

**UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO**

**FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS**

**ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA**



**PROPUESTA DE DISEÑO DE UNA RED DE  
COMUNICACIONES PARA MEJORAR EL ACCESO A  
INTERNET EN LOS AMBIENTES DE LA OFICINA DE  
CAPACITACIÓN, INVESTIGACIÓN Y DOCENCIA DEL  
HOSPITAL NACIONAL EDGARDO REBAGLIATI MARTINS**

**TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE:**

**INGENIERO ELECTRÓNICO**

Presentado por:

**Bach. Castañeda Vásquez Antony**

**Bach. Mirez Fiestas Willians Francisco**

**Lambayeque, 2019**

# **TESIS**

**PROPUESTA DE DISEÑO DE UNA RED DE COMUNICACIONES  
PARA MEJORAR EL ACCESO A INTERNET EN LOS AMBIENTES  
DE LA OFICINA DE CAPACITACIÓN, INVESTIGACIÓN Y  
DOCENCIA DEL HOSPITAL NACIONAL EDGARDO  
REBAGLIATI MARTINS**

**TESIS PARA OPTAR EL TÍTULO DE  
INGENIERO ELECTRÓNICO**

**APROBADA POR EL SIGUIENTE JURADO:**

---

**Ing. HUGO JAVIER CHICLAYO PADILLA  
PRESIDENTE**

---

**Ing. CARLOS LEONARDO OBLITAS VERA  
SECRETARIO**

---

**Mg. Ing. OSCAR UCHELLY ROMERO CORTEZ  
VOCAL**

# **TESIS**

**PROPUESTA DE DISEÑO DE UNA RED DE COMUNICACIONES  
PARA MEJORAR EL ACCESO A INTERNET EN LOS AMBIENTES  
DE LA OFICINA DE CAPACITACIÓN, INVESTIGACIÓN Y  
DOCENCIA DEL HOSPITAL NACIONAL EDGARDO  
REBAGLIATI MARTINS**

**TESIS PARA OPTAR EL TÍTULO DE  
INGENIERO ELECTRÓNICO**

**AUTORES:**

---

**Bach. Castañeda Vásquez Antony**

---

**Bach. Mirez Fiestas Willians Francisco**

**ASESOR:**

---

**Mg. Martin Augusto Nombera Lossio**

## **AGRADECIMIENTOS**

Gracias a Dios, por fortalecer mi lado espiritual desde lo más profundo de mi alma. A mis padres, por formarme en un ambiente lleno de amor, comprensión y dedicación por lo que hacemos. A todos los profesionales que forman parte del personal que nos apoyó desde el punto de vista técnico en el desarrollo de esta investigación.

Castañeda Vásquez Antony

Antes que nada, agradezco a Dios por ser el guía de mi vida y mi fortaleza en las adversidades. A mis padres, por educarme y apoyarme en el trayecto de mi vida universitaria.

Mirez Fiestas Willians Francisco

## **DEDICATORIA**

A mis padres, por saber encaminar mi vida universitaria, a mis compañeros que me brindaron su apoyo en las aulas universitarias y a todas las personas que con especial cariño dedicaron un momento de sus vidas para brindarnos su ayuda.

Castañeda Vásquez Antony

Dedico este trabajo a mis padres y familiares, porque fueron ellos quienes con su apoyo incondicional y cariño sincero, inculcaron en mí la pasión por el estudio. A mis amigos, porque a pesar de la distancia, siempre me brindan su apoyo.

Mirez Fiestas Willians Francisco

## **RESUMEN**

El Hospital Nacional Edgardo Rebagliati Martins (HNERM) es una institución de salud que busca contar con los niveles más altos de tecnología existente para brindar la mejor atención a sus pacientes. Por lo tanto, los miembros de la Oficina de Capacitación, Investigación y Docencia (OCID), necesitan una red sin filtros de navegación a internet para uso académico y además poder aprovechar el medio para desplegar servicios de videoconferencia en los auditorios donde se imparten procesos educativos con el fin de mejorar la calidad intelectual de instituciones allegadas al hospital y al personal médico.

