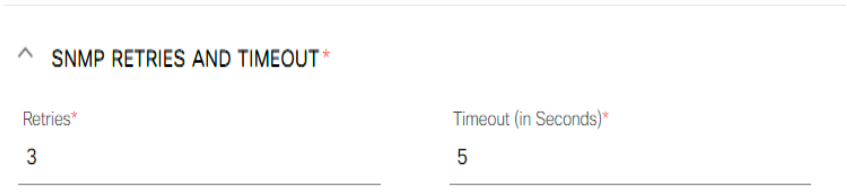


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

También se configura los reintentos y tiempos de espera para SNMP, en la Figura 120 se indica cuantos intentos de comunicación se van a realizar en lapsos de tiempos determinados (tiempo en segundos).

Figura 120

Reintentos y tiempos de espera

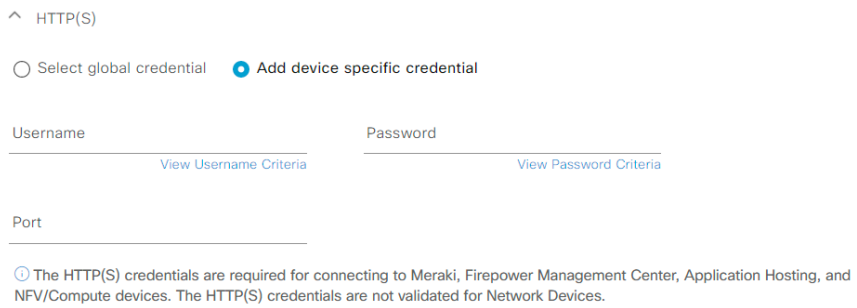


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

El siguiente paso es opcional y se lo hace a los campos de HTTP(S) como se muestra en la Figura 121.

Figura 121

Credenciales HTTP(S)

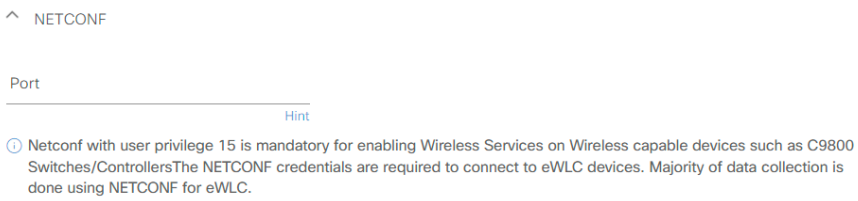


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

El siguiente paso también es opcional ya que, si existen dispositivos de red con NETCONF activado, se deberá introducir un numero de puerto en el campo puerto, tal y como se visualiza en la Figura 122.

Figura 122

Dispositivos de red con NETCONF

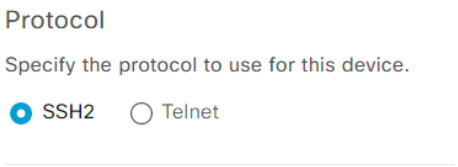


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Y por último se va a seleccionar el protocolo de comunicación para el dispositivo, de tal manera como se visualiza en la Figura 123.

Figura 123

Protocolos válidos son SSH (por defecto) y Telnet.



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Análisis

En el software de gestión Cisco DNA Center cuando se agrega un nuevo equipo a la red cableada es necesario la configuración de los parámetros de configuración del equipo como se especifica en el ***Art.9 y Art.10*** de las políticas de administración y gestión de la red, y en cumplimento del requerimiento ***Req.30***, además se realiza la activación de servicios de telemetría para obtener las bases de información gestionable de cada equipo que conforma la red cableada.

4.1.1.2. Implementación de políticas de gestión de Fallos

La implementación de la gestión de fallos tiene como objetivo mantener dinámicamente el nivel de servicio de la red y solucionarlo en el menor tiempo posible, esto a través de procesos como localizar, diagnosticar, evitar y corregir problemas antes de que ocurran en los elementos de red.

Los **Artículos 3, 4 y 5** descritos en las políticas responderá a la implementación presentada a continuación dentro del ámbito de la gestión de fallos ya que los fallos detectados en la red son regidos de acuerdo con las alertas que emite el software de gestión Cisco DNA Center, pero para él envió de notificaciones de alertas se utilizara el software de gestión Zabbix ya que estas alertas pueden ser mediante correos electrónicos o SMS que el

administrador recibe en un correo de notificaciones para el seguimiento de un problema en un dispositivo gestionado dentro de la red. La selección de este software se explicará en el aparte de alerta vía e-mail y SMS.

Existen dos funciones que se presentan dentro de la gestión de fallos:

- Para evitar fallos antes de que sucedan se toma en cuenta la gestión proactiva.
- Mientras que si el fallo ya ha sucedido se toma en cuenta la gestión reactiva.

4.1.1.2.1.Gestión Proactiva

La función principal de la gestión proactiva es evitar fallos antes de que sucedan. Esta gestión proactiva se la puede realizar mediante pruebas preventivas y para ello existen algunas herramientas que se pueden utilizar:

- **Ping:** este comando se lo utiliza para verificar y comprobar la conectividad punto a punto a través del protocolo ICMP, se lo puede hacer en el software de gestión Cisco DNA Center como en Zabbix
- **Traceroute:** su función es similar a la del ping, a diferencia que con este comando se obtiene la lista de direcciones IPs de los equipos que atraviesan el mensaje hasta llegar a su destino.

También se debe tomar en cuenta las pruebas de conectividad física al momento de realizar una gestión proactiva, para que así exista el correcto funcionamiento de los medios de transmisión mediante pruebas que se los realice a dichos elementos como: tarjetas de red, cables de red, cables de fuentes de poder y reguladores de voltaje.

- **Definición de Umbrales**

La definición de umbrales viene dada por la política descrita en el **Art.5** ya que a partir de los niveles de salud que emita el software de gestión permite determinar si el equipo se encuentra en un buen estado o requiere de atención, ya sea remota o física.

El sistema de gestión Cisco DNA Center brinda información de umbrales en los cuales trabajan los equipos, dichos umbrales sirven para que el administrador de red pueda visualizar y monitorear el estado de los dispositivos gestionados, los cuales deben estar funcionando de una manera óptima y dentro de los umbrales permitidos.

Por ello a través del dialogo con el administrador de la red, se realizará el primer paso, al criterio de proceder a revisar los datasheets de los equipos (en este caso Switchs), y verificar los umbrales en que trabajan, para así verificar con el software de gestión su correcto funcionamiento en la red. Entonces, a continuación, en la Tabla 104 se establecen umbrales de advertencia para que el administrador pueda brindar una solución rápida antes de que un dispositivo gestionado sobrepasa los umbrales de trabajo o llegue a un estado crítico.

Tabla 104

Umbrales de monitoreo

Dispositivos Gestionados	**Métrica**	**Umbrales de Advertencia (WARNING**	**Umbrales de Criticidad (CRITICAL)**
Switches	Carga de CPU	< 70%	>95%
	Memoria (RAM y FLASH)	<70%	>95%

Fuente: Elaboración Autor

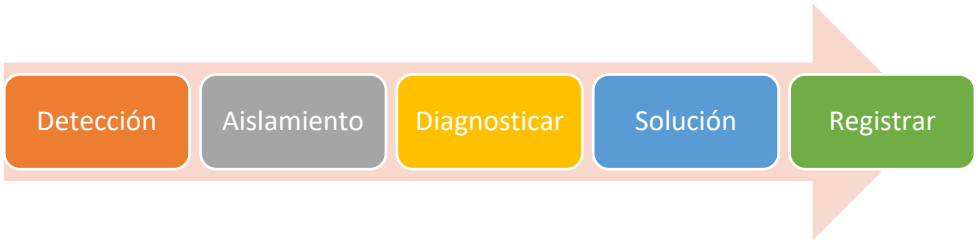
Para la definición de umbrales en switchs se consideran dos aspectos importantes, el primero son los parámetros que ya menaje el DNA que se los detalla en la Tabla 110, los cuales vienen dados en el manual de dicho software y el segundo aspecto tomado en cuenta es la monitorización de los equipos mediante sus gráficas y comandos configurados en el CLI del equipo. En el ANEXO I se detallará los comandos que el administrador de red podrá ejecutar en el CLI del dispositivo gestionado para verificar con mayor detalle y con intervalos de tiempos el uso de los umbrales.

4.1.1.2.2.Gestión reactiva

La gestión reactiva se encarga de un fallo cuando ya ha sucedido y seguidamente sigue el proceso de detectar, aislar, diagnosticar, registrar los fallos y solución. Dentro de esta gestión se realizan monitores constantes a los recursos de la red con la finalidad de detectar fallos que se produzcan y así tener una respuesta optima al problema suscitado. El proceso de documentar un fallo se observa a continuación en la secuencia de la Figura 124.

Figura 124

Secuencia del proceso para una gestión reactiva.



Fuente: Elaboración autor

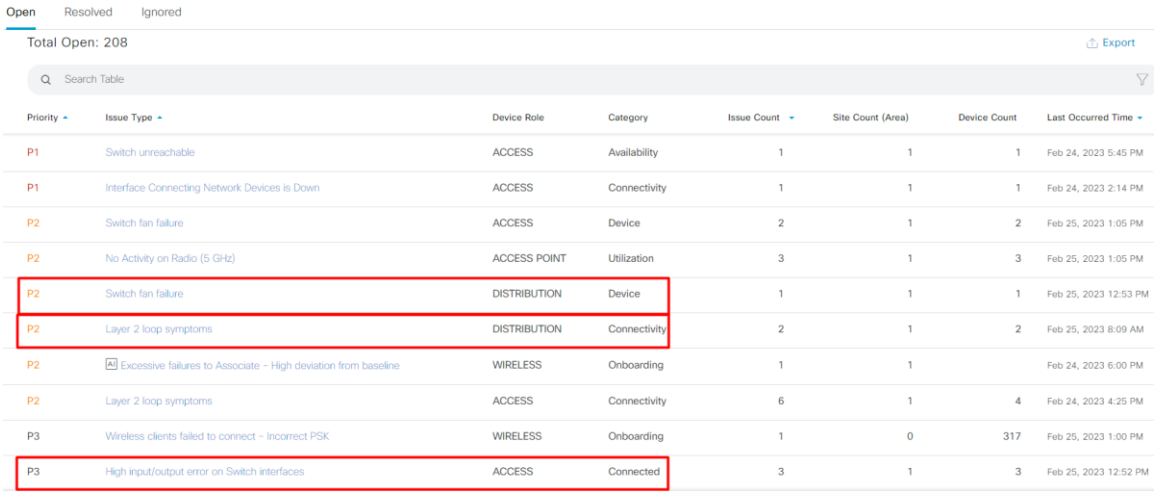
- **Detección de fallos**

El interfaz del software de gestión Cisco CNA Center presenta los principales tipos de problemas en la red, mediante un orden de prioridades con su respectivo color, el tipo de problema, la categoría (ya sea un elemento de la capa de Core, acceso, distribución o un

Access point) y la hora de la última concurrencia. En la Figura 125 se observa como el DNA permite al administrador de red detectar un fallo y tratarlo de acuerdo con su prioridad.

Figura 125

Alarmas visuales

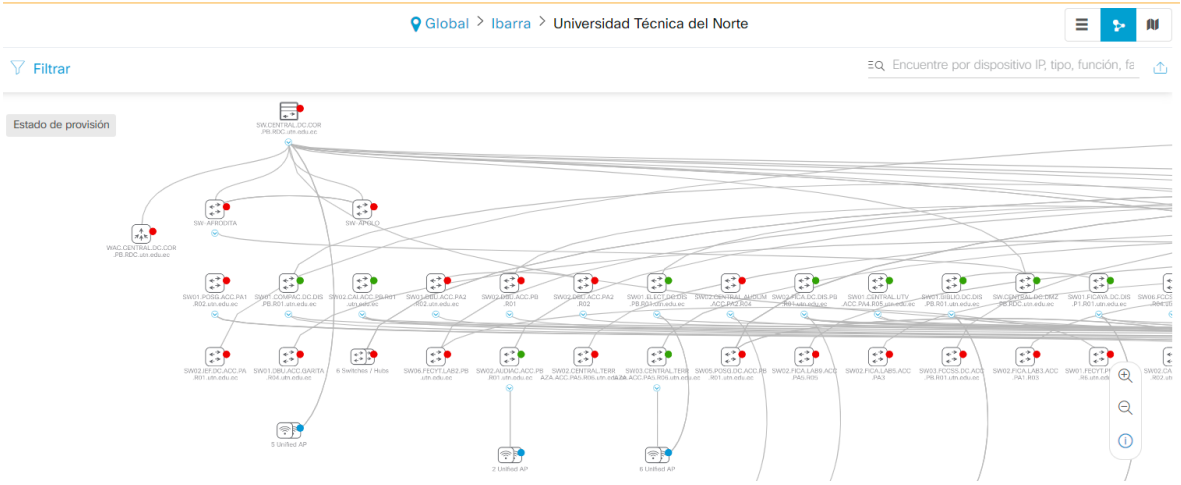


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

En la Figura 126 se muestra la detección de fallos a nivel de red en los equipos(switches), dentro del interfaz del Cisco DNA Center.

Figura 126

Detección de fallos en el mapa topológico del DNA Center.



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

- **Alerta vía Correo electrónico y SMS.**

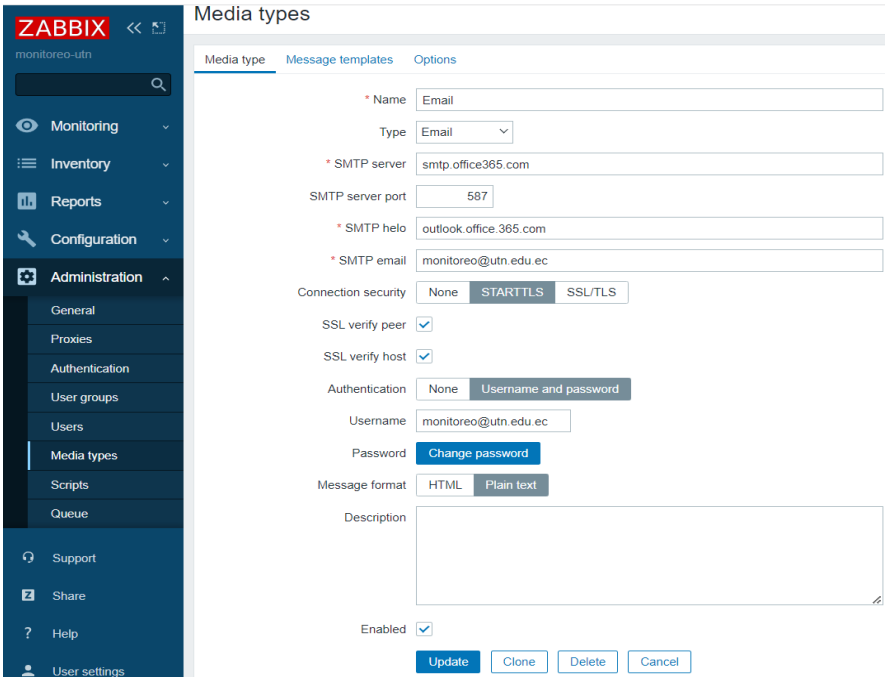
El **Art.3.** establecido en las políticas responderá a la implantación de la gestión de fallos a través de las alertas vía correo electrónico y SMS.

El Software Cisco DNA Center permite generar alertas por correo, pero debido a un problema (Sending email failed due to 451 5.7.3 STARTTLS is required to send mail), el cual tiene que ver con el cliente de correo electrónico si es compatible con StartTLS(de manera predeterminada, TLS/StartTLS está habilitado en Microsoft 365/Office 365). Entonces es un problema de licencias con Office 365 por ende no se puede realizar él envió de notificaciones por correo por medio del DNA.

Para ello se seguirá utilizando el software Zabbix para la alerta por correo y envío de mensajes de texto a la aplicación de telegram, ya que este software permite configurar alertas vía correo electrónico, y así lograr que se envíen alertas automáticamente cuando ocurre alguna eventualidad en cualquier dispositivo gestionado dentro de la red cableada. Dentro de Zabbix se encuentra ya configurada una cuenta de Gmail que es respectivamente para notificaciones que le llegan los sms y alertas al administrador, en la Figura 127 se muestra la configuración SMTP email establecida para Zabbix y en la Figura 129 se evidencia la configuraciones realizadas para el envío de las notificaciones al aplicativo de telegram, mientras que en la Figura 129 evidencia los sms en la aplicación de telegram.

Figura 127

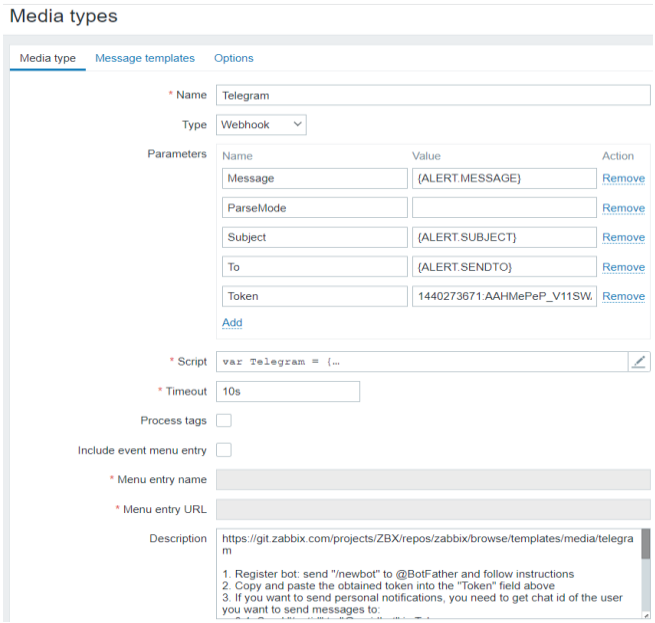
Configuración SMTP para alertas de e-mail



Fuente: Adaptado Zabbix del DDTI de la UTN

Figura 128

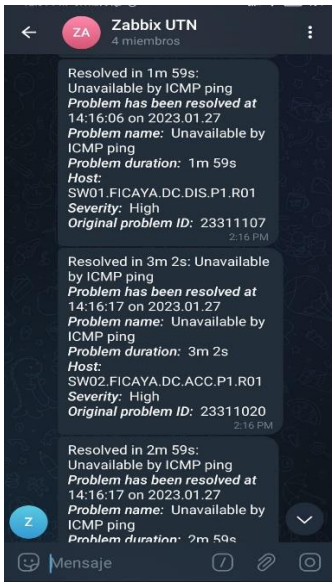
Configuración de sms de la aplicación telegram.



Fuente: Fuente: Adaptado Zabbix del DDTI de la UTN

Figura 129

Notificaciones en la aplicación telegram.



Fuente: Aplicación telegram del administrador de red.

El administrador de red recibirá las alertas hacia su correo institucional que solo está destinado a recibir las notificaciones de alertas, que se enviaran desde la cuenta zabbixutn@gmail.com. En la Figura 130 se observan las alertas más recientes, las cuales se le notificaran al administrador, indicado ciertos parámetros y en qué equipo se encuentra el problema.

Figura 130

Alertas vía e-mail

Fuente: Captura correo del administrador de red en www.outlook.com

- **Aislamiento y diagnóstico de fallos**

El **Art.5** y el **Art.6** establecidos en las políticas entran en la implementación del aislamiento y diagnóstico de fallos ya que Cisco DNA Center permite tratar un fallo mediante niveles de prioridad que van de acuerdo con la gravedad del problema, en la Tabla 105 se presentan diferentes grados de severidad, los cuales se identifican a través de los colores establecidos por el software de gestión DNA y así también pasar al siguiente paso para resolver nuevos fallos que requieran del uso de nuevos y diferentes mecanismos.

Tabla 105

Clasificación de fallos en Cisco DNA Center

Tipo de Fallo	Color	Descripción
Cuestiones críticas	Prioridad 1	Un problema crítico que requiere atención inmediata y que puede tener un impacto mayor en las operaciones de la red.
Advertencias	Prioridad 2	Problema grave que puede afectar a varios dispositivos o clientes.
Sin errores ni advertencias – Notificación de Información	Prioridad 3	Un problema menor que tiene un impacto localizado o mínimo.
No hay datos disponibles	Prioridad 4	Un problema de advertencia que puede no ser un problema inmediato pero cuya solución puede optimizar el rendimiento de la red.

Fuente: Elaboración propia basada en la herramienta Cisco DNA Center.

A continuación, se procede al diagnóstico del fallo, ya que una vez detectado y aislado el origen del fallo, se establece un diagnóstico mediante el DNA sobre las causas que han provocado dicho fallo:

- DNA maneja diferentes tipos de categorías de eventos que son probables que ocurran en la red, los cuales son: eventos de protocolos, eventos de capa 2 y eventos de plataforma de Hardware, todos estos eventos que recibe el DNA center, los recibe a través de tramas y syslogs que se muestran en la página 360 del dispositivo.
- Cuando se ha detectado y aislado un problema en el DNA Center, al momento de dar un click en el dispositivo afectado nos indicara cuando exista un consumo alto de los niveles de umbrales, a los que normalmente haya estado funcionando.
- Cisco DNA center en su manual de uso brinda una tabla que proporciona un listado seleccionado de mensajes syslog, de nivel inferior a Crítico (Error, Advertencia, Aviso e Información) que se muestran en el Visor de sucesos de la ventana Dispositivo 360, la tabla se detallara en el ANEXO C:
- Fallos relacionados con el tráfico de la red.
- Fallos relacionados con los interfaces inactivos de un dispositivo, realizando un click en una interfaz se puede observar la disponibilidad, la transmisión (tx), recepción (rx) y recibir errores para esa interfaz, todos los parámetros mencionados anteriormente se los puede visualizar hasta en 5 interfaces a la vez.

- **Solución**

  Para la solución del fallo detectado se procese a tomar acciones pertinentes para reparar el daño ocurrido. A continuación, se enlistan los siguientes mecanismos que son utilizados para la solución de fallos:

  - Se recupera conectividad y se estabilizan los dispositivos de red si son reiniciados.

- Las actualizaciones constantes en un sistema operativo, un parche, son muy importantes de realizar ya que pueden solucionar un fallo en específico.
- Para corregir fallos también se debe verificar que los cables físicos que brindan la conexión hacia los elementos de red se encuentren conectados y en buen estado para así descartar problemas de conexión.
- En la infraestructura de la red de la Universidad Técnica del Norte los equipos más susceptibles a fallos se encuentran en la capa de acceso, dichos equipos en la capa de acceso son los switchs Cisco Catalyst de la serie 2960.
- Para la gestión de los dispositivos, estos deben ser gestionados mediante un puerto de consola que permite establecer conexión vía ssh de manera local y remota.
- Para errores de transmisión y recepción de datos en los equipos de conmutación, se verificará la configuración de la interfaz.

- **Registro de Fallos**

Después de haber diagnosticado un fallo el siguiente paso es resolverlo en el menor tiempo posible mediante el proceso de la gestión reactiva, para lo cual es primordial utilizar la plantilla de notificaciones de fallos que se detalla en el ANEXO E, en donde se debe detallar el problema y la solución de dicho fallo, para en posteriores eventos se siga dicho procedimiento.

Análisis

En la implementación de las políticas de fallos para la red cableada de la Universidad Técnica del Norte, se abarco los requerimientos y las política de manejo de fallos establecido

en el **Art.3** de las políticas de administración y gestión, donde se prioriza la detección, notificación, aislamiento y resolución de fallos, habilitando los servicios de telemetría el software de gestión Cisco DNA center, el cual permite al administrador recibir las notificaciones cuando ocurre un evento en la red cableada, pero se debe tener en cuenta que las alertas son solo dentro del software de gestión, ya que el software que emite notificaciones vía correo y sms es el software Zabbix y este solo para la red cableada .

El ***Req.24 y Req.25*** engloba al ***Art.3*** antes mencionado, ya que las alarmas o notificaciones que alerten al administrador de red por parte del software de gestión deberán ser resultas con las herramientas que brinda DNA Center y en caso de no poder resolver remotamente, se procederá a tomar en cuenta la Actividad de razonamiento ya que brindaran varias actividades que se podrán analizar y realizar para resolver el fallo presente, esto se lo encontrara en la opción análisis de raíz de la causa que brinda dentro del problema en los equipos de conmutación que se encuentren en las diferentes capas de red, por ello en dicha opción se presentaran y en caso de no lograr resolver el fallo, DNA Center brinda una conclusión al problema.

4.1.1.3. Implementación de políticas de gestión de Contabilidad

La red de la Universidad Técnica del Norte ha tenido un crecimiento constante y fuerte para poder brindar mayor conectividad a los usuarios, dentro de los últimos años se han agregado nuevos equipos para potenciar la red y sus recursos, esto también implica que se dificulte saber el estado actual de la misma. Por ende, esta área de gestión de Contabilidad tiene como objetivo mantener un constante monitoreo de los dispositivos gestionados y cuidar del rendimiento, para así lograr determinar el estado en el cual se encuentra la red en intervalos de tiempo según lo requiera el administrador o en tiempo real.

4.1.1.3.1.Reportes

A continuación, se implementa el ***Art.17*** establecido en las políticas en el ámbito de la gestión de contabilidad.

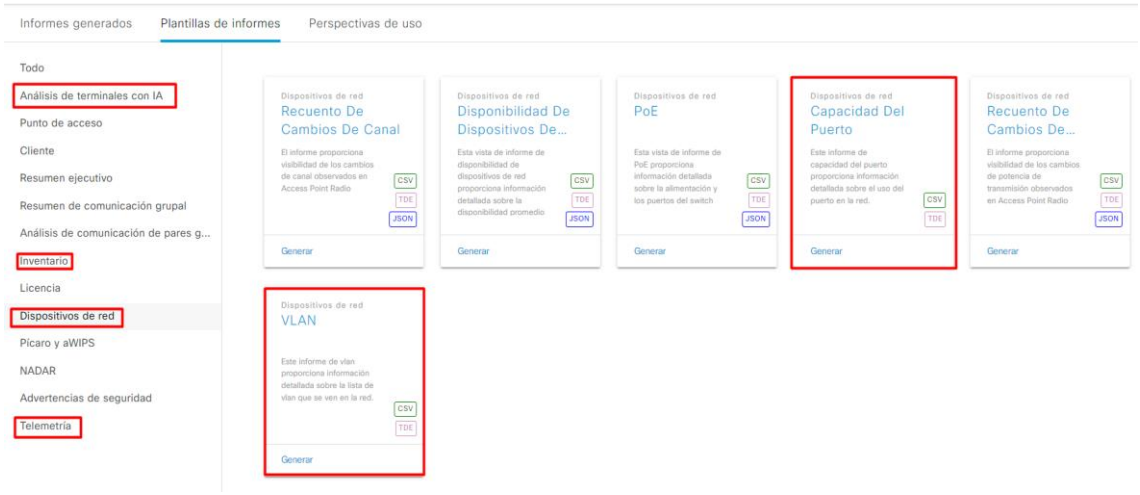
Según CISCO (2021), “la función Reportes dentro del software de gestión DNA Center permite obtener información sobre su red y su funcionamiento, dentro de la función reportes se encuentran los siguientes casos de uso:”

- Capacidad de planificación: comprensión de cómo se utilizan los dispositivos dentro de su red.
- Cambio de patrón: los cambios de las tendencias del patrón de uso en la red se lo harán mediante un seguimiento. Las tendencias de patrones de uso pueden incluir clientes, dispositivos, bandas o aplicaciones.
- Informes operativos: las operaciones de red, como actualizaciones completadas o errores de aprovisionamiento se los hará a través de una revisión de informes.
- Estado de la red: a través de informes se determina el estado general de la red.

En la Figura 131 se muestra la generación de reportes en icono de inicio>reports>generated reports, donde se puede elegir el formato el tipo de reporte que se desea generar.

Figura 131

Tipos reportes para dispositivos de red



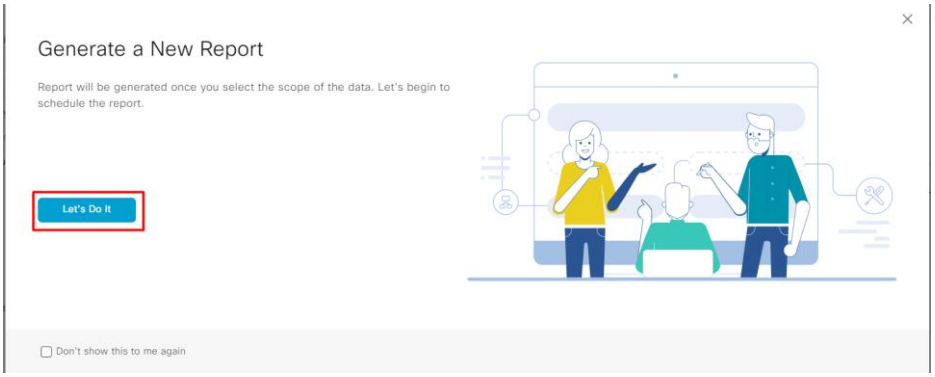
Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Para la generación de un nuevo reporte primero se debe escoger una plantilla o sea un ámbito en el cual se quiera generar un reporte, en el ANEXO G se detalla el proceso completo de la generación de nuevo reporte sobre el resumen del cliente.

En la ventana Generar un nuevo informe, haga clic en **Let´s Do it** como se visualiza en la Figura 132.

Figura 132

Generar un nuevo Reporte.



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

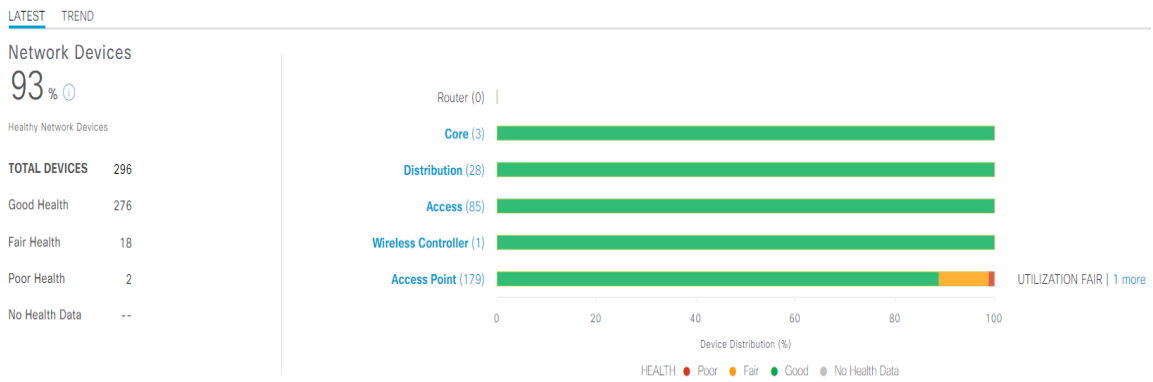
4.1.1.3.2. Parámetros de chequeo

El siguiente ítem hace referencia al ***Art.19*** que se establece en las políticas de contabilidad, ya que tiene que ver con el monitoreo de parámetros de chequeo de la red.

Cisco DNA Center permite evidenciar gráficas de tendencias codificados por colores que muestran el rendimiento de los dispositivos gestionados en intervalos de tiempos, tal y como se evidencia en la Figura 133. Dependerá del dispositivo que se esté monitoreando para poder evidenciar ciertos parámetros los cuales logran determinar si el dispositivo se encuentra en un buen o mal estado.

Figura 133

Dispositivos de red saludables



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Las gráficas codificadas por colores muestran el rendimiento de cada categoría de dispositivo (Acceso, Núcleo, Distribución, Enrutador, Controladora Inalámbrica y Puntos de Acceso).

DNA center posee niveles de puntuación de salud, los cuales se detallarán a continuación en la Tabla 106.

Tabla 106

El color representa la salud de los dispositivos de red

Tipo de Fallo	Prioridad
Dispositivo de red deficiente	El rango de puntuación es de 1 a 3.
Dispositivos de red aceptables	La puntuación de salud oscila entre 4 y 7.
Dispositivos de red en funcionamiento	La puntuación de salud oscila entre 8 y 10
No hay datos de salud	La puntuación de salud es 0

Fuente: Adaptado de (Cisco, 2022a), elaboración autor basada en la herramienta Cisco DNA Center.

El color que emana cada dispositivo corresponde a su estado de salud, dicho estado de salud se mide en una escala de 1 a 10, donde es 10 es la mejor puntuación, mientas que una puntuación de 0 indica que no se han podido obtener datos.

- **Monitoreo del tráfico de red por Aplicaciones**

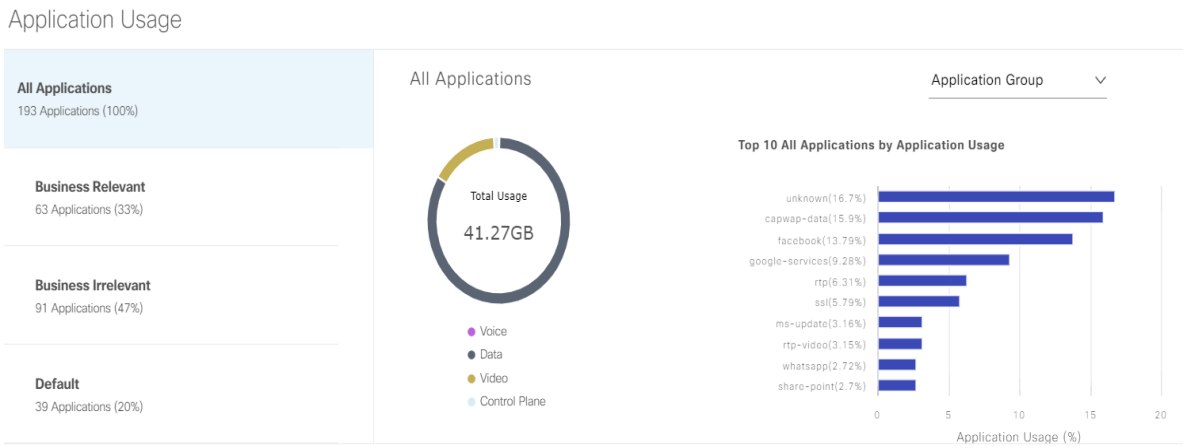
En el monitoreo de red por aplicaciones se encuentra la puntuación de salud de las aplicaciones por grupos, tal y como se evidencia en la Figura 134 y también la Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Figura *135* ya que muestran gráficos estadísticos que indican la clase de tráfico en la red,

Las gráficas muestran el porcentaje de uso de las aplicaciones el cual es calculado en el último intervalo de 5 minutos basado en los datos recogidos cada 10 minutos en el intervalo de 3 a 24 horas y cada 60 minutos para el intervalo de 7 días.

Figura 134

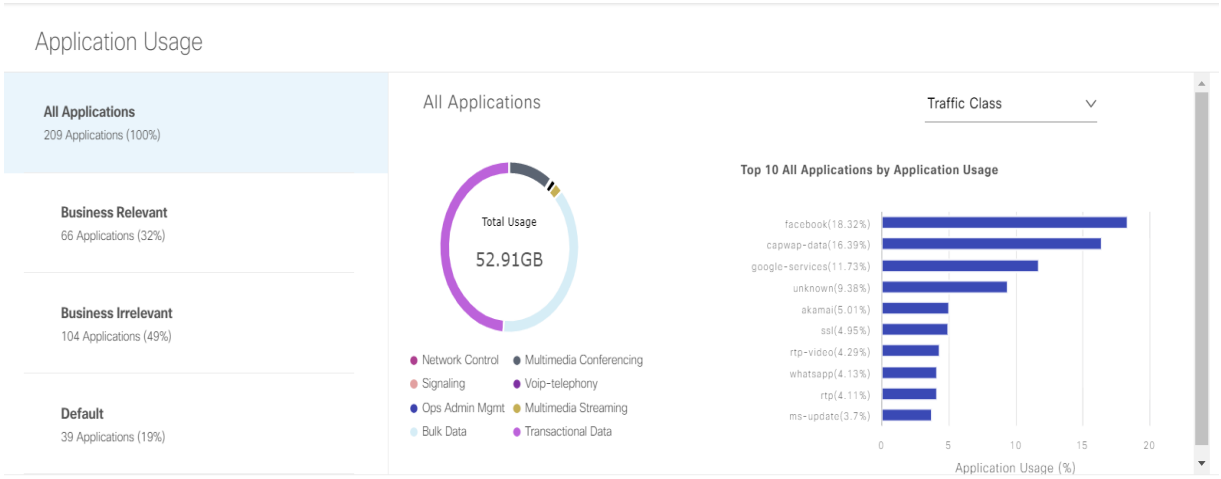
Uso de la aplicación por grupos



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Figura 135

Uso de las aplicaciones por clase de trafico

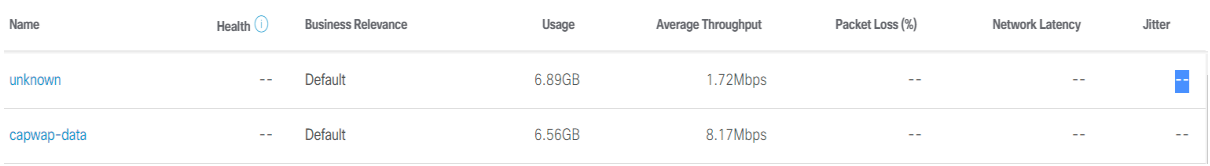


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

La Figura 136 muestra parámetros de consumo que tienen las aplicaciones como: tipo de relevancia de la aplicación, uso de datos, rendimiento de la tasa de transferencia, latencia, pérdida de paquetes y jitter.

Figura 136

Parámetros de monitoreo en aplicaciones



Name	Health	Business Relevance	Usage	Average Throughput	Packet Loss (%)	Network Latency	Jitter
unknown	--	Default	6.89GB	1.72Mbps	--	--	--
capwap-data	--	Default	6.56GB	8.17Mbps	--	--	--

Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Análisis

Cisco DNA Center permite la implementación de parámetros de gestión en telemática de equipos de red cableada, donde se abarca el ***Art.17*** de las políticas de administración y gestión de la red y el requerimiento operacional del sistema de gestión como los requerimientos para la red cableada, donde es posible generar los reportes que abarquen todos los parámetros de los recursos de cada equipo y obtener datos estadísticos que permitan al administrador tener una noción del funcionamiento de la red en individual y general. Dichos reportes responden al ***Req.26*** para la red cableada y dentro de la opción de reportes en el software de gestión DNA Center para la red cableada se seleccionarán las opciones de Executive Summary y Network Devices ya que en ellas existen opciones de generar reportes sobre VLANs, PoE, capacidad de puertos y análisis del rendimiento de la red con información sobre dispositivos de red y problemas.

4.1.1.4. Implementación de políticas de gestión de Prestaciones

En esta área del modelo de gestión, la gestión de prestaciones tiene como objetivo recolectar información acerca de los recursos que se utilizan en la red, lo cual permite obtener datos estadísticos sobre el procesamiento de dicha información.

4.1.1.4.1. Parámetros de monitoreo

El ***Art.15.*** establecido en las políticas para el ámbito de gestión de prestaciones, es el responsable de los parámetros de monitoreo, donde el objetivo principal de esta área de gestión es registrar la utilización de los recursos de la red. De acuerdo con el manual de Cisco DNA center, el software de gestión incluye métricas de monitorización del sistema (KPI).

Los dispositivos de red gestionados por el DNA center son: Switch (Acceso y Distribución) Cisco, routers, inalámbricos y de fábrica, cada uno con la descripción de los parámetros a medir como la utilización de la CPU y la utilización de la memoria. El software de gestión brinda información sobre cómo se calculan las puntuaciones de salud de la red, puntuación de salud por categoría de dispositivo, puntuación de salud del dispositivo individual y las métricas KPI, cabe mencionar que las métricas de KPI son indicador clave de rendimiento (KPI) para información específica.

- **Puntuación de salud del dispositivo individual**

Las métricas de KPI brindan información sobre la puntuación de salud del dispositivo, tal y como se detalla en la Tabla 107, Tabla 108, Tabla 109 y esto va en los siguientes planos: salud del sistema, conectividad de plano de datos, conectividad del plano de control. Las métricas varían dependiendo del tipo de dispositivo.

Tabla 107

Estados del Sistema en el software de gestión

Estado del Sistema	
Tipo de Dispositivo	**Descripción**
Switch (Acceso y Distribución)	- El sistema incluye métricas de supervisión como la utilización de la CPU y la memoria.

Inalámbrico	El sistema incluye las siguientes métricas de monitorización: - Para controladores inalámbricos, incluye utilización de memoria, temporizadores libres y Mbufs libres. - Para AP, incluye utilización de CPU y utilización de memoria.
Router	- El sistema incluye métricas de supervisión como la utilización de la CPU y la memoria.

Fuente: (Cisco Systems, 2021)

Tabla 108

Conectividad de plano de datos basado en Cisco DNA center

Conectividad de plano de datos	
Tipo de Dispositivo	**Descripción**
Switch (Acceso y Distribución)	- El sistema incluye métricas como errores de enlace y estado del enlace. Para el caso de los switchs, la métrica de disponibilidad de enlaces cuenta los puertos de la pila física, los enlaces conectados a dispositivos de red y los canales de puertos orientados al borde del tejido.

Fuente: (Cisco Systems, 2021)

Tabla 109

Conectividad de plano de datos para dispositivos inalámbricos

Conectividad de plano de datos	
Tipo de Dispositivo	**Descripción**
Wireless	Incluyes las siguientes métricas: - Para controladores inalámbricos, incluye métricas, como pool WQE, pool de paquetes y errores de enlace.

	- Para AP, incluye métricas de RF, como interfaz, ruido, calidad del aire y utilización de radio. Para KPI se incluye lo siguiente: - Para los controladores inalámbricos, incluye la conectividad con los servidores de nodos del plano de control.

Fuente: (Cisco Systems, 2021)

- **Puntuación de salud de los Switchs**

La puntuación Switch Health es la subpuntuación mínima de los siguientes parámetros, tal y como se muestra en la Tabla 110.

Tabla 110

Puntuación de salud para dispositivos Switchs

Estado del Sistema **Tipo de Dispositivo**	**Descripción**
Utilización de CPU	- Si la utilización de la CPU es del 95 por ciento o menos, la puntuación es 10. - Si la utilización de la CPU es superior al 95 por ciento, la puntuación es 1.
Utilización de Memoria	- Si la utilización de la memoria es del 95 por ciento o menos, la puntuación es 10. - Si la utilización de la memoria es superior al 95 por ciento, la puntuación es 1.
Errores de enlace (Rx y Tx)	- Para los errores de enlace sólo se tienen en cuenta los enlaces de infraestructura. Los enlaces de infraestructura son enlaces topológicos entre dispositivos de red, como conmutadores, enrutadores, controladores inalámbricos y AP.

	Si una interfaz de infraestructura física tiene errores, la puntuación es 8, si todos los enlaces están caídos, es 1; en caso contrario, es 10.
Descartes de enlaces	-Sólo se tienen en cuenta los enlaces de infraestructura para el descarte de enlaces. Los enlaces de infraestructura son enlaces topológicos entre dispositivos de red, como conmutadores, enrutadores, controladores inalámbricos y AP. Si un enlace de infraestructura física sufre pérdidas de paquetes (descartes), la puntuación es 8; si todos los enlaces sufren descartes, es 1; en caso contrario, es 10.
Estado del enlace	- Sólo se tienen en cuenta los enlaces de infraestructura para el estado de enlace ARRIBA/ABAJO. Los enlaces de infraestructura son enlaces topológicos entre dispositivos de red, tales como switches, routers, controladores inalámbricos y APs. Si una interfaz de infraestructura física está caída, la puntuación es 8, si todas las interfaces Si todas las interfaces están caídas, la puntuación es 1 y, en caso contrario, 10.
Conexión a nodo de plano de control: sólo dispositivos de tejido (borde y frontera)	- Si el nodo del plano de control es accesible, la puntuación es 10. - Si el nodo del plano de control es inalcanzable, la puntuación es 1. Nota: Si hay más de 1 nodo del plano de control en un dominio de estructura y se puede acceder a todos los nodos del plano de control, la puntuación es 10; de lo contrario, la puntuación es 1. Nota: Para que la puntuación de estado se complete correctamente para los dispositivos de estructura, habilite las métricas del recopilador de SNMP. En el ANEXO A se indica las métricas SNMP Colletor activadas.

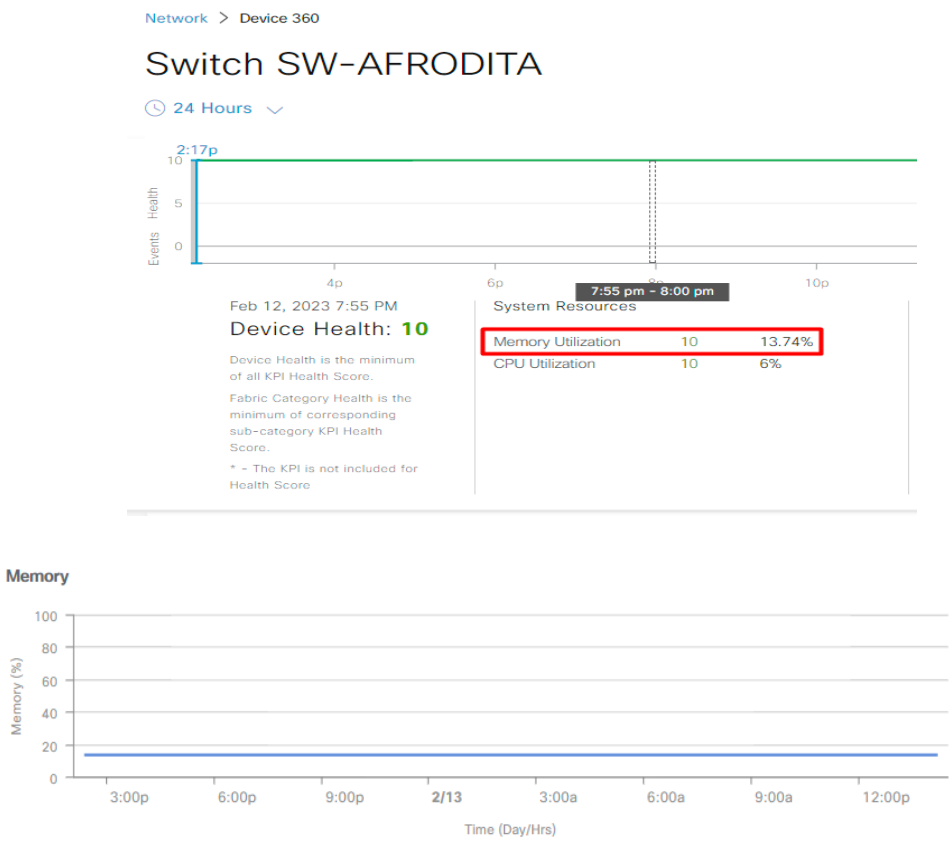
Fuente: Información de (Cisco Systems, 2021), adaptado en base a la herramienta Cisco DNA Center.

- **Monitoreo de uso de memoria**

El uso de memoria es un recurso del dispositivo que se debe tener siempre en constate monitoreo, ya que un exceso consumo de memoria por parte de los recursos en el dispositivo puede perjudicar su rendimiento. Cisco DNA Center permite visualizar de manera gráfica y estadística este recurso. En la Figura 137 se muestra el uso de memoria del Switch SW-AFRODITA que se encuentra en el Edificio Central en la capa de Core.

Figura 137

Uso de la memoria del equipo de la capa de Core



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

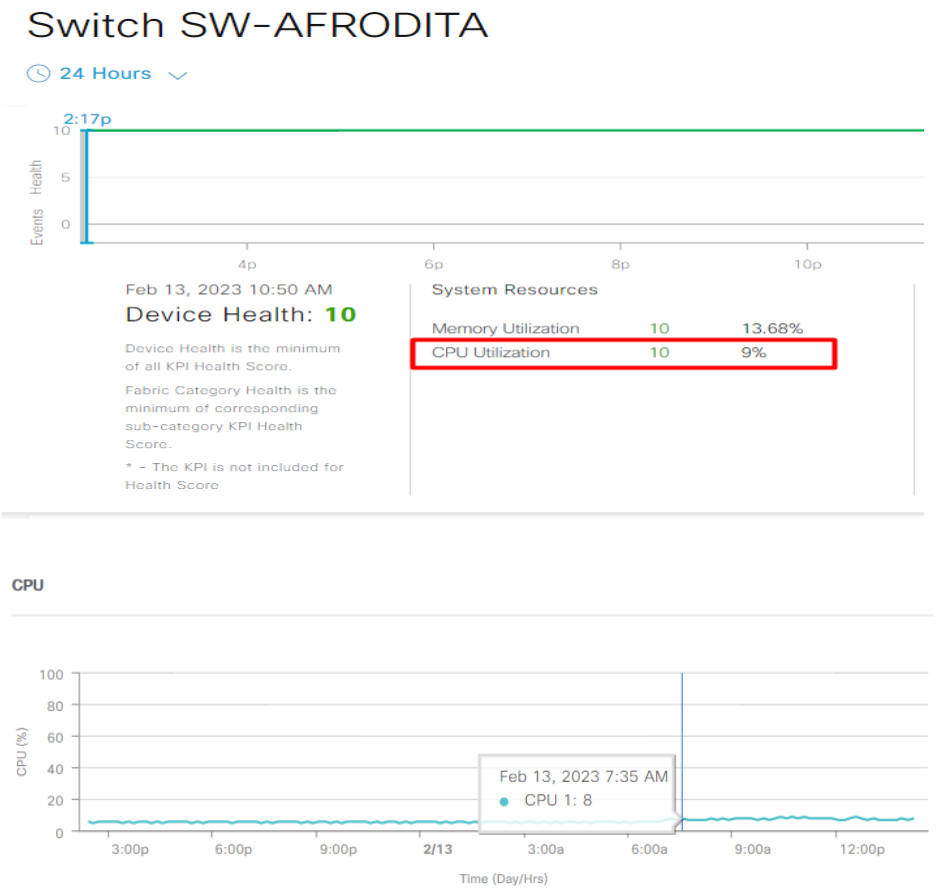
- **Monitoreo de uso de CPU**

El software Cisco DNA Center permite visualizar de manera grafica el porcentaje que está utilizando el dispositivo en CPU en tiempo real. En la Figura 138 se visualiza el

porcentaje de utilización de CPU del Switch SW-AFRODITA y como se puede evidenciar que tiene un estado de salud de 10 ya que el consumo es constante y está en el rango establecido, por lo cual no generara ningún tipo de alerta.

Figura 138

Monitoreo del uso de la CPU en un dispositivo de la capa Core.



Fuente: Adaptado de Cisco DNA Center

Análisis

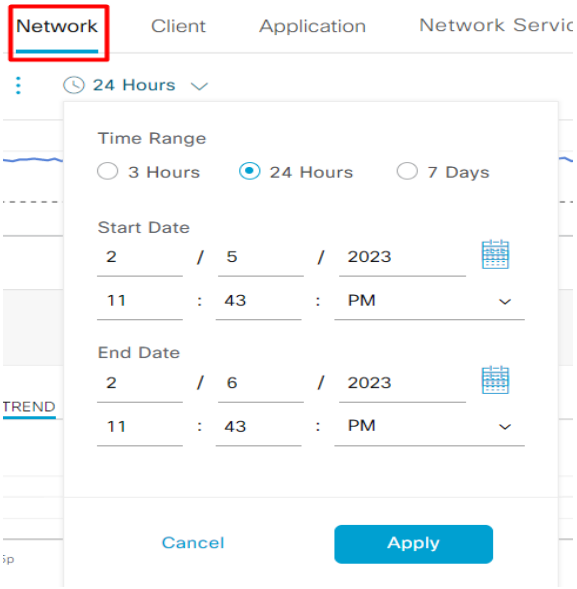
El monitoreo tanto de memoria como de CPU es importante ya que afecta al funcionamiento de la red por debajo de los niveles de rendimiento de línea de base, existen dos tipos de funcionamiento deficiente que ocurren en la capa 2 de una red. El primero hace referencia a las tramas que elijan rutas deficientes al destino, pero lleguen. Para dicho caso la red podría experimentar un uso excesivo de ancho de banda en enlaces que no deberían tener

ese nivel de tráfico. Para el segundo funcionamiento, es que se descarten algunas tramas ya que estos problemas se pueden identificar mediante las estadísticas del contador de errores y los mensajes de error de la consola en el switch. En un entorno Ethernet, se lo puedo corroborar con un ping extendido o continuo también revela si se descartan tramas.

El software de gestión también ayuda a la selección del intervalo de tiempo que haya establecido el administrador de red, tal y como se visualiza en la Figura 139.

Figura 139

Intervalos de tiempos que trabaja el DNA Center

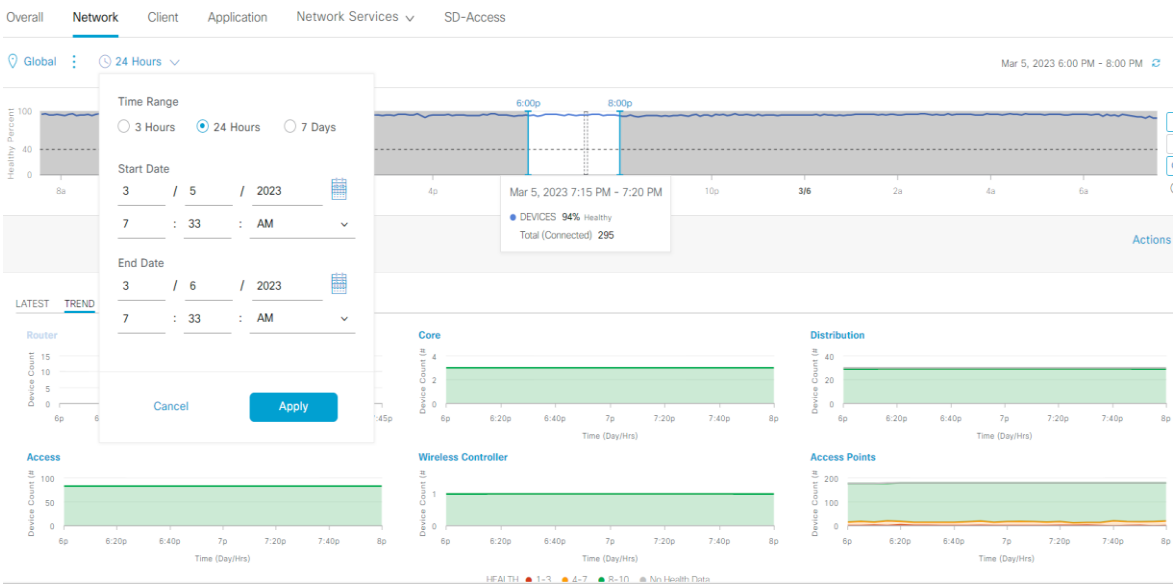


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

En el caso de la pestaña Tendencia, como se muestra en la Figura 140, proporciona una vista de la tendencia para el intervalo de tiempo seleccionado en la configuración del intervalo de tiempo. Por ejemplo, si el intervalo de tiempo se establece en las últimas tres horas, la pestaña de tendencia muestra tres horas de datos, la información se actualiza al momento que se cambian los intervalos de tiempo. Cabe mencionar que en el menú desplegable de intervalo de tiempo puedes seleccionar los siguientes intervalos de tiempo: 3 horas, 24 horas o 7 días.

Figura 140

Pestaña Tendencia



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Al recorrer la línea de tiempo a través del control deslizante se puede observar la información sobre el estado y los eventos disponibles de red a lo largo de un periodo de tiempo.

Según, Cisco Systems (2021), las siguientes funciones vienen dadas por el control deslizante de la línea de tiempo:

- **Estado:** a través de la línea de tiempo puede pasar el cursor por encima del control deslizante para lograr visualizar la puntuación de salud y los KPI del cliente para una venta de tiempo que se elija a conveniencia o por previo análisis.

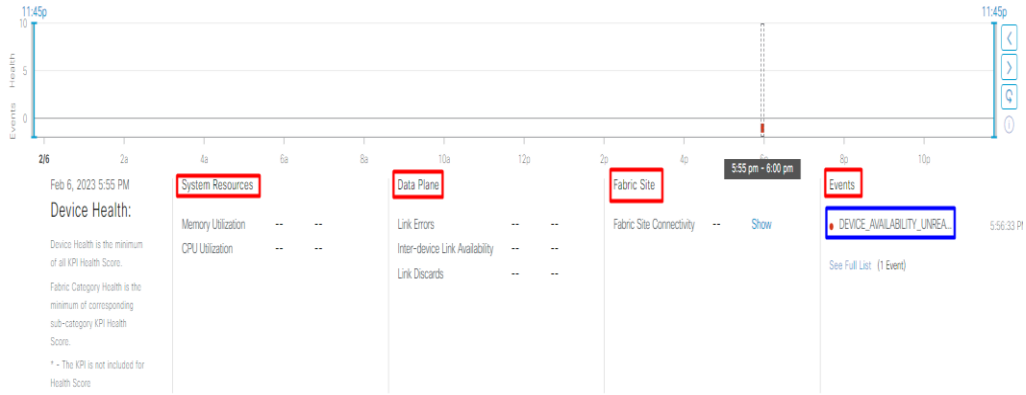
  Al hacer doble click en el grafico se muestra el control deslizante de la línea de tiempo en un periodo de tiempo de 1 hora con un evento sucedido. Como se representa en la Figura 141, al momento de realizar doble clic en la barra de tiempo de periodo toda la ventana se actualiza, proporcionando

actualizaciones para esa hora. Tenga en cuenta que las marcas de tiempo junto a cada categoría (Incidencias, Conectividad, etc.) también se actualizan.

- **Eventos:** Los datos de los eventos se muestran como barras verticales codificadas por colores en el gráfico, tal como se visualiza en la Fuente: Adaptado Cisco DNA Center del DDTI de la UTN
- **Figura *142***. Cada barra vertical representa 5 minutos de tiempo. Durante cada ventana de 5 minutos pueden generarse varios eventos significativos. Pase el cursor sobre la barra vertical para obtener más información sobre los eventos.

Figura 141

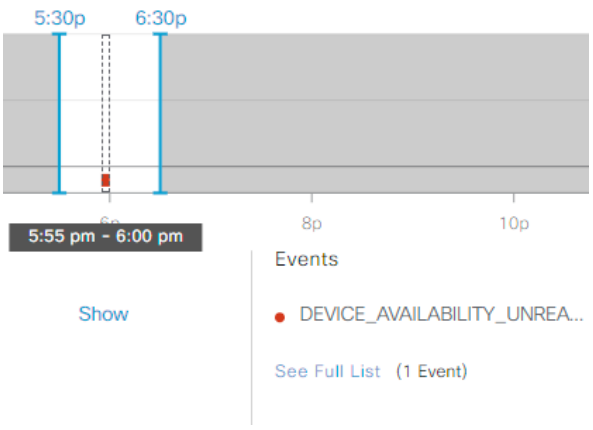
Parámetros sobre el intervalo de tiempo



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Figura 142

Datos de los eventos en un intervalo de tiempo



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

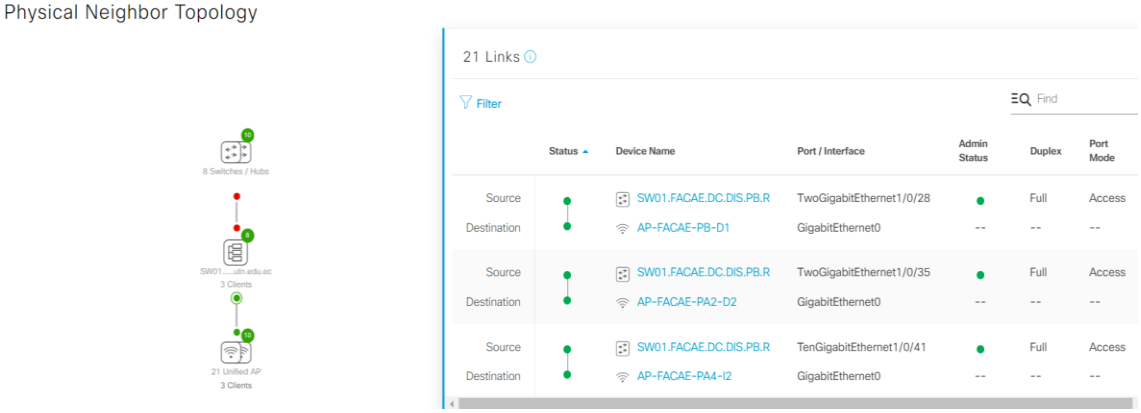
Cuando se ha detectado y aislado un problema en el DNA Center, al momento de dar un clic en el dispositivo afectado nos indicara los siguientes parámetros: Utilización de CPU, Utilización de memoria, Disponibilidad de enlace entre dispositivos, Errores de enlace, Descartes de enlace, alcanzabilidad al plano de control.

4.1.1.4.2. Disponibilidad

- En este ítem se menciona al ***Art.16*** establecido en las políticas para el ámbito de gestión de prestaciones, ya que el software de gestión Cisco DNA Center permite evidenciar y visualizar la disponibilidad de los dispositivos que se encuentran monitoreados en la red. En la Figura 143, se evidencia la disponibilidad y los problemas de cada interfaz de un equipo. Es importante tener el conocimiento del estado de los enlaces ya que la falta de funcionalidad o conectividad en la capa de red o en las capas superiores son algunos problemas de capa 2 por lo cual pueden llegar a detener el intercambio de tramas a través de un enlace, mientras que otros solo provocan un deterioro del rendimiento de la red.

Figura 143

Enlaces establecidos de un equipo



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

La Figura 144 muestra los eventos ocurridos en cada uno de los enlaces de un dispositivo gestionado, se toma en cuenta 3 colores: azul como error, rojo como enlace caído y verde como enlace disponible.

Figura 144

Visor de eventos para los enlaces

Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

4.1.1.4.3.Límites de rendimiento

- **Switchs**

Dicho los parámetros a tomar en cuenta se considera que el consumo de CPU no está en un promedio menor del 20% y mayor al 40 %, por lo tanto, si el valor llegaría hacer del 70% se consideraría una advertencia y si llegaría a ser mayor a 90% se lo tomaría como crítico.

Análisis

Cisco DNA Center permite la recolección de ciertos parámetros de los equipos de red cableada con la activación de servicios de telemetría, donde se abarca el ***Art.15*** de las políticas de administración y gestión de la red y el requerimiento operacionales del sistema de gestión como los requerimientos para la red cableada, donde es posible la visualización estadística de manera grafica de los recursos de la red, lo cual permite al administrador

acceder a los datos estadístico en tiempo real de cada equipo o a su vez de manera general y verificar la disponibilidad de la red, observando cómo se comportan los recursos de los equipos en funcionamiento y con alta cantidad de usuarios.

4.1.1.5. Implementación de políticas de gestión de Seguridad

En esta área de gestión de seguridad, solo el administrador de red tendrá los roles principales para realizar cambios de configuración al software de gestión y de acuerdo con las tareas que desempeñe un usuario externo a la red se le dará acceso al sistema de gestión con su respectivo nivel de usuario, este ya sea writre o monitor.

En la Tabla 111 se muestra el rol y el nivel de privilegio que posee cada uno.

Tabla 111

Roles de usuarios

ROL	PRIVILEGIO
SUPER-ADMIN-ROLE	Control completo de la implementación de Cisco DNA Center, todos los accesos habilitados
NETWORK-ADMIN-ROLE	El administrador de red tiene acceso a todos los aspectos de control de red de Cisco DNA Center con la exclusión del sistema y el área de la plataforma de desarrollo
OBSERVER-ROLE	Observer puede ver todos los aspectos de Cisco DNA Center, pero no tiene acceso de escritura.
DDTI-ROLE	Puede configurarse los accesos dependiendo del requerimiento.

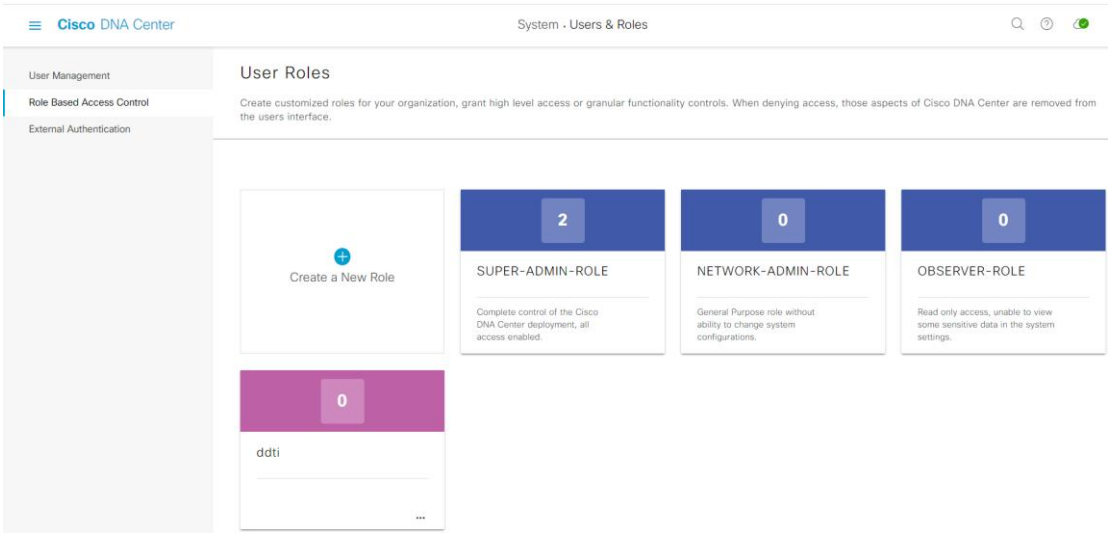
Como ya se describió, únicamente el Usuario-Super Administrador será el responsable de crear nuevos usuarios para acceder al sistema de gestión con determinados permisos. La creación de usuarios y sus respectivos niveles se detalla en el ANEXO J.

El software de gestión Zabbix envía notificaciones tanto de correo electrónico como sms de aviso a la aplicación de telegram a un único contacto para informarle de las fallas que se presentan en los dispositivos gestionados dentro de la red.

Cisco DNA Center permite crear roles personalizados para administrar de manera más optima la red, esto a través de conceder acceso de alto nivel o controles básicos de funcionalidad a otros usuarios que se les brinde el acceso al DNA center, tal y como se visualiza en la Figura 145.

Figura 145

Usuarios y roles dentro de DNA Center



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Análisis

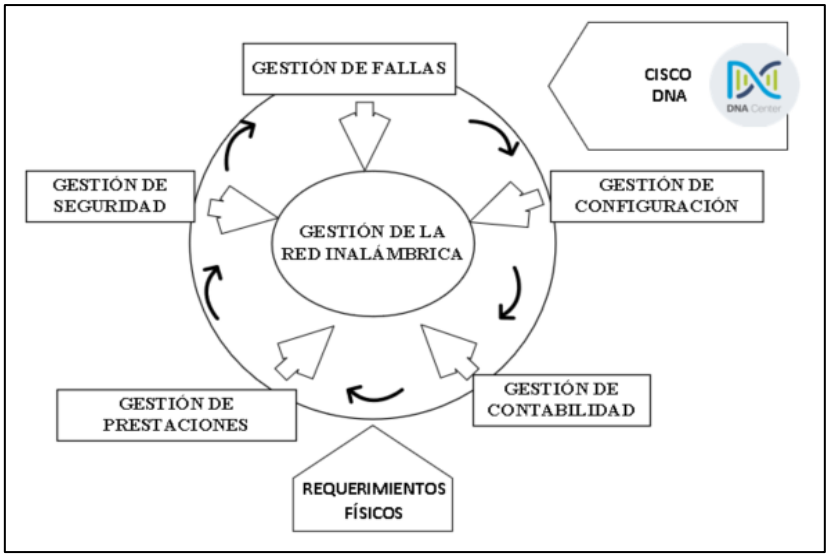
Cisco DNA Center posee tres roles de usuario y la creación de roles que se adaptarían a las necesidades de a quien vaya dirigido el rol, como se plantea en el ***Art.17*** de las políticas de administración y gestión de la red y el requerimiento ***Req.11*** que se establece en los requerimientos operacionales del sistema de gestión. Cisco DNA Center con el registro le logs permite al administrador con mayor privilegio poder saber hora y fecha que los usuarios que se accedieron a el Software de gestión y las acciones que realizaron en el caso de poseer permiso de escritura.

4.1.2. Implementación del Modelo de Gestión FCAPS en la red Inalámbrica

Para la implementación del modelo de gestión FCPAS de la ISO en la red inalámbrica se determina los requerimientos tanto en hardware como software que abarquen las 5 áreas fundamentales FCAPS, como herramienta monitora principal se tiene el software de gestión Cisco DNA Center, para la gestión de fallas se tiene el software wireshark que permite el monitoreo de los paquetes que se comparte en la red inalámbrica, logrando así cumplir el objetivo de gestión y administración de la red inalámbrica de la Universidad Técnica del Norte en su totalidad. En la Figura 146 se muestra el diagrama de gestión y las herramientas a utilizar.

Figura 146

Diagrama de gestión del Modelo FCAPS para la red Inalámbrica



Fuente: Elaboración Autor

4.1.2.1. Implementación de políticas de gestión de Fallos

La gestión de fallos se realiza mediante la detección, aislamiento, diagnóstico y solución de los fallos ocasionados en la red inalámbrica para mejorar la disponibilidad y eficiencia de la red. En la implementación de gestión de fallos se considera dos aspectos importantes de la OSI para el manejo de los fallos. los cuales se encuentra establecido en el ***Art.3*** donde describen las políticas que responderán a la implementación presentada a continuación, dentro del ámbito de la gestión de fallos, ya que los fallos detectados en la red son regidos de acuerdo con las alertas que emite el software de gestión Cisco DNA Center. Por lo cual se determina el uso de dos aspectos:

Pruebas de gestión proactiva: se aplica cuando los fallos aún no han sucedido y se pretende evitarlo.

Pruebas de gestión reactivas: se aplica cuando los fallos ya sucedieron donde se aplica la detección, aislamiento, diagnóstico y solución.

4.1.2.1.1.Gestión proactiva

Para la gestión en el manejo de fallos para la red inalámbrica de la Universidad Técnica del Norte, se manejan herramientas que permiten realizar este tipo de pruebas preventivas, estas pruebas preventivas son realizadas por el administrador de la red como se detalla en el ***Art.5*** de la Política de Administración y Gestión de la red., las cuales se detallan a continuación:

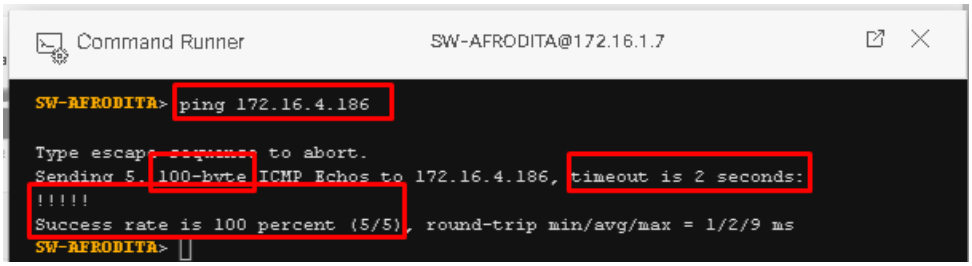
Ping: este comando se lo utiliza para verificar y comprobar la conectividad punto a punto a través del protocolo ICMP, está la herramienta incluida en el software cisco DNA permite verificar la conectividad de los diferentes equipos utilizando su dirección ipv4, se logra observar el tamaño del paquete, el tiempo que tarda cada paquete en segundos. A continuación, se muestra los pasos a seguir y en la Figura 147 se muestra la ventana command run y la respuesta obtenida al realizar el ping.

Herramienta Cisco DNA.

- ✓ Cisco DNA center/ provision/inventory/select switch /rum commands
- ✓ Ping dirección ipv4

Figura 147

Verificación de conectividad entre dos equipos de la red mediante protocolo ICMP.



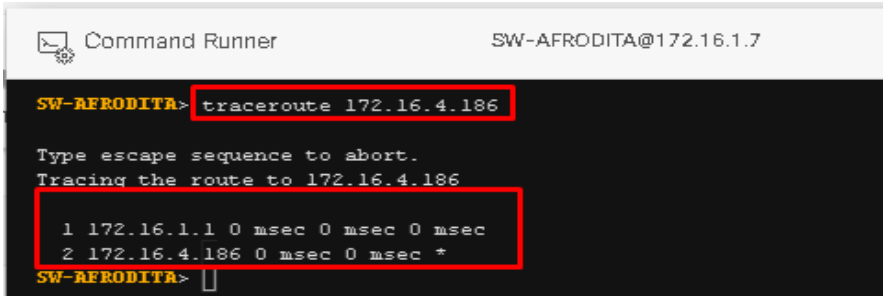
Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Traceroute: su función es similar a la del ping, a diferencia que con este comando se obtiene la lista de direcciones IPs de los equipos que atraviesan el mensaje hasta llegar a su

destino, está la herramienta incluida en el software cisco DNA center en commnad run, A continuación, se muestra la Figura 148 donde se aplica un traceroute desde un switch (SW-AFRODITA) del edificio central hacia el AP auditorio.

Figura 148

Verificación de saltos entre equipo de la red mediante traceroute



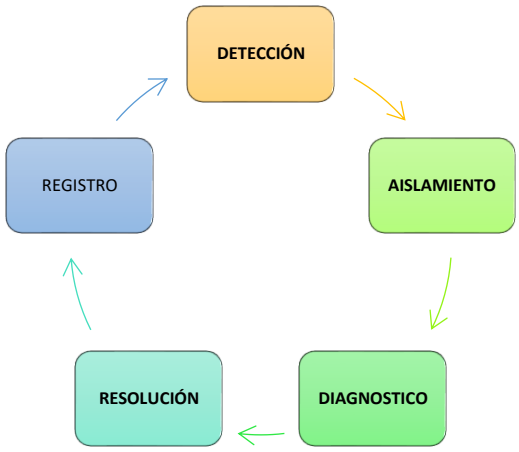
Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

4.1.2.1.2.Gestión reactiva

La gestión reactiva ocurre cuando en los equipos de la red inalámbrica ocurre un fallo inesperado, para el cual se establece un proceso el cual detecta la falla, posteriormente a diagnostica y se resuelve. En la Figura 149 se muestra el ciclo de vida de la gestión reactiva.

Figura 149

Ciclo de vida de la gestión reactiva



Fuente: Elaboración Autor

- **Detección de fallos:**

Para la detección de fallas en un equipo que conforma la red inalámbrica e la Universidad Técnica del Norte se cuenta con el software Cisco DNA center el cual presenta un mecanismo de alertas o notificaciones que le indican al administrador de la red el equipo y la falla ocurrida. Este tipo de notificaciones son establecidas de acuerdo a un modelo de puntuación de salud para los equipos de la red inalámbrica, el cual permite obtener un valor, los cuales son proporcionados de acuerdo con una puntuación que se calcula a partir de los recursos monitorizados como: utilización de memoria, utilización de CPU, errores de enlace, utilización de radio, interferencias, ruido y calidad de aire, en la

Tabla ***112*** se muestra cada parámetro y el cálculo de la puntuación para cada uno de los recursos gestionables.

Tabla 112

Parámetros y cálculos de puntuación para los recursos gestionados

Parámetros	Cálculo de la puntuación
CPU	- Si la utilización de la CPU es inferior al 90%, la puntuación es 10. - Si la utilización de la CPU es superior al 90%, la puntuación es 1.
Memoria	- Si la utilización de la memoria es inferior al 90%, la puntuación es 10. - Si la memoria disponible es igual o superior al 90%, la puntuación es 1.
Utilización de Radio	La puntuación se calcula individualmente para cada radio y, a continuación, se determina la puntuación media de la radio. - Si la utilización de la radio es inferior al 70%, la puntuación es 10. - Si la utilización de radio es del 70% o más, la puntuación es 1.

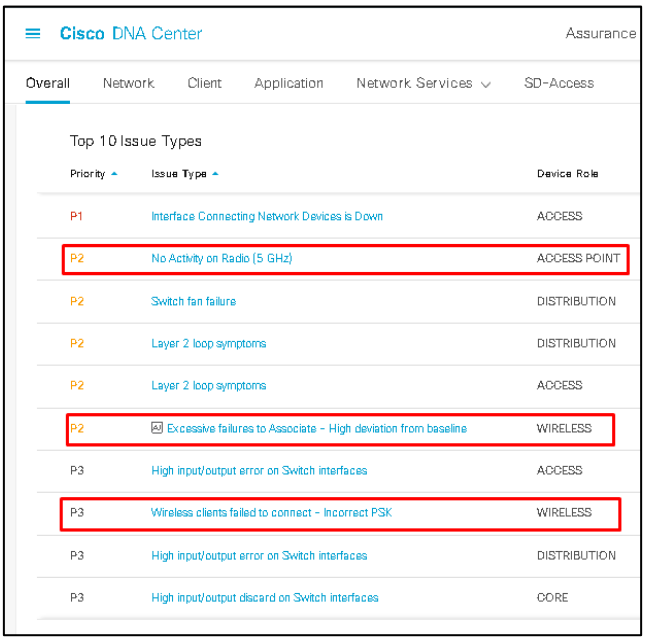
Interferencia	La puntuación se calcula individualmente para cada radio y, a continuación, se determina la puntuación media de la radio. Para radios de 2,4 GHz: - Si la interferencia es menor o igual al 50%, la puntuación es 10. - Si la interferencia es superior al 50%, la puntuación es 1. Para radio de 5 GHz: - Si la interferencia es menor o igual al 20 por ciento, la puntuación es 10. - Si la interferencia es superior al 20%, la puntuación es 1.
Ruido RF	La puntuación se calcula individualmente para cada radio y, a continuación, se determina la puntuación media de la radio. de la radio. Para la radio de 2,4 GHz: - Si el ruido RF es inferior a -81dBm, la puntuación es 10. - Si el ruido de RF es igual o superior a -81 dBm, la puntuación es 1. Para radio de 5 GHz: - Si el ruido RF es inferior a -83dBm, la puntuación es 10. - Si el ruido RF es igual o superior a -83dBm, la puntuación es 1.
Calidad del aire	La puntuación se calcula individualmente para cada radio y, a continuación, se determina la puntuación media de la radio. radio se determina la puntuación. Para la radio de 2,4 GHz: - Si la calidad del aire es del 60 por ciento o más, la puntuación es 10. - Si la calidad del aire es inferior al 60%, la puntuación es 1. Para radios de 5 GHz: - Si la calidad del aire es igual o superior al 75%, la puntuación es 10. - Si la calidad del aire es inferior al 75%, la puntuación es 1.

Fuente: (Cisco Systems, 2021)

El interfaz del software de gestión Cisco DNA Center presenta los principales tipos de alarmas visuales de los problemas en la red, mediante un orden de prioridades con su respectivo color, el tipo de problema, la categoría y la hora de la última concurrencia. En la Figura 150 se observa como el DNA permite al administrador de red detectar un fallo y tratarlo de acuerdo con su prioridad.

Figura 150

Alarmas visuales de fallos en la red inalámbrica



Fuente: Adaptado de Cisco DNA Center

- **Aislamiento de fallos:**

El proceso de aislamiento de fallos es el proceso en el cual se procede a determinar el tipo de alarma o alerta ocurrida, el cual se realizar automáticamente por el software Cisco DNA Center el cual proporciona un código de colores dependiendo a la puntuación obtenida, como se detalla en el ***Art.5*** de la Política de Administración y Gestión de la red. En la Tabla 113 se muestra el código de colores.

Tabla 113

Código de colores para la clasificación de fallos en Cisco DNA Center

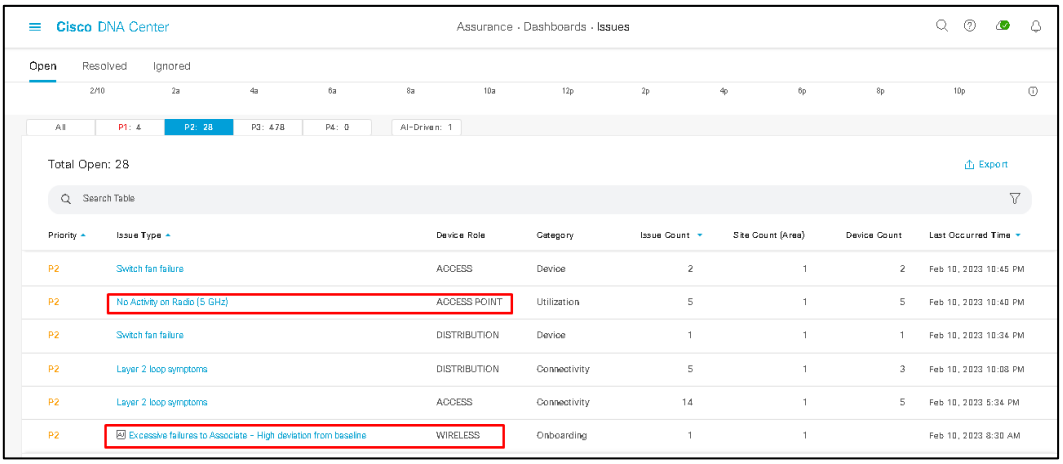
Tipo de Fallo	Color	Descripción
Cuestiones críticas	Prioridad 1	Dispositivo fuera de servicio - Malo: Dispositivos con una puntuación de salud de 1 a 3.

Advertencias	Prioridad 2	Alerta en dispositivos parcialmente caídos - Regular: Los dispositivos con una puntuación de salud van de 4 a 7.
Sin errores ni advertencias – Notificación de Información	Prioridad 3	Dispositivo Funcionando - Bueno: Los dispositivos con una puntuación de salud van de 8 a 10.
No hay datos disponibles	Prioridad 4	Dispositivo sin respuesta - Sin salud: Dispositivos sin datos de salud.

A continuación, en la Figura 151 se muestra el historial de fallas detectadas y aisladas mediante el software Cisco DNA Center

Figura 151

Aislamiento del fallo en Cisco DNA Center



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

- **Diagnóstico de fallos**

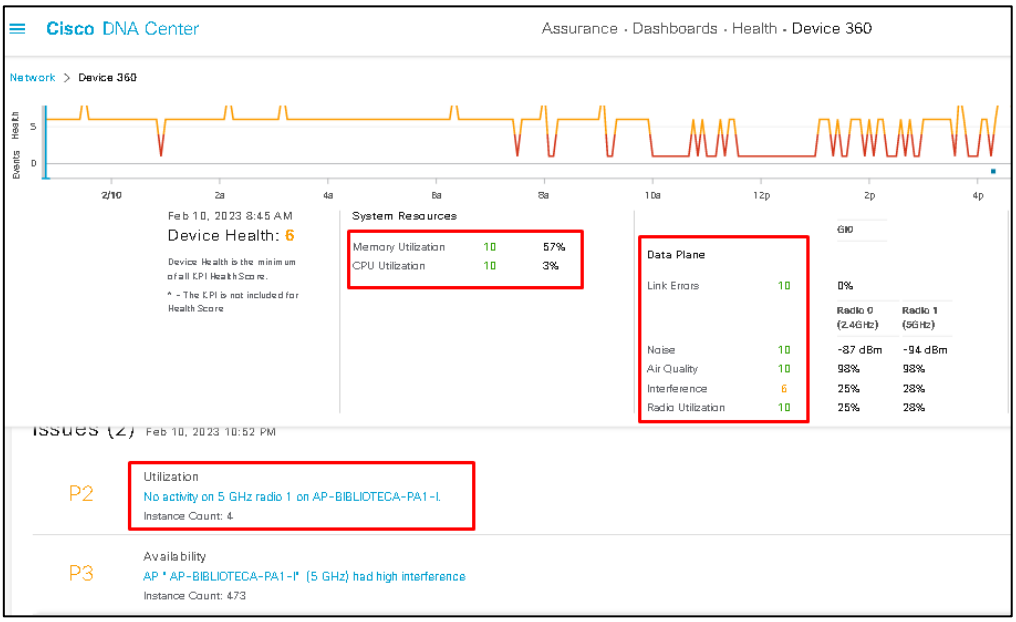
El diagnóstico de la falla ocurre después de aislar la falla, el software Cisco DNA Center muestra el estado de los recursos de cada equipo de la red inalámbrico, con el cual el administrador de la red visualiza el estado de los recursos y puede verificar el fallo suscitado

logrando así determinar el tipo de fallo en base a la información obtenida y el manual de gestión de fallas.

Dispositivo origen de fallo/ Network/Divice 360: en esta opción se logra la visualización de los recursos del dispositivo, en la Figura 152 se muestra la ventana de visualización que contiene toda la información relacionada al dispositivo.

Figura 152

Información de los recursos del dispositivo



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

- **Resolución para fallos**

Una vez diagnosticada la falla, se procede a la solución de la misma con la ayuda del software Cisco DNA center donde se debe proceder de acuerdo al manual de gestión de fallas, a continuación, se detalla una serie de pasos a seguir recomendadas por cisco center para la posible resolución del fallo.

a. Compruebe si hay una configuración incorrecta con WLAN no configuradas en la radio.

b. Reinicie la radio 1 de 5 GHz en AP ejecutando estos comandos en el controlador inalámbrico
c. Reinicie AP ejecutando este comando en el controlador inalámbrico.
d. Si no puede resolver el problema, comuníquese con el TAC de Cisco para obtener asistencia.

- **Registros de Fallos**

Después de haber diagnosticado un fallo el siguiente paso es resolverlo en el menor tiempo posible mediante el proceso de la gestión reactiva, para lo cual es primordial utilizar la plantilla de notificaciones de fallos que se detalla en el ANEXO E, en donde se debe detallar el problema y la solución de dicho fallo, para en posteriores eventos se siga dicho procedimiento.

Análisis

En la implementación de las políticas de fallos para la red inalámbrica de la Universidad Técnica del Norte, se abarco los requerimientos y las política de manejo de fallos establecido en el ***Art.3*** de las políticas de administración y gestión, donde se prioriza la detección, notificación, aislamiento y resolución de fallos, habilitando los servicios de telemetría el software de gestión Cisco DNA center, el cual permite al administrador recibir las notificaciones cuando ocurre un evento en la red inalámbrica dentro del software de gestión, ya que el software que emite notificaciones vía correo y sms es el software Zabbix y este solo para la red cableada .

4.1.2.2. Implementación de políticas de gestión de Configuraciones

Dentro de las políticas de gestión de configuraciones, el objetivo principal es la gestión de configuraciones de los equipos de red inalámbrica en totalidad, como la agregación de un nuevo equipo y la habilitación de servicios de telemetría.

4.1.2.2.1.Proceso de configuración de AP

El proceso de configuración para los APs se empieza desde que se agrega un nuevo equipo y se procede a activar los servicios de monitoreo para lograr tener un completo informe de los recursos de cada AP, enfocado en los parámetros establecidos en el ***Art.9*** de las políticas de administración y gestión de la red.

- Design > Network Hierarchy.
- En el panel izquierdo, haga clic en la planta del edificio.
- En la barra de herramientas del mapa, haga clic en Añadir/Editar.
- Asegúrese de que el conmutador APs está activado en la barra de herramientas del mapa.
- En el panel izquierdo del mapa, haga clic en Añadir AP.
- En el panel deslizante Agregar AP, marque las casillas de verificación de los puntos de acceso para seleccionar los AP en bloque y haga clic en Agregar Seleccionado. También puede hacer clic en Añadir junto a un punto de acceso.

Utilice el panel deslizante Editar AP para configurar detalles del AP como:

l) **Associated**

m) **Name**.

n) **MAC Address.**

o) **Model.**

p) **Admin/Mode.**

q) **Type Radio**

r) **OP/Admim(Operational status and AP mode.)**

s) **Channel**

t) **Antenna name.**

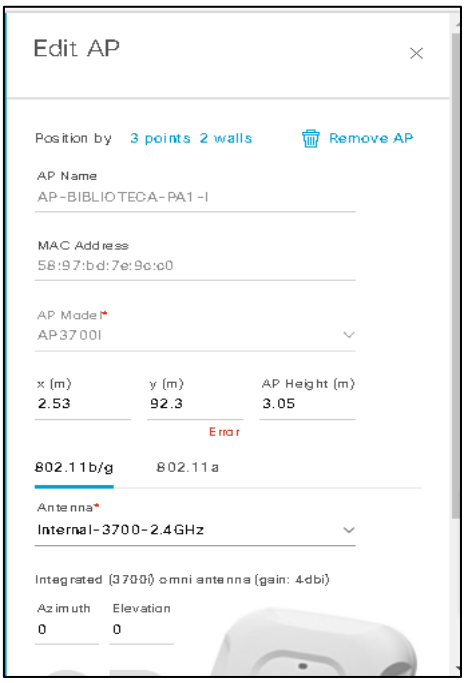
u) **Azimuth**: dirección de la antena.

v) **Elevation:** elevación en grados.

A continuación, en la Figura 153 se muestra la ventana de visualización de configuraciones después de agregar un AP.

Figura 153

Ventana de visualización de configuraciones de AP



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

4.1.2.2.2.Proceso de configuración de servicios de telemetría

La configuración de servicio de telemetría como Syslog, SNMPTraps, servidores colectores de NetFlow y Recopilación de datos de clientes enfocado en los parámetros establecidos en el ***Art.10*** de las políticas de administración y gestión de la red, a continuación, se muestra el proceso de configuración:

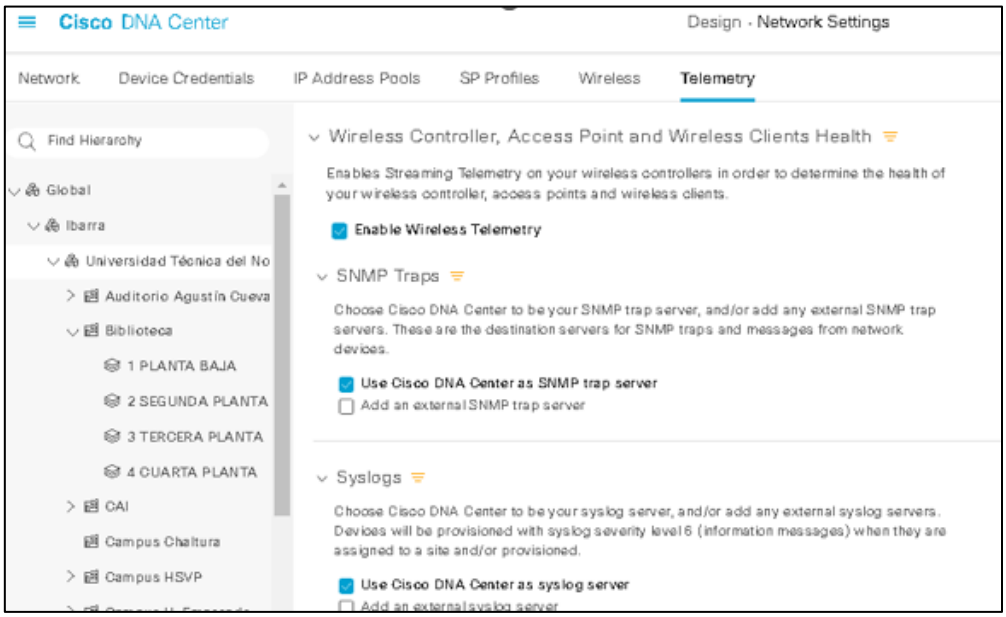
- Design > Network Settings > Telemetry.
- Marque la casilla Cisco DNA Center como servidor de traps SNMP.

- Marque la casilla Agregar un servidor de traps SNMP externo e introduzca la dirección IP del servidor de traps SNMP externo.
- El servidor seleccionado recopila trampas y mensajes SNMP de los dispositivos de red.
- Expanda el área Syslogs si no está visible y realice una de las siguientes acciones:
- Marque la casilla de verificación Utilizar Cisco DNA Center como servidor syslog.
- Marque la casilla Agregar un servidor syslog externo e introduzca la dirección IP del servidor syslog externo.
- Expanda el área NetFlow si no está visible y realice una de las siguientes acciones:
- Seleccione la casilla de verificación Utilizar Cisco DNA Center como servidor de recopilación de NetFlow.
- La configuración de NetFlow en las interfaces del dispositivo sólo se completa cuando habilita la telemetría de aplicaciones en el dispositivo.
- Seleccione el recopilador NetFlow a nivel de sitio para configurar el servidor de destino de NetFlow en el dispositivo.
- Expanda el área Recopilación de datos de clientes cableados y marque la casilla de verificación **Supervisar** clientes cableados.
- Expanda el área Salud de la controladora inalámbrica, el punto de acceso y los clientes inalámbricos y active la casilla Activar telemetría inalámbrica.
- Haga clic en Guardar.

A continuación, en la Figura 154 se muestra la ventana de visualización de configuración de servicios telemetría.

Figura 154

Configuración de telemetría



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

4.1.2.2.3.Proceso de registro de configuraciones

Se tiene el registro de las configuraciones realizadas en el software Cisco DNA Center, donde se registra toda configuración realizada, como agregar un nuevo AP, cambios de direcciones IP, cambios de canal RF, cambio de AP, actualizaciones de firmware entre otras configuraciones en la red inalámbrica que se detallan en el manual de procedimientos de gestión de configuraciones enfocado en los parámetros establecidos en el ***Art.11*** de las políticas de administración y gestión de la red.

Cisco DNA Center cuenta con un registro de configuraciones, el cual permite el registro de la siguiente información:

Hora y fecha: donde se detalla la hora y fecha exacta en el momento que se realizó la configuración.

Descripción: donde se detalla la configuración realizada.

Usuario: de detalla el usuario que realizo la configuración.

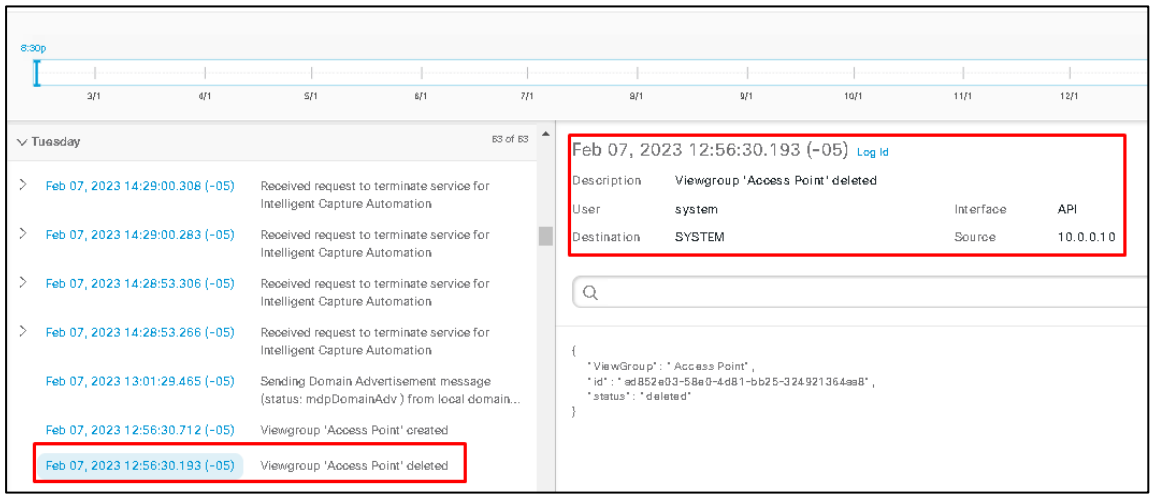
Destino: el equipo en el que se realizó la configuración.