Recordando que la misión de EsSalud tiene como propósito brindar una atención eficiente, en este proyecto se plantea una **PROPUESTA DE DISEÑO DE UNA RED DE COMUNICACIONES PARA MEJORAR EL ACCESO A INTERNET EN LOS AMBIENTES DE LA OFICINA DE CAPACITACIÓN, INVESTIGACIÓN Y DOCENCIA DEL HOSPITAL NACIONAL EDGARDO REBAGLIATI MARTINS.**

En la realización del diseño, se tuvieron como prioridad los siguientes criterios principales: escalabilidad, seguridad, rendimiento. De esta forma, la red (cableada e inalámbrica) tendrá un buen desempeño y una cobertura inicial de un número máximo de 200 usuarios en las áreas de auditorios y bibliotecas.

***Palabras clave:*** estructura de red, cableado estructurado, red inalámbrica.

## **ABSTRACT**

The Edgardo Rebagliati Martins National Hospital (HNERM) is a health institution that seeks to have the highest levels of existing technology to provide the best care for their patients. Therefore, the members of the Office of Training, Research and Teaching (OCID), need a network without internet surfing filters for academic use and also be able to take advantage of the medium to deploy videoconferencing services in the auditoriums where educational processes are taught. In order to improve the intellectual quality of institutions close to the hospital and medical personnel.

Remembering that the mission of EsSalud is intended to provide efficient care, in this project a PROPOSAL FOR DESIGN OF A COMMUNICATIONS NETWORK IS RAISED TO IMPROVE INTERNET ACCESS IN THE ENVIRONMENTS OF THE TRAINING, RESEARCH AND TEACHING OFFICE OF THE EDGARDO NATIONAL HOSPITAL REBAGLIATI MARTINS.

In the realization of the design, the following main criteria were taken as priority: scalability, security, performance. In this way, the network (wired and wireless) will have a good performance and initial coverage of a maximum number of 200 users in the areas of auditoriums and libraries.

**Keywords:** *network structure, structured cabling, wireless network.*

# ÍNDICE GENERAL

## CONTENIDO

<b>ASPECTOS DE LA INVESTIGACIÓN .....</b>	<b>3</b>
<b>CAPITULO I .....</b>	<b>3</b>
1.1.    Aspecto informativo .....	4
1.1.1.    Título .....	4
1.1.2.    Personal Investigador .....	4
1.1.3.    Área de Investigación.....	4
1.1.4.    Lugar de ejecución .....	4
1.1.5.    Duración .....	4
1.2.    Aspecto de la investigación.....	4
1.2.1.    Situación problemática .....	4
1.2.2.    Antecedentes .....	5
1.2.3.    Formulación del problema científico .....	8
1.2.4.    Objetivos .....	8
1.2.5.    Justificación e importancia de la investigación .....	9
1.2.6.    Hipótesis.....	10
1.2.7.    Diseño y contrastación de la hipótesis .....	10
<b>MARCO TEÓRICO .....</b>	<b>11</b>
<b>CAPITULO II.....</b>	<b>11</b>
2.1.    Redes inalámbricas.....	12
2.1.1.    Estándares de conexión .....	12
2.1.2.    Tipos de redes inalámbricas .....	13
2.1.2.1.    Red WPAN.....	13
2.1.2.2.    Red WLAN .....	15
2.1.2.3.    Red WMAN .....	15



2.1.2.4.	Red WWAN .....	15
2.1.3.	Elementos inalámbricos .....	16
2.1.3.1.	Antenas.....	16
2.1.3.2.	Adaptadores inalámbricos .....	17
2.1.3.3.	Puntos de acceso.....	17
2.1.3.4.	Puentes inalámbricos.....	18
2.1.3.5.	Routers inalámbricos.....	18
2.1.4.	Seguridad en redes inalámbricas .....	19
2.1.4.1.	WEP .....	19
2.1.4.2.	WPA/WPA2.....	20
2.1.5.	Ventajas y desventajas de las redes inalámbricas.....	20
2.2.	Cableado estructurado .....	21
2.2.1.	Estándares de cableado estructurado .....	22
2.2.1.1.	ISO/IEC.....	22
2.2.1.2.	IEEE 802 .....	23
2.2.1.3.	IEEE 802.3 (Ethernet) .....	23
2.2.1.4.	IEEE 802.11 (Wi-Fi) .....	24
2.2.1.5.	Estándares TIA EIA .....	24
2.3.	VLANs .....	24
2.3.1.	Tipos de VLANs .....	25
<b>DISEÑO DE LA RED.....</b>		<b>27</b>
<b>CAPITULO III.....</b>		<b>27</b>
3.1.	Estado situacional.....	28
3.2.	Requerimientos para la propuesta de solución .....	32
3.2.1.	Cableado estructurado .....	32
3.2.2.	Red inalámbrica.....	32
3.3.	Análisis de la topología .....	32
3.4.	Análisis de arquitectura.....	33
3.5.	Análisis de usuarios y de medios .....	34

3.6.	Análisis de ancho de banda .....	36
3.7.	Análisis de seguridad LAN .....	36
3.8.	Red inalámbrica.....	36
3.8.1.	Análisis de frecuencia .....	36
3.8.2.	Análisis de dimensionamiento.....	37
3.8.3.	Análisis de tráfico.....	39
3.8.4.	Análisis de seguridad .....	40
3.9.	Ingeniería de red.....	40
3.9.1.	Distribución de direcciones IP .....	40
3.9.2.	Diseño de arquitectura.....	41
3.9.3.	Simulación de la red .....	42
3.9.4.	Características técnicas y ubicación de los equipos .....	50
<b>SELECCIÓN DE EQUIPOS Y ANÁLISIS DE COSTOS .....</b>		<b>56</b>
<b>CAPITULO IV .....</b>		<b>56</b>
<b>CONCLUSIONES .....</b>		<b>59</b>
<b>BIBLIOGRAFÍA .....</b>		<b>61</b>
<b>ANEXOS .....</b>		<b>67</b>

## LISTA DE FIGURAS

<b>Figura 1:</b> Redes inalámbricas. ....	12
<b>Figura 2:</b> Cableado estructurado.....	22
<b>Figura 3:</b> VLANs. ....	25
<b>Figura 4:</b> Auditorio 2 - Entrada de cable. ....	29
<b>Figura 5:</b> Auditorio 3 - Entrada de cable. ....	29
<b>Figura 6:</b> Auditorio 4 - Entrada de cable. ....	30
<b>Figura 7:</b> Auditorio 5 - Entrada de cable. ....	30
<b>Figura 8:</b> Distribución de cableado en los exteriores de la OCID. ....	31
<b>Figura 9:</b> Modelo de diseño jerárquico.....	33
<b>Figura 10:</b> Arquitectita de la red. ....	41

## LISTA DE TABLAS

<b>Tabla 1:</b> Número de usuarios y distancias de cableado.....	35
<b>Tabla 2:</b> Análisis de ancho de banda.....	36
<b>Tabla 3:</b> Estándares IEEE 802.11. ....	37
<b>Tabla 4:</b> Cálculo de capacidad en Mbps.....	39
<b>Tabla 5:</b> Cálculo del número de AP. ....	39
<b>Tabla 6:</b> Trafico de red. ....	39
<b>Tabla 7:</b> Análisis de opciones de seguridad. ....	40
<b>Tabla 8:</b> Distribución de direcciones IP.....	41
<b>Tabla 9:</b> Ubicación de gabinetes y equipos (ver Anexos),.....	55
<b>Tabla 10:</b> Recomendación de dispositivos.....	57
<b>Tabla 11:</b> Costo total del proyecto.....	57

## **INTRODUCCIÓN**

En esta tesis se presenta una propuesta de diseño de una red de comunicaciones para mejorar el acceso a internet en los ambientes de la Oficina de Capacitación, Investigación y Docencia (OCID) del Hospital Nacional Edgardo Rebagliati Martins (HNERM).

En el Capítulo I se explica la problemática que existe en el HNERM debido a la deficiencia en la estructura de red, pues el hospital utiliza VLAN's para la conexión de equipos y teléfonos con una sola red cableado; la deficiencia en el cableado estructurado causa que para la conexión entre los diferentes gabinetes se utilicen enlaces en cascada por gabinete a fin de transportar los servicios; adicionalmente, se pudo comprobar que actualmente no existe una red inalámbrica que permita brindar cobertura a más usuarios del hospital.

En el Capítulo II se presenta el fundamento teórico, el cual contiene los bases del funcionamiento de las redes inalámbricas y sus componentes, la normativa y recomendaciones de las normas TIA/EIA para aplicaciones de cableado estructurado y las principales ventajas de contar con VLAN's dentro de una institución.