Origen: desde que dirección ip se realizó la configuración.

A continuación, en la Figura 155 se muestra el registro de las configuraciones.

Figura 155

Registro de configuraciones



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Análisis

En el software de gestión Cisco DNA Center cuando se agrega un nuevo equipo a la red inalámbrica es necesario la configuración de los parámetros de configuración del equipo como se especifica en el ***Art.9*** de las políticas de administración y gestión de la red, en cumplimento del requerimiento ***Req.15***, además se realiza la activación de servicios de telemetría para obtener las bases de información gestionable de cada equipo que conforma la red inalámbrica.

A continuación, se presenta el proceso para que un usuario final se conecte a la red del campus universitario:

1. Obtener credenciales de acceso: el usuario final debe obtener un nombre de usuario y contraseña de la institución para poder conectarse a la red.
2. Comprobar la compatibilidad del dispositivo: es importante asegurarse de que el dispositivo que el usuario final desea conectar sea compatible con la red. Esto puede implicar comprobar si el dispositivo tiene un adaptador de red adecuado y si cumple con los requisitos de hardware y software de la red.
3. Configurar el dispositivo: el dispositivo del usuario final debe configurarse correctamente para conectarse a la red. Esto puede implicar la configuración de la dirección IP, el servidor DNS y otros parámetros de red
4. Conectar al SSID de la red: el usuario final debe seleccionar la red Wi-Fi adecuada en su dispositivo y proporcionar las credenciales de acceso. En algunos casos, el usuario puede necesitar aceptar un acuerdo de usuario o una política de uso antes de conectarse a la red
5. Autenticar el usuario: después de conectar a la red, el usuario final debe autenticar su identidad utilizando su nombre de usuario y contraseña. Dependiendo de la configuración de la red, puede ser necesario proporcionar otros detalles, como un número de identificación o una dirección de correo electrónico
6. Acceder a la red: una vez autenticado, el usuario final debería poder acceder a los recursos de la red, como internet, recursos

compartidos, bibliotecas digitales, sistemas de gestión académica, entre otros.

En la topología de red de la Universidad Técnica del Norte, los usuarios finales se conectan a los APs, los cuales a su vez se conectan a la controladora de la red inalámbrica. La controladora está conectada a uno de los switches en la capa de acceso, y en esta conexión se encuentra el equipo Cisco DNA Center, que contiene la WLC. La función principal de la controladora es propagar los SSID (identificadores de red) a los APs como se especifica en el paso número 4. Además, para garantizar la seguridad de la red, el servidor Radius se utiliza para verificar las credenciales de los usuarios. Es importante destacar que la controladora se integra con el servidor Radius a través de Eudoram

Nota: Para la red inalámbrica, es importante incluir en el manual de procedimientos los equipos relevantes, como los Access Points (APs) y el Wireless LAN Controller (WLC).

4.1.2.3. Implementación de políticas de gestión de Contabilidad

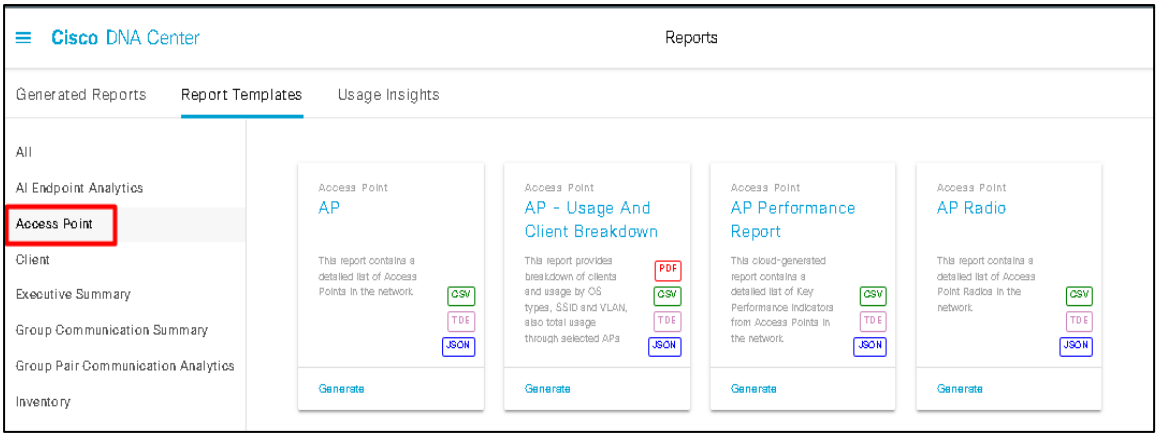
4.1.2.3.1. Reportes

En la implementación de políticas de gestión de contabilidad, enfocado en los parámetros establecidos en el ***Art.17*** de las políticas de administración y gestión de la red, ya que tiene como objetivo principal obtener informes de los recursos actuales de cada uno de los equipos de la red inalámbrica, Cisco DNA Center genera informes donde se muestra datos estadísticos de los recursos y servicios de la red inalámbrica.

En la Figura 156 se muestra la generación de reportes en icono de inicio>reports>generated reports, donde se puede elegir el formato el tipo de reporte que se desea generar.

Figura 156

Tipos reportes para Access Point



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Una vez seleccionado el tipo de reportes se procede a elegirlos siguientes parámetros:

Nombre del reporte

Alcance (reporte individual o todos los APs)

Formato de archivo (CSV, JSON, Tabla de datos)

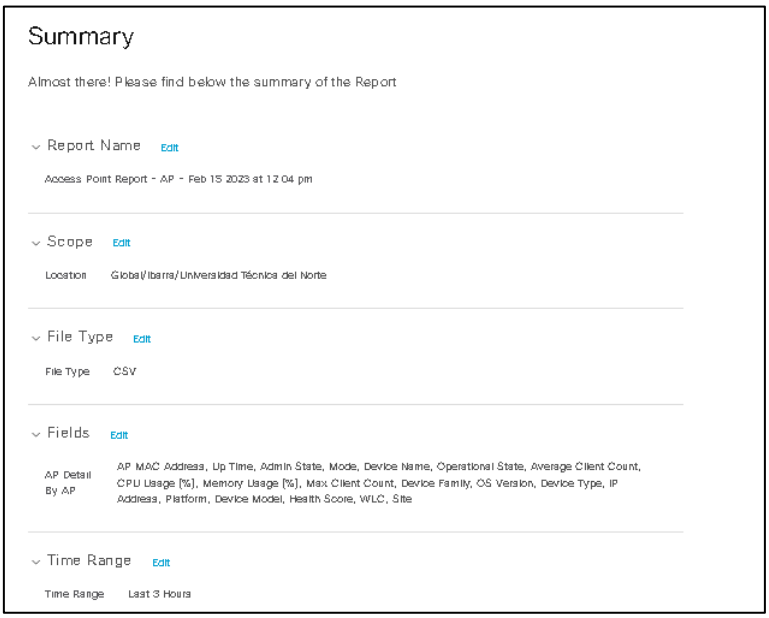
Rango de tiempo (3, 24 Horas, 7 días)

Programar (ejecutar ahora, ejecutar más tarde (una sola vez), ejecutar de forma recurrente)

En la Figura 157 se muestra un resumen de las configuraciones realizadas para la generación de reportes.

Figura 157

Resumen de configuraciones de reportes

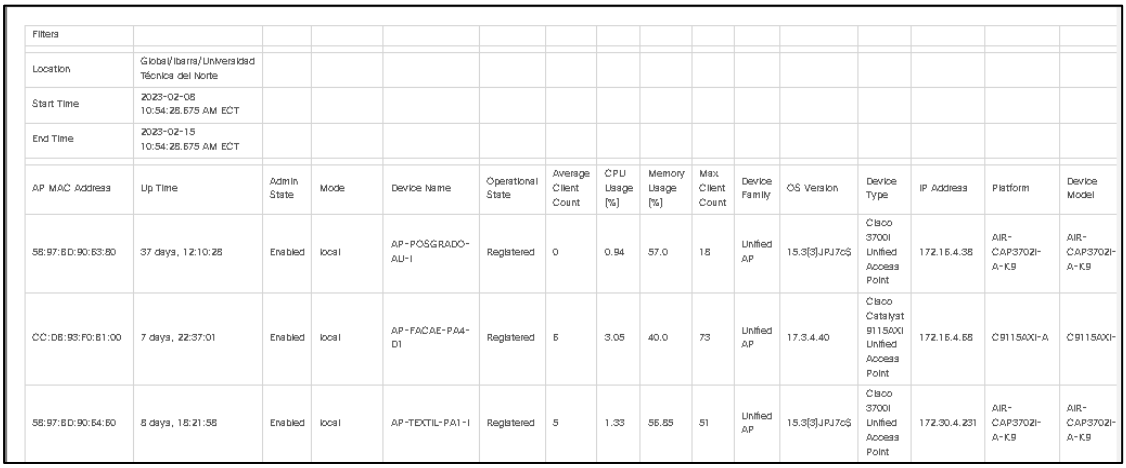


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

En la Figura 158 se muestra la tabla final de reportes generada, donde se puede observar los parámetros de monitoreo de todos los APs que conforman la red inalámbrica de la Universidad Técnica del Norte.

Figura 158

Reporte de APs generado



Filters															
Location	Global/Ibarra/Universidad Técnica del Norte														
Start Time	2023-02-08 10:54:28.575 AM ECT														
End Time	2023-02-15 10:54:28.575 AM ECT														
AP MAC Address	Up Time	Admin State	Mode	Device Name	Operational State	Average Client Count	CPU Usage [%]	Memory Usage [%]	Max Client Count	Device Family	OS Version	Device Type	IP Address	Platform	Device Model
58:97:BD:90:63:80	37 days, 12:10:28	Enabled	local	AP-POSGRADO-AU-1	Registered	0	0.94	57.0	18	Unified AP	15.3[3]JPJ7cS	Cisco 3700I Unified Access Point	172.16.4.38	AIR-CAP3702I-A-K9	AIR-CAP3702I-A-K9
CC:DB:93:F0:B1:00	7 days, 22:37:01	Enabled	local	AP-FACAE-PA4-D1	Registered	5	3.05	40.0	73	Unified AP	17.3.4.40	Cisco Catalyst 9115AXI Unified Access Point	172.16.4.58	C9115AXI-A	C9115AXI-
58:97:BD:90:64:60	8 days, 18:21:58	Enabled	local	AP-TEXTIL-PA1-1	Registered	5	1.33	56.85	51	Unified AP	15.3[3]JPJ7cS	Cisco 3700I Unified Access Point	172.30.4.231	AIR-CAP3702I-A-K9	AIR-CAP3702I-A-K9

Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A demás de los reportes Cisco DNA Center muestra los parámetros de monitoreo en tiempo real accediendo directamente al equipo que se desea verificar los recursos, en la Figura 159 se muestra la ventana de visualización de los recursos del equipo.

- Inventary>network>localitation>AP>divece360

Figura 159

Visualización de parámetros de monitoreo

Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Como herramienta del sistema de gestión Cisco DNA Center, permite la visualización de gráficos estadísticos de hardware de la red inalámbrica de toda la Universidad Técnica del Norte. Para la generación de un nuevo reporte primero se debe escoger una plantilla o sea un ámbito en el cual se quiera generar un reporte, en el ANEXO G se detalla el proceso completo de la generación de nuevo reporte sobre el resumen del cliente.

4.1.2.3.2.Administración de redes en la Universidad Técnica del Norte

Este ítem está relacionado al ***Art.18*** en el cual se establecen las políticas para el ámbito de contabilidad, donde se realiza un estudio estadístico del número de clientes conectados exitosamente a la red inalámbrica, la Universidad Técnica del Norte posee seis redes inalámbricas distribuidas en el campus, donde la red con mayor cantidad de usuarios es

EDUROAM, la cual está diseñada exclusivamente para el brindar acceso a toda la comunidad universitaria, la distribución de redes en el campus universitario se muestra en la Figura 160. En la Tabla 114 se realiza un muestreo del número de usuarios conectados, con la finalidad de contabilizar el número de usuarios por red.

Figura 160

Distribución por nombre de las redes inalámbricas

Network Name (SSID)	SSID Type	L2 Security	L3 Security
DDTI	Enterprise	wpa2_personal	open
eduroam	Enterprise	wpa2_enterprise	None
LAB YUYUCOCHA	Enterprise	wpa2_wpa3_personal	open
WUTN.Admin	Enterprise	open	None
WUTN.Autoridades	Enterprise	wpa2_wpa3_personal	open
WUTN.Docentes	Enterprise	wpa2_wpa3_personal	open
WUTN.Eventos	Enterprise	wpa2_wpa3_personal	open

Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

NOTA: La red inalámbrica que se encuentra en la granja Yuyococha no entra en el análisis de muestreo, ya que el análisis se delimita al campus Universitario y no a sus extensiones.

En la siguiente Figura 161 se evidencia la distribución de las redes en el horario de 7:00am a 9:00am y se encuentran con los siguientes porcentajes de uso:

Red eduroam: 1757 registros con un porcentaje de 88.23%

Red WUTN Eventos: 119 registros con un porcentaje de 6.83%

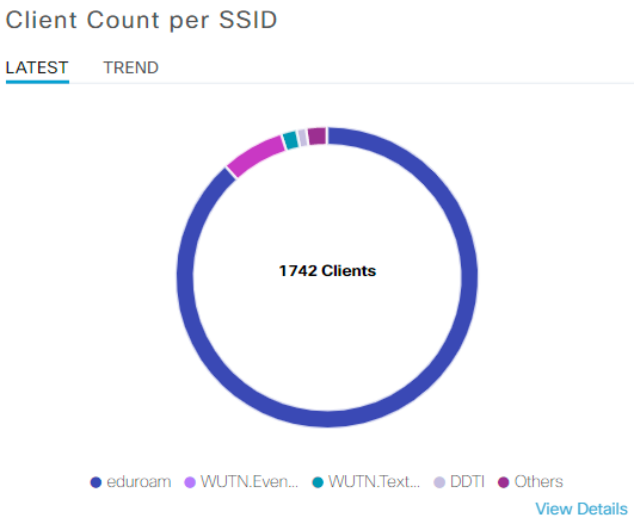
Red DDTI: 18 registros con un porcentaje de 1.03%

Otras Redes: 39 registros con un porcentaje de 2.24%

Todas estas redes suman un total de 1742 clientes que se encuentran conectados a las diferentes redes de la universidad conectados a través del SSID.

Figura 161

Recuento de clientes por SSID

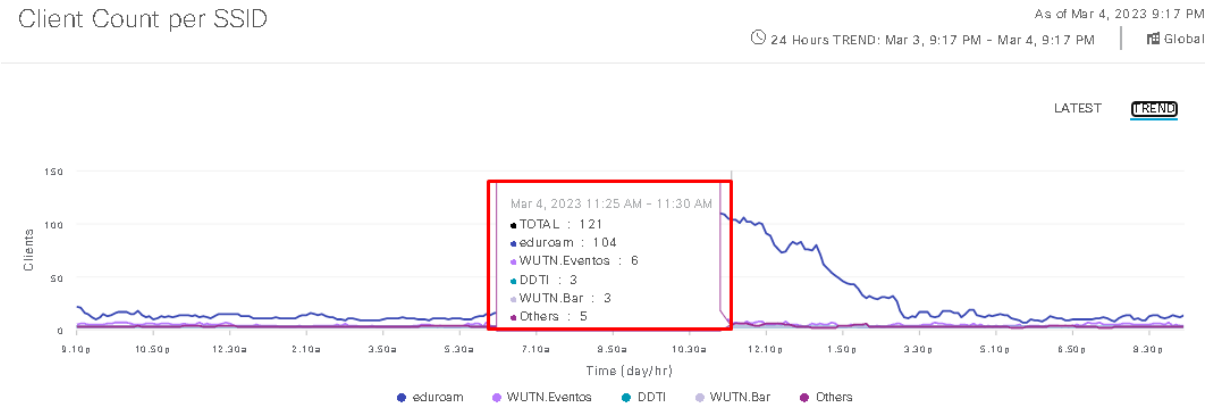


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

La cantidad de usuarios conectados por cada red también es posible visualizar un gráfico tipo histograma como se muestra en la Figura 162.

Figura 162

Muestra de clientes en grafico tipo histograma



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Tabla 114 se procede a realizar un muestreo para determinar un promedio de clientes conectados a las diferentes redes inalámbricas, para esto se ha tomado un numero de muestras en los horarios establecidos entre las 7h00 a 19h00, debido a que en este horario se presenta la mayor cantidad de clientes conectados.

Tabla 114

Muestreo de redes inalámbricas por SSDI

	Lunes 9H00	**Martes 11H00**	**Miércoles 13H00**	**Jueves 14H00**	**Promedio**
DDTI	16	18	18	18	18
EDUROAM	1142	2121	3320	4201	2696
WUTN.Admin	15	23	25	24	22
WUTN.Autoridades	80	100	105	120	101
WUTN.Docentes	252	320	312	400	321
WUTN.Eventos	152	187	189	235	191

Fuente: Elaboración Autor

Como se puede observar en la tabla anterior, se estableció un horario en el que se registra la mayor cantidad de clientes inalámbricos, destacándose la red EDUROAM como la red de uso general para los estudiantes con un promedio de 2696 clientes por semana. No se tuvo en cuenta el viernes debido a que se observó un número reducido de clientes, y hacer un muestreo durante las vacaciones no sería relevante ya que no permitiría estresar la red y determinar su comportamiento

4.1.2.3.3.Monitoreo de estado de conexión

En este ítem se hace mención el ***Art. 19*** que se establece en las políticas dentro del ámbito de gestión de contabilidad, ya que dentro de este ámbito toma como objetivo la visualización de los datos estadísticos de estado de clientes, se ingresa a

Assurance>Health>client, en esta ventana se logra la visualización del estado de conexión de clientes, donde se logra obtener la información como número de clientes de acceso inalámbricos, clientes activos, inactivos y nuevos. En la Figura 163 se muestra la ventana de visualización del estado de conexión de clientes.

Figura 163

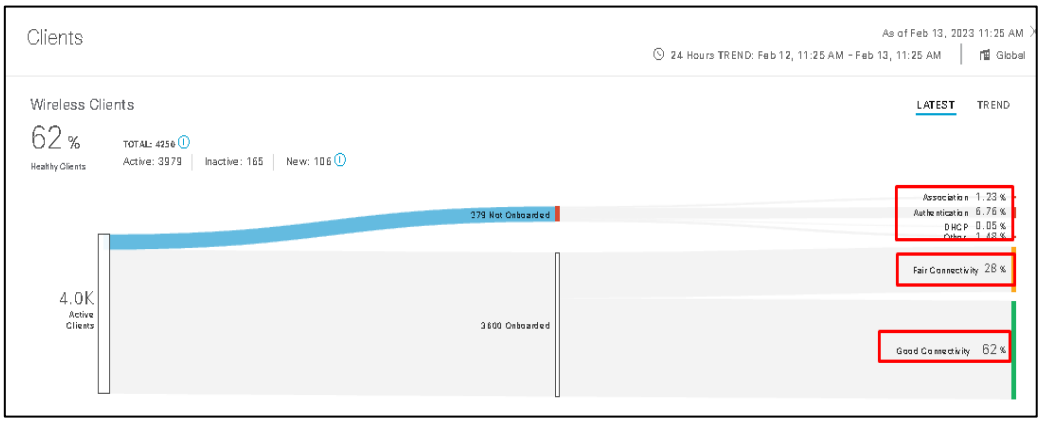
Ventana de visualización del estado de conexión de clientes Wireless

Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

En la Figura 164 se muestra información adicional donde se detalla en porcentaje el número de usuarios autenticados, asociados, clientes dhcp, mala conectividad y buena conectividad.

Figura 164

Información de conexión de cliente inalámbricos



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Análisis

Cisco DNA Center permite la implementación de parámetros de gestión mediante la activación de servicios de telemática en los equipos de red inalámbrica, cumpliendo con los parámetros relacionados al monitoreo remoto de los recursos de la red inalámbrica, donde es posible generar los reportes que contienen los parámetros de los recursos de cada equipo que conforma la red inalámbrica y obtener datos estadísticos que permitan al administrador tener una noción del comportamiento de la red de manera individual y general.

4.1.2.4. Implementación de políticas de gestión de Prestaciones

En la implementación de políticas de gestión de prestaciones, se tiene como objetivo principal cuantificar la información para generar reportes sobre el rendimiento de la red, a continuación, se lista los parámetros principales que permiten obtener el rendimiento de la red:

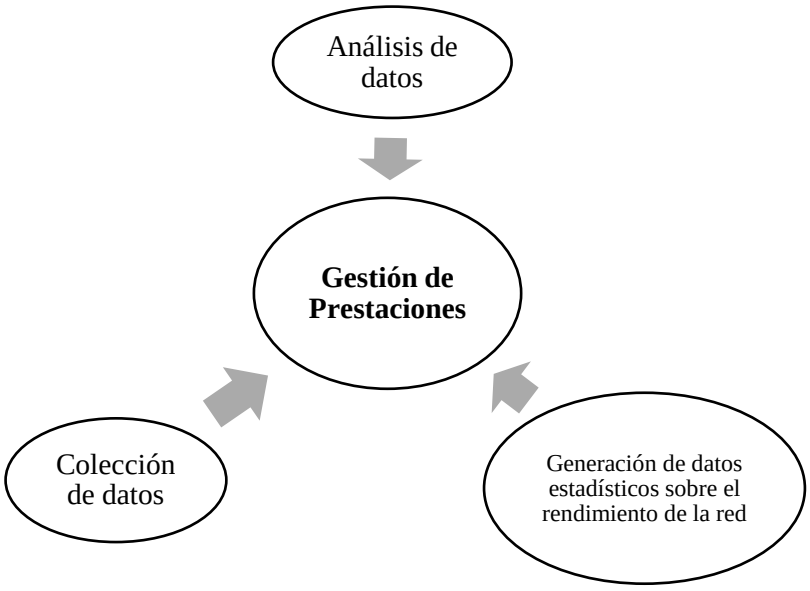
- ✓ Número de usuarios en la red inalámbrica
- ✓ Ssid
- ✓ Intensidad de la señal

- ✓ Canal en uso
- ✓ Frecuencia
- ✓ Cantidad de antenas
- ✓ Relación señal-ruido
- ✓ Velocidad de transmisión

Estos parámetros permiten la creación de reportes de forma textual, estadística e histórica de los recursos de la red inalámbrica, estos datos permiten al administrador conocer el estado de la red em cualquier momento y lograr así la disponibilidad, fiabilidad y funcionamiento correcto de la red. En la Figura 165 se muestra el diagrama propuesto por el modelo de gestión OSI para la gestión de prestaciones.

Figura 165

Diagrama de gestión de prestaciones



Fuente: Elaboración Autor

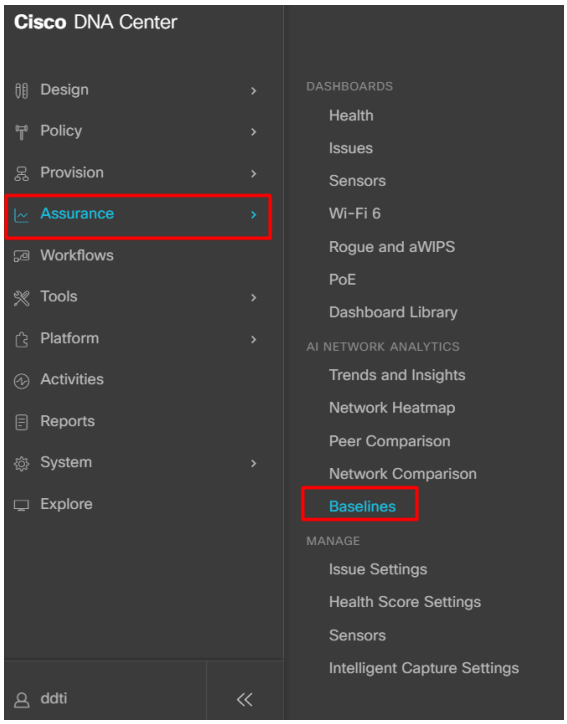
4.1.2.4.1.Métricas de rendimiento

Las métricas de rendimiento son medidas utilizadas para evaluar y cuantificar el desempeño de un sistema, proceso o actividad en relación con un conjunto de objetivos o

estándares. Estas métricas proporcionan información valiosa para medir el rendimiento y evaluar la eficacia, lo cual permite al administrador visualizar información relacionada a el comportamiento de la red inalámbrica y la interacción con los clientes, es decir se visualiza el número de clientes activos, tiempo de asignación de direcciones IP por DHCP, clientes autenticados y el tiempo que tardo en autenticar, clientes asociados y el tiempo de Asociación, estos parámetros logran brindar información relevante para determinar el correcto funcionamiento de la red inalámbrica, por ello este ítem hace referencia al ***Art.15*** establecido dentro de las políticas en el ámbito de la gestión de prestaciones. Para acceder a visualizar los parámetros de chequeo se dirige a MenuCisco>Assurance>Baselines, en la Figura 166 se muestra de manera grafica el acceso a las métricas de rendimiento o línea base de las métricas de utilización.

Figura 166

Acceso a parámetros de chequeo

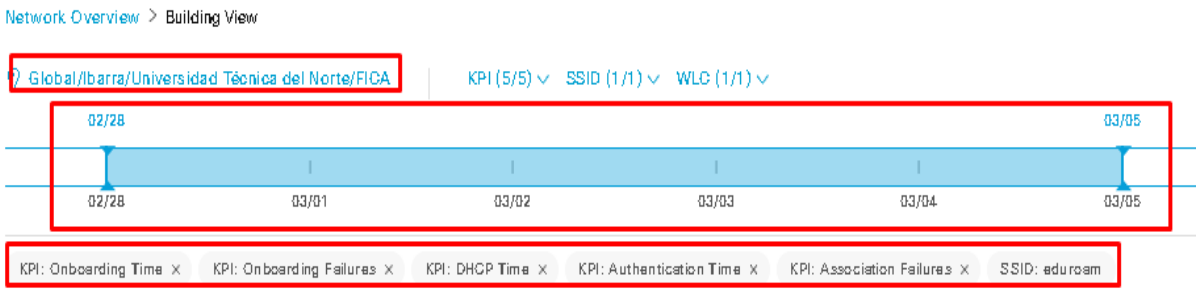


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

En la Figura 167 se muestra el edificio o facultad, los parámetros de chequeo disponibles y el lapso de tiempo en el cual se generarán los datos de chequeo.

Figura 167

Parámetros de chequeo



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

- **Tiempo de asociación**

En tiempo de asociación se puede visualizar el tiempo que han tardado los clientes en formar parte de la red, donde se puede visualizar por edificios y por pisos, en la Figura 168 se muestra la visualización de tiempo de asociación en el edificio de la Fica, donde se puede visualizar el tiempo que tardaron en asociarse a la red EDUROAM, en número de clientes asociados por planta y los tipos de dispositivos asociados.

Figura 168

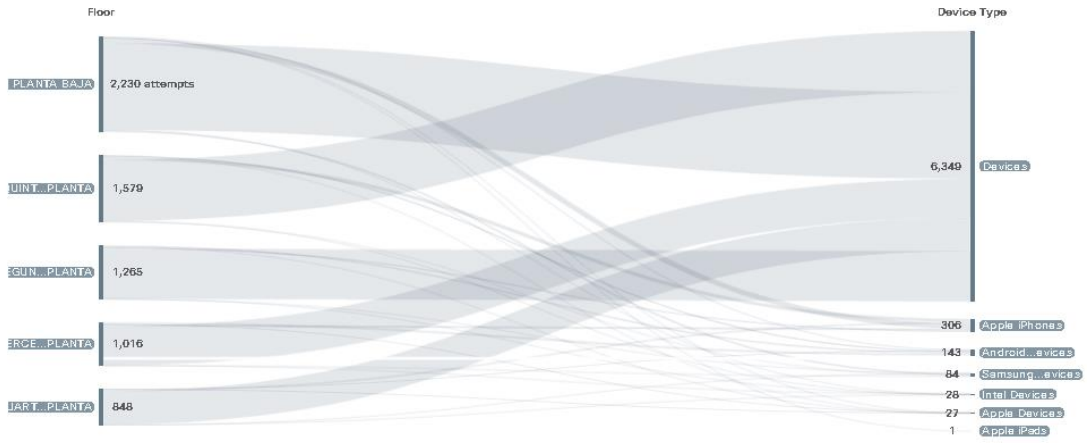
Tiempo de asociación

Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Además, es posible la visualización del número de asociaciones fallidas por edificio y por planta, como se muestra en la Figura 169

Figura 169

Número de asociaciones fallidas



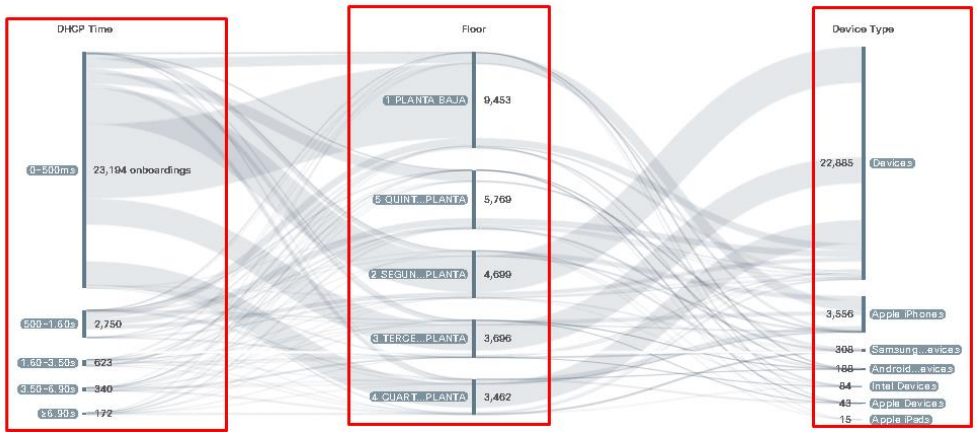
Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

- **Tiempo de asignación de dirección IPv4 por DHCP**

Este parámetro de chequeo permite al administrador de la red, saber el tiempo que ha tardado el servidor DHCP en asignar direcciones IPv4 a los clientes que se asociaron correctamente con la red. En la Figura 170 se muestra el tiempo em microsegundos que se tardó en asignar una dirección IPv4, el número de usuarios asignados dirección ip por piso y el tipo de dispositivo asociado.

Figura 170

Tiempo DHCP



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

- **Tiempo de autenticación**

El tiempo de autenticación muestra a la administración el tiempo que está tardando en realizar la autenticación de credenciales, en la Figura 171 se muestra el tiempo en milisegundos que se tardó en autenticarse, el número de autenticaciones por piso y el tipo de dispositivos que se autentico.

Figura 171

Tiempo de autenticación

Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

4.1.2.4.2.Monitoreo de estado de la red inalámbrica

Para la visualización de los datos estadísticos del estado de la red inalámbrica se da un seguimiento a los procesos de funcionamiento, lo cual hace referencia al ***Art.16*** que se encuentra planteado en las políticas en el ámbito de la gestión de prestaciones, para entender el estado de los recursos de los equipos es necesario conocer los umbrales diseñados para cada uno de los parámetros de monitoreo, en la Tabla 115 se muestran los umbrales establecidos.

Tabla 115

Umbrales para parámetros de monitoreo

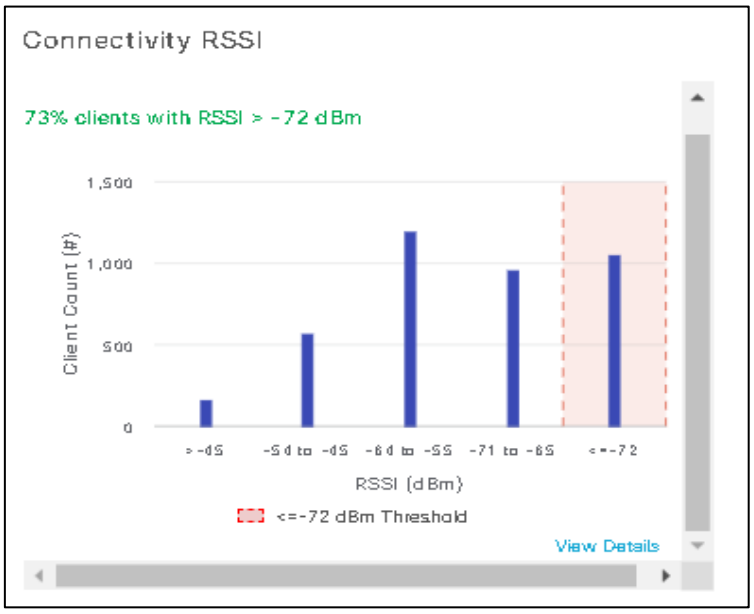
RF Metric	Good (Green)	Fair (Orange)	Poor (Red)
RSSI	> -69 dBm	-69 dBm to -71dBm	< -71 dBm
SNR	> 25 dBm	10dB to 25dB	<10dB
Data Rate	MCS 3, 4, 5, 6, 7, 11 ,12,13,14,15,19, 20, 21, 22, 23	MCS 1, 2, 9, 10, 17, 18 - QPSK	MCS 0,8, 16 - BPSK
Throughput	> 10 Kbps	2 ~ 10 Kbps	< 1Kbps
Packet Retry	y 1 or less	2	3 or above

Fuente: Extraído de (Cisco, 2019) Cisco DNA Assurance

Para acceder a los parámetros de monitoreo se ingresa a Assurance>Health>client, en la Figura 172 se muestra la ventana donde se logra visualizar el estado de conectividad de fuerza de la señal recibida por parte del cliente.

Figura 172

Fuerza de conexión de la señal

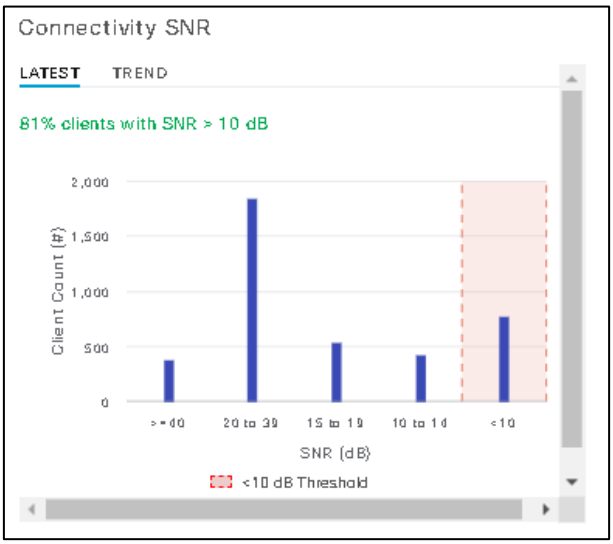


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

En la Figura 173 se muestra estado de conectividad SNR de los clientes, donde se logra apreciar la potencia de la señal con relación al ruido del medio, se muestra en porcentajes el número de clientes y en decibeles (dB) la potencia obtenida. Es importante visualizar este tipo de datos estadísticos que hacen referencia a la conectividad SNR ya que aquí pueden surgir errores de entramado, por cual estos errores de entramado pueden ser el resultado de una línea serial ruidosa, un cable diseñado de manera incorrecta (demasiado largo o blindado en forma inadecuada) o un reloj de línea de unidad de servicio de canal (CSU) configurado de manera incorrecta.

Figura 173

Relación señal ruido de la potencia de la señal

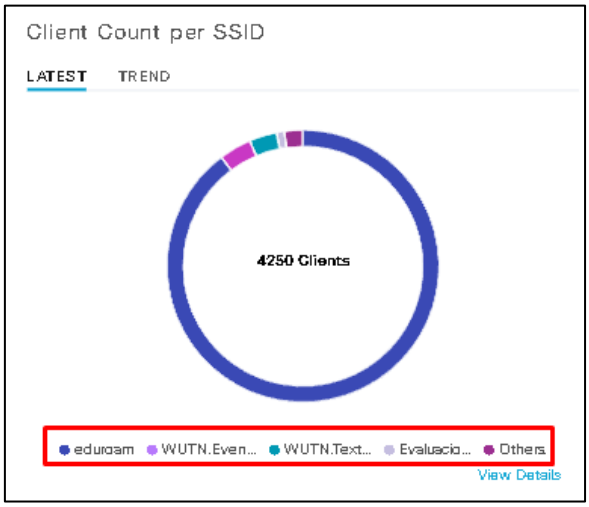


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

En la Figura 174 se muestra el numero de clientes asosciados a un SSID, en la Universidad Tecnica del Norte existe la red Eduroam la cual posee el mayor numero de clientes ya que es la red inalambrica de acceso para estudientes.

Figura 174

Clientes asociados por SSID

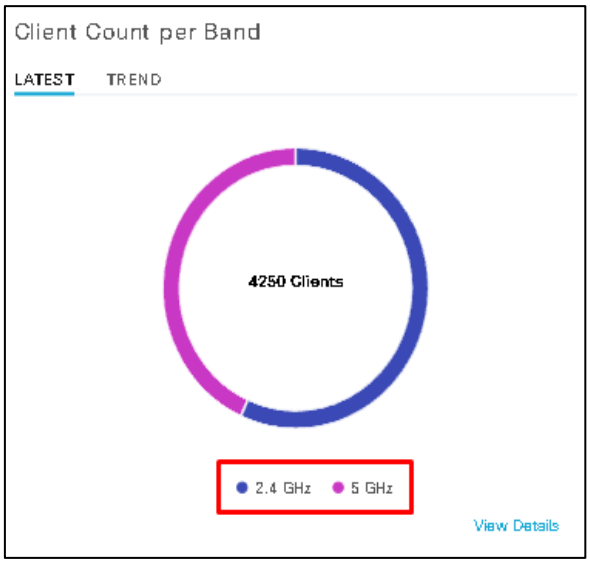


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

En la Figura 175 se muestra en detalle el porcentaje de clientes conectados dependiendo de la radio frecuencia de conexión al AP.

Figura 175

Radio frecuencia de conexión



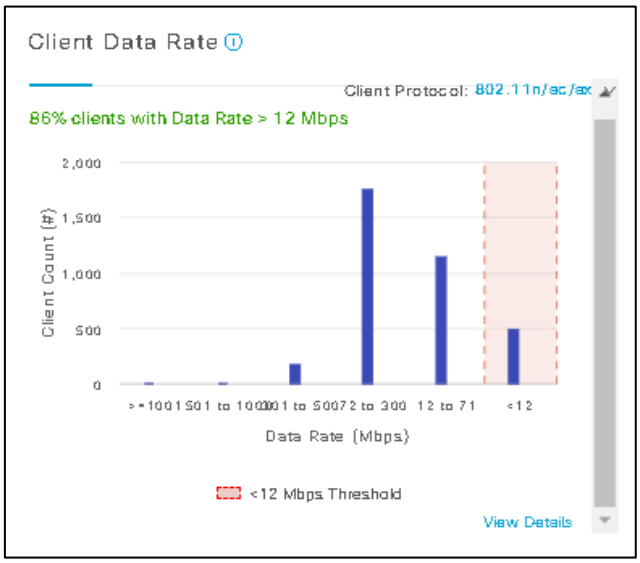
Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

- **Monitoreo del data rate**

La herramienta Cisco DNA Center presenta una opción donde permite al administrador conocer el protocolo de capa de acceso al medio está utilizando y el data rate utilizado, para ello se tiene los protocolos IEEE 802.11n/ac/ax, donde existe un data rate > 12Mbps para el 86% de los clientes, tal y como se visualiza en la Figura 176.

Figura 176

Visualización del data rate

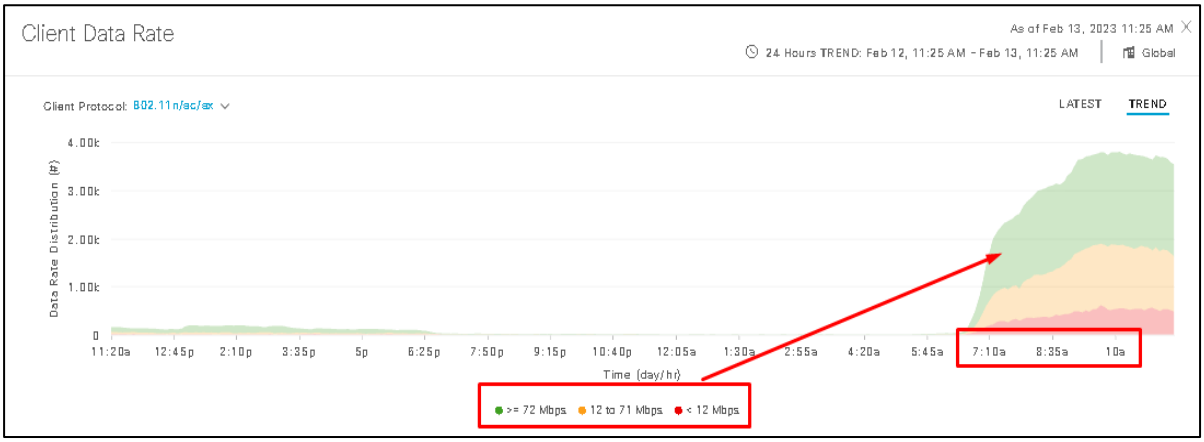


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Para obtener una visualización más detallada, se puede acceder a 'View Detail' en la esquina inferior derecha, donde se puede observar una gráfica tipo histograma que muestra el data rate utilizado. La gráfica utiliza diferentes colores para facilitar la identificación de cada tipo de data rate En la Figura 177 se muestra el data rate de la red inalambrica detallada.

Figura 177

Histograma de data rate de la red inalámbrica



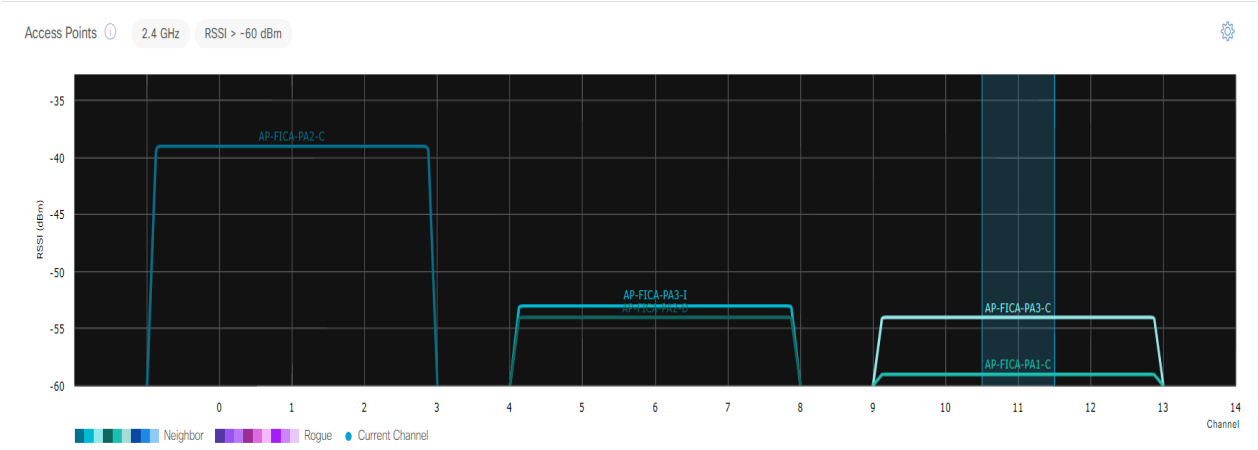
Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

- **Monitoreo de canales de radio**

La herramienta Cisco DNA Center presenta una opción donde permite al administrador conocer los diferentes canales de radio activos en el medio, permitiendo observar de manera grafica la distribución de canales de radio existentes, para la asignación de canales de radio en caso de existir interferencia y realizarlo manualmente, en la Figura 178 se muestra los canales de radio activos.

Figura 178

Canales de radió

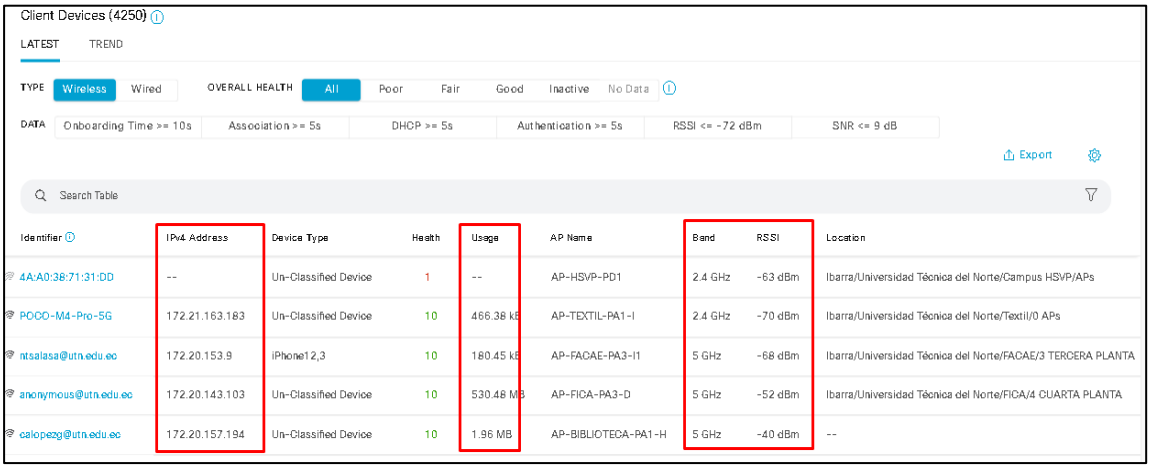


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Además, Cisco DNA Center permite la visualización más detalla del consumo de recursos de la red, en este apartado se puede observar detalladamente la identificación de cada cliente conectado, dirección ip, tipo de dispositivo conectado, consumo de datos, ap está conectado, frecuencia, potencia de señal y la ubicación de conexión. En la Figura 179 se muestra la ventana de visualización de la descripción de cada usuario.

Figura 179

Ventana de visualización de los detalles de conexión de cada cliente



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Análisis

Cisco DNA Center permite la recolección de determinados parámetros correspondientes a los recursos de los equipos de la red inalámbrica, con la activación de servicios de telemetría, como se especifica en el ***Art.15*** de las políticas de administración y gestión de la red, conjuntamente con los requerimientos operacional del sistema de gestión que abarcan los criterios de monitoreo remoto, donde es posible la visualización estadística de manera grafica de los recursos de la red, donde el administrador puede acceder a los datos estadístico en tiempo real de cada equipo o a su vez de manera general y verificar la disponibilidad de la red, observando cómo se comportan los recursos de los equipos en funcionamiento y con alta cantidad de clientes.