En el Capítulo III se encuentra el diseño de la red. En este capítulo se describe la situación actual de la red de comunicación de la OCID; esta información fue obtenida después de realizar una serie de recorridos los ambientes de la OCID. Luego, se presenta el análisis de dimensionamiento de la red cableada y de la red inalámbrica, realizando comparaciones ente distintas tecnologías para poder elegir las que más se ajusten a las condiciones especificaciones técnicas del diseño.

En el Capítulo IV se realiza la selección de equipos que cumplan con las especificaciones técnicas planteadas en el Capítulo III. Además, se muestra el costo total necesario para poder implementar el proyecto

El Capítulo V se presentan las conclusiones obtenidas luego de finalizar este proyecto.

# **ASPECTOS DE LA INVESTIGACIÓN**

## **CAPITULO I**

## **1.1. Aspecto informativo**

### **1.1.1. Título**

Propuesta de diseño de una red de comunicaciones para mejorar el acceso a internet en los ambientes de la Oficina de Capacitación, Investigación y Docencia del hospital nacional Edgardo Rebagliati Martins.

### **1.1.2. Personal Investigador**

#### **1.1.2.1. Autor**

Bach. Mirez Fiestas Willians Francisco

#### **1.1.2.2. Autor**

Bach. Mirez Fiestas Willians Francisco

#### **1.1.2.3. Asesor**

Mg. Martin Augusto Nombera Lossio.

### **1.1.3. Área de Investigación**

Ingeniería Electrónica – Redes y Telecomunicaciones.

### **1.1.4. Lugar de ejecución**

Hospital Nacional Edgardo Rebagliati Martins.

### **1.1.5. Duración**

04 meses.

## **1.2. Aspecto de la investigación**

### **1.2.1. Situación problemática**

El Hospital Nacional Edgardo Rebagliati Martins (HNERM) es una institución de salud que busca estar con los niveles más altos de tecnología existente, así como brindar la mejor atención a sus pacientes. Por lo cual, los miembros del departamento de Capacitación, exigen una red sin filtros de navegación para uso académico.

Actualmente, en el HNERM existe un modelo de CORE COLAPSADO formado por 01 CORE modelo Alcatel de Capa 03 y 12 cuchillas de

Switches de Capa 02, de donde parte la distribución a todos los gabinetes del hospital.

La Oficina de Capacitación, Investigación y Docencia del HNERM presenta las siguientes deficiencias:

### **1) Deficiencia en la Estructura de Red**

Al existir muchos tipos de usuarios y necesidades de seguridad para el HNERM, el hospital cuenta con distintos tipos de segmentos los cuales poseen diferentes tipos de permisos y seguridades para los usuarios. El HNERM utiliza VLANs para la conexión de equipos y teléfonos con una sola red cableada.

### **2) Deficiencia en el Cableado Estructurado**

La institución posee un sistema de cableado estructurado que fue diseñado con el fin de transportar datos, voz e imágenes. Los segmentos de red se interconectan por VLAN. Esto causa que para la conexión entre los diferentes gabinetes se utilice enlaces en cascada por gabinete a fin de transportar los servicios. En el HNERM la red está constituida por cableado UTP categoría 6 TIA/EIA 568-B tanto para el cableado vertical como para el horizontal, esto debido a que la cantidad de tráfico que transporta no es muy alta y además no se supera las distancias máximas de 100 metros permitidas. La única excepción es el segmento de imagen que utiliza fibra multimodo 1000BASE-SX.

### **3) Deficiencia en la Red Inalámbrica**

Actualmente, la institución no cuenta con una Red Inalámbrica existente.

## **1.2.2. Antecedentes**

### **1) Nacional**

**Nombre:** Diseño de una red de datos y de telefonía para la intercomunicación de establecimientos de salud ubicados en la cuenca del bajo napo (Lima, Perú – 2013).



**Universidad:** Pontificia Universidad Católica del Perú.

**Tesis para optar el Título de INGENIERO ELECTRÓNICO, que presenta el bachiller:** Edwin Leopoldo Liñán Benítez.

**Resumen:** La red diseñada en la presente tesis utiliza tecnología inalámbrica 802.11g de larga distancia (alrededor de 30, 40 y 50 Km) utilizando torres ventadas de telecomunicaciones. El equipamiento principal de la red es el enrutador inalámbrico, y está conformado por una computadora, radios 802.11g OEM (fabricante de equipamiento original) y un software no comercial basado en Linux. En el diseño también se contempla el uso de seguridad WPA2, el enrutamiento dinámico OSPF y la implementación de la telefonía interna utilizando Asterisk.

**Nombre:** Implementación de una red informática hospitalaria, usando metodología TOP DOWN NETWORK DESIGN: para el hospital chancay y servicios básicos de salud (Trujillo, Perú – 2017).

**Universidad:** Universidad Privada Antenor Orrego – UPAO.

**Tesis para optar el Título de INGENIERO ELECTRÓNICO, que presenta los bachilleres:** Lujan Vergara, Esmyder Arnaldo y Medina Osorio, Cesar Alejandro.

**Resumen:** El presente proyecto de tesis, consiste en la “IMPLEMENTACIÓN DE UNA RED INFORMÁTICA HOSPITALARIA, USANDO METODOLOGÍA TOP-DOWN NETWORK DESIGN; PARA EL HOSPITAL CHANCAY Y SERVICIOS BÁSICOS DE SALUD”, la cual permitirá que la institución cuente con una red informática hospitalaria moderna y automatizada tecnológicamente, con la finalidad de agilizar la transferencia de información (voz, datos, texto, imágenes) entre sus unidades y áreas de trabajo, en beneficio de los usuarios finales que son los pacientes. Para el desarrollo de este proyecto de tesis, se tuvo en cuenta en primer lugar el estado actual en el que se encuentra la red de informática del Hospital Chancay y Servicios Básicos de Salud, realizando un análisis e

identificando la realidad problemática por la que viene atravesando el hospital, en cuanto a la velocidad de transmisión de información entre sus diversas unidades y áreas. Finalmente, se definen los componentes tecnológicos para el Diseño e Implementación de una Red Informática Hospitalaria, usando Metodología Top-Down Network Design; para el Hospital Chancay y Servicios Básicos de Salud; cuya plataforma para la Administración de la Red Informática Hospitalaria es Windows Server 2012.

## **2) Internacional**

**Nombre:** Red de datos para las comunicaciones en el hospital básico de PELILEO” (Ambato, Ecuador – 2012).

**Universidad:** Universidad Técnica de Ambato.

**Tesis para optar el Título de INGENIERO ELECTRÓNICO, que presenta el bachiller:** Céspedes Velasco Jorge Enrique.

**Resumen:** En la presente tesis se realiza el Diseño de una Red de datos para las comunicaciones en el Hospital Básico de la Ciudad de PELILEO, que con una gran visión, se ha propuesto como uno de sus principales propósitos mejorar su seguridad y sus comunicaciones de datos, en base a la aplicación de nuevas tecnologías permitiéndoles ser una institución de primer nivel. El presente proyecto pretende mostrar que los avances tecnológicos para las comunicaciones tienen una incidencia directa en esta institución, dejando los métodos caducos, dando paso a nuevas tecnologías para el control, comunicación y vigilancia.

**Nombre:** Diseño e implementación del sistema de cableado estructurado de telecomunicaciones "construcción bloque nuevo hospital materno infantil D.10 de la ciudad de Cochabamba” para la empresa I.S.T. Bolivia (Cochabamba, Bolivia – 2017).

**Universidad:** Universidad del Valle Cochabamba.

**Artículo científico presentado por:** Fuentes Telleria, Remmy y Lujan Apaza, Jorge Junior.

**Resumen:** El presente trabajo está dedicado al estudio de las partes constitutivas de un sistema de cableado estructurado de telecomunicaciones para el diseño e implementación en el Hospital Materno Infantil del distrito 10 de la ciudad de Cochabamba. Este estudio fue planteado con base a estándares internacionales de cableado estructurado para edificios comerciales y a los requerimientos del Documento Base de Contratación (DBC) para la contratación de obras ("Licitación pública Ira convocatoria - Construcción Bloque Nuevo Hospital Materno Infantil de Cochabamba F-2 D.10"), así como también al estudio general del cableado estructurado y al estudio específico de los componentes internos del sistema como: distribuidores del edificio, espacios o ambientes que conforman el sistema, medios de transmisión, dispositivos electrónicos, elementos pasivos y elementos activos del sistema. En ese contexto se emplearon tecnologías aplicadas a la comunicación y seguridad para gestionar de manera eficiente la infraestructura hospitalaria. Los sistemas de comunicación que se implementaron en dicha infraestructura son: sistema de datos y telefonía, sistema de perifoneo y música ambiental, sistema de control de enfermerías y sistema de CATV. Los sistemas de seguridad con los que cuenta el hospital materno infantil son los siguientes: sistema de video vigilancia y sistema de alarma contra incendios.