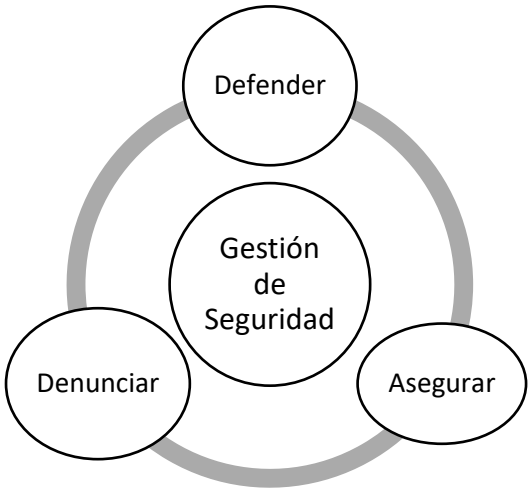
4.1.2.5. Implementación de políticas de gestión de Seguridad

Para la implementación de políticas de gestión de seguridad, su objetivo es garantizar la confidencialidad, integridad y disponibilidad de los datos en la red inalámbrica, encaminados por el ***Art.22*** de las políticas de administración y gestión de la red, la cual

propone un ciclo de seguridad de gestión activa. En la Figura 180 se muestra el ciclo de seguridad de gestión activa.

Figura 180

Gestión de seguridad



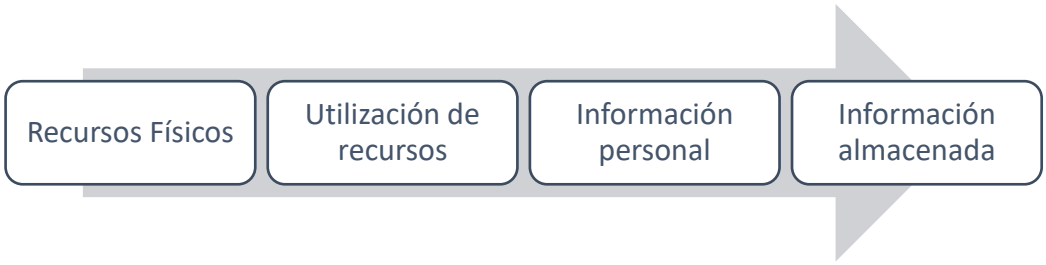
Fuente: Elaboración Autor

4.1.2.5.1.Gestión de seguridad activa

La gestión de seguridad activa representa los recursos que posee la Universidad Técnica del Norte para mantener la integridad de la red inalámbrica, donde se especifica los accesos posibles de usuarios al sistema de gestión Cisco DNA Center y los privilegios de nivel. A continuación, en la Figura 181 se muestra el proceso de seguridad activa.

Figura 181

Procesos de seguridad activa

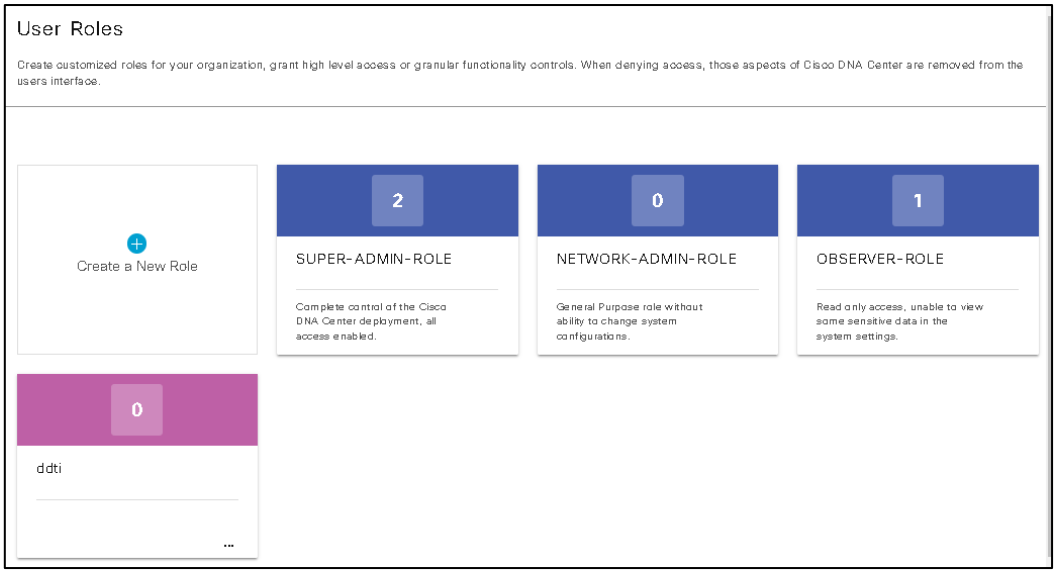


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

La gestión de seguridad se encarga de manejar el acceso al sistema de gestión Cisco DNA Center, por lo que se determina la creación de cuatro tipos de roles de usuarios los cuales poseen diferentes privilegios, para lo cual se debe ingresar en system>users&roles>Role based Access control. En la Figura 182 se muestra los tipos de roles creados.

Figura 182

Roles de usuario



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

En la Tabla 116 se muestra el rol y el nivel de privilegio que posee cada uno.

Tabla 116

Roles de Usuario

ROL	PRIVILEGIO
SUPER-ADMIN-ROLE	Control completo de la implementación de Cisco DNA Center, todos los accesos habilitados
NETWORK-ADMIN-ROLE	El administrador de red tiene acceso a todos los aspectos de control de red de Cisco DNA Center con la exclusión del sistema y el área de la plataforma de desarrollo

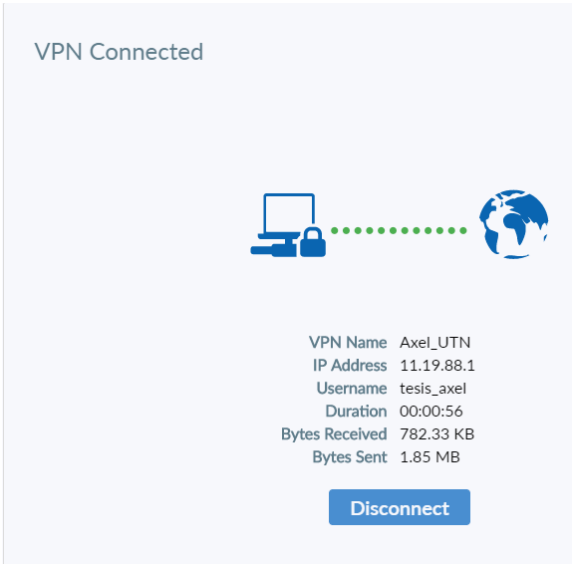
OBSERVER-ROLE	Observer puede ver todos los aspectos de Cisco DNA Center, pero no tiene acceso de escritura.
DDTI-ROLE	Puede configurarse los accesos dependiendo del requerimiento.

Fuente: Elaboración Autor

Para acceder de manera remota a Cisco DNA Center se puede realizar a traves de VPN FortiClient, el cual proporciona mayor seguridad en la coneccion a traves de internet, en la Figura 183 se muestra el estado de coneccion de la VPN, el manual para establecer la conexión remota a traves de la VPN a la red de la Universidad Técnica del Norte de detallara en el ANEXO H.

Figura 183

Conexión remota mediante VPN

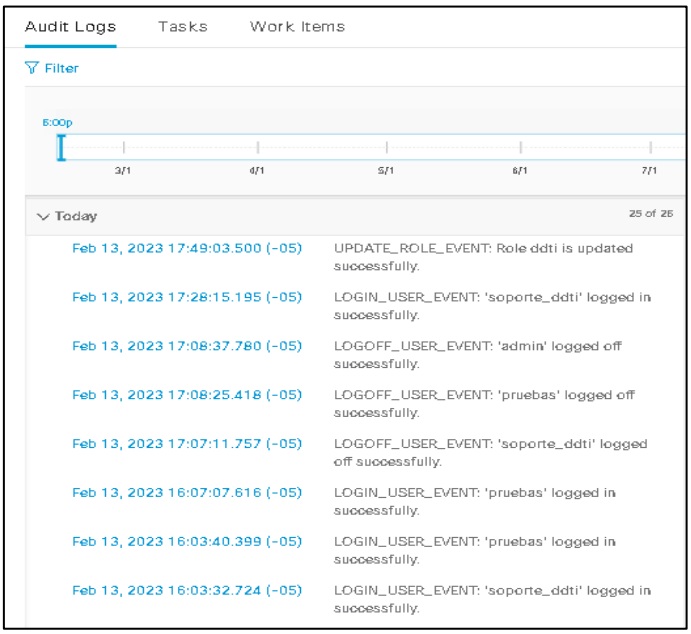


Fuente: Elaboracion Autor

Cisco DNA Center ofrece la herramienta de registro de logs, donde se puede monitorear el usuarios, hora y fecha de cada log que se realizó y el estado, en la Figura 184 se muestra la ventana de visualización de log.

Figura 184

Registro de logs



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Análisis

Cisco DNA Center posee tres roles de usuario y la creación de roles que se adaptarían a las necesidades de a quien vaya dirigido el rol, como se plantea en el ***Art.17*** de las políticas de administración y gestión de la red y el requerimiento ***Req.11*** que se establece en los requerimientos para la red Inalámbrica. Además de proporcionar la seguridad a los clientes finales asignando un método único de autenticación en la red inalámbrica, permitiendo que la red inalámbrica sea más robusta, evitando el acceso indebido a la red que pueda comprometer algún equipo de red. Cisco DNA Center con el registro le logs permite al administrador con mayor privilegio poder saber hora y fecha que los usuarios que accedieron a el Software de gestión y las acciones que realizaron en el caso de poseer permiso de escritura.

5. MANUAL DE PROCEDIMIENTOS Y PRUEBAS

5.1. Introducción

Para el presente capítulo se presentan los manuales de procedimientos estructurados en base a cada área funcional del estándar de gestión de red funcional basados en el estándar ISO, dichos manuales deberán ser utilizados por el personal encargado de la administración de la red, con la finalidad de diagnosticar y corregir problemas de manera más optimo.

El Manual de Procedimientos es una guía base que permite al administrador seguir procesos o pasos para brindar soluciones inmediatas ante cualquier fallo presentado en la red de la Universidad Técnica del Norte, dicho manual describe procesos que se trabajan en cada área del Modelo Funcional FCAPS de la ISO, todo aquello con el objetivo de gestionar y administrar los recursos de la red, mediante el uso de las herramientas que brinda el software de gestión Cisco DNA Center, para así lograr tener una red funcional en todo momento.

5.2. Manual De Procedimiento Para La Gestión FCAPS De Red Cableada

5.2.1. Manual de Procedimientos para la gestión de Configuraciones

<table>
<tr><td colspan="3">UNIVERSIDAD TÉCNICA DEL NORTE</td></tr>
<tr><td colspan="3">POLÍTICAS DE ADMINISTRACIÓN Y GESTIÓN PARA LA RED INALÁMBRICA Y CABLEADA DE LA UTN</td></tr>
<tr><td rowspan="5"></td><td>Elaborado por:</td><td>Axel Almeida</td></tr>
<tr><td>Revisado por:</td><td>Ing. Vinicio Guerra, Administrador de red</td></tr>
<tr><td>Aprobado por:</td><td>Ing. Jorge Caraguay, Director de DDTI</td></tr>
<tr><td>Versión:</td><td>1.0</td></tr>
<tr><td>Fecha:</td><td>22/03/2023</td></tr>
</table>

Objetivo. – Mostrar el procedimiento a seguir al momento de incorporar un dispositivo a la red, realizando las respectivas configuraciones del equipo.

Alcance. – Este manual esta realizado para incorporar nuevos ingresos de nuevos dispositivos en la red cableada de la Universidad Técnica del Norte, la configuración que se realizara a los equipos de red se encontrara presente en el manual desde el día que entre en vigor.

Descripción del Procedimiento

En los ***Artículos 7, 8, 9, 10, 11, 12, 13, 14*** se realiza todo un proceso para obtener disponibilidad de información relativa al diseño y configuración de la red, dicho proceso a seguir se describe en la siguiente Tabla 117 donde se muestra las actividades que comprenden el manual de procedimientos para la gestión de configuraciones.

Tabla 117

Procedimiento para la gestión de configuraciones.

Nº	**ACTIVIDAD**	**DESCRIPCIÓN**	**RESPONSABLE**
1	Ingreso de equipos	1) Verificación del equipo a ingresar a la red. 2) Definir el tipo de equipo: Switchs, APs, Firewall, Servidor, Controladora	Asistente de Redes y Comunicaciones
2	Configuración de equipos	1) Realizar las configuraciones necesarias en el equipo: • Configuraciones básicas de seguridad.	Asistente de Redes y Comunicaciones

		• Configuraciones de protocolos, habilitación del protocolo SNMP, tiempos de monitoreo en el protocolo SNMP y selección de versión SNMP que se elija. • Selección de las credenciales de lectura o escritura para el dispositivo a agregar a la red. • Selección del protocolo de comunicación en el dispositivo a gestionar, teniendo en cuenta que siempre será el protocolo SSH que se escoja. 2) Registro del nuevo dispositivo en el inventario de la herramienta phpIPAM, teniendo en cuenta la siguiente información: • Nombre del equipo • Dirección IP • Tipo de Dispositivo • Ubicación del equipo • Descripción del equipo: Fecha de ingreso, marca y modelo.	

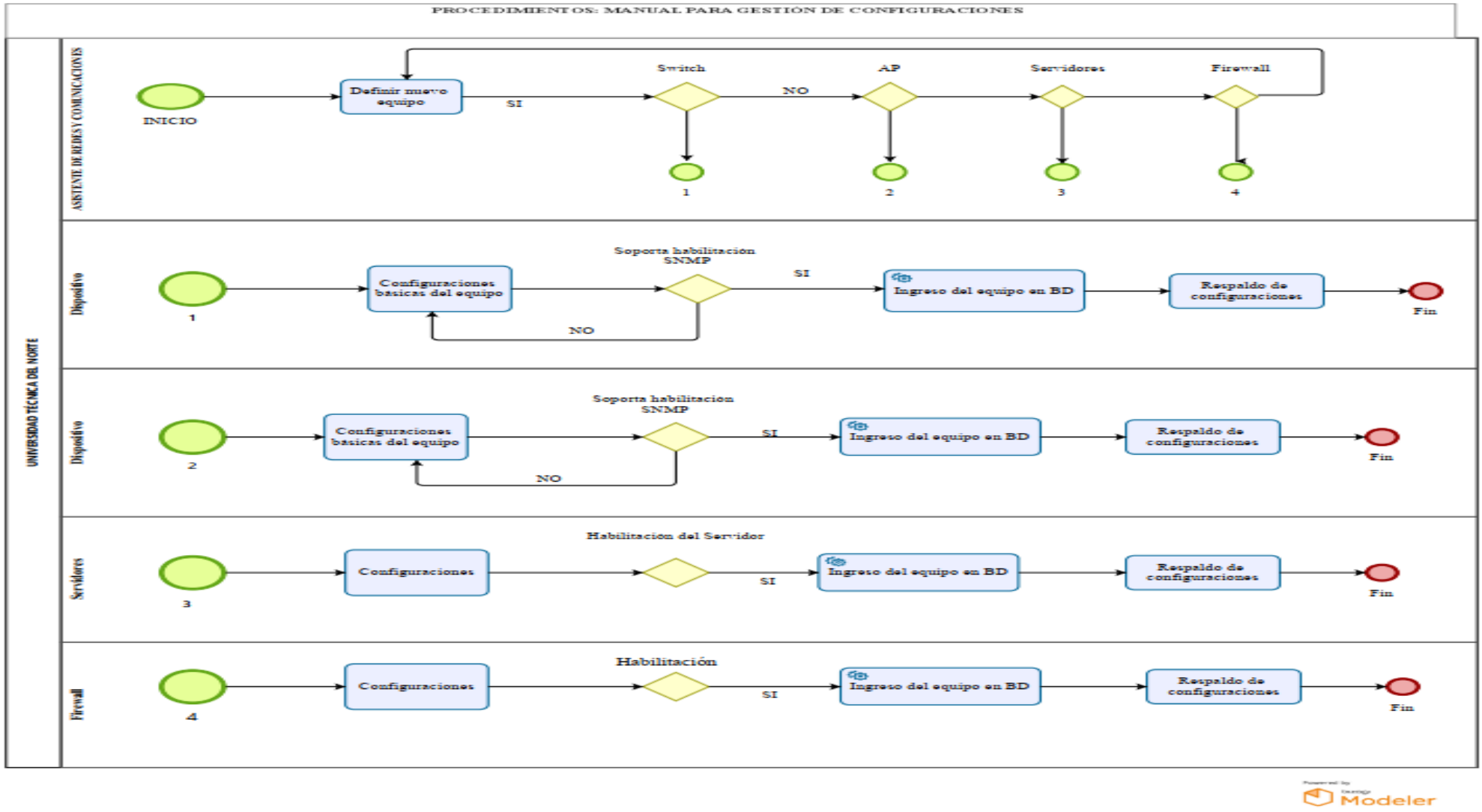
		Nota: El ANEXO K muestra la información para poder registrar el dispositivo en la herramienta phpIPAM.	
3	Documentación de configuraciones	1) Realizar respaldos de las configuraciones que se realicen en los dispositivos gestionados. 2) Si se realizan cambios a nivel de infraestructura(ubicación) y cambios a nivel lógico(configuraciones) realizar la actualización en la base de datos. 3) Registrar los cambios realizados en los dispositivitos gestionados en la plantilla propuesta en el ANEXO F. 4) Realizar el respectivo respaldo de la información actualizada de la base de datos en el cloud institucional del administrador de red.	Asistente de Redes y Comunicaciones

Flujograma

En la Figura 185 se presenta el flujograma que explica el procedimiento para la gestión de configuraciones.

Figura 185

Procedimiento grafico del proceder para la gestión de configuraciones



5.2.2. Manual de Procedimientos para la gestión de Fallos

<table>
<tr><td colspan="3">UNIVERSIDAD TÉCNICA DEL NORTE</td></tr>
<tr><td colspan="3">POLÍTICAS DE ADMINITRACIÓN Y GESTIÓN PARA LA RED IMABLAMBRICA Y CABLEADA DE LA UTN</td></tr>
<tr><td rowspan="5"></td><td>Elaborado por:</td><td>Axel Almeida</td></tr>
<tr><td>Revisado por:</td><td>Ing. Vinicio Guerra, Administrador de red</td></tr>
<tr><td>Aprobado por:</td><td>Ing. Jorge Caraguay, Director de DDTI</td></tr>
<tr><td>Versión:</td><td>1.0</td></tr>
<tr><td>Fecha:</td><td>22/03/2023</td></tr>
</table>

Objetivo. – Mejorar los tiempos de respuesta ante problemas que se presenten en la red cableada, todo esto mediante el proceso de detección, asilamiento y solución de fallos.

Alcance. – Este manual va dirigido a todos los dispositivos gestionados de la red, ya que trabajan con umbrales de funcionamiento, dichos umbrales permiten determinar si el dispositivo funciona correctamente y por ende está gestionando los recursos de la red de manera óptima. Identificar y analizar la causa de una falla es esencial para restaurar el servicio del dispositivo de manera oportuna.

Conocer los fallos con sus respectivos niveles de prioridad ayudara a dar un seguimiento y solución a cualquier eventualidad que se suscite en los dispositivos gestionados de la red. Los fallos resueltos se documentarán junto con sus respectivas soluciones, con el fin de que cualquier falla futura pueda ser abordada siguiendo el procedimiento de solución correspondiente, lo que permitirá reducir el tiempo de respuesta.

Descripción del Procedimiento

En los ***Artículos 3, 4, 5 y 6*** que se establecen en las políticas del ámbito de fallos, se engloba las actividades descritas en la Tabla 118, donde se muestra las actividades que comprenden el manual de procedimientos para la gestión de fallos.

Tabla 118

Procedimiento para la gestión de fallos.

Nº	**ACTIVIDAD**	**DESCRIPCIÓN**	**RESPONSABLE**
1	Detección del Fallo	1) Monitoreo constante de la red y sus alertas. 2) Revisión constante de las alertas y notificaciones que envía el software de gestión.	Asistente de Redes y Comunicaciones
2	Aislamiento y diagnóstico del fallo	1) Identificar qué tipo de fallo 2) Analizar el problema. Cisco DNA Center permite establecer niveles de prioridades a los problemas que se suscitan en la red, los cuales son: Rojo(P1): Un problema crítico que necesita atención inmediata. Naranja(P2): Problema grave que puede afectar a varios dispositivos o clientes. Negro(P3): Problema localizado o mínimo.	Asistente de Redes y Comunicaciones

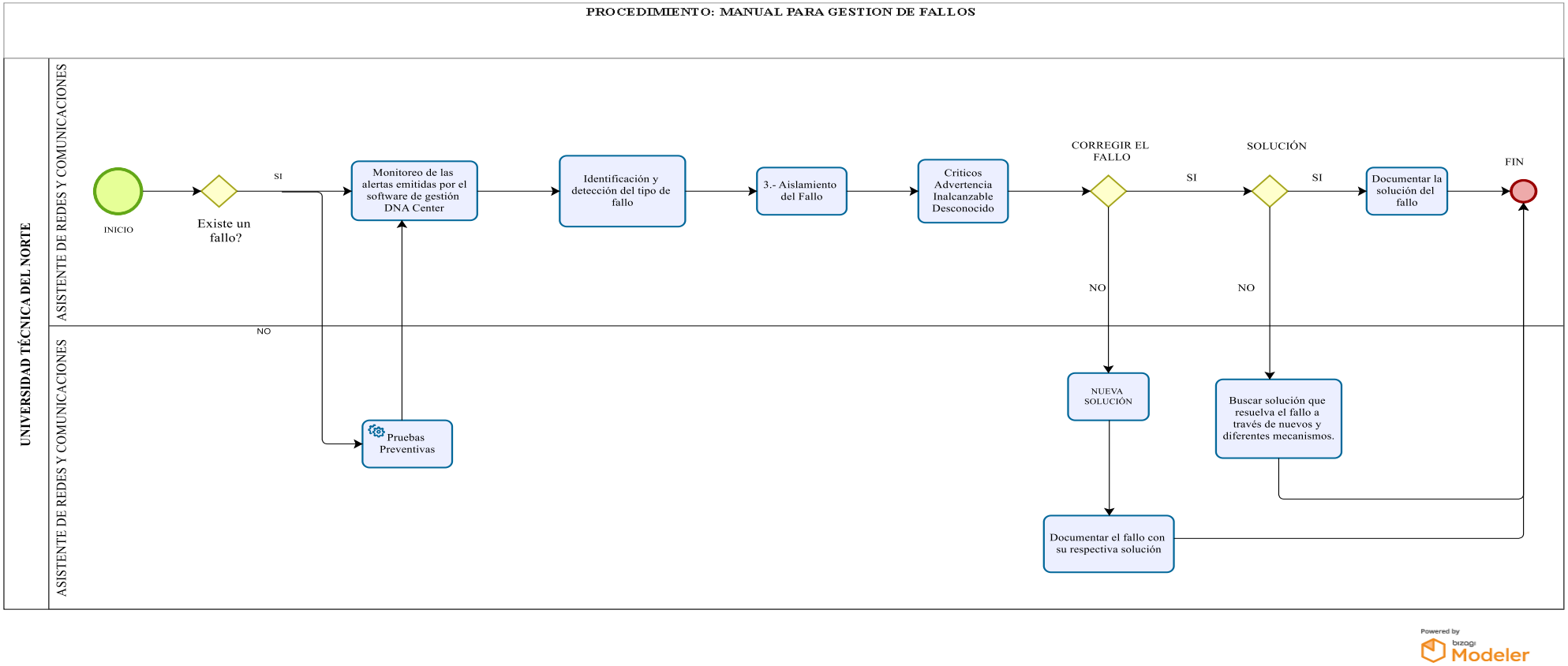
		Negro(P4): Problema de advertencia.	
3	Corrección del fallo	1) Determinar el fallo, ya sea este que haya sobrepaso de los umbrales del equipo o problemas que pueden ser resueltos por software de gestión mediante sus herramientas. 2) Para ciertos fallos que se presenten en la red y no puedan ser resueltos por medio del software de gestión, se realizara la respectiva inspección técnica por parte del personal encargado. 3) Corregir el fallo presentado en la red. 4) Realizar un respaldo previo de las configuraciones, lo cual permitira mantener la integridad de la topología de la red, todo aquello antes de proceder a corregir el fallo presentado. 5) Ver la base de datos para la gestión de fallos en el ANEXO K.	Asistente de Redes y Comunicaciones
4	Documentar solución de fallo	1) Documentar el fallo ocurrido 2) La solución del problema al fallo será detallado según la plantilla establecida en el ANEXO E.	Asistente de Redes y Comunicaciones

Flujograma

En la Figura 186 se presenta el flujograma que ilustra de manera gráfica los procedimientos necesarios para llevar a cabo la gestión de fallos.

Figura 186

Procedimiento grafico del proceder para la gestión de fallos



5.2.3. Manual de Procedimientos para la gestión de Contabilidad

UNIVERSIDAD TÉCNICA DEL NORTE		
POLÍTICAS DE ADMINITRACIÓN Y GESTIÓN PARA LA RED IMABLAMBRICA Y CABLEADA DE LA UTN		
	Elaborado por:	Axel Almeida
	Revisado por:	Ing. Vinicio Guerra, Administrador de red
	Aprobado por:	Ing. Jorge Caraguay, Director de DDTI
	Versión:	1.0
	Fecha:	22/03/2023

Objetivo. – Presentar el procedimiento a seguir sobre la recopilación y análisis de la información que genera el rendimiento de la red y los recursos gestionados de los dispositivos.

Alcance. – Este manual presenta los procesos a seguir sobre el constate monitoreo y la recolección de información sobre el tráfico que genera la red, todo ello a través de la generación y obtención de reportes que el software de gestión brinda, ya que este supervisa la utilización de los recursos, realiza un seguimiento de los problemas y recursos de dicha red. Se debe tener en cuenta que este ámbito de gestión se relacióna con la gestión de fallos, ya que se determina el comportamiento en diversos aspectos de la red para luego tomar decisiones asertivas de acuerdo con los resultados generados en los reportes por parte del administrador de red.

Descripción del Procedimiento

Los ***Artículos 17 y 19*** abarcan el proceso de generación de reportes para el establecimiento del estado actual de la red, en la siguiente Tabla 119 se muestra las actividades que comprenden el manual de procedimientos para la gestión de contabilidad.

Tabla 119

Procedimiento para la gestión de contabilidad.

Nº	**ACTIVIDAD**	**DESCRIPCIÓN**	**RESPONSABLE**
1	Interfaz Cisco DNA Center	1) A través del uso del interfaz del software de gestión se puede visualizar de manera gráfica y estadísticamente el desempeño a nivel de capas y a nivel de dispositivos. Los siguientes indicadores se tomarán en cuenta al momento de generar un reporte: • Alcance (reporte individual o general). • Formato de archivo (CSV, JSON, Tabla de datos) • Rangos de tiempos (3, 24 horas o 7 dias). • Programar (ejecutar ahora, ejecutar más tarde (una	Asistente de Redes y Comunicaciones

		sola vez), ejecutar de forma recurrente). • Disponibilidad porcentual. • Estado de administración. • Estado de interfaces. • Tiempos de actividad	
2	Generación de reportes	1) Cisco DNA Center permite generar diferentes tipos de reportes según la necesidad del administrador de la red, dicha generación de reportes se encuentra en el ANEXO G. 2) Los reportes se generarán por parte del Asistente de Redes y Comunicaciones, se mantendrán de manera digital, ya que se los alojará en una carpeta que será designada por el Analista de Redes y Comunicaciones.	Analista de Redes y Comunicaciones y Asistente de Redes y Comunicaciones
3	Reportes con relevancia	1) Los reportes de mayor relevancia, que genere el Analista de Redes y Comunicaciones, deberán ser evaluados para posteriores análisis o pronósticos.	Analista de Redes y Comunicaciones y Asistente de Redes y Comunicaciones

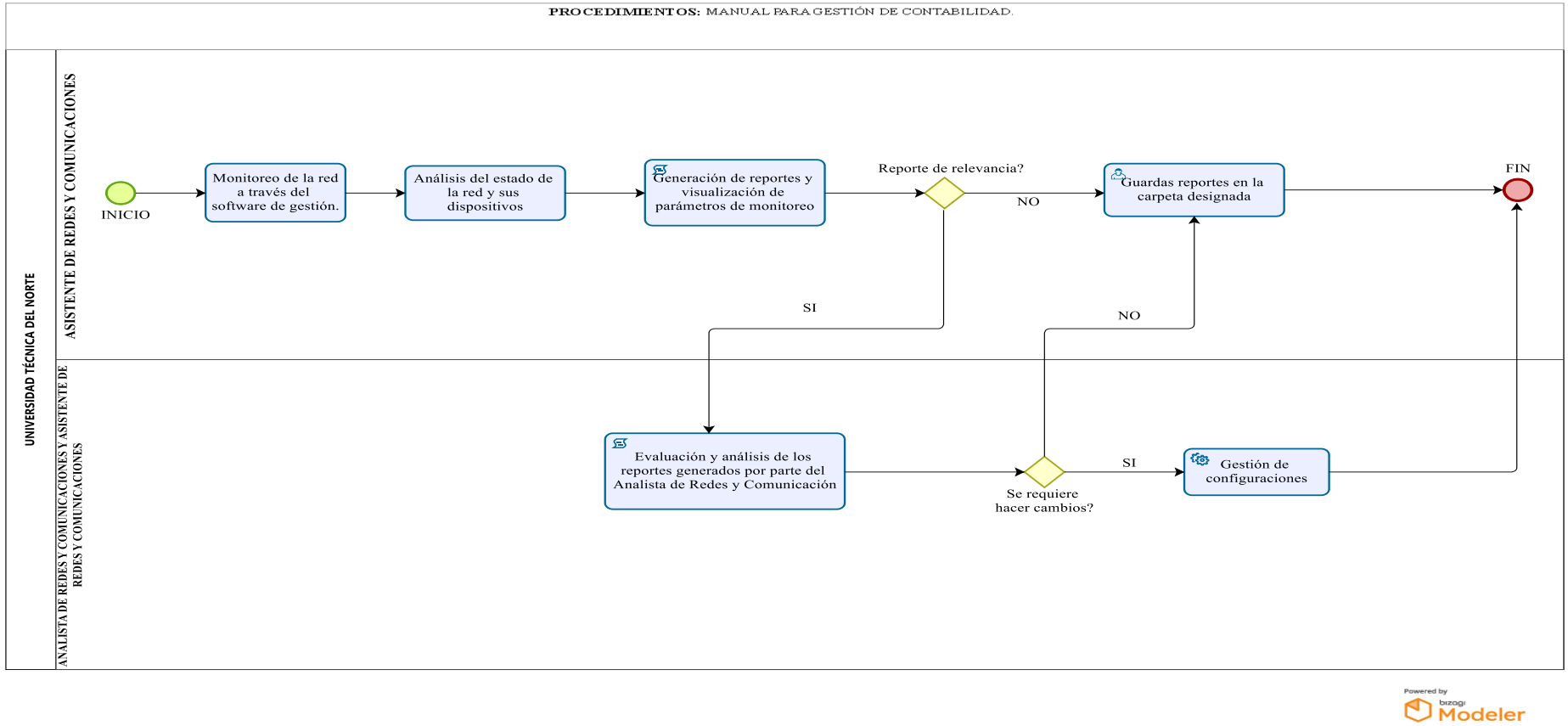
		2) De acuerdo con el resultado obtenido sobre el reporte se tomarán decisiones concretas. 3) Dependiendo cual sea el resultado del reporte generado, se procederá a realizar el proceso de gestión de configuraciones.	

Flujograma

En la Figura 187 se presenta un flujograma que explica de manera gráfica el procedimiento para la gestión de contabilidad.

Figura 187

Procedimiento grafico del proceder para la gestión de contabilidad



5.2.4. Manual de Procedimientos para la gestión de Prestaciones

UNIVERSIDAD TÉCNICA DEL NORTE		
POLÍTICAS DE ADMINITRACIÓN Y GESTIÓN PARA LA RED IMABLAMBRICA Y CABLEADA DE LA UTN		
	Elaborado por:	Axel Almeida
	Revisado por:	Ing. Vinicio Guerra, Administrador de red
	Aprobado por:	Ing. Jorge Caraguay, Director de DDTI
	Versión:	1.0
	Fecha:	22/03/2023

Objetivo. – Dar a conocer el procedimiento sobre la visualización y obtención de parámetros de monitoreo de los dispositivos gestionados que se encuentran en la red, todo ello con la finalidad de tener un conocimiento constante sobre el desempeño de la red.

Alcance. – Dicho manual presenta los procesos para obtener y dar un seguimiento a los recursos que son gestionados por los dispositivos de red, ya que la gestión de prestaciones implica varias tareas que ayudan a dar un mayor tiempo de funcionalidad, disponibilidad del servicio, mediante la recopilación de datos estadísticos sobre el procesamiento de información que permite obtener una correcta medición de los parámetros de utilización de los dispositivos que se encuentran en la red.

Descripción del procedimiento

Los ***Artículos 15 y 16*** establecidos en las políticas en el ámbito de prestaciones, ayudaran al administrador a dar un total seguimiento de los recursos activos de la red, lo cual permitirá conocer parámetros de monitoreo de los dispositivos gestionados, por ende, en la

siguiente Tabla 120 se muestra las actividades que comprenden el manual de procedimientos para la gestión de prestaciones.

Tabla 120

Procedimiento para la gestión de prestaciones

Nº	**ACTIVIDAD**	**DESCRIPCIÓN**	**RESPONSABLE**
1	Verificación de las características técnicas de los dispositivos gestionados.	1) Revisar las características técnicas (datasheet) de los dispositivos gestionados por el software de monitoreo. 2) Establecer parámetros de monitoreo.	Asistente de Redes y Comunicaciones
2	Monitoreo de la red	1) Constante monitoreo a los dispositivos gestionados y a sus tipos de alertas. 2) El monitoreo se lo puede realizar mediante los gráficos estadísticos o a través de comandos en el CLI del dispositivo gestionado.	Asistente de Redes y Comunicaciones
3	Cumplimiento de parámetros de monitoreo	1) Cumplir con las métricas de supervisión del dispositivo, los cuales son: soportar protocolo SNMP, Consumo de memoria RAM, Consumo de CPU, Errores de	Asistente de Redes y Comunicaciones

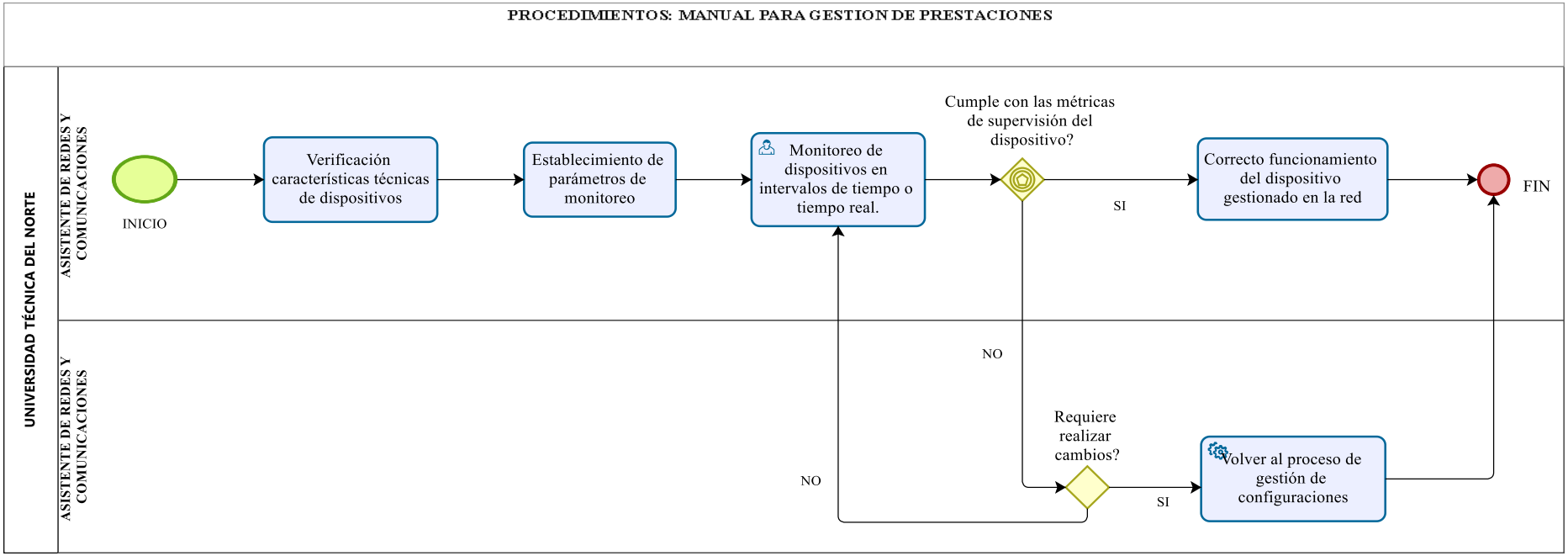
		enlace (Rx y Tx) y estados de enlaces. 2) Los dispositivos gestionados deben cumplir con los umbrales de trabajo establecidos para mantenerse funcionales y sin novedades en la red.	
4	Toma de decisiones	1) Si mediante el monitoreo a los dispositivos gestionados se requiere tomar acciones de acuerdo con las alertas emitidas por el software de gestión, volver al proceso de gestión de configuraciones.	Asistente de Redes y Comunicaciones

Flujograma

En la Figura 188 se presenta el flujograma que explica de manera gráfica el procedimiento para la gestión de prestaciones.

Figura 188

Procedimiento grafico del proceder para la gestión de prestaciones



5.2.5. Manual de procedimientos para la gestión de Seguridad

UNIVERSIDAD TÉCNICA DEL NORTE		
POLÍTICAS DE ADMINITRACIÓN Y GESTIÓN PARA LA RED IMABLAMBRICA Y CABLEADA DE LA UTN		
	Elaborado por:	Axel Almeida
	Revisado por:	Ing. Vinicio Guerra, Administrador de red
	Aprobado por:	Ing. Jorge Caraguay, Director de DDTI
	Versión:	1.0
	Fecha:	22/03/2023

Objetivo. – Presentar el procedimiento a seguir de la gestión de seguridad ya que se enfoca en proteger los recursos de la entidad y garantizar que el acceso a la gestión este restringido a los usuarios no Autorizados.

Alcance. – Este manual presenta el proceso para la asignación de roles de usuario y los privilegios que posee cada rol, además del registro activo de cada acceso de usuario y las acciones que realiza dentro del software de gestión Cisco DNA Center.

Descripción del procedimiento

En las ***Artículos 20 y 23*** establecidos en las políticas para el ámbito de seguridad, se dirigen hacia establecer accesos únicos al software de gestión y también a llevar un control sobre usuarios externos que se tengan en el software de gestión, esto a través de la asignación de niveles de usuario, tal y como se describe en la siguiente Tabla 121 donde se visualizan las actividades que comprenden el manual de procedimientos para la gestión de seguridad.

Tabla 121

Procedimiento para la gestión de seguridad

Nº	**ACTIVIDAD**	**DESCRIPCIÓN**	**RESPONSABLE**
1	Acceso al software de gestión Cisco DNA Center	1) Las cuentas de usuario que se creen, deberán tener previa Autorización por parte del Analista de Redes y Comunicaciones. 2) El usuario que se vaya a crear será a partir del primer apellido y nombre.	Analista de Redes y Comunicaciones y Asistente de Redes y Comunicaciones
2	Roles de acceso y privilegios	1) Los usuarios creados, tendrán acceso remoto al software de gestión y los niveles de usuario que se le asigne dependerá del administrador de la red. 2) Solo el SUPER-ADMIN-ROLE y el NETWORK-ADMIN-ROLE tendrán el acceso completo sobre la implementación, accesos y aspectos de control de Cisco DNA Center.	Analista de Redes y Comunicaciones y Asistente de Redes y Comunicaciones
3	Registro	El software de gestión Cisco DNA Center registrara los	

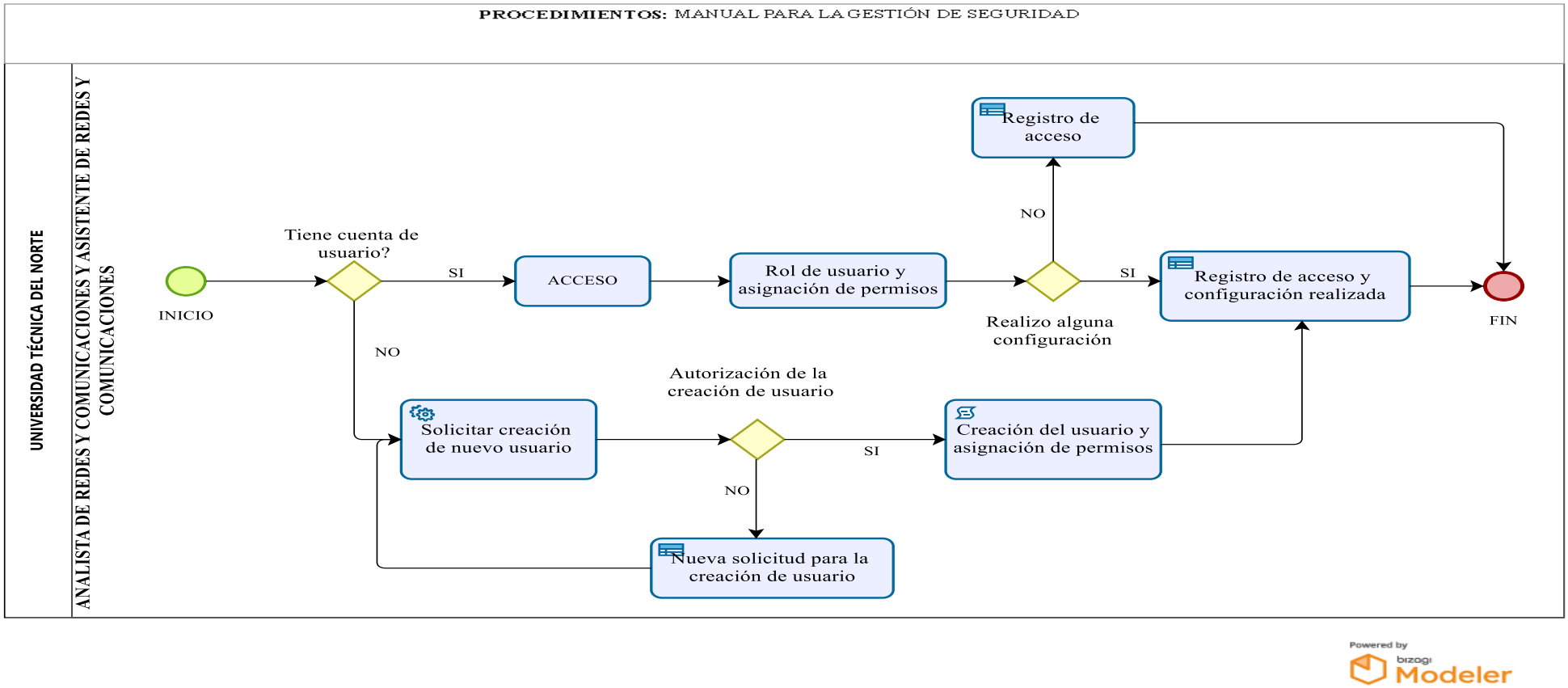
		accesos y las configuraciones realizadas con los siguientes parámetros: • Hora y fecha de cada log • Descripción de la acción realizada. • Estado del loggin	

Flujograma

En la Figura 189 se presenta el flujograma que explica de manera gráfica el procedimiento para la gestión de seguridad.

Figura 189

Procedimiento grafico del proceder para la gestión de seguridad



5.3. Manual de Procedimiento para la Gestión FCAPS de la red Inalámbrica

5.3.1. Manual De Procedimientos Para La Gestión De Configuraciones

UNIVERSIDAD TÉCNICA DEL NORTE		
PROCEDIMIENTOS PARA LA GESTIÓN DE CONFIGURACIONES		
	Elaborado por:	Almeida Axel
	Revisado por:	Ing. Vinicio Guerra, Administrador de red
	Aprobado por:	Ing. Jorge Caraguay, Director DDTI
	Versión:	1.0
	Fecha:	17/02/2023

Objetivo. - presentar el procedimiento a seguir cuando se requiera realizar una configuración de equipos de red inalámbrica en el sistema de gestión Cisco DNA Center.

Alcance. – el presente manual se enfoca directamente brindar el procedimiento a seguir en la creación, configuración y vinculación de un nuevo equipo de red inalámbrica en el sistema de gestión Cisco DNA Center, este procedimiento se aplica a todos los equipos de red que se agreguen desde que el manual entre en vigencia.

Descripción del procedimiento

En la siguiente Tabla 122 se muestra las actividades que comprenden el manual de procedimientos para la gestión de configuraciones, con referencia a los ***Artículos 9, 10 y 11*** de las políticas de administración y gestión de la red.

Tabla 122

Procedimiento para la gestión de configuraciones

Nº	**Actividad**	**Descripción**	**Responsable**

1	Ingreso de equipos	I. Verificación de funcionamiento hardware. II. Registrar el equipo en el inventario de phpipam, donde se registra la siguiente información: • Nombre del equipo • Dirección IP • Tipo de Dispositivo • Ubicación del equipo • Descripción del equipo: Fecha de ingreso, marca y modelo.	Asistente de Redes y Comunicaciones
2	Configuraciones en equipo físico.	Realizar las configuraciones principales como: ✓ Configuraciones de servicios tanto para el acceso de usuarios como para la autenticación con la red. ✓ Habilitación de servicios de telemetría. ✓ Vinculación con Wireless LAN controller	Asistente de Redes y Comunicaciones
3	Configuración en Cisco DNA Center	1) Se realiza las configuraciones del equipo como:	Asistente de Redes y Comunicaciones

		✓ Add ✓ Name. ✓ MAC Address. ✓ Model. ✓ Admin/Mode. ✓ Tipo Radio ✓ OP/Admim(Operational status and AP mode.) ✓ Channel ✓ Antenna name. ✓ Azimuth: dirección de la antena. ✓ Elevation: elevación en grados. 2) Configuraciones de telemetría como: ✓ Syslog ✓ SNMPTraps ✓ Servidores colectores de NetFlow y recopilación de datos de clientes	
4	Documentación de configuraciones	1) Generar respaldos de las configuraciones realizadas en los equipos. 2) Registrar la configuración realizada en la plantilla de registros	Asistente de Redes y Comunicaciones

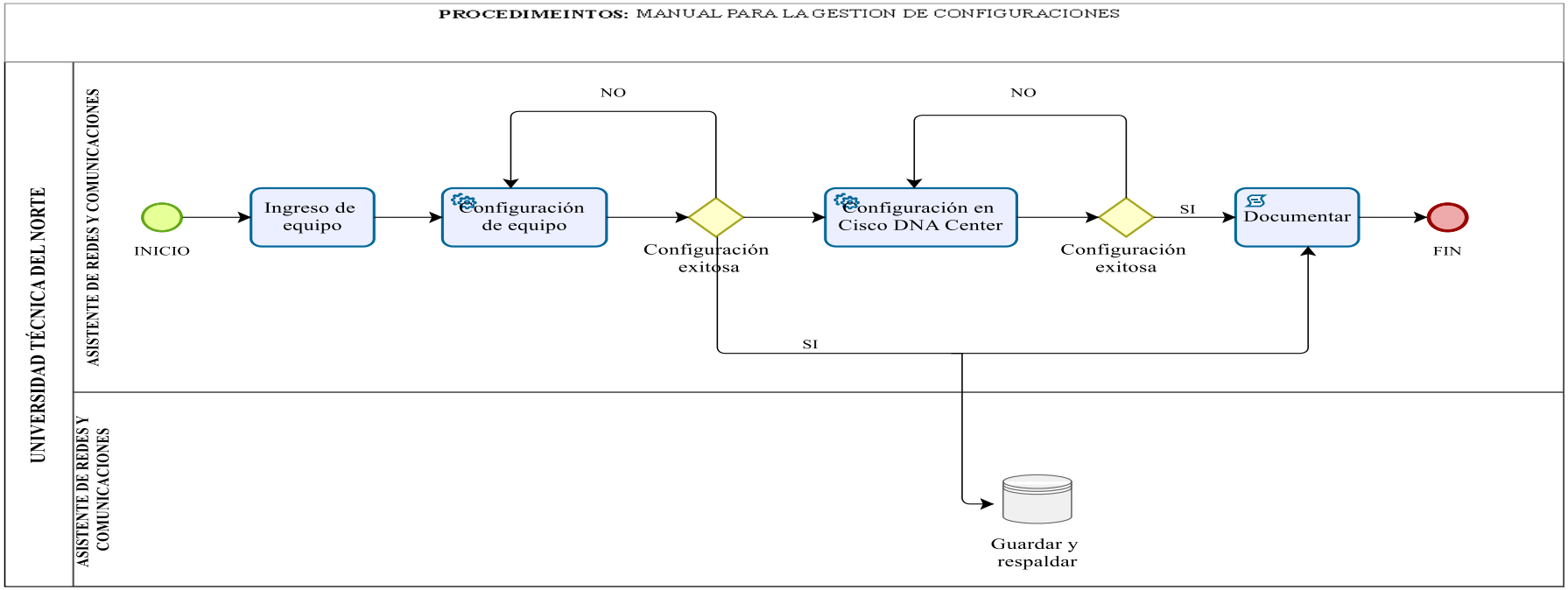
		de configuraciones como se detalla en el ANEXO F.	

Flujograma

En la Figura 190 se presenta un flujograma que explica de manera gráfica el procedimiento para la gestión de configuraciones

Figura 190

Procedimiento grafico del proceder para la gestión de configuraciones.



5.3.2. Manual De Procedimientos Para La Gestión de Fallos

UNIVERSIDAD TÉCNICA DEL NORTE		
PROCEDIMIENTOS PARA LA GESTIÓN DE FALLOS		
	Elaborado por:	Axel Almeida
	Revisado por:	Ing. Vinicio Guerra, Administrador de red
	Aprobado por:	Ing. Jorge Caraguay, Director de DDTI
	Versión:	1.0
	Fecha:	22/03/2023

Objetivo. - Presentar el proceso a seguir para la detección, aislamiento y solución de fallos que se presentan por causas de algún fallo dentro de la red inalámbrica de la Universidad Técnica del Norte, para mejorar la disponibilidad de los recursos.

Alcance. – el presente manual se enfoca directamente en los puntos de red que conforman la red inalámbrica, con el objetivo del monitoreo continuo para la detección, aislamiento y solución de los fallos que puedan acontecer. El monitoreo se realiza a través del sistema de gestión Cisco DNA Center.

Descripción del procedimiento

En la siguiente Tabla 123 se muestra las actividades que comprenden el manual de procedimientos para la gestión de fallos, con referencia a los ***Artículos 3, 4 y 5*** de las políticas de administración y gestión de la red.

Tabla 123

Procedimiento para la gestión de configuraciones

Nº	**Actividad**	**Descripción**	**Responsable**

1	Detección de fallas	La detección de fallas se detecta a través de la vigilancia continua de los agentes instalados en cada uno de los equipos de red, los cuales notifican al administrador de la red vía correo electrónico, SMS y notificaciones visuales en el software de gestión Cisco DNA Center en caso de ocurrir un evento, además de la generación de un incidente correspondiente a el fallo ocurrido.	Administrador de la red
2	Aislamiento y diagnóstico de la falla	El aislamiento de la falla se realiza a través de la identificación y comparativa de umbrales establecidos en el software de gestión Cisco DNA Center, el cual aísla y muestra en colores el puntaje que se le otorga a la falla. Como se muestra a continuación: Rojo(P1): Un problema crítico que necesita atención inmediata. Naranja(P2): Problema grave que puede afectar a varios dispositivos o clientes.	Administrador de la red

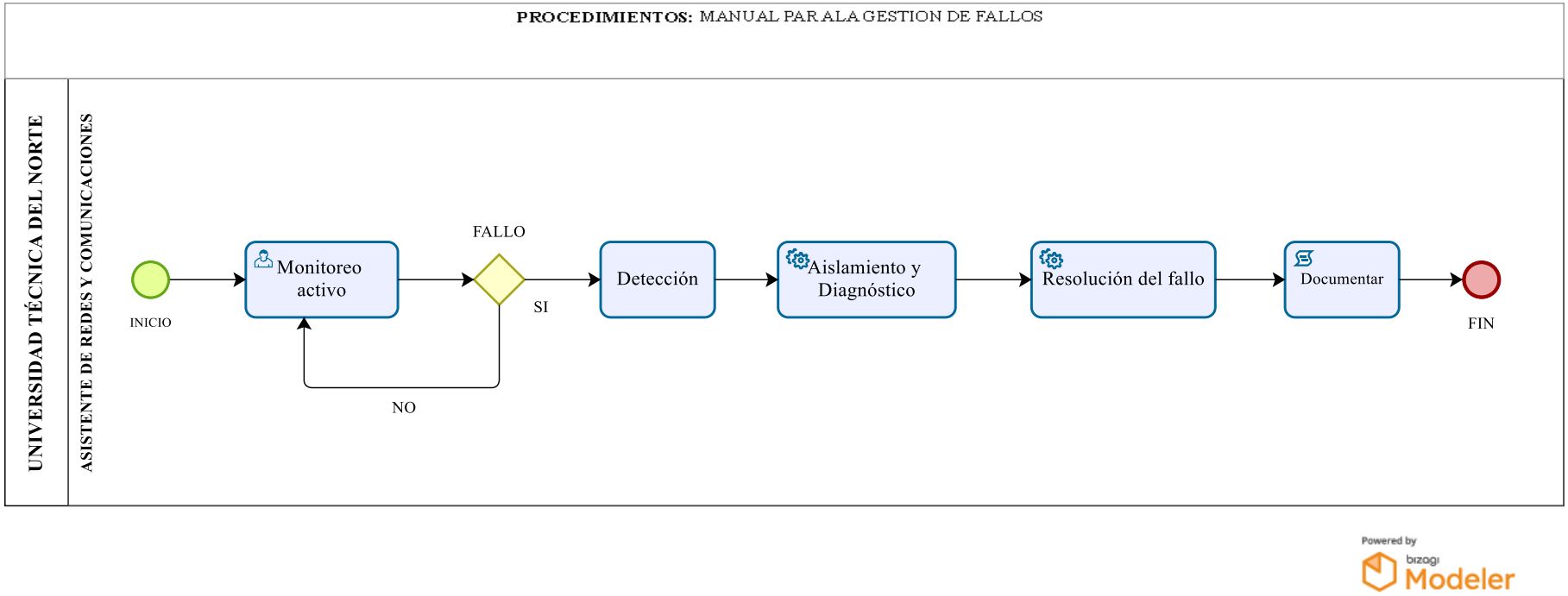
		Negro(P3): Problema localizado o mínimo. Negro(P4): Problema de advertencia.	
3	Resolución de la falla	1. Identificar la solución del problema. 2. Corregir el problema de manera remota o a su vez en el equipo físico. 3. Cerrar el incidente generado.	Administrador de la red
4	Documentación de Fallos	1. Documentar el fallo. 2. Detallar el procedimiento que se realizó para la solución del fallo, según la plantilla establecida en el ANEXO E.	Administrador de la red

Flujograma

En la Figura 191 se presenta el flujograma que explica de manera gráfica el procedimiento para la gestión de fallos.

Figura 191

Procedimiento grafico del proceder para gestión de fallos



5.3.3. Manual De Procedimientos Para La Gestión de Contabilidad

UNIVERSIDAD TÉCNICA DEL NORTE		
PROCEDIMIENTOS PARA LA GESTIÓN DE CONTABILIDAD		
	Elaborado por:	Axel Almeida
	Revisado por:	Ing. Vinicio Guerra, Administrador de red
	Aprobado por:	Ing. Jorge Caraguay, Director de DDTI
	Versión:	1.0
	Fecha:	22/03/2023

Objetivo. - Presentar el proceso a seguir para la recolección de información relacionada con los recursos de los equipos de red, y la generación de reportes individuales o generales a través del software de gestión Cisco DNA Center.

Alcance. – el presente manual presenta el proceso a seguir para la realizar la medición del consumo de los recursos de la red y la generación de reportes que presenta el sistema de gestión Cisco DNA Center.

Descripción del procedimiento

En la siguiente Tabla 124 se muestra las actividades que comprenden el manual de procedimientos para la gestión de contabilidad, con referencia en los ***Artículos 17 y 19*** de las políticas de administración y gestión de la red.

Tabla 124

Procedimiento para la gestión de contabilidad

N°	Actividad	Descripción	Responsable
1	Generación de reportes	Configurar los parámetros para la generación del reporte. 1. Nombre del reporte Alcance (reporte individual o todos los APs) 2. Formato de archivo (CSV, JSON, Tabla de datos) 3. Rango de tiempo (3, 24 Horas, 7 días) 4. Programar (ejecutar ahora, ejecutar más tarde (una sola vez), ejecutar de forma recurrente) Los parámetros de monitoreo como tiempo activo, uso de CPU, uso de memoria, número máximo de clientes conectados. Se analiza los reportes Si en el análisis de determina que existe algún parámetro que sobrepasa los umbrales de estado, se	Administrador de la red

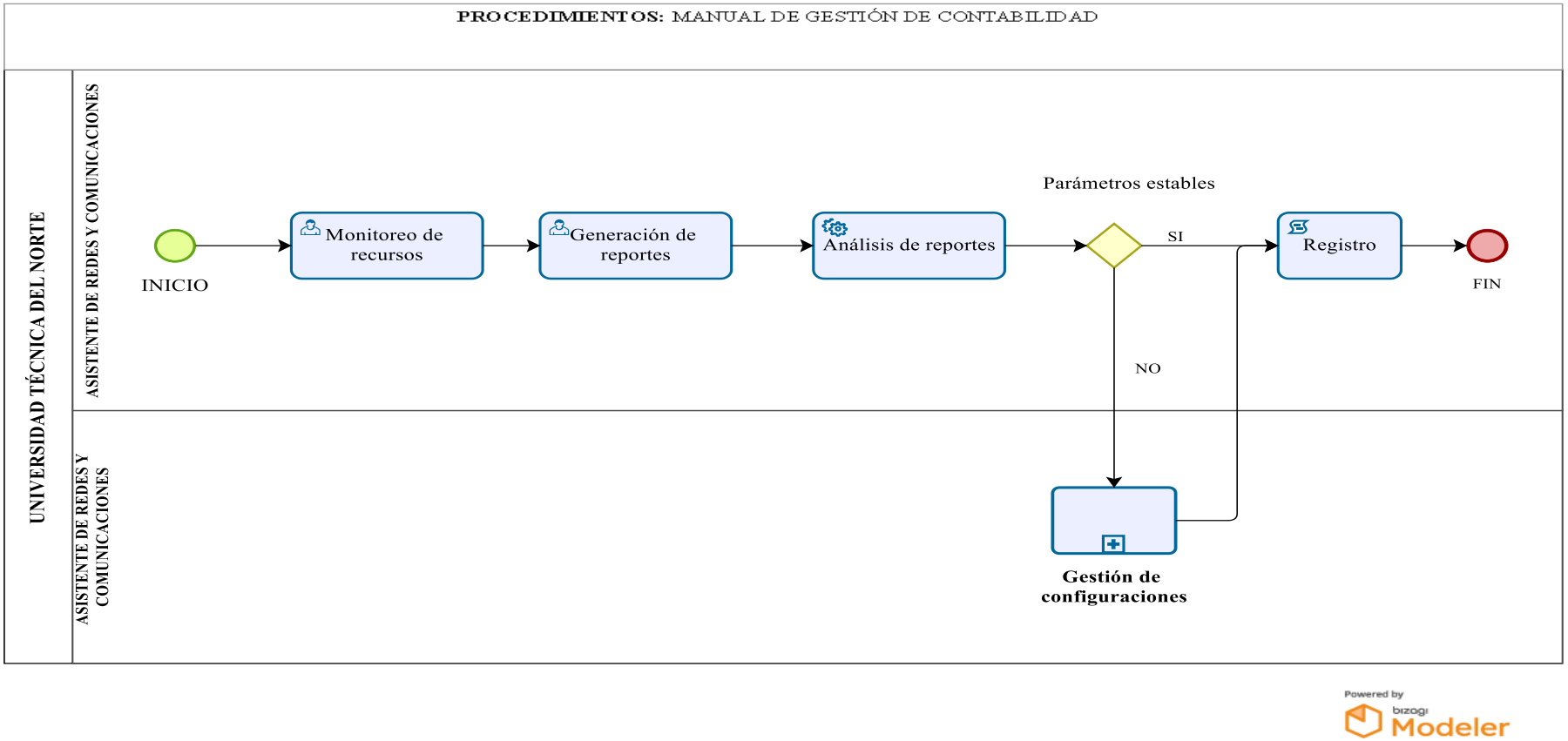
		procede al a pasar al proceso de gestión de configuraciones.	
2	Registrar	Se procede a registrar el reporte realizado donde se detalla, hora y fecha, detalle de reporte y frecuencia.	Administrador de la red

Flujograma

En la Figura 192 se presenta un flujograma que explica de manera gráfica el procedimiento para la gestión de contabilidad.

Figura 192

Procedimiento grafico del proceder para la gestión de contabilidad



5.3.4. Manual De Procedimientos Para La Gestión de Prestaciones

UNIVERSIDAD TÉCNICA DEL NORTE		
PROCEDIMIENTOS PARA LA GESTIÓN DE PRESTACIONES		
	**Elaborado por:**	Axel Almeida
	Revisado por:	Ing. Vinicio Guerra, Administrador de red
	Aprobado por:	Ing. Jorge Caraguay, Director de DDTI
	Versión:	1.0
	Fecha:	22/03/2023

Objetivo. - Presentar el proceso a seguir para la recolección de datos estadísticos de los recursos de la red a través del software de gestión Cisco DNA Center.

Alcance. – el presente manual se enfoca directamente en recolectar información estadística de los diferentes parámetros que contiene una red inalámbrica y la generación de graficas que permitan al administrador una mejor visualización de la información recolectada.

Descripción del procedimiento

En la siguiente Tabla 125 se muestra las actividades que comprenden el manual de procedimientos para la gestión de prestaciones, con referencia a los ***Artículos 15 y 16*** de las políticas de administración y gestión de la red.

Tabla 125

Procedimiento para la gestión de prestaciones

N°	Actividad	Descripción	Responsable
1	Recolección de datos estadísticos	1) Mediante las herramientas proporcionadas por el Software	Administrador de la red

		de gestión Cisco DNA Center se procede a la recolección de datos estadísticos de la red inalámbrica. Los principales parámetros para visualizar son: a) Número de usuarios en la red inalámbrica b) Número de usuarios por SSID c) Intensidad de la señal d) Canal en uso e) Número de usuarios por canal f) Frecuencia g) Cantidad de antenas h) Relación señal-ruido i) Velocidad de transmisión • Establecer umbrales para determinar el buen funcionamiento de la red inalámbrica. • Generación de gráficos estadísticos para visualizar los estados de los recursos de la red.	
2	Generación de reportes.	1) Establecer la recurrencia de la generación de reportes.	Administrador de la red

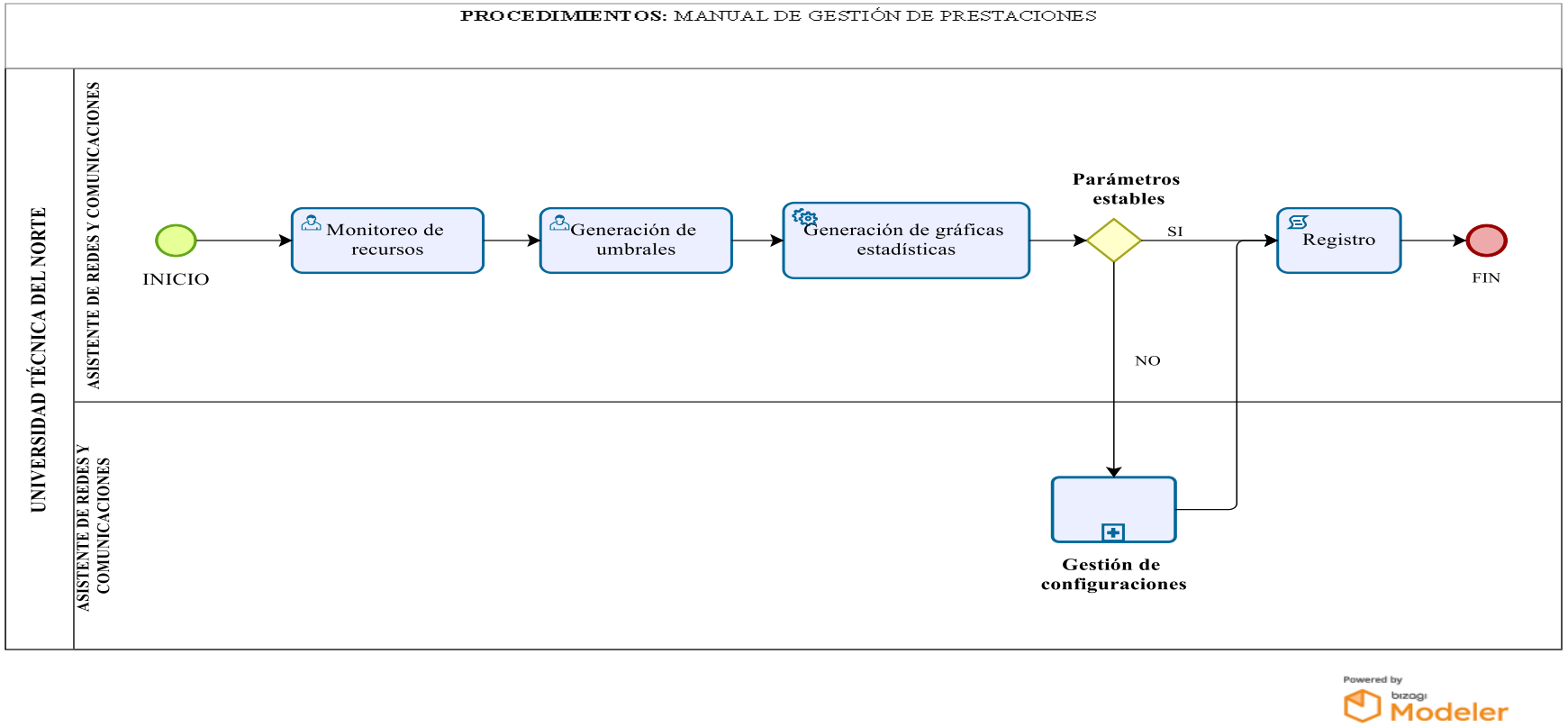
		2) Establecer si los reportes se envían a el correo del administrador. 3) Posterior al análisis del reporte planificar si se procede a pasar a gestión de configuraciones.	

Flujograma

En la Figura 193 se presenta un flujograma que ilustra de manera gráfica los procedimientos necesarios para llevar a cabo la gestión de prestaciones

Figura 193

Procedimiento grafico del proceder para la gestión de prestaciones



5.3.5. Manual De Procedimientos Para La Gestión de Seguridad

UNIVERSIDAD TÉCNICA DEL NORTE		
PROCEDIMIENTOS PARA LA GESTIÓN DE SEGURIDAD		
	Elaborado por:	Axel Almeida
	Revisado por:	Ing. Vinicio Guerra, Administrador de red
	Aprobado por:	Ing. Jorge Caraguay, Director de DDTI
	Versión:	1.0
	Fecha:	22/03/2023

Objetivo. - Presentar el proceso a seguir para la asignación los roles de usuario y los accesos al sistema de gestión Cisco DNA Center.

Alcance. – Este manual presenta el proceso para la asignación de roles de usuario y lo privilegios que posee de cada rol, además del registro activo de cada acceso de usuario y las acciones que realiza dentro del software de gestión Cisco DNA Center

Descripción del procedimiento

En la siguiente Tabla 126 se muestra las actividades que comprenden el manual de procedimientos para la gestión de seguridad, con referencia en los ***Artículos 22*** de las políticas de administración y gestión de la red.

Tabla 126

Procedimiento para la gestión de seguridad

N°	Actividad	Descripción	Responsable
1	Acceso al software de	1) Las cuentas de usuario que se creen, deberán tener previa Autorización por	Usuarios.

	gestión Cisco DNA Center	parte del Analista de Redes y Comunicaciones. 2) El usuario que se vaya a crear será a partir del primer apellido y nombre.	
2	Roles de acceso y privilegios	1) El administrador de la red creara las nuevas cuentas de usuario y asignara el rol de privilegio, previo a la Autorización del director del DDTI. 2) El administrador de la red puede crear nuevos roles personalizados. 3) El nombre se creará de acuerdo lo especifique el administrador de la red. 4) Solo los usuarios con rol super admin pueden realizar modificaciones en el software de gestión Cisco DNA Center.	Administrador de la red
3	Acceso Remoto	1) Conectarse a VPN-UTN a través de VPN FortiClient 2) Ingresar a la dirección ipv4 del software de gestión Cisco DNA Center. Ingresar usuario y contraseña	
4	Registro	El software de gestión Cisco DNA Center registrara los accesos y las configuraciones realizadas con los siguientes parámetros:	Cisco DNA Center

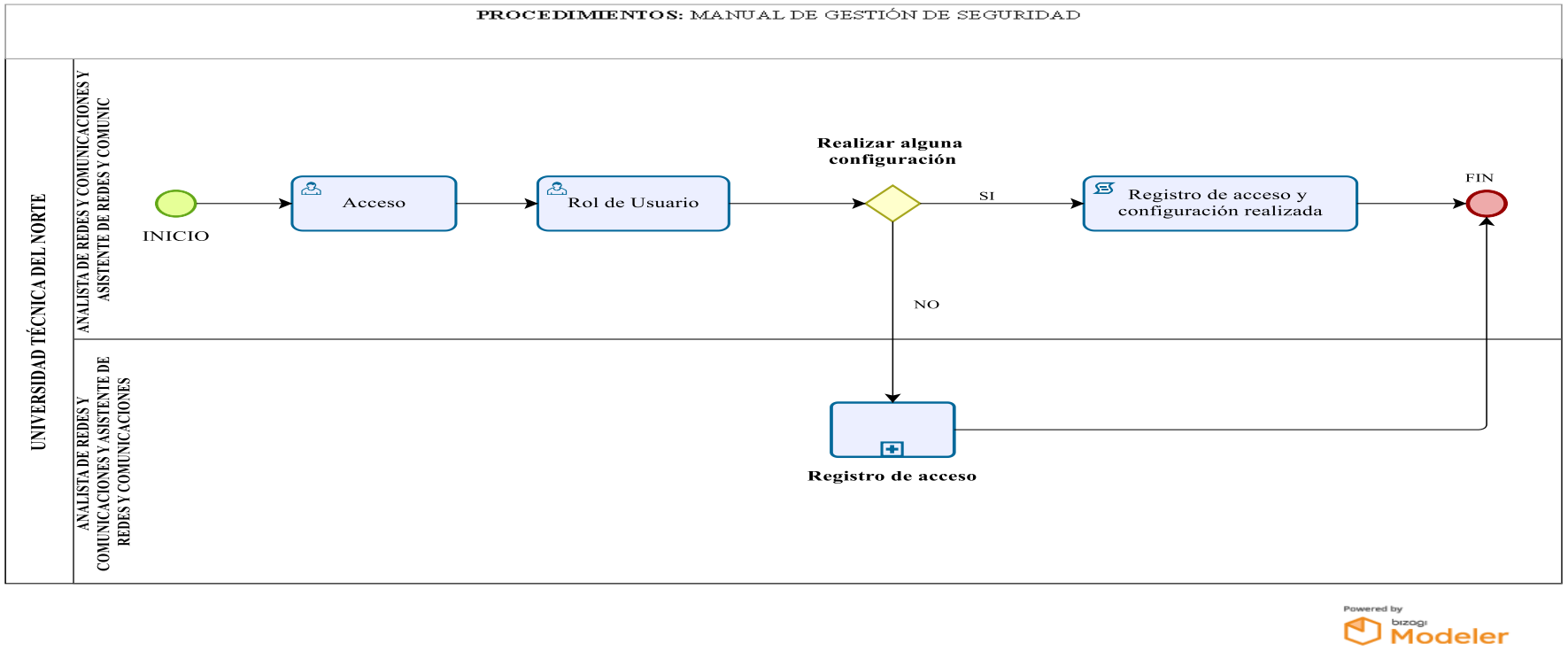
		• Hora y fecha de cada log • Descripción de la acción realizada. • Estado del loggin.	

Flujograma

En la Figura 194 se presenta un flujograma que ilustra de manera gráfica los procedimientos necesarios para llevar a cabo la gestión de seguridad.

Figura 194

Procedimiento grafico del proceder para la gestión de seguridad



6. CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

La implementación del modelo de gestión FCAPS basado en el estándar ISO, es necesario en una red de la dimensión de la Universidad Técnica del Norte ya que posee una alta disponibilidad de equipos de red y recursos para así poder brindar un servicio optimo y de calidad a toda la comunidad Universitaria que goza del servicio de conectividad a Internet.

Con la implementación de nuevas tecnologías en el campo de las redes inalámbricas y softwares de gestión de redes, es necesario la implementación de un modelo de gestión proactivo que permita planificar, monitorizar y evaluar los recursos de la red, como lo define la ISO en las áreas funcionales de su modelo de gestión FCAPS, el cual fue implementado en este proyecto para la red cableada e inalámbrica de la Universidad Técnica del Norte.

El software de gestión Cisco DNA Center es una herramienta robusta que presenta una mejor capacidad a la hora de la administración y gestión de la red cableada e inalámbrica de la Universidad Técnica del Norte, permitiendo que las políticas de gestión implementadas logren asegurar el desempeño de la red mediante datos estadísticos y provistos en tiempo real, ya que esto permite aprender, adaptarse e incluso detectar problemas antes que sucedan. Esto con la finalidad de tener una gestión simplificada de la red que conlleve a ganar visibilidad de lo que sucede, transformando así conocimientos en acción y por ende así resolver los problemas en menor tiempo.

A través de una recolección de información y un exhaustivo monitoreo sobre el software de gestión Cisco DNA Center, se logró descubrir nuevas herramientas, las cuales permitieron elaborar los manuales de procedimientos en base a las áreas funcionales del modelo de gestión, esto permitirá que los Administradores de red puedan tener un mejor

análisis y desempeño al momento de emitir criterios e información sobre el estado actual de la red cableada e inalámbrica de la Universidad Técnica del Norte, ya que Cisco DNA Center posee una visibilidad integral de red, puede administrar fácilmente todos sus dispositivos y servicios conectados, identificar y resolver inconvenientes antes de que se conviertan en problemas, lo cual permitirá brindar una mejor experiencia del usuario en toda la red.

La Universidad Técnica del Norte es una entidad pública que mantiene estatus y políticas para determinar procesos que tengan un correcto funcionamiento, este proyecto fue enfocado al establecimiento de policitas para la red cableada e inalámbrica de la Universidad Técnica del Norte, guiado por el personal del DDTI, quienes tendrán como guía a los manuales de procedimiento, para la utilización del software Cisco DNA Center y herramientas potentes para una resolución practica y eficaz ante eventos inesperados que se susciten en la red.

A través del análisis de la auditoria que se realizó al estado actual de la red cableada e inalámbrica mediante del software de gestión y de manera física, se establecieron requerimientos operaciones tanto como para el software de gestión como para la red inalámbrica y cableada, entonces a partir de los requerimientos propuestos se establecieron las políticas y dichas políticas responden a los requerimientos, por ende, esto se refleja en la implementación de cada modelo de gestión del FCAPS que cubren las áreas funcionales de: fallas, configuración, contabilidad, prestaciones y seguridad.

6.2. Recomendaciones

Se recomienda al personal del DDTI que cada cierto tiempo tome capacitaciones sobre las herramientas que posee el software de gestión Cisco DNA Center, ya que posee una gran variedad de herramientas que pueden ayudar a obtener una mejor administración de los

recursos y también a solventar fallos e inconvenientes que se presenten en la red de la Universidad Técnica del Norte.

Verificar que los nuevos equipos sean compatibles con soporte telemático, ya que esto permite al administrador y al software de gestión, la recolección de datos relacionados con el estado de los recursos del equipo de red.

Es recomendable llevar un registro de fallas y soluciones, ya que dicha información servirá para mejorar el tiempo de resolución de fallos y ayudar a nuevos administradores con información para la resolución de fallos similares.

Mantener la disponibilidad de información sobre del estado actual, ya sea esta sobre el estado físico y lógico de la red, es importante ya que así se podrá determinar requerimientos que llevan a plantear buenas políticas de administración y gestión permitiendo así cubrir y controlar el uso de la eficiencia de los recursos que el administrador gestiona.

Es recomendable emigrar a una nueva base datos con respecto a la actualmente utilizada dentro del DDTI, esto permitirá llevar un mayor control sobre los dispositivos que se encuentren dentro de la red, además de mantener la documentación necesaria y organizada, todo ello con la finalidad de tener como referencia para evitar que se produzcan problemas dentro de la red de la Universidad Técnica del Norte.

Se recomienda que las políticas y manuales de procedimientos que abarcan al modelo de gestión, se los tome como una guía que orienten a la correcta utilización de los recursos de la red y al manejo de herramientas del software de gestión Cisco DNA Center, teniendo en cuenta que no son procedimientos establecidos por ley a seguir, si no una referencia a futuro para resolver eventualidades inesperadas que se presenten y así obtener un servicio optimo y de calidad en la red de la Universidad Técnica del Norte.

Realizar estudios de cobertura utilizando los diagramas unifilares de calor y la herramienta **Baselines** del software de gestión Cisco DNA Center, esto con la finalidad de mejorar las zonas de coberturas y reducir los tiempos de autenticación, incorporación y asociación, ya que si se mantiene un umbral mayor a -69dBm y menor que -71dBm garantizamos un mayor data rate.

7. BIBLIOGRAFIA

Adroit Information Technology Academy (AITA). (2022, October 19). *What is Cisco DNA Center*.

Andrea, D., Castaño, G., María, G., Taborda, M., Yulieth, M., & Múnera, P. (2018). *Modelo de optimización de la red Wifi en el politécnico Grancolombiano sede Medellín*.

Barba Martí, A. (1999). *Gestion de red*.

Behrouz A. Forouzan, & Firouz Mosharraf. (2012). *Computer Networks. A Top-Down Approach*. www.elsolucionario.org

Bonilla Fonte, E. P., Cachiguango Maldonado, V. M., Ipiales Matango, J. G., & Rojas Rojas, C. M. (2017). *REDISEÑO DEL SISTEMA DE CABLEADO ESTRUCTURADO PARA LA RED DE DATOS EN LA BIBLIOTECA DE LA UNIVERSIDAD TECNICA DEL NORTE*.

Boston, A. •, Heidelberg, •, London, •, San, P. •, San, D., Singapore, F. •, Tokyo, S. •, Abeck, S., Bryskin, I., Evans, J., Farrel, A., Filsfi, C., Hegering, H.-G., Mccabe, J. D., Morrow, M., Nadeau, T. P., Neumair, B., Ramaswami, R., Sivarajan, K. N., … Vijayananda, K. (2009). *Network Management Know It All*. www.mkp.com

Carrera, D., Guachán, C., & Tapia, R. (2017). *DISEÑO DE CABLEADO ESTRUCTURADO DE LA FACULTAD DE CIENCIAS ADMINISTRATIVAS Y ECONÓMICAS (FACAE) NORTE*.

Cervi. (2018). *Sistema de cableado UTP Cat.6A*.

Cisco. (2017, May 11). *Troubleshoot the "OSPF Neighbor Down: Too many retransmissions" Error Message*.

CISCO. (2021). *Cisco DNA Center Platform User Guide, Release 2.2.2*. http://www.cisco.com

Cisco. (2022a). *Cisco DNA Center 2.3.3*.

Cisco. (2022b, June 28). *Cisco DNA Center second-generation appliance installation guide, release 2.2.3 - review the Cisco DNA Center appliance features [Cisco DNA Center]*.

CISCO. (2022, November 18). *Utilizar el comando Mostrar procesos*.

Cisco Systems. (2021). *Cisco DNA Assurance User Guide, Release 2.2.3*. http://www.cisco.com

Clark, M. P. (2003). *Data networks, IP and the Internet : protocols, design and operation*. Wiley.

Clemm, Alexander. (2006). *Network management fundamentals*. Cisco Press.

Consultivo, C. (1993). *UNIÓN INTERNACIONAL DE TELECOMUNICACIONES CCITT X.700 REDES DE COMUNICACIÓN DE DATOS MARCO DE GESTIÓN PARA LA INTERCONEXIÓN DE SISTEMAS ABIERTOS PARA APLICACIONES DEL CCITT Recomendación X.700*.

Cristina Liberatori, M. (2018). *Redes de Datos y sus Protocolos*.

Ding, J. (2010). *Advances in Network Management*. Auerbach Publications.

Escobar César, V. C. T. B. B. S. (2017). *DISEÑO DEL CABLEADO ESTRUCTURADO DE LA FACULTAD DE EDUCACION CIENCIA Y TECNOLOGÍA (FECYT) EN AUTOCAD Y SKETCHUP*.

Espinosa Padilla, G. I. (2017). *IMPLEMENTACIÓN DE UN SERVIDOR FIREWALL-PROXY BAJO LA PLATAFORMA DE GNU/LINUX PARA LA FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS, A FIN DE LIBERAR PROCESAMIENTO DE LOS EQUIPOS DEL DATA CENTER DE LA UNIVERSIDAD TÉCNICA DEL NORTE*.

Goralski, W. (2017). *The Illustrated Network*.

Guerrero Ipiales, D. C. (2019). *METODOLOGÍA PARA DESARROLLAR UN SISTEMA DE GESTIÓN DE LA CALIDAD APLICADO AL DATA CENTER DE LA FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS BAJO LA NORMA ISO 9001:201*.

Guerrero Pantoja, C. D. (2011). *UNIVERSIDAD POLITÉCNICA SALESIANA SEDE QUITO-CAMPUS SUR CARRERA DE INGENIERÍA DE SISTEMAS MENCIÓN TELEMÁTICA EVALUACIÓN DE SISTEMAS DE GESTIÓN DE REDES BAJO SOFTWARE LIBRE DE LA ADMINISTRACIÓN ZONAL NORTE "EUGENIO ESPEJO" TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS*. https://dspace.ups.edu.ec/bitstream/123456789/1678/9/UPS%20-%20ST000185.pdf

Informe Diseño Cableado Estructurado. (2017).

IPCisco. (2020, May 16). *Cisco DNA Center*. https://ipcisco.com/lesson/cisco-dna-center/

Jácome Chávez, V. M. (2019). *PLAN DE SEGURIDAD PARA LA GESTIÓN DE RIESGOS EN EL DATACENTER DE LA FACULTAD DE INGENIERA EN CIENCIAS APLICADAS CON LA METODOLOGÍA MAGERIT V3.0*.

Juniper.net. (2021, January 13). *Understanding MAC limiting and MAC move limiting*.

ManageEngine. (n.d.). *Network Monitoring Software by*.

Manuel Mora. (2014). *Sistemas Avanzados de Comunicaciones. Tema 10: Gestión de Redes Contenido*. https://www.academia.edu/6895273/Sistemas_Avanzados_de_Comunicaciones_Tema_10_Gesti%C3%B3n_de_Redes_Contenido

Narváez Manosalvas, C. R. (2016). *DISEÑO DE LA INFRAESTRUCTURA FÍSICA DE UN DATA CENTER TIER I BASADO EN EL ESTÁNDAR TIA 942, PARA LA FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS DE LA UNIVERSIDAD TÉCNICA DEL NORTE*.

New, D., St, Y., San, L., Auckland, F., Caracas, B., Lumpur, K., London, L., Mexico, M., Milan, C., San, M., Santiago, J., Sydney, S., Toronto, T., Forouzan, B. A., & Mosharraf, F. (2012). *Computer Networks*. Tata McGraw Hill Education Private Limited. www.elsolucionario.org

Nicolalde Quilca, W. A. (2021). *DISEÑO DE UN SISTEMA DE DETECCIÓN DE INTRUSOS (IDS), BASADO EN REDES NEURONALES PARA UNA RED DEFINIDA POR SOFTWARE (SDN) EN LA FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS (FICA) DE LA UNIVERSIDAD TÉCNICA DEL NORTE*.

Quilca Fernández, L. E., Mora Ayala, J. J., Noguera Salazar, J. J., & López Flores, P. A. (2017). *DISEÑO DEL SISTEMA DE CABLEADO ESTRUCTURADO CAT. 6ª PARA EL EDIFICIO CENTRAL DE LA UNIVERSIDAD TECNICA DEL NORTE*.

Ruiz, A. (2018, July 4). *Infraestructuras (I) Redes Inalámbricas: Capítulo 11*.

Sapalomera.cat. (2023, March 20). *Resolución de problemas de la capa de enlace de datos*.

Sosa Sosa, V. J. (n.d.). *GESTIÓN DE REDES*.

Vallejos Garzón, E. M. (2019). *DISEÑO DE SISTEMA DE SEGURIDAD A NIVEL DE CAPA DE ENLACE DE DATOS EN REDES CABLEADAS MEDIANTE EL ESTÁNDAR IEEE 802.1X EN LA LAN DE LA UNIVERSIDAD TÉCNICA DEL NORTE*.

William Stallings. (2007). *DATA AND COMPUTER COMMUNICATIONS*. Pearson/Prentice Hall.

William Stallings. (2014). *Data and Computer Communications*. http://www.pearsonhighered.com/stallings/

8. ANEXOS

8.1. ANEXO A

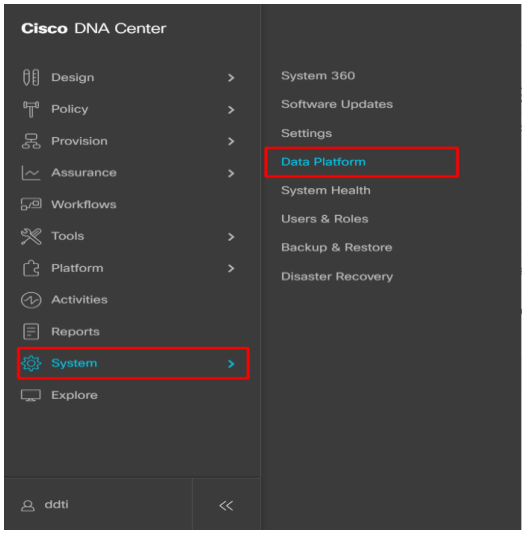
- **Activación de métricas de SNMP COLLECTOR para dispositivos de red**

Para que la puntuación de estado se rellene correctamente para los dispositivos de red, debe activar las métricas del recopilador SNMP, a continuación, se visualiza las métricas que están actualmente activadas en el DNA Center.

Como primer paso nos dirigiremos a System y luego a Data Plataform, tal y como se visualiza en la Figura 195.

Figura 195

Despliegue del menú

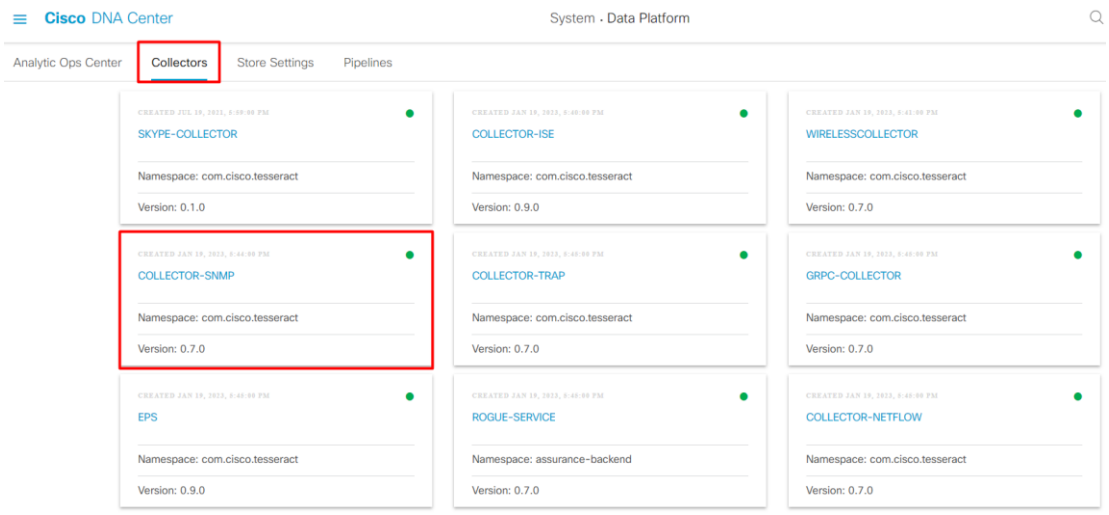


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

En la Figura 196, se muestra el siguiente paso, el cual es realizar click en COLLECTR-SNMP.

Figura 196

COLLECTOR-SNMP



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

En la Figura 197 se visualiza el siguiente paso es realizar click en Add

Figura 197

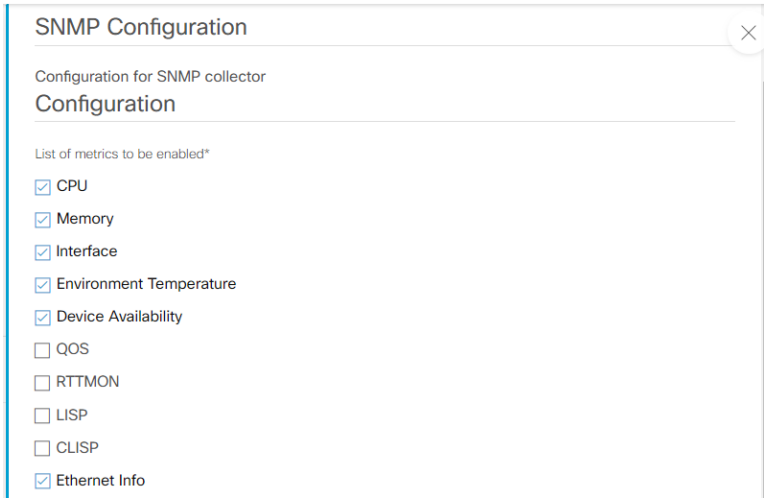
Agregar métricas

Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Seguido de ello se abrirá el cuadro de diálogo de configuración SNMP, donde también se encontrar opciones como: intervalo de sondeo, ID de satélite, ID de sitio y nombre de configuración, el cual debe mantenerse como único nombre para la configuración, tal y como se observa en la Figura 198.

Figura 198

Lista de métricas a habilitadas

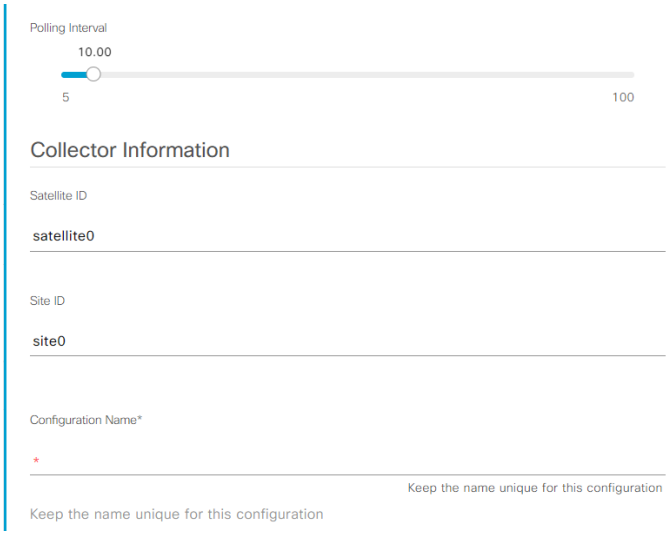


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Figura 199 se visualiza los campos de Collector-SNMP.

Figura 199

Opciones e información de COLLECTOR-SNMP.

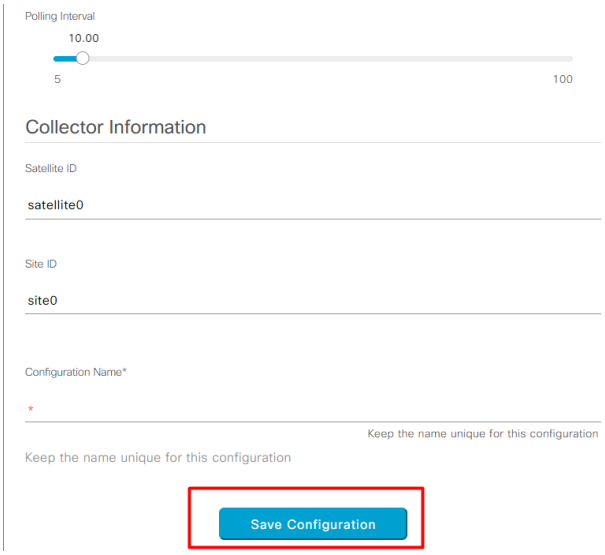


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Y por último se guarda las configuraciones y se representa en la Figura 200.

Figura 200

Guardar configuraciones



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

8.2. ANEXO B

En la Figura 201 se presentan las configuraciones realizadas en los equipos de conmutación para la habilitación de los servicios de SNMP, también se detalla todos los servicios activos para snmp-server

Figura 201

Activación de servicios snmp-server

```
180 |snmp-server community xxxxxxxx RO
181 |snmp-server community xxxxxxxx RO
182 |snmp-server community xxxxxxxx RO
183 |snmp-server community xxxxxxxx RO
184 |snmp-server trap-source FastEthernet0
185 |snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
186 |snmp-server enable traps transceiver all
187 |snmp-server enable traps tty
188 |snmp-server enable traps cluster
189 |snmp-server enable traps entity
190 |snmp-server enable traps cpu threshold
191 |snmp-server enable traps vtp
192 |snmp-server enable traps vlancreate
193 |snmp-server enable traps vlandelete
194 |snmp-server enable traps flash insertion removal
195 |snmp-server enable traps port-security
196 |snmp-server enable traps envmon fan shutdown supply temperature status
197 |snmp-server enable traps config-copy
198 |snmp-server enable traps config
199 |snmp-server enable traps bridge newroot topologychange
200 |snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
201 |snmp-server enable traps syslog
202 |snmp-server enable traps mac-notification change move threshold
203 |snmp-server enable traps vlan-membership
204 |snmp-server host [redacted] version 2c xxxxxxxx
```

Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

8.3. ANEXO C

En la Tabla 127 se visualiza los Syslogs seleccionados por debajo del nivel Crítico para Switches y Routers.