### **1.2.3. Formulación del problema científico**

¿Cómo la propuesta de diseño de una red de comunicaciones puede mejorar el acceso a internet en los ambientes de la oficina de capacitación, investigación y docencia del Hospital Nacional Edgardo Rebagliati Martins?

### **1.2.4. Objetivos**

#### **1.2.4.1. Objetivo general**

Proponer el diseño de una red de comunicaciones para mejorar el acceso a internet en los ambientes de la oficina de capacitación, investigación y docencia del Hospital Nacional Edgardo Rebagliati Martins.

#### **1.2.4.2. Objetivos específicos**

- 1) Realizar visitas a las instalaciones del HNERM para obtener información actual sobre las condiciones de su Estructura de Red, el Cableado Estructurado y el motivo por el cual no se ha implementado una Red inalámbrica.
- 2) Diseñar una red (cableada e inalámbrica) escalable, segura y eficiente, que inicialmente tenga una cobertura de un número máximo de 200 usuarios de las áreas de Auditorios y Biblioteca del HNERM.
- 3) Seleccionar los equipos que formarán parte de la red (cableada e inalámbrica).
- 4) Simular el funcionamiento general de la red a través del software Cisco Packet Tracer.
- 5) Calcular el costo de inversión del proyecto.

#### **1.2.5. Justificación e importancia de la investigación**

La Oficina de Capacitación, Investigación y Docencia (OCID), ubicada en el Block G del HNERM, tiene la necesidad de dotar a su área de trabajo una red de comunicaciones que le permita el acceso sin filtros a internet y aprovechar el medio para desplegar servicios de videoconferencia en los auditorios que esta comprende.

La red actual que el hospital maneja, cobertura el área con un servicio limitado de páginas web administradas remotamente por la Sede Central, siendo esta elección una limitante para la navegación libre que necesitan realizar los organismos educativos, doctores, internos, estudiantes y el mismo personal.

Por lo tanto, este proyecto de tesis tiene como propósito plantear la propuesta de diseño de una red de comunicaciones (cableada e inalámbrica) para mejorar el acceso a internet en los ambientes de la Oficina de Capacitación, Investigación y Docencia del Hospital Nacional Edgardo Rebagliati Martins con una cobertura de 200 usuarios como máximo.

### **1.2.6. Hipótesis**

Con la propuesta de diseño de una red de comunicaciones se puede mejorar el acceso a internet en los ambientes de la Oficina de Capacitación, Investigación y Docencia y además utilizar este medio para realizar videoconferencia en los auditorios del Hospital Nacional Edgardo Rebagliati Martins.

### **1.2.7. Diseño y contrastación de la hipótesis**

El presente proyecto es una propuesta para el diseño de una red de comunicaciones para mejorar el acceso a internet en los ambientes de la oficina de capacitación, investigación y docencia del Hospital Nacional Edgardo Rebagliati Martins.

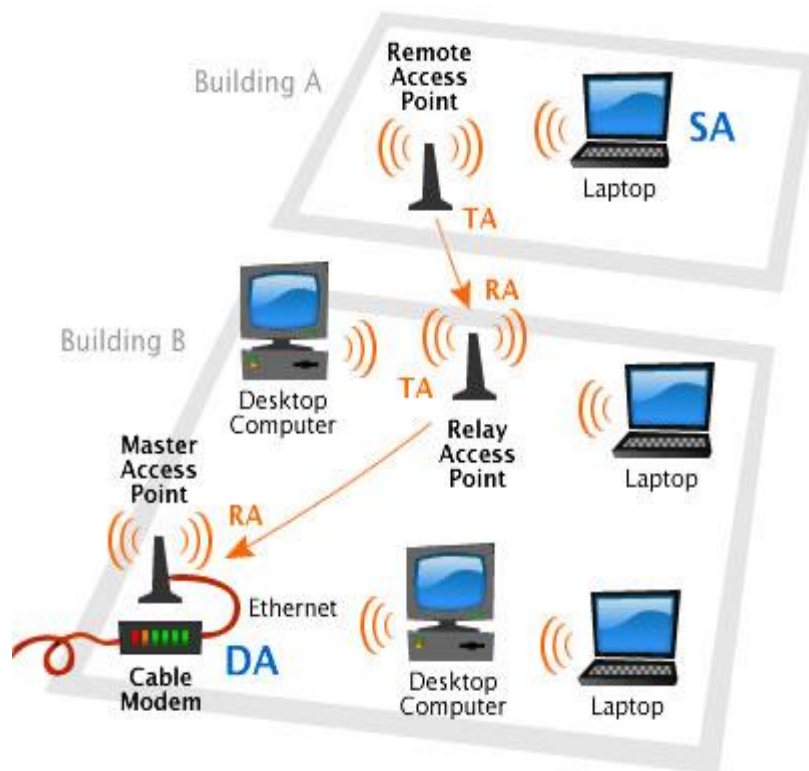
Para poder dimensionar correctamente la red, se realizaron visitas a las instalaciones de los ambientes de la Oficina de Capacitación, Investigación y Docencia del Hospital Nacional Edgardo Rebagliati Martins para conocer el estado actual de la estructura de red, el cableado estructurado y conocer la razón por la que no se ha implementado una red inalámbrica. En la realización del proyecto se tendrá como prioridad el dimensionamiento de la red para un buen desempeño, teniendo como criterio: la escalabilidad, seguridad, rendimiento y cobertura de la red.