Tabla 127

Syslogs

Eventos de Protocolos	Eventos de capa 2

OSPF-5-ADJCHG IFDAMP-5-UPDOWN BGP-5-ADJCHANGE DUAL-5-NBRCHANGE BGP-5-ADJCHANGE-bfd CLNS-5-ADJCHANGE LDP-5-NBRCHG-TDP LDP-5-NBRCHG-LDP CDP-4-NATIVE_VLAN_MISMATCH LISP-4-LOCAL_EID_RLOC_INCONSISTENCY LISP-4-LOCAL_EID_NO_ROUTE LISP-4-CEF_DISABLED LISP-4-LOCAL_EID_MAP_REGISTER_FAILURE LISP-4- MAP_CACHE_WARNING_THRESHOLD_REACHED	SW_MATM-4-MACFLAP_NOTIF MAC_LIMIT-4-PORT_EXCEED MAC_LIMIT-4-VLAN_EXCEED IGMP-6-IGMP_GROUP_LIMIT SPANTREE-5-ROOTCHANGE UDLD-4-UDLD_PORT_DISABLED PM-4-ERR_DISABLE CDP-4-DUPLEX_MISMATCH LINK-5-CHANGED PORT-5-IF_DOWN PORT-5-IF_UP
Eventos de plataforma de hardware	
SYS-5-CONFIG_I SYS-5-RELOAD SYS-5-RESTART OIR-6-INSCARD OIR-6-REMCARD OIR-SP-6-INSCARD	

OIR-SP-6-REMCARD
PLATFORM_STACKPOWER-6-CABLE_EVENT
PLATFORM_STACKPOWER-6-LINK_EVENT
PLATFORM_STACKPOWER-4-TOO_MANY_ERRORS
PLATFORM_STACKPOWER-4-VERSION_MISMATCH
PLATFORM_STACKPOWER-4-UNDER_BUDGET
PLATFORM_STACKPOWER-4-INSUFFICIENT_PWR
PLATFORM_STACKPOWER-4-REDUNDANCY_LOSS
ILPOWER-5-POWER_GRANTED
ILPOWER-5-LINKDOWN_DISCONNECT
ILPOWER-5-IEEE_DISCONNECT
ILPOWER-5-INVALID_IEEE_CLASS
ILPOWER-4-LOG_OVERDRAWN
ILPOWER-5-CLR_OVERDRAWN

Fuente: (Cisco Systems, 2021)

Según Sapalomera.cat, (2023) “Los problemas de capa 2 causan síntomas específicos que, al reconocerse, ayudan a identificar problemas rápidamente. A continuación, algunos síntomas frecuentes de los problemas de red en la capa 2:”

- **Falta de funcionalidad o conectividad en la capa de red o en las capas superiores**: algunos problemas de capa 2 pueden detener el intercambio de tramas a través de un enlace, mientras que otros solo provocan un deterioro del rendimiento de la red.

- **Funcionamiento de la red por debajo de los niveles de rendimiento de línea de base:** en una red, pueden ocurrir dos tipos de funcionamiento deficiente en la capa 2. En primer lugar, que las tramas elijan una ruta deficiente al destino, pero lleguen. En este caso, la red podría experimentar un uso de ancho de banda elevado en enlaces que no deberían tener ese nivel de tráfico. En segundo lugar, que se descarten algunas tramas. Estos problemas se pueden identificar mediante las estadísticas del contador de errores y los mensajes de error de la consola en el switch o el router. En un entorno Ethernet, un ping extendido o continuo también revela si se descartan tramas.

- **Difusiones excesivas:** los sistemas operativos usan difusiones y multidifusiones ampliamente para detectar los servicios de red y otros hosts. Por lo general, las difusiones excesivas son el resultado de una de las siguientes situaciones: aplicaciones programadas o configuradas incorrectamente, grandes dominios de difusión de capa 2 o problemas de red subyacentes, como bucles de STP o rutas inestables.

- **Mensajes de la consola:** a veces, un router reconoce que se produjo un problema de capa 2 y envía mensajes de alerta a la consola. Generalmente, un router hace esto cuando detecta un problema con la interpretación de las tramas entrantes (problemas de encapsulación o entramado) o cuando se esperan keepalives pero no llegan. El mensaje de la consola más común que indica que existe un problema de Capa 2 es un mensaje que indica que el protocolo de línea está desactivado.

A continuación, se detalla ciertos problemas, esto con la finalidad de tener más información al momento de presentarse dichos syslogs.

Para el caso del evento SW_MATM-4-MACFLAP_NOTIF: está queriendo indicar que el dentro del switch existe un Loop en la red, y esto se debe a que está viendo la misma MAC

address en dos interfaces totalmente diferentes para 2 VLANs especificas (ejemplo: VLAN1 y 20).

Para el evento OSPF-5-ADJCHG: Dicho mensaje de error significa que las retransmisiones de los paquetes OSPF ocurren hasta que OSPF alcanza su límite de 25 retransmisiones. En ese momento, la adyacencia OSPF se reduce y se genera el mensaje de error. Y una solución a dicho syslog podría ser ejecutar el siguiente comando: **log-adyacency-changes detail** a la configuración OSPF en el dispositivo. Esto debería permitirnos ver más información sobre los cambios en los estados vecinos.(Cisco, 2017)

Mientras que para el syslog MAC_LIMIT-4-PORT_EXCEED y MAC_LIMIT-4-VLAN_EXCEED, La limitación de MAC protege contra la inundación de la tabla de conmutación de Ethernet y está habilitada en las interfaces de capa 2 (puertos). La limitación de movimiento de MAC detecta el movimiento de MAC y la suplantación de MAC en las interfaces de acceso. Está habilitado en las VLAN.(Juniper.net, 2021)

8.4. ANEXO E

Formulario De Registro De Fallos Y Soluciones

<table>
<tr><td colspan="2">  </td><td colspan="4">UNIVERSIDAD TÉCNICA DEL NORTE
FORMATO ÚNICO DE REPORTES DE FALLOS
DIRECCIÓN DE DESARROLLO TECNOLÓGICO E INFORMÁTICO</td></tr>
<tr><td colspan="3">Número de reporte:</td><td colspan="3">Fecha del reporte:</td></tr>
<tr><td colspan="3">Área/ Departamento:</td><td colspan="3">Fecha de solución:</td></tr>
<tr><td colspan="3">Reportado por:</td><td colspan="3">Tiempo empleado:</td></tr>
<tr><td colspan="6">Solucionado por:</td></tr>
<tr><td>Tipo de fallo:</td><td colspan="2">Software ☐</td><td colspan="2">Hardware ☐</td><td>Otros_____</td></tr>
<tr><td>Nivel de prioridad:</td><td>P1 ☐</td><td>P2 ☐</td><td>P3 ☐</td><td colspan="2">P4 ☐</td></tr>
<tr><td colspan="6">Detalle del dispositivo:</td></tr>
<tr><td>Tipo de dispositivo</td><td colspan="2">Descripción</td><td colspan="2">Marca</td><td>Modelo</td></tr>
<tr><td></td><td colspan="2"></td><td colspan="2"></td><td></td></tr>
<tr><td colspan="6">Diagnóstico del problema:</td></tr>
<tr><td>Tipo de solución</td><td colspan="2">Remota ☐</td><td colspan="3">Lugar físico ☐</td></tr>
<tr><td colspan="6">Detalle de la solución:</td></tr>
</table>

8.5. ANEXO F

Formulario De Registro De Configuraciones

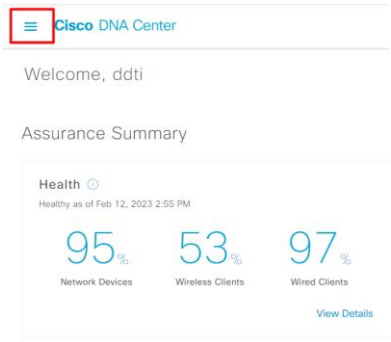
		UNIVERSIDAD TÉCNICA DEL NORTE					
		FORMATO ÚNICO DE REGISTRO DE CONFIGURACIONES					
		DIRECCIÓN DE DESARROLLO TECNOLÓGICO E INFORMÁTICO					
N°	Fecha y Hora (dd/mm/aa) / (hh:mm)	Marca y Modelo	Nombre del dispositivo	Ubicación del dispositivo	Dirección IP	Tipo de Dispositivo	Configuración realizada

8.6. ANEXO G

A continuación, se presenta el procedimiento para generar reportes mediante el software de gestión Cisco DNA Center, los reportes de mayor relevancia serán presentados por el asistente de la red para el posterior análisis del analista de la red. Como primer paso haga clic en el menú que se encuentra seleccionado en la Figura 202.

Figura 202

Menú principal

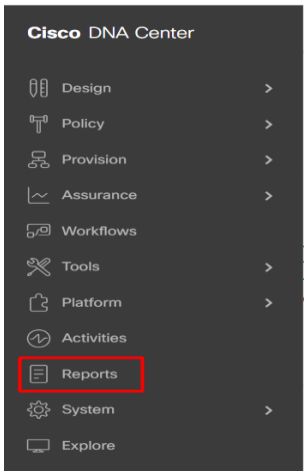


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Realizar clic en la función **Reports,** tal y como se observa en la Figura 203.

Figura 203

Función Reportes

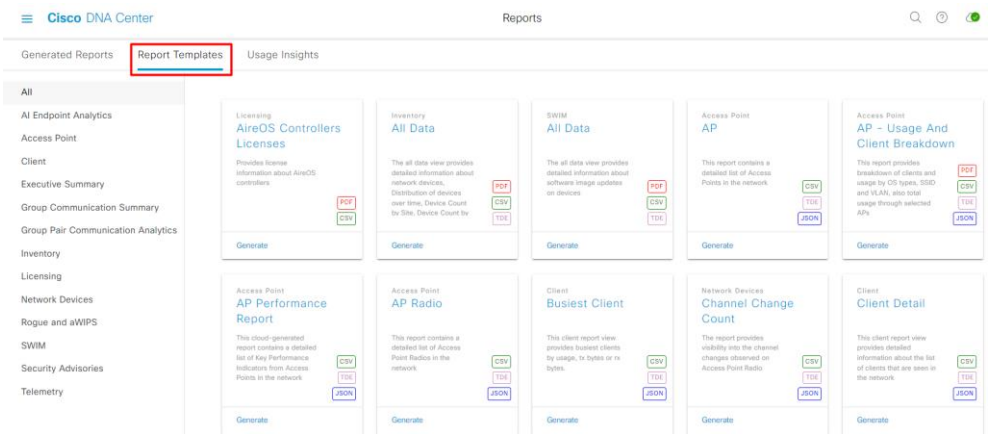


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

En la siguiente Figura 204 nos dirigimos a la pestaña **Report Templates** para visualizar las plantillas de informes que existen.

Figura 204

Ventana plantilla de informes

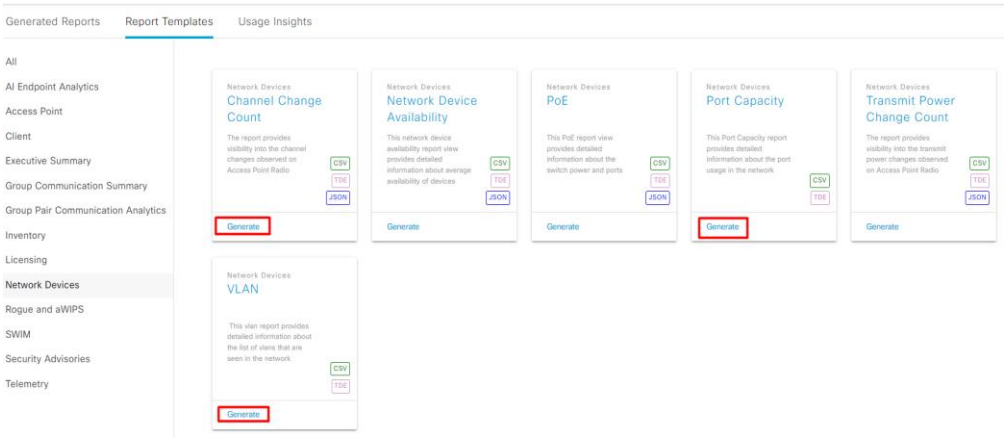


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Para generar un nuevo reporte deberá seleccionar un tipo de formato para el informe y luego realizar clic en Generar > Let´s Do it, tal y como se visualiza en la Figura 205.

Figura 205

Generar reporte

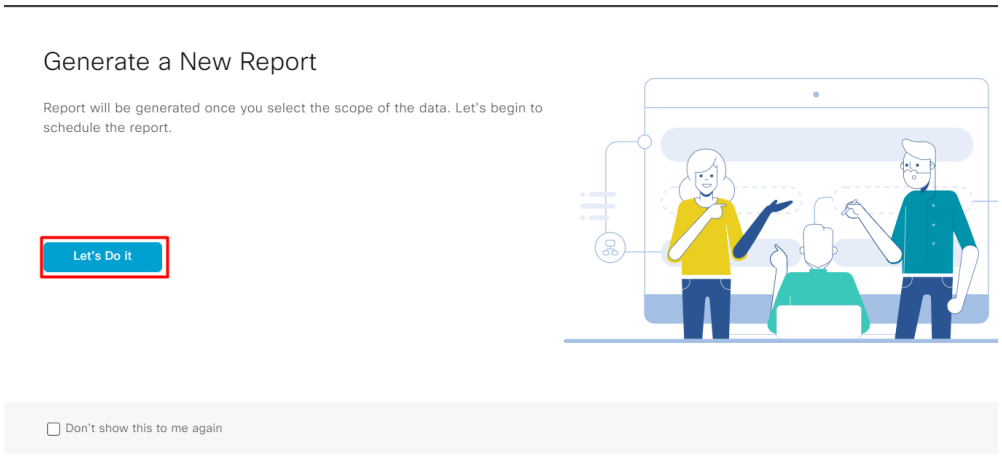


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

La Figura 206 presenta la acción de ejecutar un reporta realizando clic en el botón **Let´s Do it.**

Figura 206

Acción de realizar el reporte

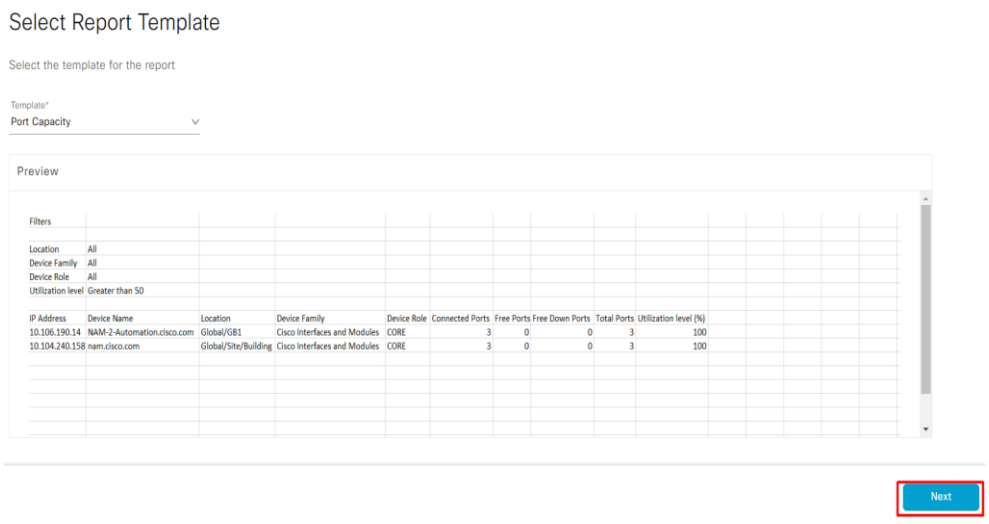


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

En la siguiente Figura 207 se selecciona la plantilla para el informe

Figura 207

Plantilla del informa para la capacidad de puertos

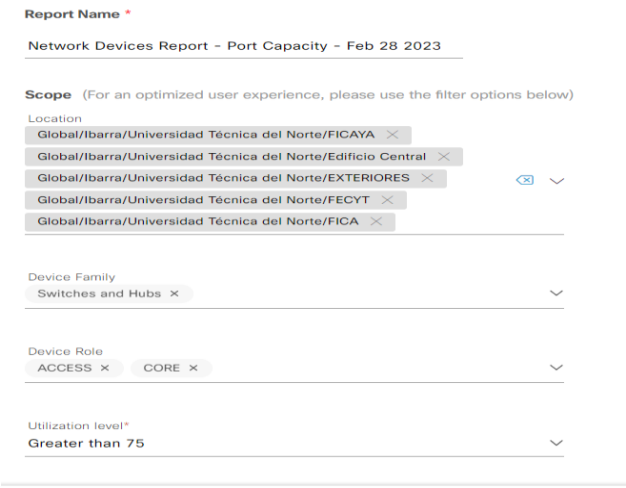


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

En la Figura 208 visualizamos como podemos escogemos parámetro como: nombre del reporte, como la ubicación, el tipo de dispositivo, rol de los dispositivos seleccionados y el nivel de utilización.

Figura 208

Parámetros del reporte

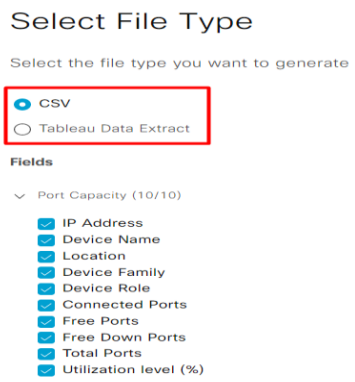


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

En la Figura 209 se muestra un resumen de las configuraciones realizadas para la generación de reportes y el formato de archivo (CSV, JSON, Tabla de datos).

Figura 209

Formato del reporte

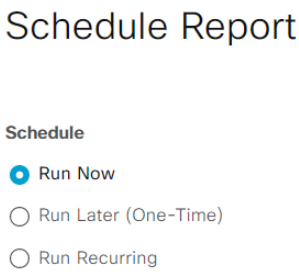


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

En la Figura 210 se procede a seleccionar la manera de programar el reporte (ejecutar ahora, ejecutar más tarde (una sola vez), ejecutar de forma recurrente).

Figura 210

Programación de tiempo para el reporte

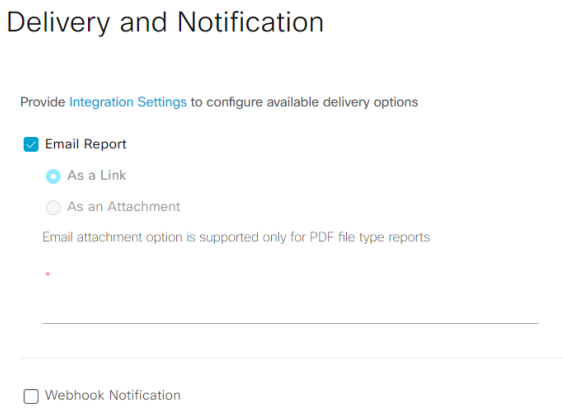


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

En la siguiente Figura 211 nos brinda la opción que el reporte a generar pueda llegar directamente a un correo en formato PDF, para esta ocasión se desmarca la opción y solo se generar el reporte. El administrador de la red tomara la decisión de colocar el correo de notificaciones para que el reporte le llegue como documento PDF.

Figura 211

Entrega y notificaciones del reporte

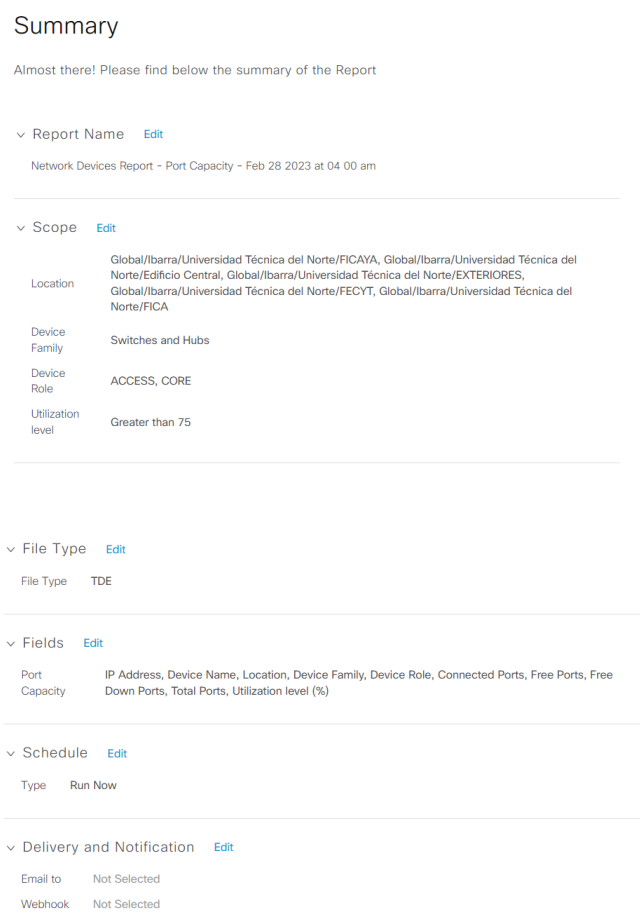


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

A continuación, en la Figura 212 se muestra un resumen de todos los parámetros elegidos a la hora de generar un reporte.

Figura 212

Resumen del reporte

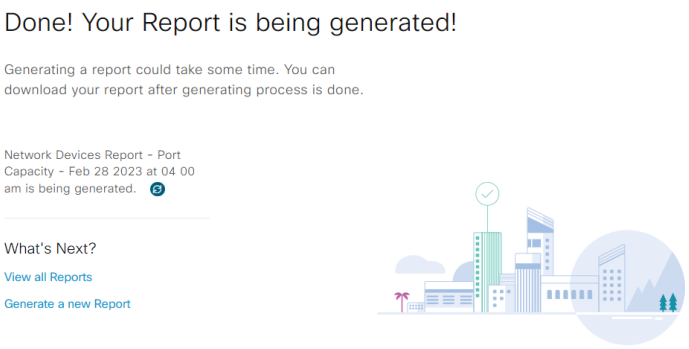


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

En la siguiente Figura 213 se observa que el reporte se ha generado exitosamente.

Figura 213

Reporte Generado

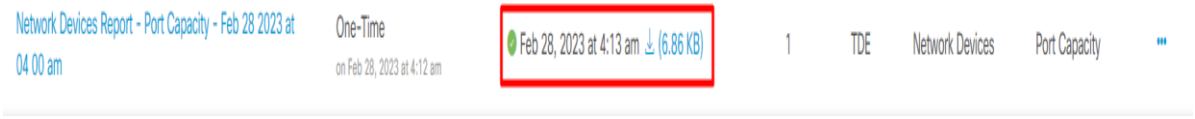


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

En la Figura 214 se indica que ya se puede descargar el reporte realizado

Figura 214

Reporte listo para descargar

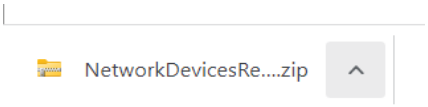


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

La Figura 215 indica el reporte ya descargo en un formato zip.

Figura 215

Reporte descargado



Fuente: Elaboración Autor

8.7. ANEXO H

En el siguiente ANEXO se precede a detallar el proceso de instalación del software FortiClient ya que es una solución VPN que permite el acceso remoto. En la siguiente Figura 216 se empieza el proceso de instalación.

Figura 216

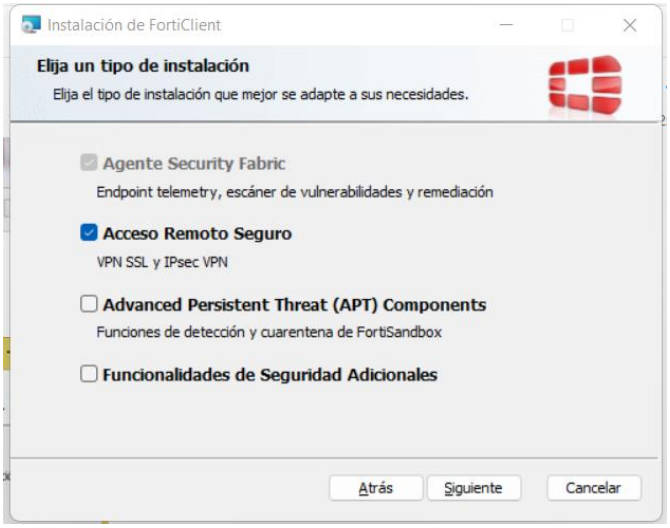
Asistente para la instalación de FortiClient

Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

En la Figura 217 se muestra el tipo de instalación que se desea realizar, para este caso será a través de un acceso remoto seguro por medio de una VPN SSL y Ipsec VPN.

Figura 217

Tipo de instalación

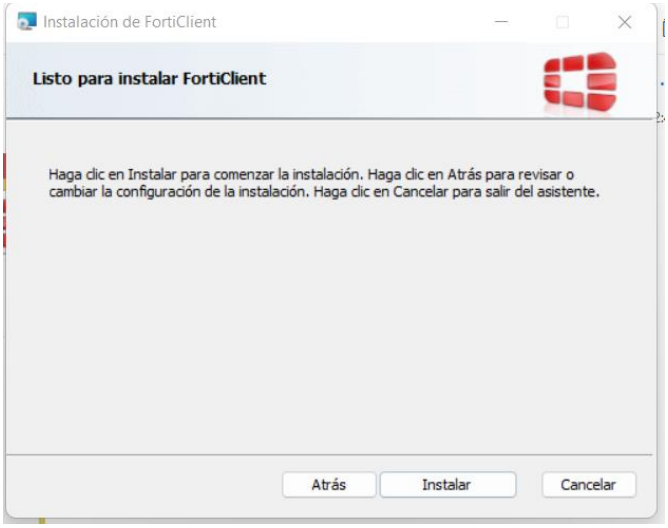


Fuente: Elaboración Autor

Se realiza clic en la opción instalar, tal y como se indica en la Figura 218.

Figura 218

Instalación lista para empezar.

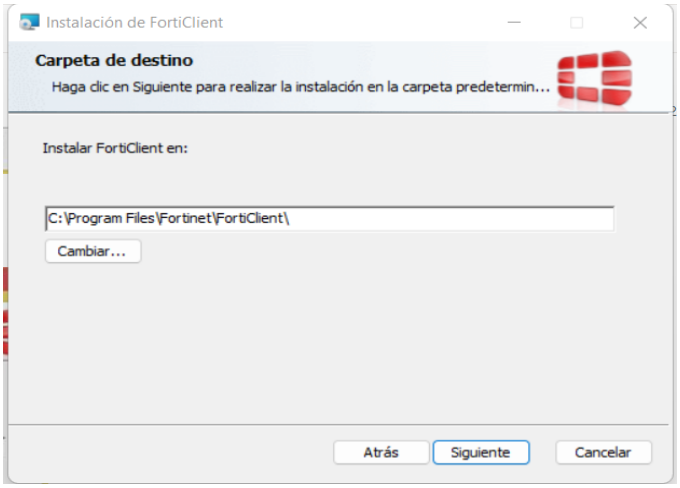


Fuente: Elaboración Autor

El siguiente paso es elegir la carpeta de destino para alojar al software y sus respectivos archivos, en la Figura 219 se muestra la ubicación por defecto que nos brinda el software, se mantiene la ubicación de la instalación y se da clic a siguiente.

Figura 219

Carpeta de destino para software

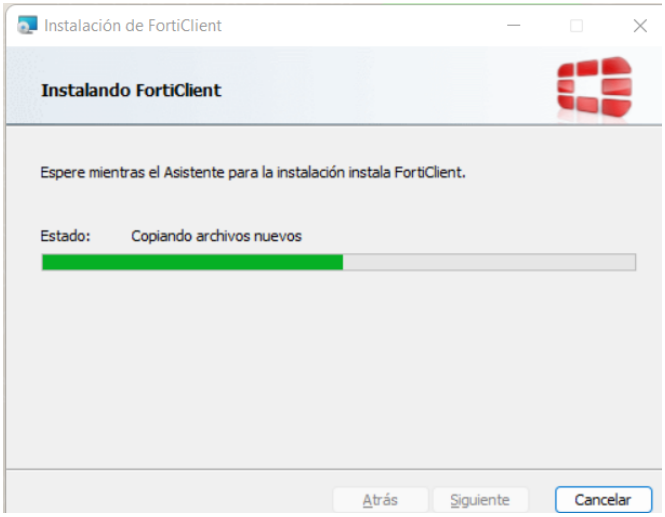


Fuente: Elaboración Autor

En la Figura 220 se muestra el proceso de instalación de FortiClient

Figura 220

Ejecución del proceso de instalación

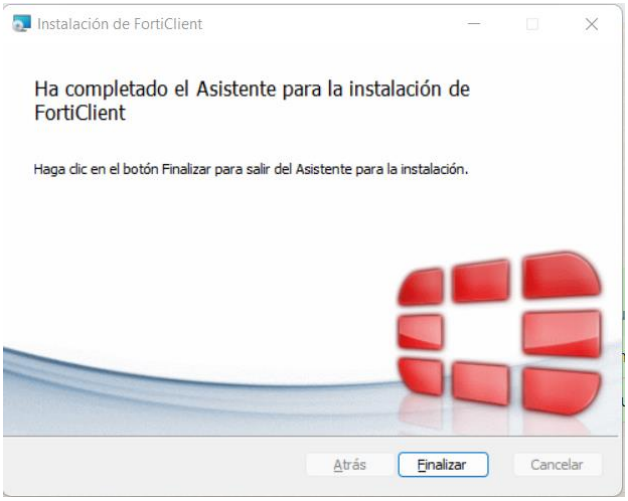


Fuente: Elaboración Autor

La Figura 221 indica la finalización de la instalación del software Forticlient

Figura 221

Instalación finalizada

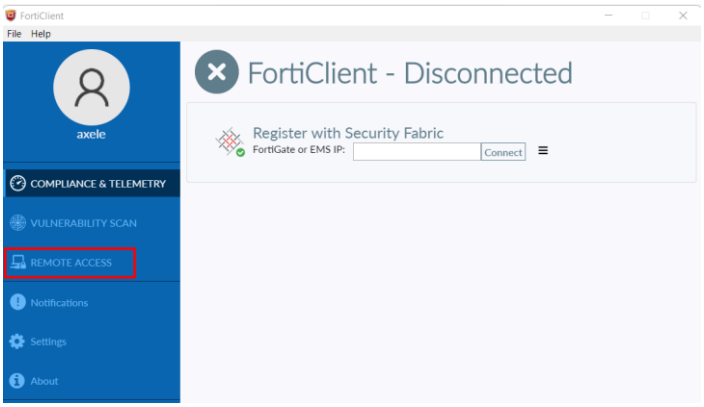


Fuente: Elaboración Autor

FortiClient realiza los respectivos escaneos de vulnerabilidades para poder establecer conexión, después de ello nos dirigimos a la pestaña REMOTE ACCESS, como se visualiza en la Figura 222.

Figura 222

Interfaz principal de FortiClient

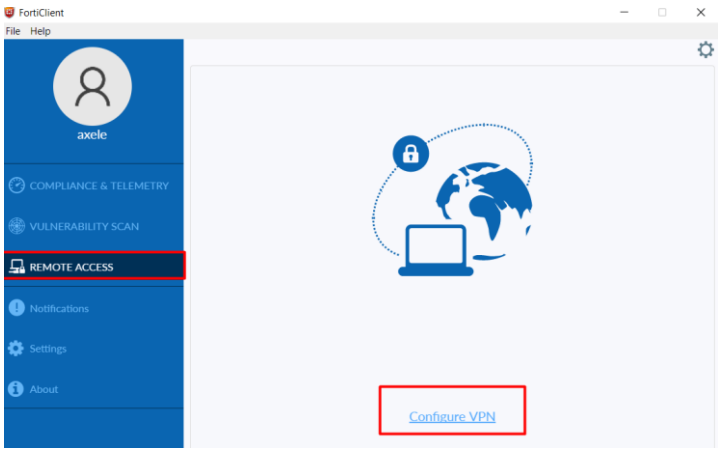


Fuente: Elaboración Autor

A continuación, en la Figura 223 se realiza la configuración de la VPN.

Figura 223

Configuración VPN

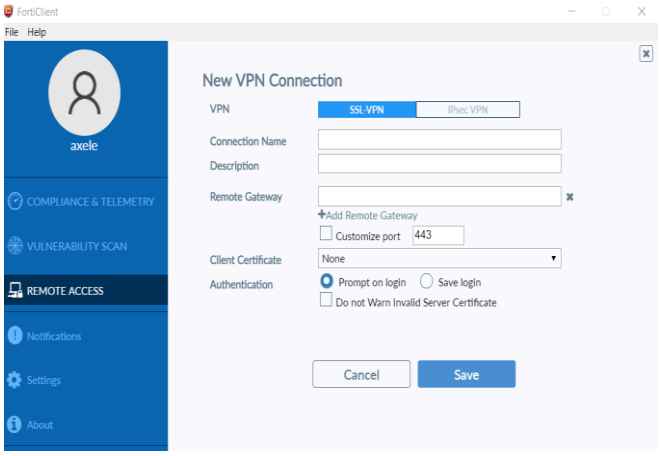


Fuente: Elaboración Autor

En la Figura 224 se visualizan los campos que se procederán a llenar con la información pertinente para así establecer la conexión VPN.

Figura 224

Campos para la nueva conexión VPN



Fuente: Elaboración Autor

La siguiente Figura 225 detalla los campos a llenar, los cuales son los siguiente.

Nombre de conexión: Axel_UTN

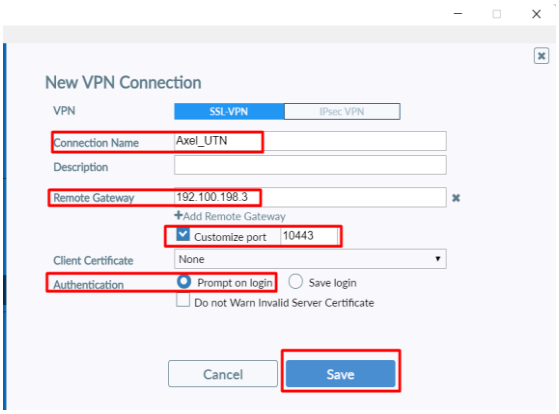
Gateway remoto: 192.100.198.3

Puerto personalizado: 10443

Autenticación: Preguntar al iniciar la sesión

Figura 225

Campos llenados con información



Fuente: Elaboración Autor

Nota. El puerto numero 10443 corresponde al componente de puerto de acceso remoto el cual cuya función es ser Puerto Proxy Rewriter.

Para seguir con el proceso de establecimiento de conexión mediante VPN, se procede a ingresar el usuario y contraseña asignado por parte del administrador de la red de la Universidad Técnica del Norte, tal y como se visualiza en la Figura 226.

Figura 226

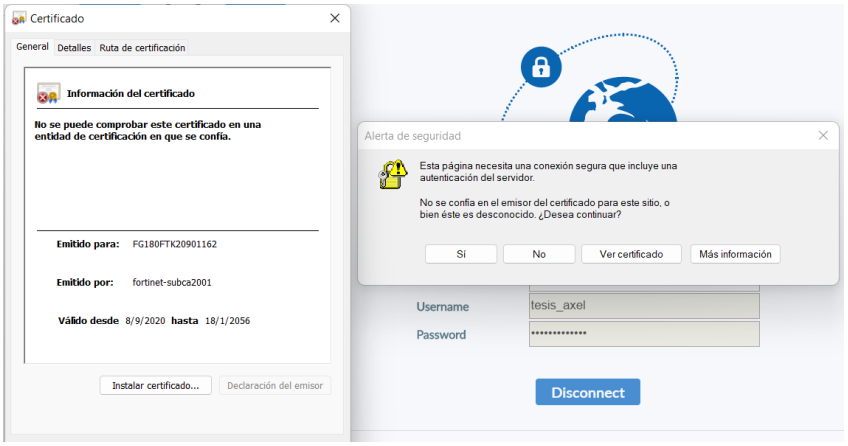
Ingreso de usuario y contraseña

Fuente: Elaboración Autor

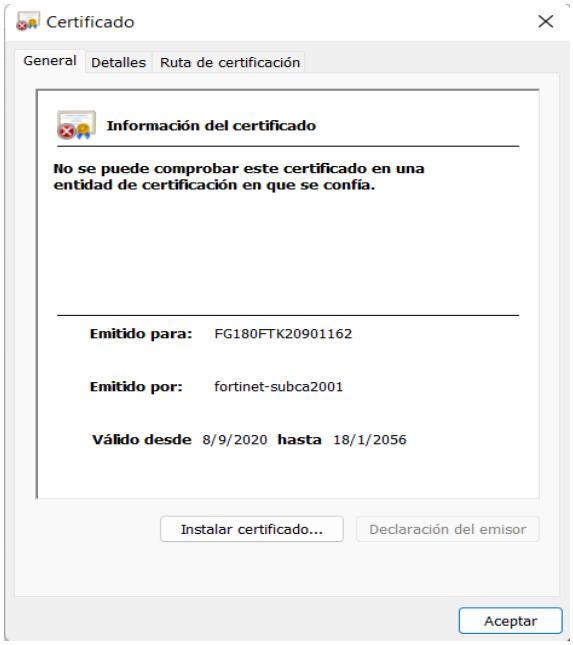
En la siguiente Figura 227 se muestra la generación de un certificado emitido por FortiClient.

Figura 227

Información del certificado



Fuente: Software FortiClient



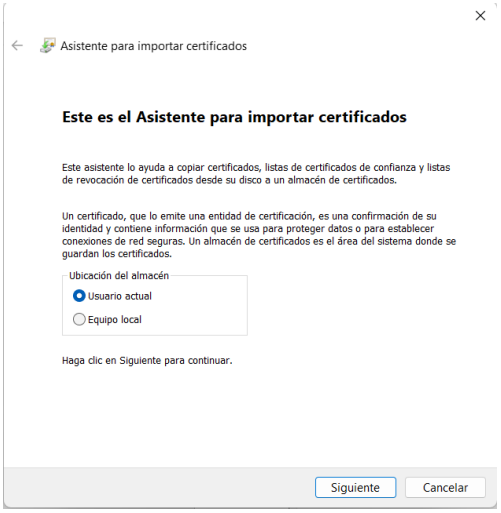
Fuente: Software FortiClient

En la siguiente Figura 228 se indica el asistente para importar certificados, lo cual confirma que el certificado emitido es legal, lo cual indica que se tiene un respaldo, una

confirmación de identidad y también contiene información que usa para proteger datos o para establecer conexiones seguras.

Figura 228

Asistente para importar certificados

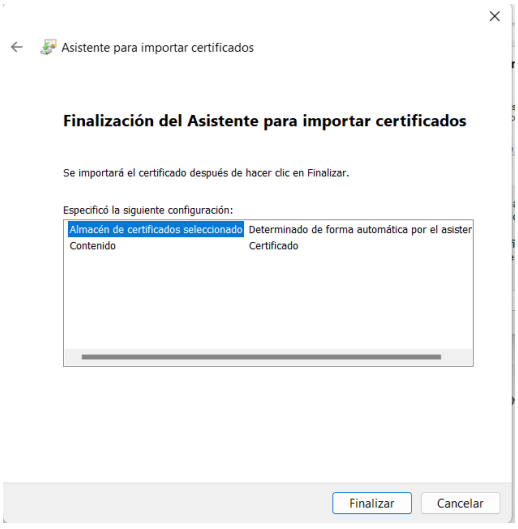


Fuente: Software FortiClient

En la Figura 229 se realiza uno de los últimos pasos para establecer la conexión remota a través de la VPN, donde se procede a almacenera el certificado generado.

Figura 229

Almacenamiento del certificado seleccionado

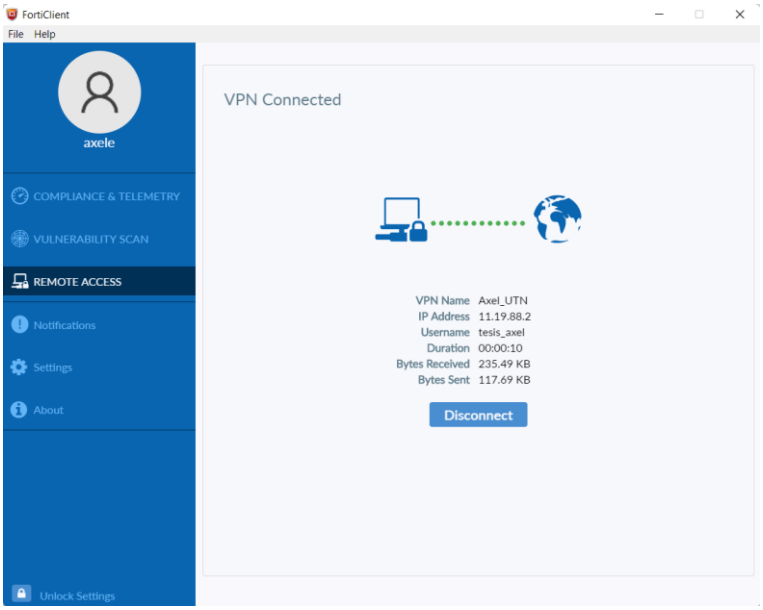


Fuente: Software FortiClient

Y como último paso se visualiza en la Figura 230 la conexión establecida a través de la VPN por medio del aplicativo FortiClient.

Figura 230

Conexión establecida por VPN



Fuente: Software FortiClient

8.8. ANEXO I

A continuación, se detallan los comandos que se ejecutaran en el interfaz (CLI) del dispositivo gestionado en caso de presentar umbrales que exceden su límite, esto con la finalidad de obtener gráficos estadísticos con más información de los umbrales de trabajo que se presentan en los dispositivos gestionados, lo cual permitirá al administrado de la red dar una solución rápida antes de que el dispositivo llegue a un estado crítico.

Los comandos que se presentaran a continuación permitirán repasar el estado de la memoria y de la CPU de aquellos dispositivos cisco que soporten estos comandos.

Los comandos que se deberían ejecutar se los presenta a continuación:

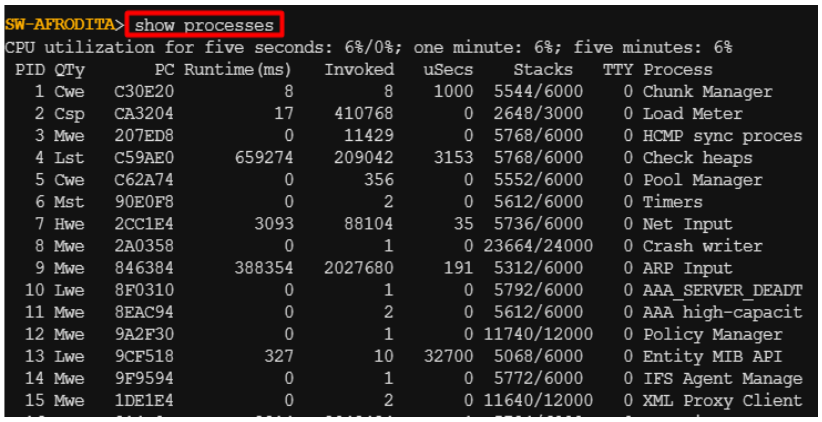
El comando **show processes** muestra información sobre los procesos activos en un dispositivo. El comando **show processes cpu** mostrara graficas estadísticas de uso de la CPU detalladas sobre este proceso, mientras que el comando **show processes memory** se utilizara para mostrar la cantidad de memoria usada.

- **Comando show processes**

En la Figura 231 se detalla el uso del comando show process en el SW-AFRODITA que se encuentra en la capa de core.

Figura 231

*Ejecución del comando **show procecesses***

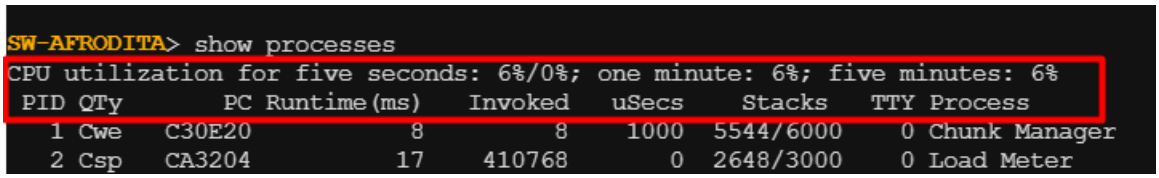


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

En la Figura 232 se detallan los campos del resultado del comando show processes.

Figura 232

Campos del resultado del comando show processes



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Por ello en la Tabla 128 descrita a continuación se detalla dichos campos.

Tabla 128

Campos y descripción del comando ejecutado

Campo	Descripción
Utilización del campo por 5 segundos	Utilización de la CPU durante los últimos 5 segundos. El numero siguiente muestra el porcentaje de tiempo de CPU que paso en el nivel de interrupción
Un minuto	Utilización de la CPU para el último minuto
Cinco minutos	Utilización de la CPU para los últimos 5 minuto
PID	ID de proceso
QTY	Prueba del programador. Valores posibles: * (que se ejecuta actualmente), E (que espera un evento), S (procesador listo para ejecutarse, abandonado voluntariamente), rd (preparado para ejecutarse, se han producido condiciones de activación), we (que espera un evento), sa (duerme hasta una hora absoluta), si (duerme durante un intervalo de tiempo), sp (duerme durante un intervalo de tiempo (llamada alternativa), st (duerme hasta que caduca un temporizador), hg (colgado; el proceso no se vuelve a ejecutar), xx (muerto: el proceso ha finalizado, pero aún no se ha eliminado).
PC	Contador de programa actual
Runtime (uS)	Tiempo de CPU que ha utilizado el proceso, en microsegundos
Invoked	Cantidad de veces que se ha activado el proceso
uSecs	Microsegundos de tiempo de CPU para cada invocación de proceso.

Stacks (pilas)	Marca de agua baja o espacio de pila total disponible, representado en bytes
TTY	Terminal que controla el proceso
Process	Nombre del proceso. Para más información, consulte la sección Procesos de este documento.

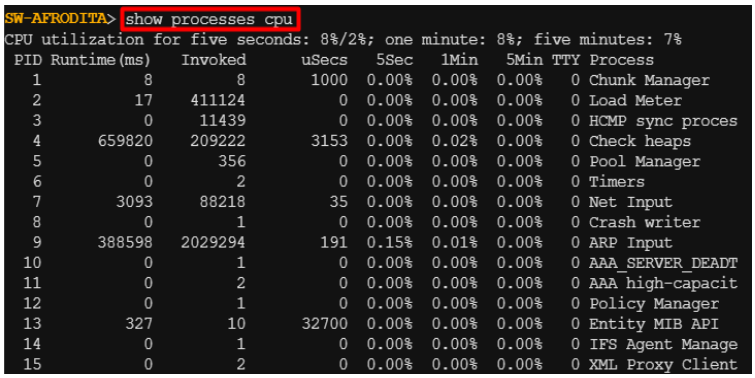
Fuente: Adapto de (CISCO, 2022)

- **Comando show processes cpu**

A continuación, en la Figura 233 se visualiza el comando show processes cpu detalla información sobre los procesos activos en el switch y sus estadísticas de uso de CPU.

Figura 233

*Ejecución del comando **show procecesses cpu***

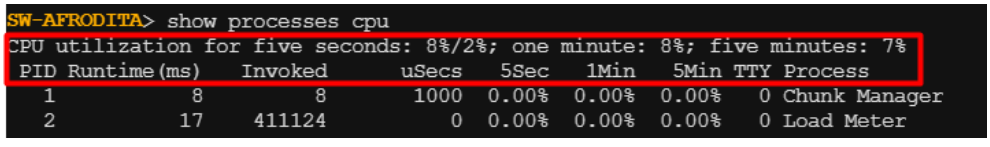


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

En la Figura 234 se detallan los campos del resultado del comando show processes.