# **MARCO TEÓRICO**

## **CAPITULO II**

## 2.1. Redes inalámbricas

Una red inalámbrica es un conjunto de ordenadores, o de cualquier otro dispositivo informático, comunicados entre sí mediante soluciones que no requieran el uso de cables de interconexión. Para disponer de una red inalámbrica, solo hace falta instalar una tarjeta de red inalámbrica en los ordenadores involucrados, hacer una pequeña configuración y listo; por esta razón es un proceso mucho más rápido y flexible que instalar una red cableada. («TIPOS REDES INALÁMBRICAS», s. f.)



**Figura 1:** Redes inalámbricas.

### 2.1.1. Estándares de conexión

La organización de las tecnologías WLAN con soporte Wi-Fi que ha llevado a la estandarización de los diferentes grupos de trabajo ha sido la IEEE, aunque no es la única que los respalda. De hecho, se ha desarrollado a partir de los dos rangos de frecuencias libres ISM: 2,4 GHz y 5 GHz. («WiFi - Wikitel», s. f.)

### **2.1.2. Tipos de redes inalámbricas**

Las redes inalámbricas se pueden clasificar en cuatro grupos específicos según el área de aplicación y el alcance de la señal: redes inalámbricas de área personal (Wireless Personal Area Networks - WPAN), redes inalámbricas de área local (Wireless Local Area Networks - WLAN), redes inalámbricas de área metropolitana (Wireless Metropolitan Area Networks - WMAN), y redes inalámbricas de área amplia (Wireless Wide-Area Networks - WWAN). («REDES INALÁMBRICAS», s. f.)

#### **2.1.2.1. Red WPAN**

Se basan en el estándar IEEE 802.15, se caracterizan por su bajo consumo de energía, baja velocidad de transmisión, y permiten la comunicación en un rango de distancias muy corto, unos 10 metros. A diferencia de otras redes inalámbricas, una conexión realizada a través de una WPAN implica, por lo general, poca o ninguna infraestructura o conectividad directa fuera del enlace establecido. Esto permite soluciones pequeñas, eficientes en energía y de bajo coste que pueden ser implementadas en una amplia gama de dispositivos, como por ejemplo teléfonos inteligentes, PDAs, entre otros. («Redes Inalámbricas de Área Personal», s. f.)

Se basan en tecnologías como Bluetooth, IrDA, ZigBee o UWB («Redes Inalámbricas de Área Personal», s. f.):

##### **a) Bluetooth**

Pertenece al estándar IEEE 802.15.1. Originalmente fue diseñado para comunicaciones omnidireccionales (punto a multipunto), de bajo consumo de energía, corto alcance y con dispositivos baratos, reemplazando el uso de cables y conectando los dispositivos a través de una conexión ad hoc por radio. Hoy en día los desarrolladores están diseñando componentes y sistemas habilitados para Bluetooth para una gama de aplicaciones adicionales. Los dispositivos que incorporan esta tecnología se clasifican en tres grupos diferentes según su alcance máximo: Clase 01, Clase 02 y Clase 03, donde el rango es de unos 100 metros, 10



metros y 1 metro, respectivamente. La clase 2 es la más utilizada. Una red Bluetooth también se denomina picored (piconet), y se compone de hasta 8 dispositivos activos en una relación maestro-esclavo (master-slave).