Figura 234

Campos del resultado del comando show processes cpu



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Por ello, en la Tabla 129 descrita a continuación se detalla dichos campos.

Tabla 129

Campos y descripción del comando ejecutado

Campo	Descripción
Utilización del campo por 5 segundos	utilización de la CPU durante los últimos 5 segundos. El numero siguiente muestra el porcentaje de tiempo de CPU que paso en el nivel de interrupción
Un minuto	Utilización de la CPU para el último minuto
Cinco minutos	Utilización de la CPU para los últimos 5 minuto
PID	ID de proceso
Runtime (uS)	Tiempo de CPU que ha utilizado el proceso, en microsegundos
Invoked	Cantidad de veces que se ha activado el proceso
uSecs	Microsegundos de tiempo de CPU para cada invocación de proceso.
5 segundos	Utilización de la CPU por tarea en los últimos cinco segundos
1 minuto	Marca de agua baja o espacio de pila total disponible, representado en bytes
5 minutos	Terminal que controla el proceso
TTY	Terminal que controla el proceso.
Process	Nombre del proceso. Para más información, consulte la sección Procesos de este documento.

Fuente: Adaptado de (CISCO, 2022)

- **Comando show processes cpu history**

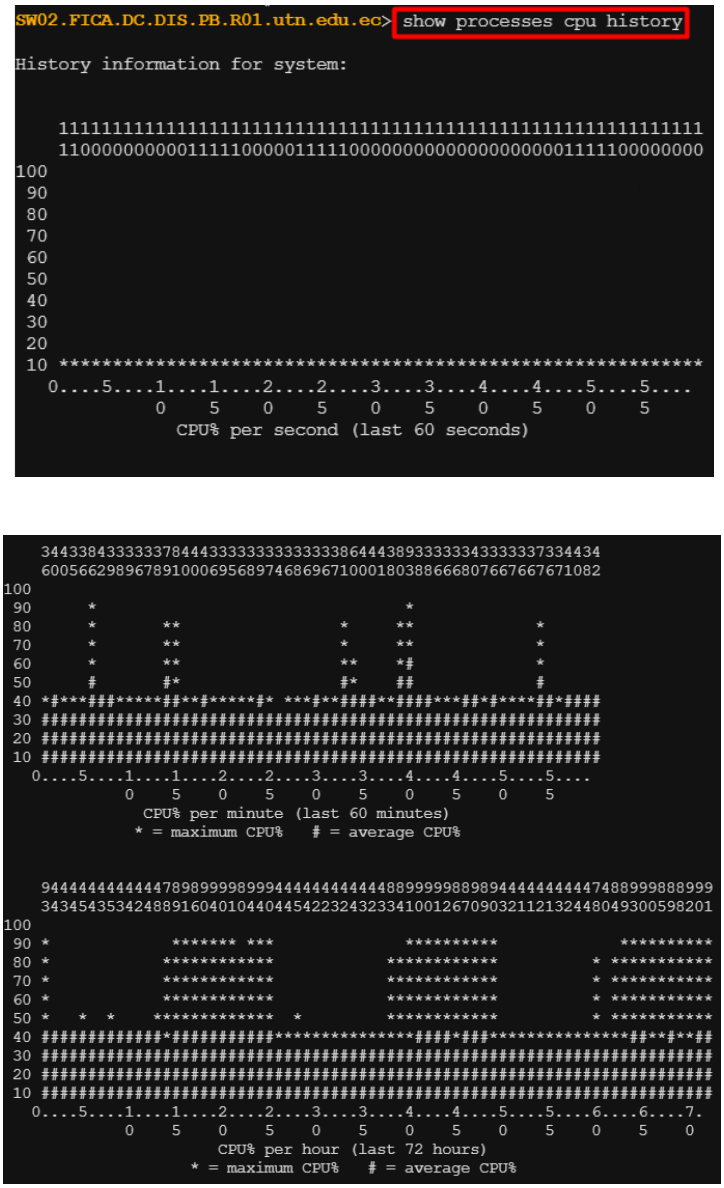
El comando **show processes cpu history** muestra en forma gráfica ASCII el uso total de la CPU en el switch durante un período de tiempo: un minuto, una hora y 72

horas, que se muestran en incrementos de un segundo, un minuto y una hora, respectivamente, tal como se evidencia en la Figura 235. El uso máximo se mide y registra cada segundo; el uso medio se calcula en períodos de más de un segundo.

A continuación, el comando ejecutado se lo realizo en el siwtch SW02.FICA.DC.DIS.PB.R01 que se encuentra en la capa de distribución.

Figura 235

*Ejecución del comando **show procecesses cpu***



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Se debe tener en consideración las siguientes indicaciones para el análisis de los grafico presentados anteriormente.

- El eje Y del grafico hace referencia a la utilización de la CPU. La medición más reciente se encuentra en el extremo izquierdo del eje X.
- El eje X del grafico indica el incremento dentro del periodo.
- Las dos filas superiores, leídas verticalmente, muestran el porcentaje más alto de utilización de CPU registrado mientras se incrementaba.

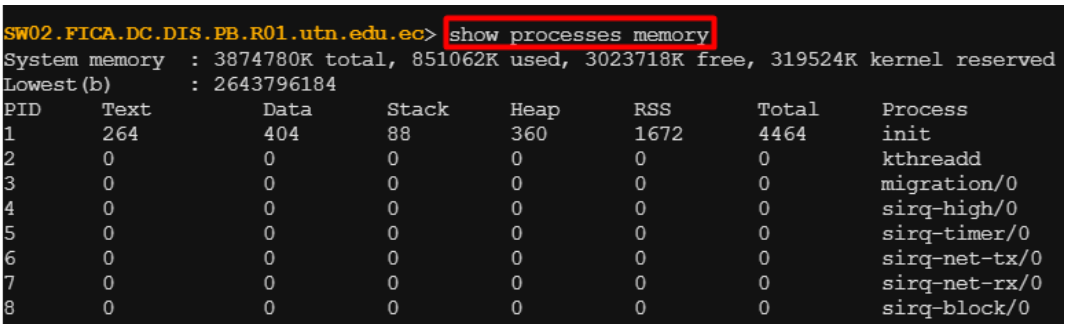
En la Figura 235 para la tercera representación gráfica, muestra la utilización de la CPU durante el último minuto registrado es del 45 por ciento. El switch puede alcanzar el 45% solo una vez durante ese minuto, o puede alcanzar el 45% varias veces; el switch registra solo el pico alcanzado mientras aumenta y el promedio a lo largo de ese incremento.

- **Comando show processes memory**

El comando **show processes memory** muestra información sobre los procesos activos en el switch y su memoria utilizada. En la siguiente Figura 236 se ejecuta el comando mencionado anteriormente, obtenido así los campos para dicho comando.

Figura 236

*Ejecución del comando **show procecesses memory***

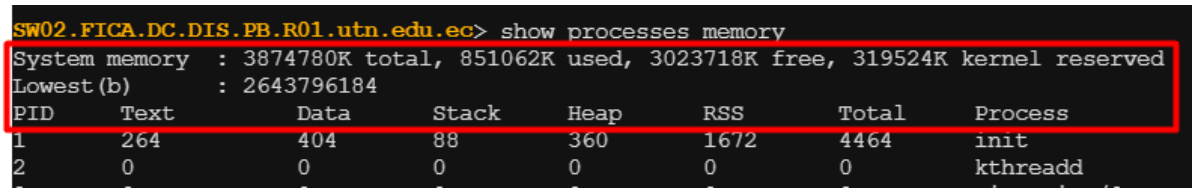


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

En la Figura 237 se detallan los campos del resultado del comando show processes.

Figura 237

Campos del resultado del comando show processes memory



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Por lo tanto, en la Tabla 130 describen los campos y las descripciones en el resultado del comando show processes memory.

Tabla 130

Campos y descripción del comando ejecutado

Campo	Descripción
Total	Cantidad total de memoria contenida.
Usado	Cantidad total de memoria utilizada.
Libre	Cantidad total de memoria libre.
PID	ID de proceso
TTY	Terminal que controla el proceso
Asignado	Bytes de memoria asignados por el proceso.
Liberado	Bytes de memoria liberados por el proceso, independientemente de quién lo haya asignado.
En espera	Cantidad de memoria que contiene un proceso. Este parámetro le ayuda a resolver problemas cuando se sospecha una fuga de memoria. Si un proceso consume memoria y ese consumo aumenta con el tiempo, es probable que se produzca una pérdida de memoria.

Getbufs	Cantidad de veces que el proceso ha solicitado un búfer de paquete.
Retbufs	Cantidad de veces que el proceso ha abandonado una memoria intermedia de paquetes.
Proceso	El nombre del proceso. Para más información, consulte la sección Procesos de este documento.
Total	Cantidad total de memoria en poder de todos los procesos.

Fuente: Adaptado de (CISCO, 2022)

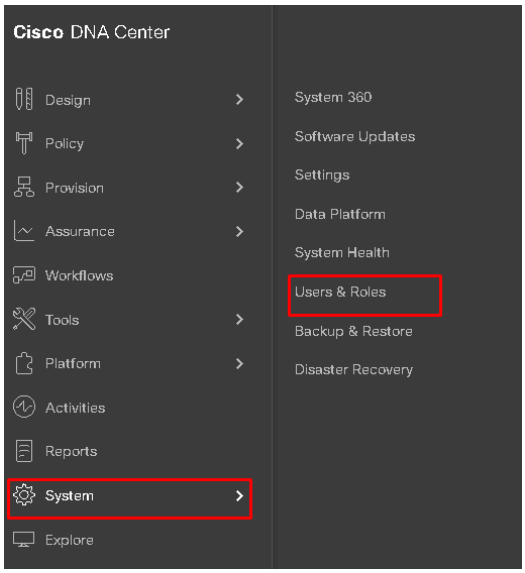
8.9. ANEXO J

Creación De Roles

Se accede al menú de Cisco DNA Center>system>users&roles, tal y como se visualiza en la Figura 238.

Figura 238

Usuario y roles

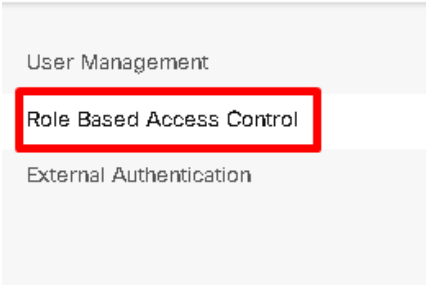


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

En la parte superior izquierda se selecciona role based Access control, como se muestra en la Figura 239 en el recuadro rojo

Figura 239

Creación de nuevo rol

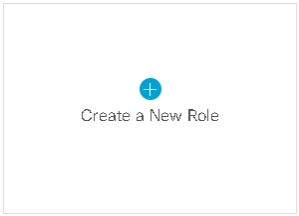


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Se selecciona créate new role, tal y como se observa en la Figura 240.

Figura 240

Acceso a nuevo rol

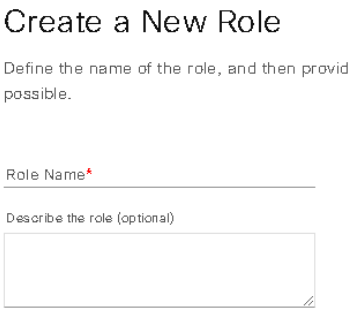


Fuente: Adaptado de Cisco DNA Center

Se ingresa un nombre de rol y un comentario para el rol(opcional), tal y como se visualiza en la Figura 241.

Figura 241

Nombre del nuevo rol



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Y se procede a seleccionar los accesos que poseerá el nuevo rol y asignar los permisos, en la siguiente Tabla 131 se muestran los accesos disponibles.

Tabla 131

Accesos para roles

Acceso	Sub-acceso	Permisos	Descripción
Assurance Garantice niveles de servicio consistentes con visibilidad completa en todos los aspectos de su red.	**Monitoring and Troubleshooting**	Deny Write Read	Garantice niveles de servicio consistentes con visibilidad completa en todos los aspectos de su red.
	Monitoring Settings	Deny Write Read	Acceso a los componentes relacionados con Network Analytics.
	Troubleshooting Tools	Deny Write Read	Configure la jerarquía de red, actualice su repositorio de imágenes de software y configure perfiles y configuraciones de red para administrar sus sitios y dispositivos de red.
Network Analytics Acceso a los componentes relacionados con Network Analytics.	**Data Access**	Deny Write Read	Acceso a las API del motor de consulta
Network Design Configure la jerarquía de red, actualice su repositorio de imágenes de software y configure perfiles y configuraciones de red	**Advanced Network Settings**	Deny Write Read	Actualice la configuración de red, como las credenciales globales del dispositivo, los servidores de políticas y autenticación, los certificados, el grupo de confianza, las claves de acceso a la nube, Stealthwatch, Umbrella y la anonimización de datos en la Configuración del sistema.

para administrar sus sitios y dispositivos de red	**Image Repository**	Deny Write Read	Administre imágenes de software y facilite mejoras y actualizaciones en entidades de red físicas y virtuales.
	Network Hierarchy	Deny Write Read	Administre imágenes de software y facilite mejoras y actualizaciones en entidades de red físicas y virtuales
	Network Profiles	Deny Write Read	Cree perfiles de red para enrutamiento, NFV empresarial, conmutación e inalámbrica, y asigne perfiles a los sitios. Esta función incluye Editor de plantillas, Etiquetado, Editor de configuración de modelos y Plantilla de autenticación.
	Network Settings	Deny Write Read	Configuración de red común en todo el sitio, como AAA, NTP, DHCP, DNS, Syslog, SNMP y Telemetría. Los usuarios con esta función pueden agregar un servidor SFTP y modificar el intervalo de resincronización de red en la configuración del sistema.
	Virtual Network	Deny Write Read	Administrar redes virtuales (VN). Segmente las redes físicas en múltiples redes lógicas para el aislamiento del tráfico y la comunicación entre VN controlada.
Network Provision Configure, actualice, aprovisione y administre sus dispositivos de red.	**Compliance**	Deny Write Read	Administrar la provisión de cumplimiento
	Image Update	Deny Write Read	Actualice una imagen de software en dispositivos que no coincidan con la configuración de Golden Image después de un ciclo de vida de actualización completo.
	Inventory Management	Deny Write Read	Descubra, agregue, reemplace o elimine dispositivos en su red mientras administra los atributos de los dispositivos y las propiedades de configuración.
	License	Deny Write Read	Escribir Vista unificada de su software y activos de red en relación con el uso y el cumplimiento de licencias
	Network Telemetry	Deny Write	Habilite o deshabilite la recopilación de telemetría de aplicaciones desde el dispositivo y configure los ajustes de telemetría asociados con el sitio

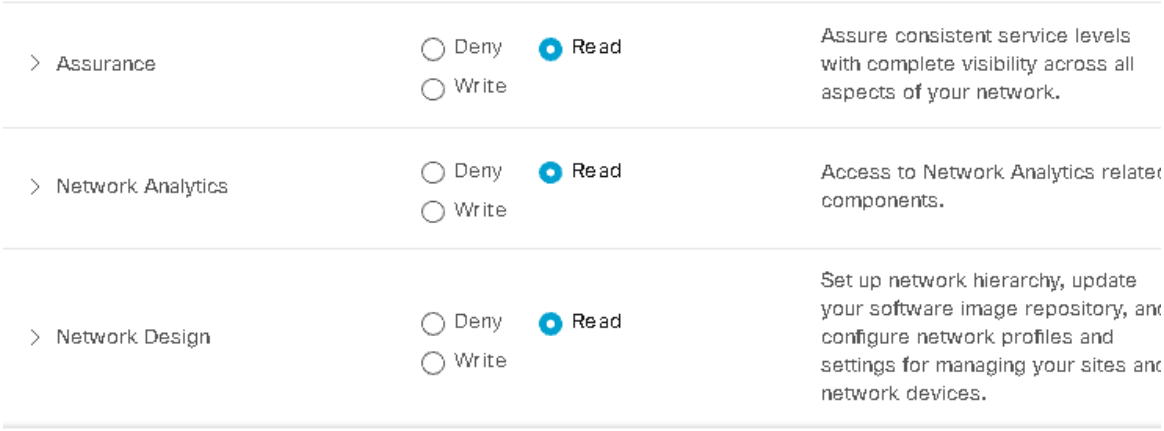
		Read	asignado y otros ajustes como Garantía de servicio inalámbrico, Certificados de controlador.
	PnP	Deny Write Read	Incorpore automáticamente nuevos dispositivos, asígnelos a sitios y configúrelos con configuraciones contextuales específicas del sitio.
	Provision	Deny Write Read	Este rol incluye Fabric, Política de aplicaciones, Visibilidad de aplicaciones, Nube, VPN de sitio a sitio, Red
Network Services Configure capacidades adicionales en la red más allá de la conectividad y el acceso básicos a la red	**App Hosting**	Deny Write Read	Implemente, administre y monitoree aplicaciones virtualizadas y basadas en contenedores que se ejecutan en dispositivos de red.
	Bonjour	Deny Write Read	Habilite el servicio bonjour de área amplia en su red para habilitar el descubrimiento de servicios basado en políticas.
	Stealthwatch	Deny Write Read	Configure elementos de red para enviar datos a Cisco Stealthwatch para detectar y mitigar amenazas, incluso en tráfico cifrado
	Umbrella	Deny Write Read	Configure los elementos de la red para usar Cisco Umbrella como la primera línea de defensa contra las amenazas de ciberseguridad.
Platform Plataforma abierta para flujos de trabajo accesibles basados en intenciones, intercambio de datos, notificaciones e integraciones de aplicaciones de terceros.	**APIs**	Deny Write Read	Impulse el valor accediendo a Cisco DNA Center a través de las API REST.
	Bundles	Deny Write Read	Mejore la productividad configurando y activando paquetes preconfigurados para la integración de ITSM.
	Events	Deny Write Read	Suscríbase para recibir notificaciones casi en tiempo real sobre eventos de interés en la red y el sistema e iniciar acciones correctivas.
	Reports	Deny Write Read	Genere informes usando plantillas de informes predefinidas para todos los aspectos de su red.

Security Administrar y controlar el acceso seguro a la red.	**Group-Based Policy**	Deny Write Read	Administre políticas basadas en grupos para redes que imponen la segmentación y el control de acceso según la etiqueta de grupo de seguridad de Cisco.
	IP Based Access Control	Deny Write Read	Administre listas de control de acceso basadas en IP que imponen la segmentación de la red según las direcciones IP
	Security Advisories	Deny Write Read	Escanee la red en busca de avisos de seguridad. Revise y comprenda el impacto de los avisos de seguridad de Cisco publicados que pueden afectar su red.
System Administración centralizada de su Cisco DNA Center, que incluye administración de configuración, conectividad de red, actualizaciones de software y más.	**Machine Reasoning**	Deny Write Read	Configure actualizaciones automáticas de la base de conocimientos de razonamiento automático para identificar rápidamente las vulnerabilidades de seguridad y mejorar el análisis automatizado de problemas
	System Management	Deny Write Read	Administre la funcionalidad central del sistema y la configuración de conectividad. Este rol incluye Credenciales de Cisco, Verificación de integridad, EULA del dispositivo, HA, Configuración de integración, Recuperación ante desastres, Registros de depuración, Recopilación de telemetría
Utilities One-stop-shop productivity resource for the most commonly used troubleshooting tools and services.	**Audit Log**	Deny Write Read	Registro detallado de los cambios realizados a través de la interfaz de usuario o API en los dispositivos de red o Cisco DNA Center.

Se procede a seleccionar los accesos para el nuevo rol que se mostraron anteriormente, la selección se presenta como se muestra en la Figura 242.

Figura 242

Asignación de accesos



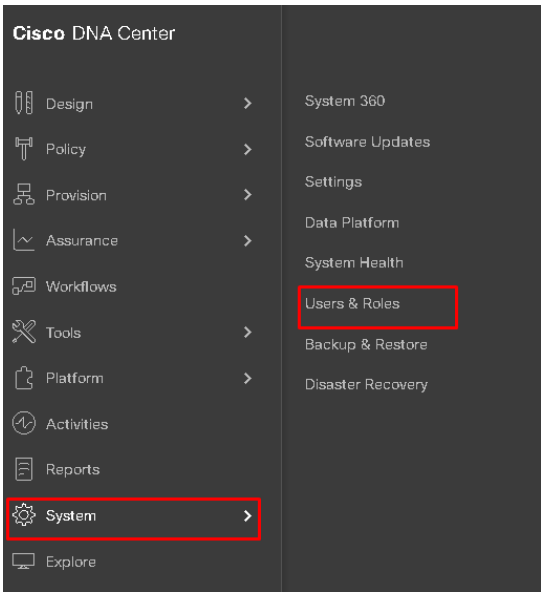
Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Creación de usuarios

Se accede al menú de Cisco DNA Center>system>users&roles, en la Figura 243 se visualiza las opciones a escoger.

Figura 243

Roles y usuarios

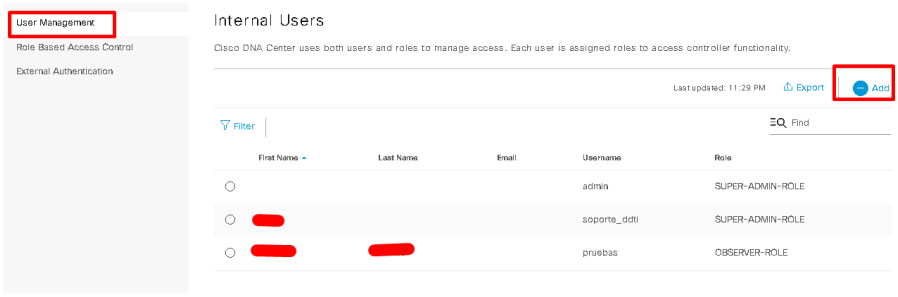


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

En la parte superior izquierda se selecciona user managament y add, tal y como se observa en la Figura 244.

Figura 244

Agregar nuevo usuario

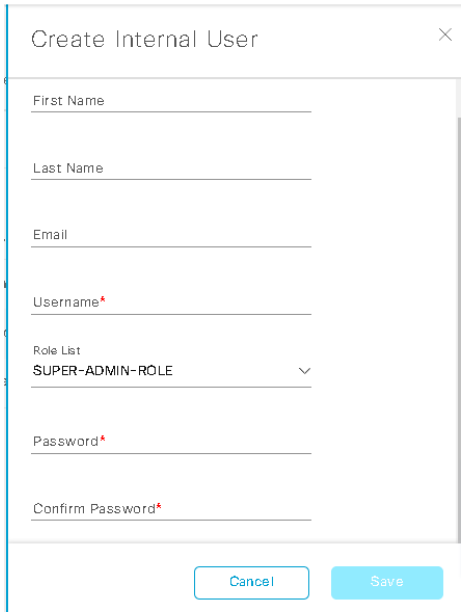


Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

Y se procede a asignar las credenciales y el rol que poseerá el nuevo usuario, los campos a llenar se muestran a continuación, tal como se visualiza en la Figura 245:

Figura 245

Parámetros para nuevo usuario



Fuente: Adaptado Cisco DNA Center del DDTI de la UTN

8.10. ANEXO K

A continuación, se presenta la instalación del distro Alma Linux, se eligió este distro ya que no dios fallos al momento de realizar su instalación y seguido de ello se presenta un manual de uso de algunas herramientas del programa de software libre phpIPAM.

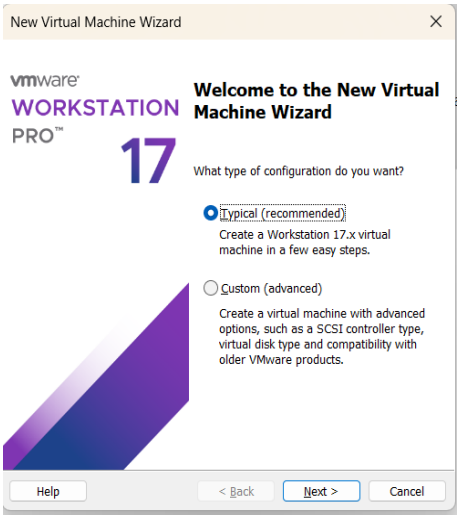
Como primer paso se va a documentar los pasos para la instalación de Alma Linux en VMware.

Instalación de alma Linux en VMware

En la siguiente Figura 246 se selecciona la instalación típica y recomendada.

Figura 246

Instalación recomendada

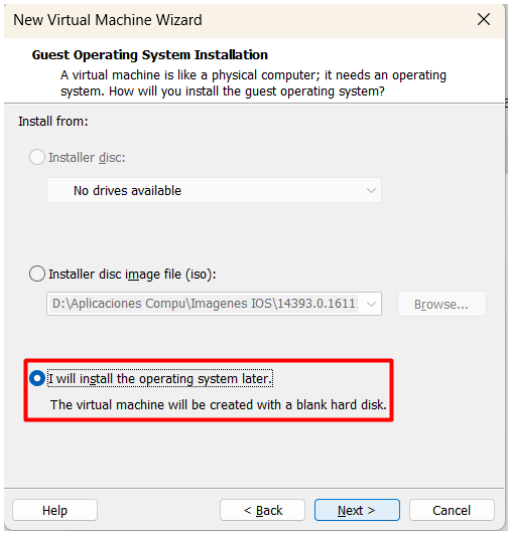


Fuente: Elaboración Autor

La siguiente Figura 247 presenta la selección de la instalación para la máquina virtual, la cual se creará un disco duro en blanco.

Figura 247

Instalación de un sistema operativo invitado

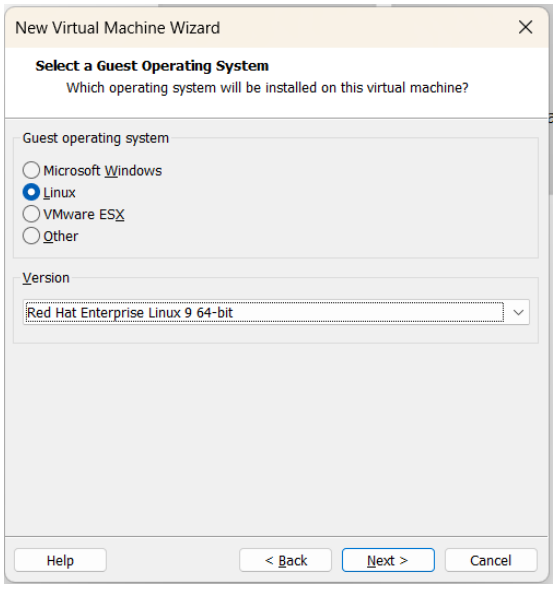


Fuente: Elaboración Autor

En la siguiente Figura 248 se elige el sistema operativo a escoger para instalar, en este caso es Linux con versión **Red Hat Enterprise Linux 9 64-bit.**

Figura 248

Selección del sistema operativo

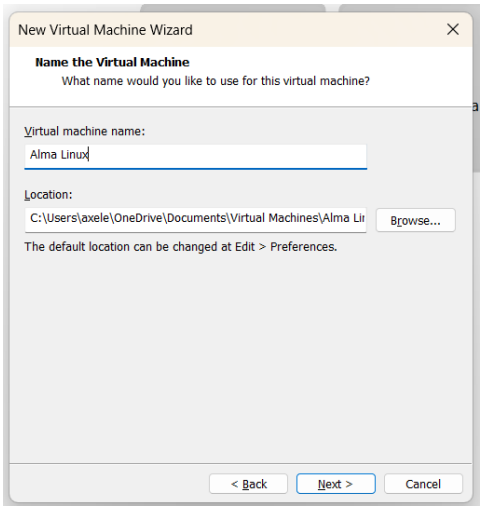


Fuente: Elaboración Autor

A continuación, en la Figura 249 se presenta el nombre de la máquina virtual y la ubicación de esta.

Figura 249

Nombre y ubicación de la máquina virtual

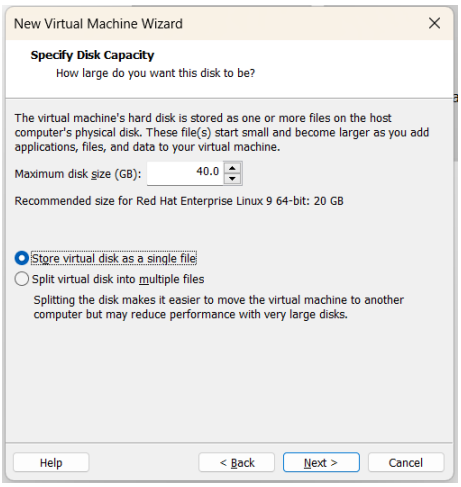


Fuente: Elaboración Autor

Se coloca el espacio que sea optimo en el disco y se elige la opción de almacenar el disco virtual como un único archivo, como se observa en la Figura 250.

Figura 250

Especificación d la capacidad del disco

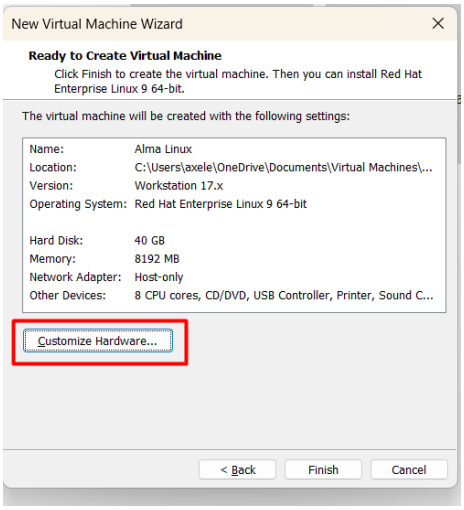


Fuente: Elaboración Autor

En los siguientes pasos se van a realizar configuración personalizadas de hardware, esto dependerá del administrador y de las capacidades del equipo. En la siguiente Figura 251 se dirige a el icono de **Customize Hardware.**

Figura 251

Personalización del hardware

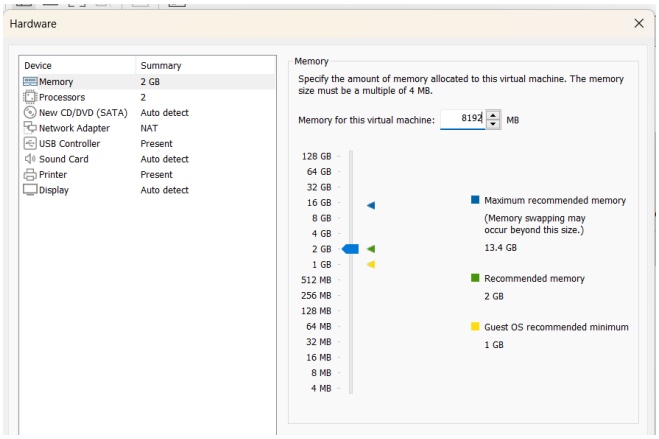


Fuente: Elaboración Autor

En la siguiente Figura 252 se especifica la cantidad de memoria asignada a la máquina virtual y para este caso se dispondré de 8192 MB.

Figura 252

Selección de memoria

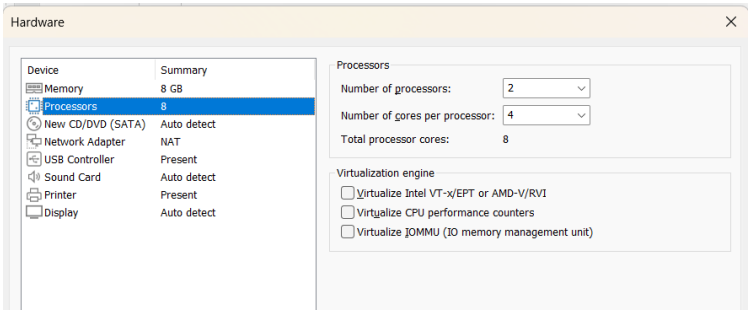


Fuente: Elaboración Autor

Se selección el número de procesadores y el número de núcleos por procesador, como se evidencia en la Figura 253.

Figura 253

Procesadores

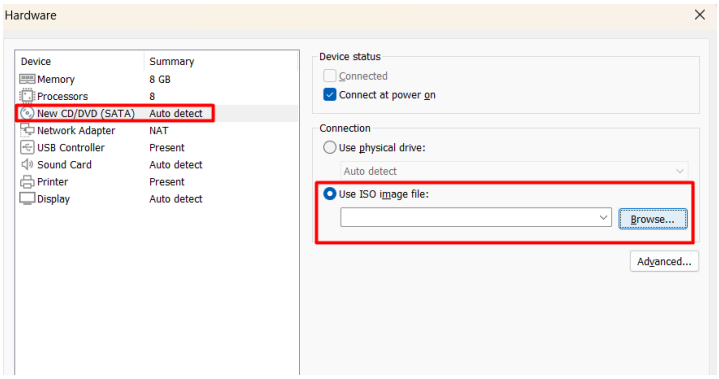


Fuente: Elaboración Autor

A continuación, se procede a selección la imagen ISO de la máquina virtual a instalar, tal y como se visualiza en la Figura 254.

Figura 254

Selección de la imagen ISO

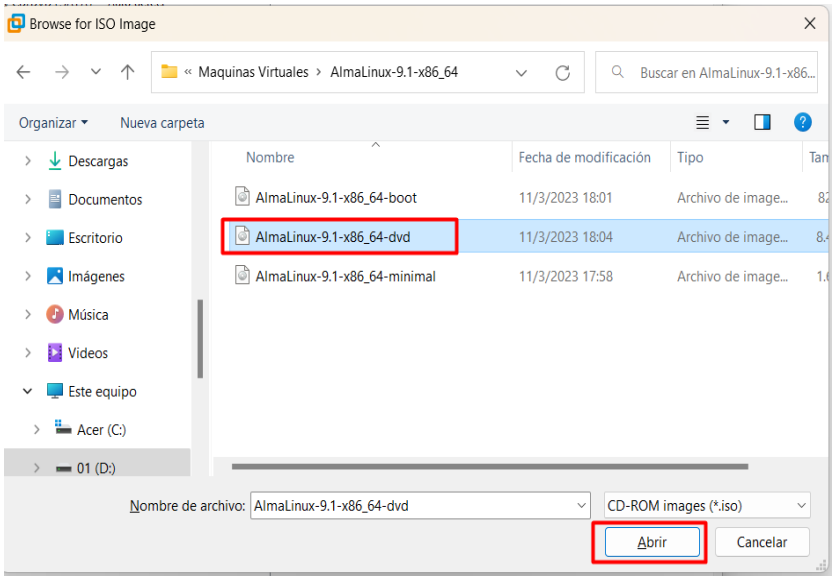


Fuente: Elaboración Autor

En la siguiente Figura 255 se selección el archivo correspondiente a la imagen ISO de la máquina virtual Alma Linux.

Figura 255

Selección de la imagen ISO

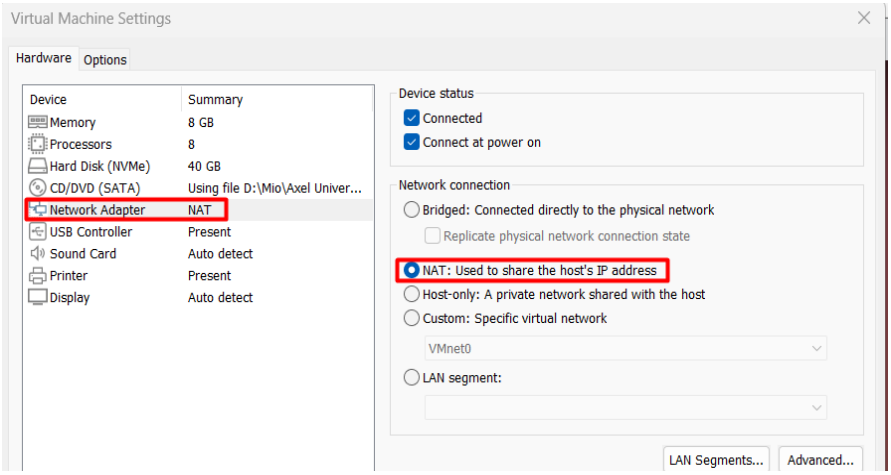


Fuente: Elaboración Autor

También se procede a selección el adaptador de red, para este caso se selección el adaptador NAT el cual se utiliza para compartir la dirección IP del host, tal y como se observa en la Figura 256.

Figura 256

Adaptador de red

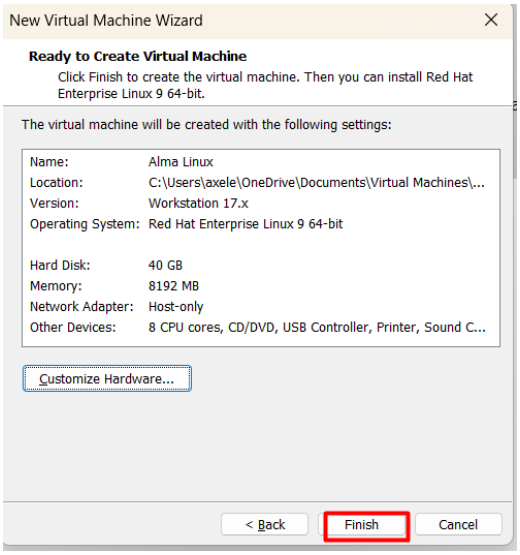


Fuente: Elaboración Autor

En la siguiente Figura 257se procese de finalizar el proceso de personalizar los parámetros del hardware.

Figura 257

Finalización a la personalización del hardware

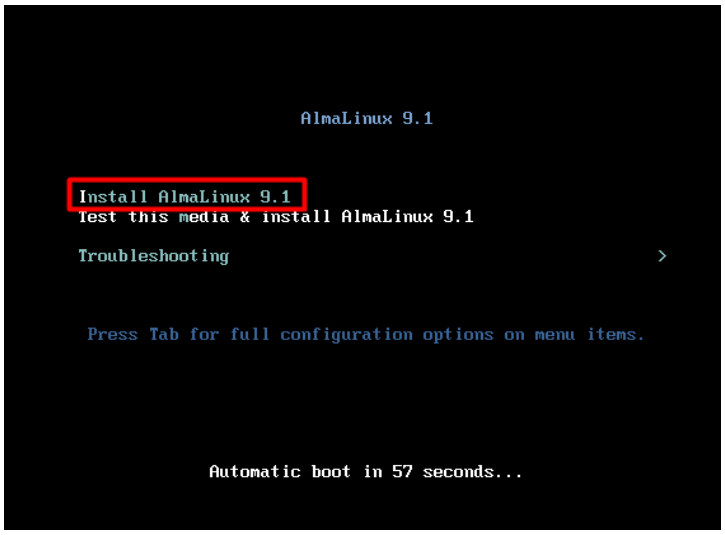


Fuente: Elaboración Autor

A continuación, se presenta el proceso de instalación del distro Alma Linux y el programa de software libre phpIPAM. En la Figura 258 seleccionamos la primera opción de instalar AlmaLinux 9.1.

Figura 258

Instalación de AlmaLinux 9.1

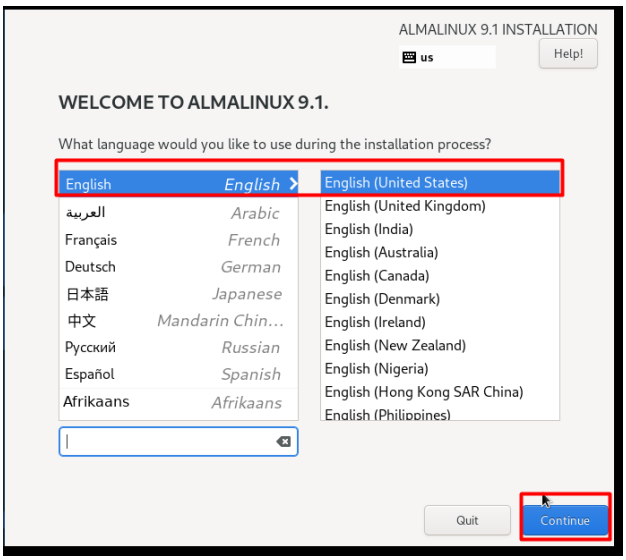


Fuente: Elaboración Autor

Se elige el idioma a instalar, para la siguiente Figura 259 se escoge el idioma de inglés.

Figura 259

Selección de idioma

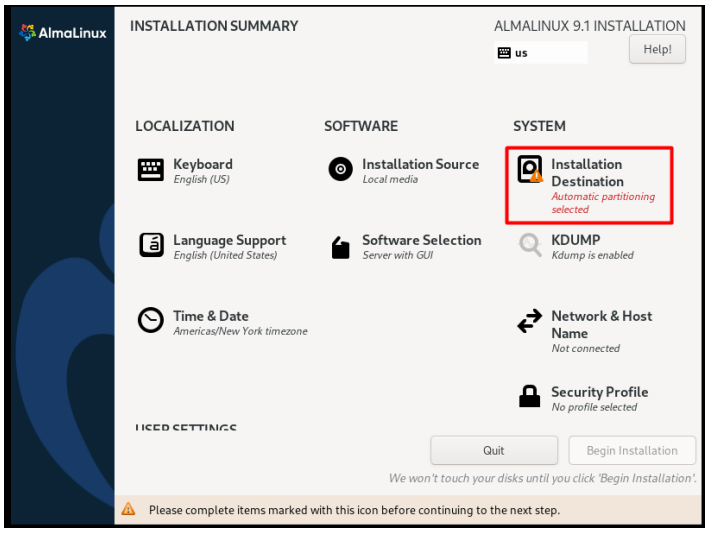


Fuente: Elaboración Autor

En la Figura 260 se observa la selección de instalación automática.

Figura 260

Resumen de la instalación

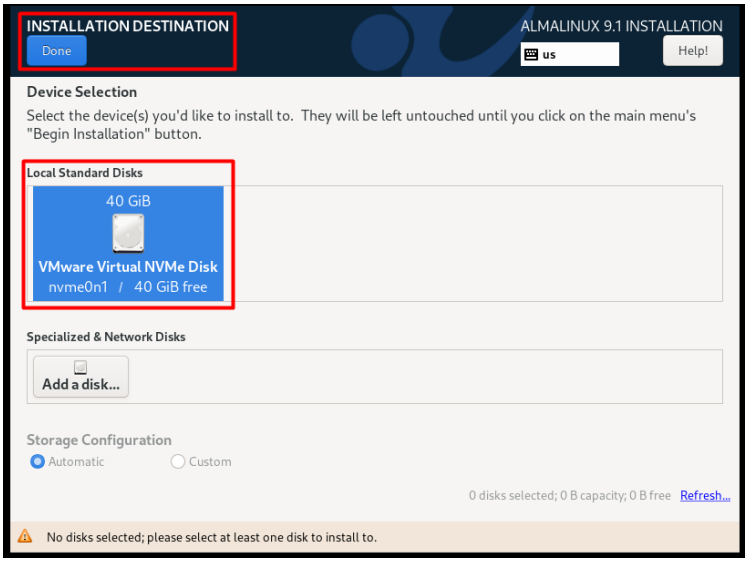


Fuente: Elaboración Autor

En la Figura 261 se observa la selección del destino de instalación.

Figura 261

Selección de Disco estándar local

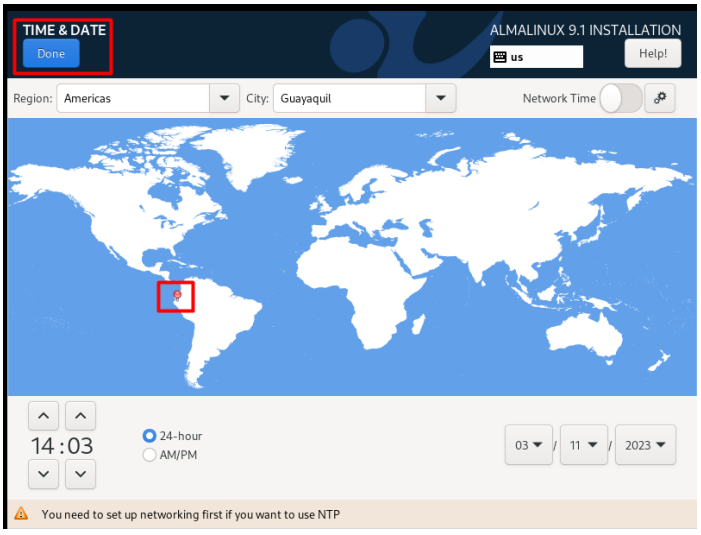


Fuente: Elaboración Autor

En la Figura 262 se configura la fecha y hora con la finalidad de tener una máquina virtual sincronizada para no tener eventualidad.

Figura 262

Configuración de Fecha y Hora

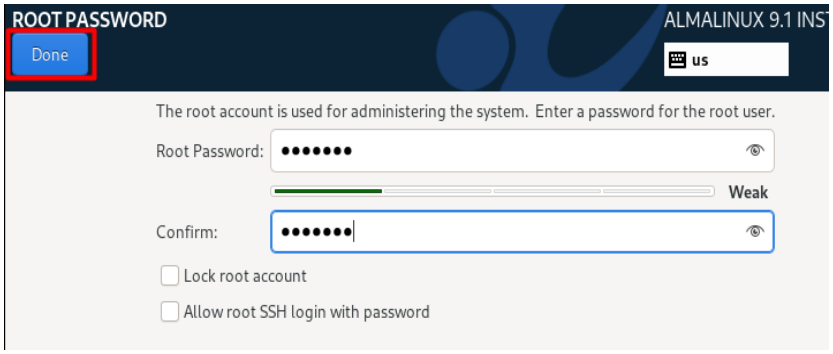


Fuente: Elaboración Autor

También se realiza el ajuste de usuarios donde se crea una contraseña para el ingreso a la máquina virtual, tal y como se evidencia en la siguiente Figura 263, se toma en cuenta que la clave colocada es: 0123456

Figura 263

Establecimiento de contraseña

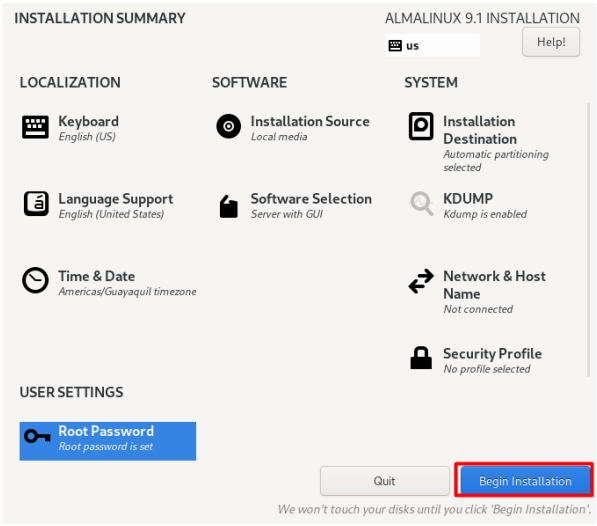


Fuente: Elaboración Autor

A continuación, se procede a comenzar la instalación, realizando clic en el botón Azul que se encuentra seleccionad, de tal manera como se visualiza en la Figura 264.

Figura 264

Comienzo de la instalación

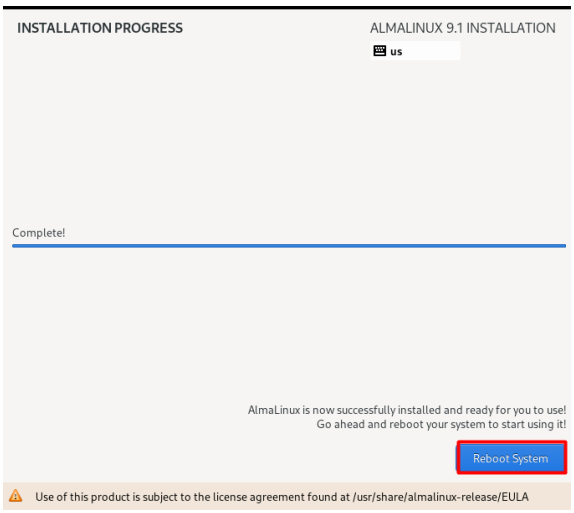


Fuente: Elaboración Autor

En la Figura 265 se visualiza el proceso de instalación finalizado, por lo cual se procede a reiniciar el sistema.

Figura 265

Proceso de instalación culminado

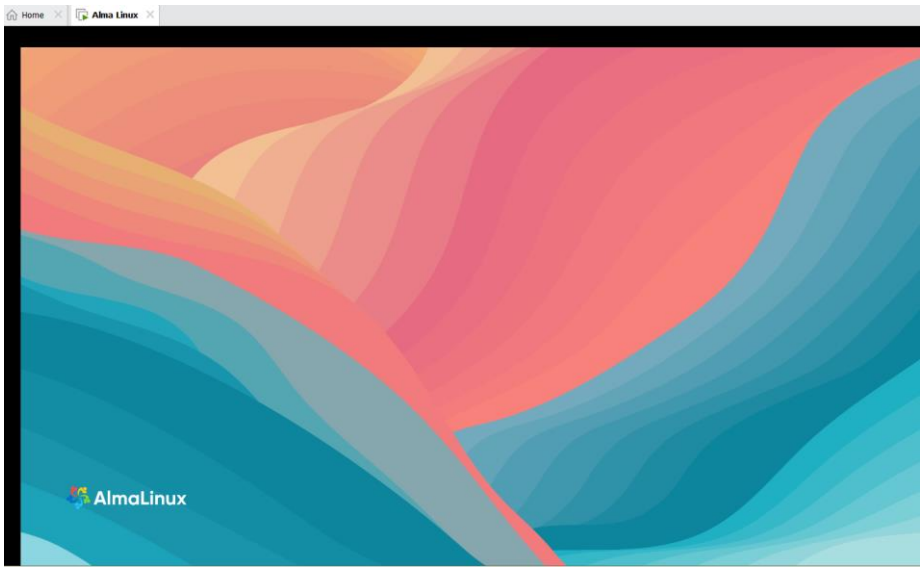


Fuente: Elaboración Autor

La Figura 266 muestra la pantalla principal del distro Alma Linux ya instalado.

Figura 266

Interfaz del Alma Linux

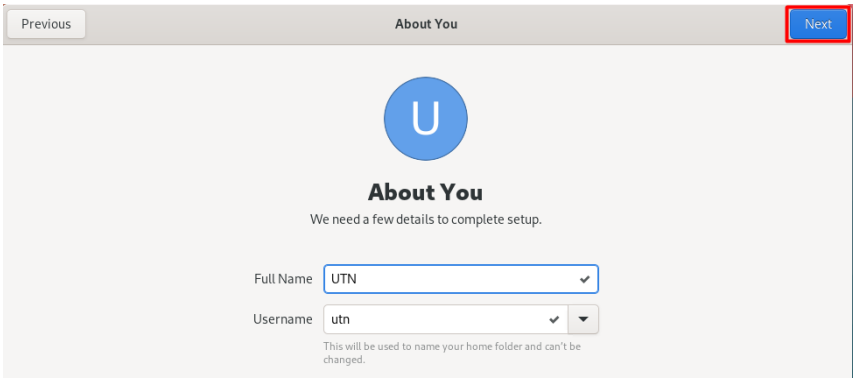


Fuente: Elaboración Autor

A continuación, se seguirán los siguientes pasos para la creación de un usuario y su respectiva contraseña, tal y como se visualiza en la Figura 267.

Figura 267

Creación de usuario

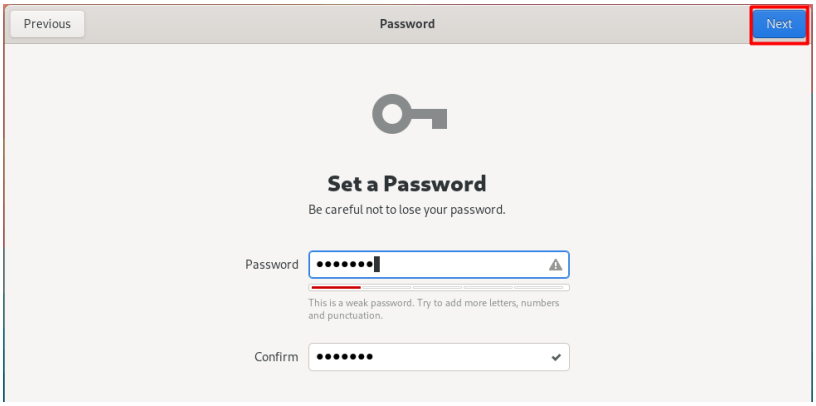


Fuente: Elaboración Autor

También se establece la Clave, la cual es: 0123456, tal y como se visualiza en la Figura 268.

Figura 268

Establecimiento de contraseña

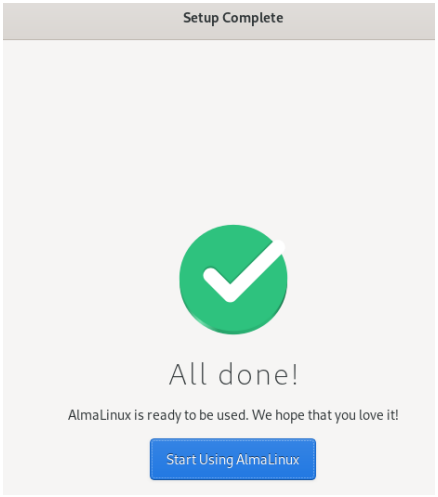


Fuente: Elaboración Autor

En la Figura 269 se completaron los pasos para la creación del usuario y su contraseña.

Figura 269

Creación de usuario realizado con éxito



Fuente: Elaboración Autor

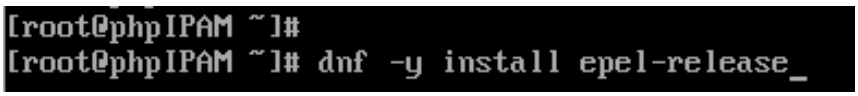
A continuación, se presenta la instalación del software libre phpIPAM

Paso 1: Instalación de repositorios y actualización

En la Figura 270 se procede a instalar los paquetes de Extra Packages Enterprise Linux que proporcionan paquetes de alta calidad para empresas el siguiente comando**# dnf -y install epel-release.**

Figura 270

Instalación de repositorio



Fuente: Elaboración Autor

Se procede a instalar el paquete remi-release paquete que proporciona la configuración del repositorio para YUM / DNF y la clave GPG utilizada para firmar el RPM con el siguiente comando: **#dnf -y install dnf-utils**

https://rpms.remirepo.net/enterprise/remi-release-9.rpm, tal y como se visualiza en la Figura 271

Figura 271

Instalación del release 9

Fuente: Elaboración Autor

Se procede a actualizar la herramienta dnf con el comando que se muestra en la Figura 272.

Figura 272

Actualización de la herramienta dnf

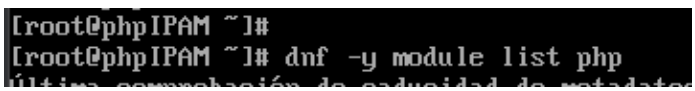
Fuente: Elaboración Autor

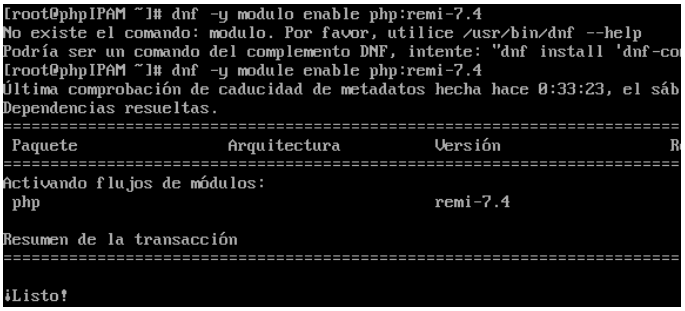
Paso 2: Instalar HTTP y PHP

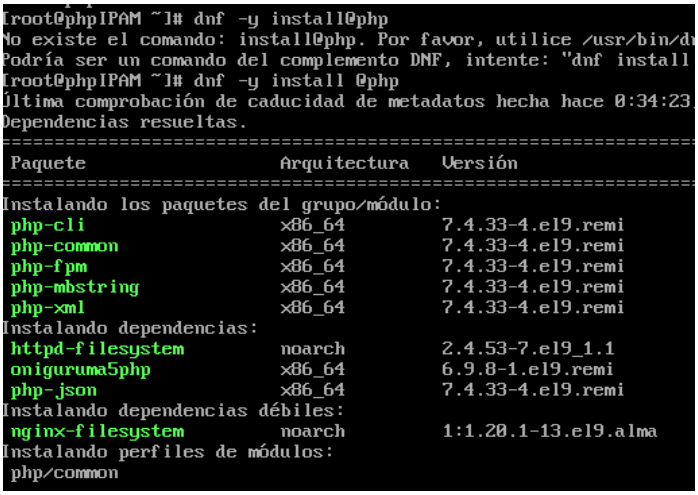
Instalación servidor web (Apache), PHP y las extensiones de PHP requeridas. En la siguiente Figura 273 se observan los comandos que se ejecutaron para la instalación de dichos servicios y extensiones de PHP.

Figura 273

Comandos utilizados para la instalación de servidores web y sus extensiones







Fuente: Elaboración Autor

En la siguiente Figura 274 se procede a instalar las dependencias utilizados para la la administración base de datos con php con el comando # dnf -y install php-{mysqlnd,curl,gd,intl,pear,recode,xmlrpc,mbstring,gettext,gmp,json,xml,fpm} para la instalación de todas las extensiones del servidor php.

Figura 274

Instalación de extensiones

Fuente: Elaboración Autor

Se procede a instalar los paquetes para el servidor Apache http con el comando **dnf -y install httpd**, como se muestra en la siguiente Figura 275.

Figura 275

Instalación del servidor de apache http.

Fuente: Elaboración Autor

A continuación, en la Figura 276 se procede a verificar que la versión de servidor apache http instalada.

Figura 276

Versión de Apache http instalada

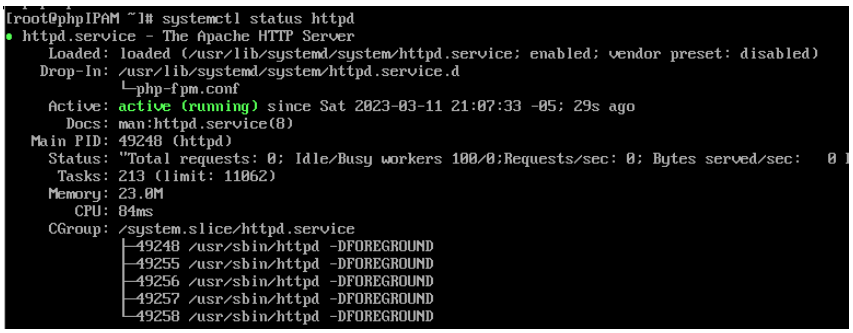
Fuente: Elaboración Autor

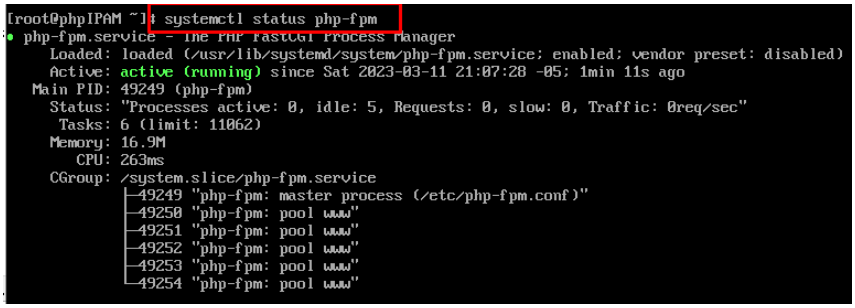
Una vez instalada las dependencias utilizadas para el servidor Apache y Php se procede a iniciar y habilitar los servicios http y php-fpm

Se ejecutan los siguientes comandos se puede verificar el estado de cada servicio: **systemctl status httpd, systemctl status php-fpm,** En la Figura 277 se muestra el estado activo(running) lo cual indica que el servicio está activo y ejecutándose.

Figura 277

Servicios activos





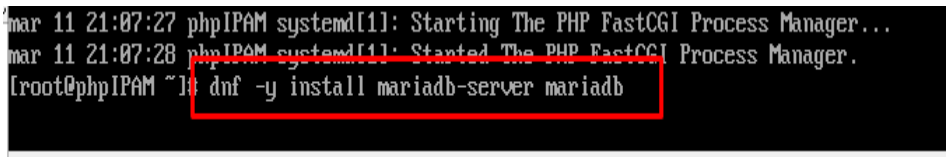
Fuente: Elaboración Autor

Paso 3: Instalación del servidor de base de datos MARIADB

El siguiente paso será instalar **MariaDB** que está basado en **MySQL**, para ello utilizaremos el comando que se encuentra marcada en el cuadro rojo de la Figura 278.

Figura 278

Instalación y configuración de MariaDB.

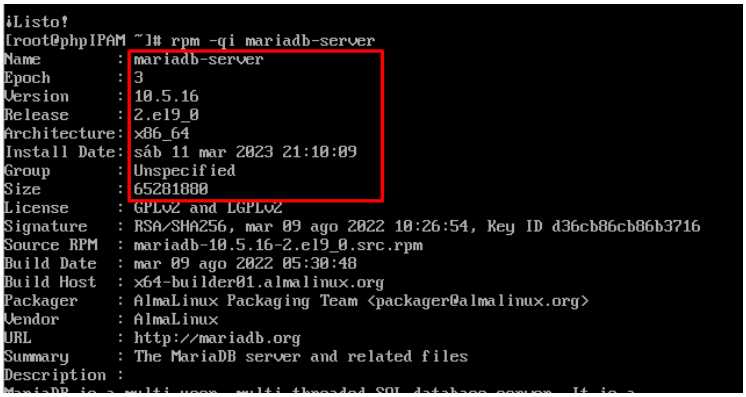


Fuente: Elaboración Autor

El siguiente Figura 279 comando **# rpm -qi mariadb-server** confirmar la versión instalada de MariaDB.

Figura 279

Versión de MariaDB instalada

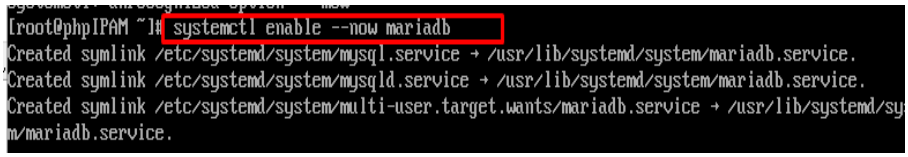


Fuente: Elaboración Autor

En la Figura 280 se procede a habilitar la base de datos MariaDB. Con el comando **#systemctl enable --now mariadb**

Figura 280

Habilitación de la base de datos MariaDB

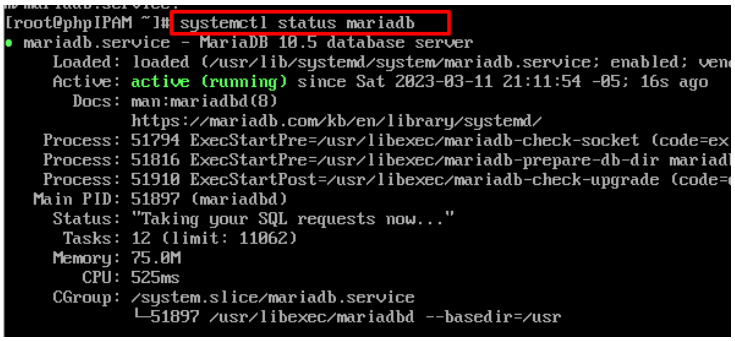


Fuente: Elaboración Autor

Se procede a verificar el estado de la base de datos y verificar que se encuentre activa y ejecutándose, como se muestra en la Figura 281.

Figura 281

Estado de MariaDB

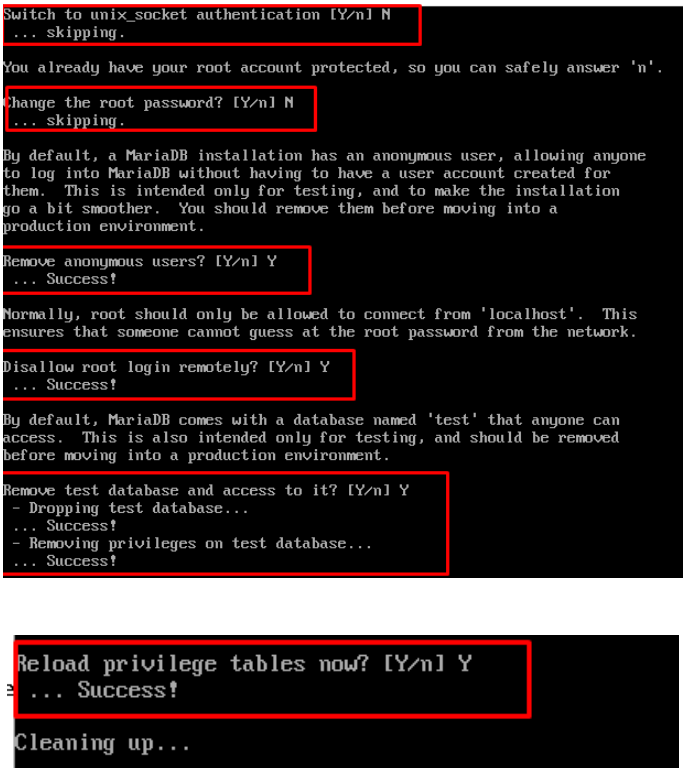


Fuente: Elaboración Autor

A continuación, en la Figura 282 se procede a configurar la seguridad de la base de datos.

Figura 282

Fortalecer la seguridad de la base de datos mariadb

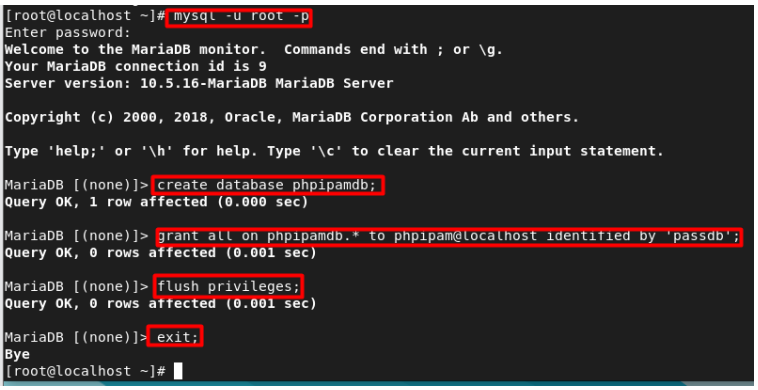


Fuente: Elaboración Autor

Una vez finalizada la instalación, inicie sesión en MySQL CLI como usuario raíz y cree la base de datos y el usuario phpIPAM. Después de instalado el gestor de bases de datos, se deben establecer mecanismos de seguridad necesarios para el entorno de trabajo de MariaDB (establecer contraseña del usuario), tal y como se visualiza en la Figura 283.

Figura 283

Gestor de base de datos MariaDB

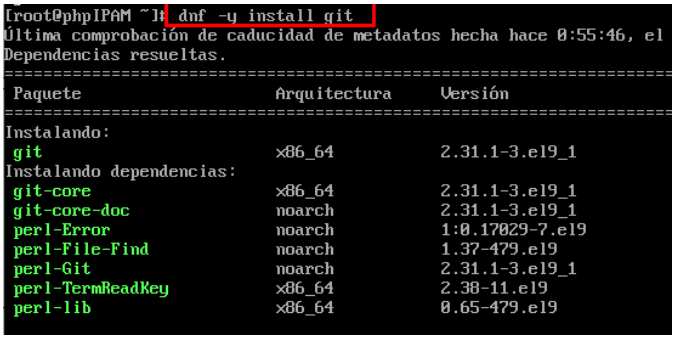


Fuente: Elaboración Autor

Se procede a instalar GIT para el control de versiones para el repositorio GITHUB, usando el comando #**dnf -y install git** como se muestra en la Figura 284.

Figura 284

Instalación de git

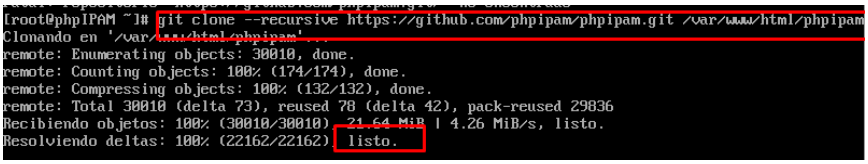


Fuente: Elaboración Autor

Se procede a extraer del repositorio GITHUB phpIPAM usando el siguiente comando #**git clone --recursive https://github.com/phpipam/phpipam.git /var/www/html/phpipam,** como se muestra en la Figura 285

Figura 285

Extracción de phpipam de github



Fuente: Elaboración Autor

Se accede al directorio phpIPAM y se procede a realizar una copia del archivo **config.dist.php** a **config.php** como se muestra a continuación en la Figura 286.

Figura 286

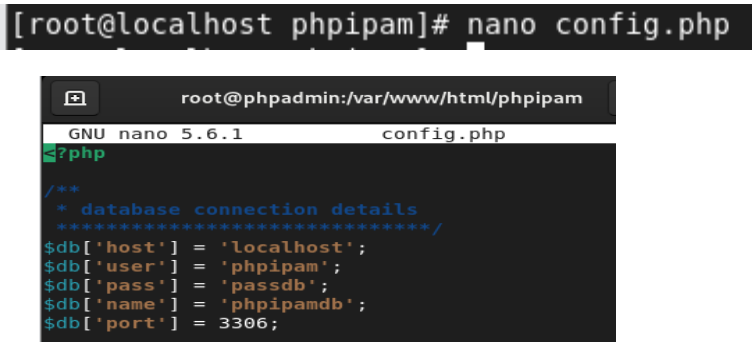
Copia de archivo config.dist.php

Fuente: Elaboración Autor

Se procede a editar las configuraciones para realizar el vínculo con la base de datos y phpipam como se muestra en la Figura 287.

Figura 287

Configuración del archivo config.php



Fuente: Elaboración Autor

Se importar el archivo SQL SCHEMA.sql en la base de datos phpipamdb utilizando el usuario root de MySQL y la autenticación de contraseña, como se muestra en la Figura 288

Figura 288

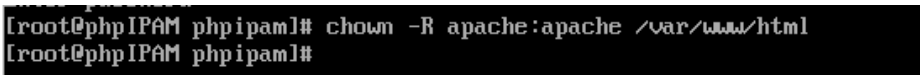
Importar archivo SQL

Fuente: Elaboración Autor

Se procede a establecer al usuario apache y el grupo apache para que sean los propietarios del directorio /var/www/html y todo su contenido, lo que permite que el servidor web tenga acceso y pueda escribir en estos archivos y directorios, mediante le código que se muestra en la Figura 289

Figura 289

Establecimiento de usuarios

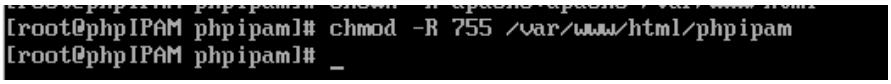


Fuente: Elaboración Autor

Se establece que el propietario puede leer, escribir y ejecutar los archivos y directorios dentro de /var/www/html/phpipam, mientras que el grupo y otros solo pueden leer y ejecutar. Con el comando que se muestra en la Figura 290.

Figura 290

Asignación de permisos de lectura y escritura



Fuente: Elaboración Autor

PASO 5: Configurar servidor web apache

Crear el archivo de configuración de phpipam con el siguiente comando # nano /etc/httpd/conf.d/phpipam.conf

En la siguiente Figura 291 se crea un host virtual en la dirección que se enmarca en el casillo rojo seleccionado.

Figura 291

Creación del VirtualHost

Fuente: Elaboración Autor

Se procede a validar configuraciones httpd a través del siguiente comando que se muestra en la Figura 292.

Figura 292

Validación de configuraciones

Fuente: Elaboración Autor

Si la validación salió exitosa, tal y como se visualiza en la figura anterior con el mensaje de **Syntax OK**, se procede a reiniciar el servicio, mediante los siguientes comandos que se encuentran en la Figura 293.

Figura 293

Reinicio del servicio

```
[root@phpIPAM phpipam]# systemctl restart httpd
[root@phpIPAM phpipam]# systemctl restart php-fpm
[root@phpIPAM phpipam]#
```

Fuente: Elaboración Autor

En la Figura 294 se visualiza el estado del servicio.

Figura 294

Estado del servicio activo

```
[root@phpIPAM phpipam]# systemctl status httpd
● httpd.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
    Drop-In: /usr/lib/systemd/system/httpd.service.d
             └─php-fpm.conf
     Active: active (running) since Sat 2023-03-11 21:43:23 -05; 1min 2s ago
       Docs: man:httpd.service(8)
   Main PID: 53742 (httpd)
     Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes served/sec:   0 B
      Tasks: 213 (limit: 11062)
     Memory: 22.9M
        CPU: 94ms
     CGroup: /system.slice/httpd.service
             ├─53742 /usr/sbin/httpd -DFOREGROUND
             ├─53744 /usr/sbin/httpd -DFOREGROUND
             ├─53745 /usr/sbin/httpd -DFOREGROUND
             ├─53746 /usr/sbin/httpd -DFOREGROUND
             └─53747 /usr/sbin/httpd -DFOREGROUND
```

```
[root@phpIPAM phpipam]# systemctl status php-fpm
● php-fpm.service - The PHP FastCGI Process Manager
     Loaded: loaded (/usr/lib/systemd/system/php-fpm.service; enabled; vendor preset: disabled)
     Active: active (running) since Sat 2023-03-11 21:43:37 -05; 1min 29s ago
   Main PID: 53964 (php-fpm)
     Status: "Processes active: 0, idle: 5, Requests: 0, slow: 0, Traffic: 0req/sec"
      Tasks: 6 (limit: 11062)
     Memory: 16.7M
        CPU: 256ms
     CGroup: /system.slice/php-fpm.service
             ├─53964 "php-fpm: master process (/etc/php-fpm.conf)"
             ├─53965 "php-fpm: pool www"
             ├─53966 "php-fpm: pool www"
             ├─53967 "php-fpm: pool www"
             ├─53968 "php-fpm: pool www"
             └─53969 "php-fpm: pool www"
```

Fuente: Elaboración Autor

Se procede a asignar permisos para que el servidor web Apache acceda a la red en sistemas Linux que utilizan SELinux para implementar políticas de seguridad de acceso obligatorio, con los comandos que se muestran en la Figura 295.

Figura 295

Habilitación de permisos

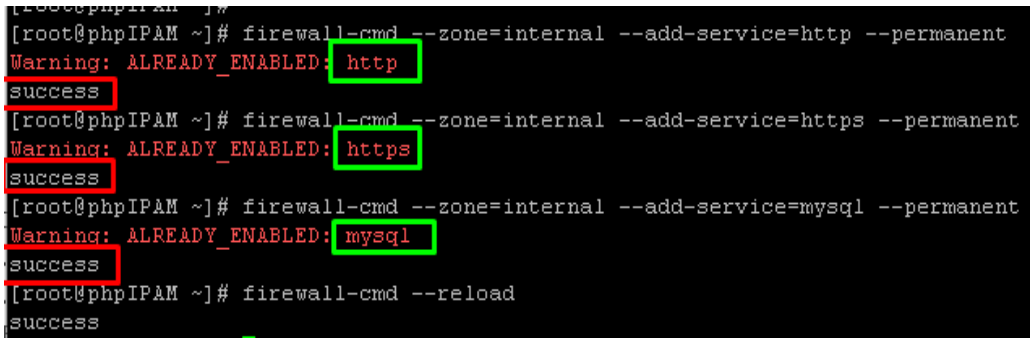
```
[root@phpIPAM phpipam]# systemctl stop httpd
[root@phpIPAM phpipam]# setsebool httpd_can_network_connect 1
[root@phpIPAM phpipam]# setsebool httpd_can_network_connect_db 1
[root@phpIPAM phpipam]# systemctl start httpd
```

Fuente: Elaboración Autor

Se procede a configurar y dar permisos en el firewall para el acceso a los servicios de http, https, mysql, en la Figura 296 se muestra los comandos utilizados.

Figura 296

Servicios activos de firewall

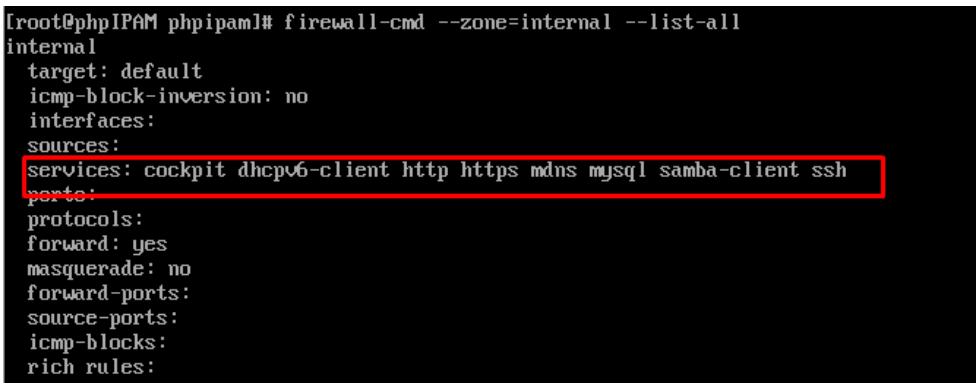


Fuente: Elaboración Autor

Se precede a verificar que los servicios activos en la zona interna estén configurados, en la Figura 297 se muestra los servicios activos.

Figura 297

Servicios http, https y mysql

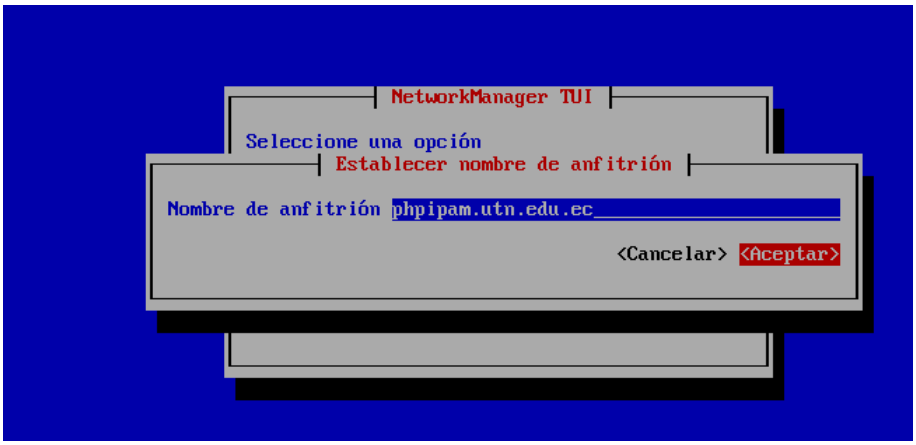


Fuente: Elaboración Autor

Antes de acceder al dominio para ingresar al programa phpIPAM se debe realizar la siguiente configuración, tal y como se visualiza en la Figura 298.

Figura 298

Configurar el nombre del servidor



Fuente: Elaboración Autor

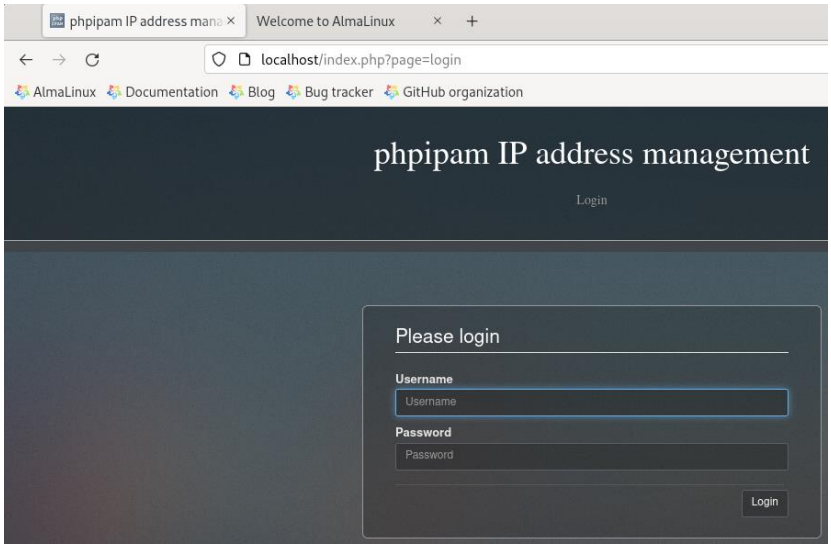
En la siguiente Figura 299 se presenta la pantalla principal para acceder al programa phpIPAM. Las credenciales para ingresar a phpIPAM son las siguiente:

Username: admin

Password: Tesis123

Figura 299

Ingreso a phpIPAM con credenciales

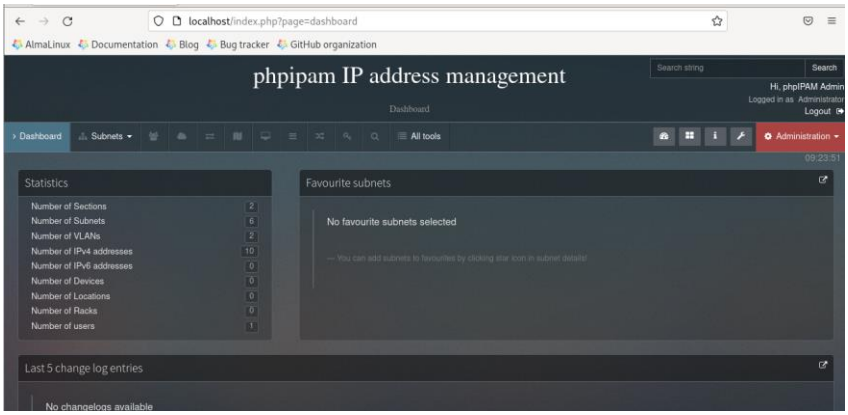


Fuente: Elaboración Autor

En la siguiente Figura 300 se visualiza el interfaz principal del software phpIPAM.

Figura 300

Interfaz de phpipam

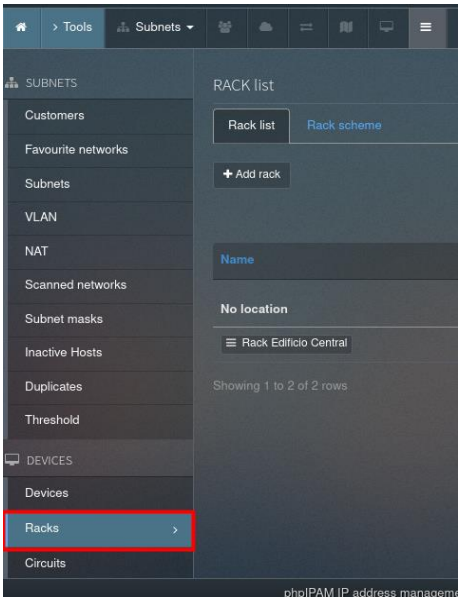


Fuente: Elaboración Autor

Para agregar un dispositivo a phpipam, primero se debe crear un espacio físico para dicho dispositivo, en este caso será un Rack, tal y como se muestra en la Figura 301.

Figura 301

Creación del rack

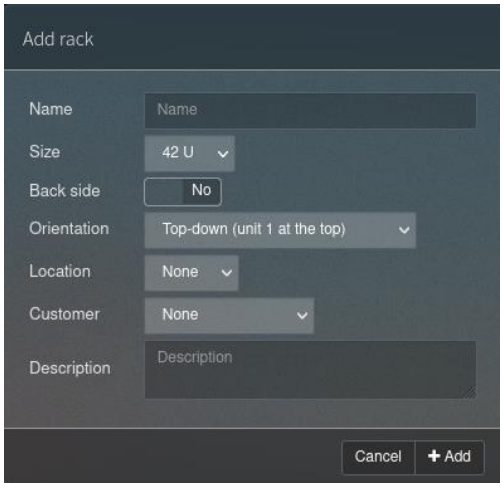


Fuente: Elaboración Autor

En la Figura 302 figura se muestra los campos que se deben llenar al momento de agregar un rack.

Figura 302

Agregar rack

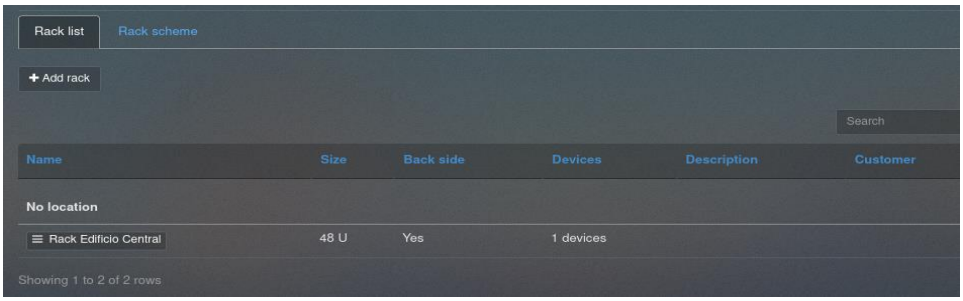


Fuente: Elaboración Autor

En la Figura 303 se visualiza el rack agregado, que tiene por nombre, Rack Edificio Central.

Figura 303

Rack añadido al inventario

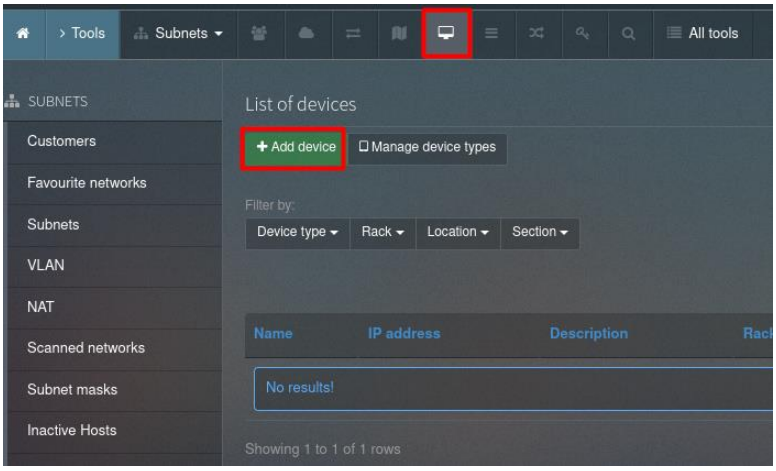


Fuente: Elaboración Autor

Se hace referencia en dicho ANEXO a los ***Artículos 7, 8, 11, 12 y 13*** para lograr cumplir el objetivo de implementar dichas políticas establecidas en los artículos antes mencionados. En los manuales establecidos en el ítem 5.2.1 y 5.3.1. se describe el procedimiento a seguir para agregar los dispositivos al inventario, y por ende en esta sección se documentan los pasos para agregar dispositivos al inventario de phpipam, tal y como se visualiza en la Figura 304.

Figura 304

Agregar dispositivos

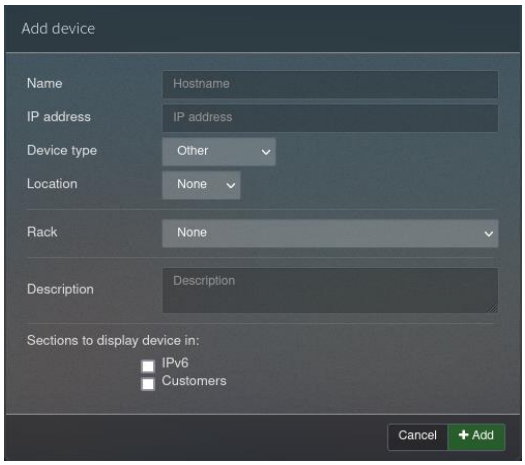


Fuente: Elaboración Autor

En la siguiente Figura 305 se visualiza los campos que se deben llenar para agregar a un nuevo dispositivo al inventario.

Figura 305

Agregar dispositivo al inventario

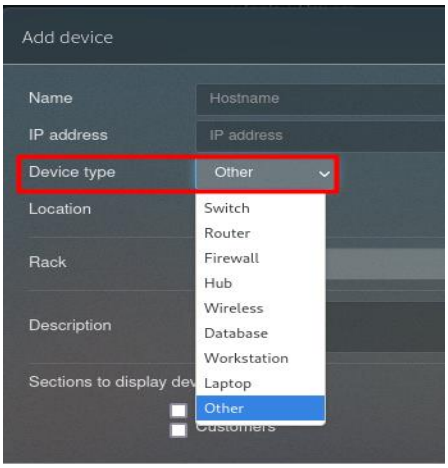


Fuente: Elaboración Autor

En la Figura 306 se visualiza la selección del tipo de dispositivo que se desea agregar al inventario.

Figura 306

Selección del tipo de dispositivo.



Fuente: Elaboración Autor

A continuación, se realiza un ejemplo de los campos a llenar para agregar un dispositivo al inventario, para ello se coloca: el nombre del switch, dirección IP, tipo de dispositivo, localización, rack donde se encuentra, y la descripción del dispositivo a ingresar,

luego de a ver llenado todos los campos se selecciona la opción Add y ya se agregaría el dispositivo al inventario, tal y como se observa en la Figura 307.

Figura 307

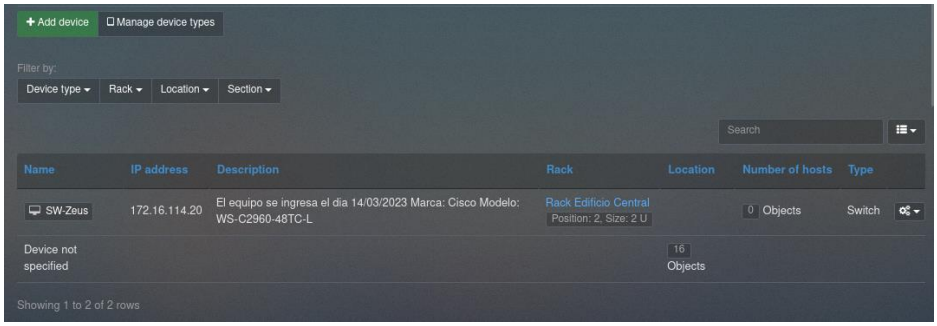
Campos del dispositivo

Fuente: Elaboración Autor

En la Figura 308 se visualiza el dispositivo agregado al inventario de phpipam, con todos los campos descritos.

Figura 308

Dispositivo agregado en el inventario de phpipam



Fuente: Elaboración Autor

Además, se realizará la gestión de los diferentes tipos de dispositivos utilizando la función de administración de dispositivos que ofrece phpipam, la cual se muestra en la Figura 309 correspondiente

Figura 309

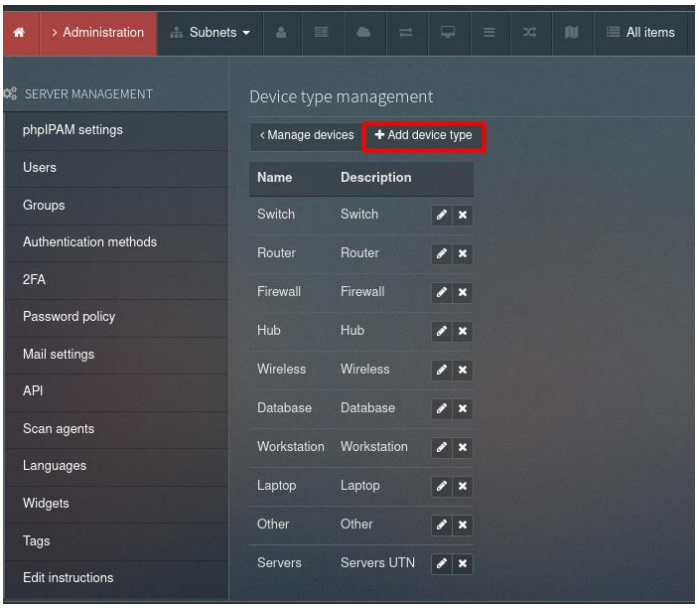
Gestión de tipos de dispositivos

Fuente: Elaboración Autor

Como se observa en la Figura 310 se procede agregar un tipo de dispositivo

Figura 310

Agregar tipo de dispositivo

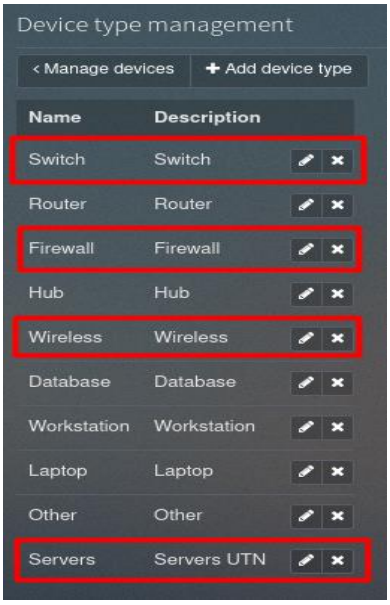


Fuente: Elaboración Autor

En la siguiente figura se observan las 4 categorías del tipo de dispositivos con los cuales se van a trabajar en la base de datos de la Universidad Técnica del Norte

Figura 311

Categorías a trabajar en la red

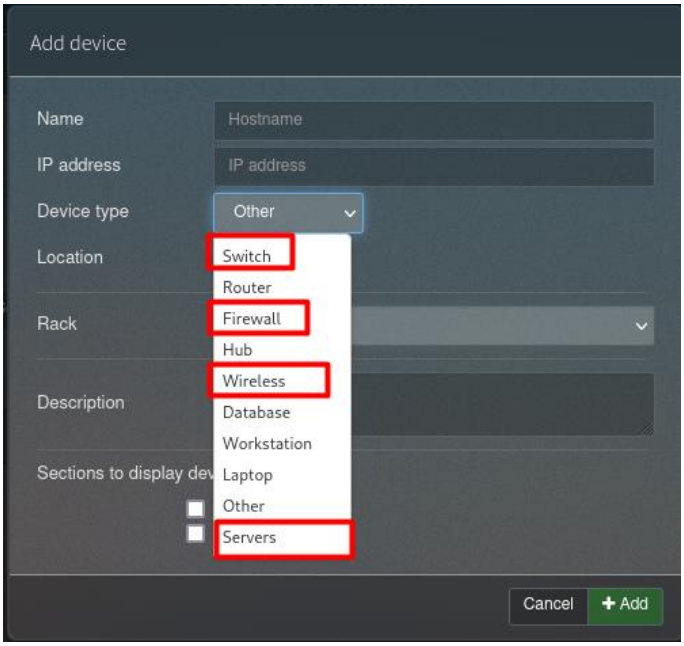


Fuente: Elaboración Autor

En la Figura 312 al agregar un nuevo tipo de dispositivo, se deberá seleccionar una de las cuatro categorías previamente creadas en el inventario, con el objetivo de lograr una mejor administración de los dispositivos en la base de datos y obtener información disponible sobre todos los equipos que conforman la red.

Figura 312

Agregar el tipo de dispositivo



Fuente: Elaboración Autor