#### **b) IrDA**

La Asociación de Datos por Infrarrojos (Infrared Data Association - IrDA) se refiere a ese conjunto de normas y se utiliza para proporcionar conectividad inalámbrica a los dispositivos que normalmente utilizan cables para la conectividad. IrDA es un estándar de transmisión de datos ad-hoc de bajo consumo de energía, bajo coste, unidireccional (punto a punto), cono de ángulo estrecho ( $<30^\circ$ ), diseñado para operar con distancias de hasta 1 metro y a velocidades de 9600 bps a 4 Mbps (actualmente), 16 Mbps (en desarrollo). Algunos de los dispositivos que utilizan IrDA son portátiles, PDAs, impresoras y cámaras.

#### **c) ZigBee**

Está basado en el estándar IEEE 802.15.4 que fue desarrollado como un estándar global abierto para abordar las necesidades de fácil aplicación, alta fiabilidad, bajo costo, bajo consumo y bajas velocidades de transmisión de datos en redes de dispositivos inalámbricos. ZigBee opera en las bandas sin licencia 2.4 GHz, 900 MHz y 868 MHz con una velocidad de transmisión máxima de 250 Kbps, lo suficiente para satisfacer las necesidades de un sensor y de automatización usando redes inalámbricas.

#### **d) UWB**

Basado en el estándar IEEE 802.15.3, la tecnología UWB ha atraído recientemente mucha atención como una red inalámbrica para comunicaciones de alta velocidad y corto alcance en interiores. UWB sirve a un propósito muy diferente que las otras tecnologías ya mencionadas, UWB permite la transmisión de grandes archivos de datos a altas velocidades en distancias cortas.

Ofrece una velocidad de transmisión de datos de más de 110 Mbps hasta 480 Mbps a distancias de hasta unos pocos metros capaz de satisfacer a la mayoría de las aplicaciones multimedia como pueda ser el audio y video en las redes del hogar, y también puede actuar como un sustituto inalámbrico del cable de buses serie de alta velocidad tales como el USB 2.0 y IEEE 1394.

#### **2.1.2.2. Red WLAN**

Las redes inalámbricas de área local (WLAN) están diseñadas para proporcionar acceso inalámbrico en zonas con un rango típico de hasta 100 metros y se utilizan sobre todo en el hogar, la escuela, una sala de ordenadores, o entornos de oficina, esto proporciona a los usuarios la capacidad de moverse dentro de un área de cobertura local y permanecer conectado a la red. Las WLAN se basan en el estándar 802.11 del IEEE y son comercializadas bajo la marca Wi-Fi. («Introducción a las Redes Inalámbricas», s. f.)

#### **2.1.2.3. Red WMAN**

Las WMAN se basan en el estándar IEEE 802.16, a menudo denominado WiMAX (Worldwide Interoperability for Microwave Access). Es una tecnología de comunicaciones con arquitectura punto a multipunto orientada a proporcionar una alta velocidad de transmisión de datos a través de redes inalámbricas de área metropolitana. Esto permite que las redes inalámbricas LAN más pequeñas puedan ser interconectadas por WiMAX creando una gran WMAN. Consecuentemente, la creación de redes entre ciudades puede lograrse sin la necesidad de cableado costoso. Es similar a Wi-Fi, pero proporciona cobertura a distancias mayores. (Macanella, s. f.)

#### **2.1.2.4. Red WWAN**

Las redes inalámbricas de área amplia se extienden más allá de los 50 kilómetros y suelen utilizar frecuencias con licencia. Este tipo de redes se pueden mantener en grandes áreas, tales como ciudades

o países, a través de los múltiples sistemas de satélites o ubicaciones con antena atendidos por un proveedor de servicios de Internet. Existen principalmente dos tecnologías disponibles: la telefonía móvil y los satélites. (Guerrero, s. f.)

#### **a) Red de telefonía móvil**

En la red de telefonía móvil, el área de cobertura se divide en celdas. Un transmisor de celda o estación base, en el centro de la celda, está diseñado para servir a una celda individual. Los dispositivos móviles están conectados a una estación base y estas últimas a una central de conmutación de telefonía móvil que une el teléfono móvil y la red cableada de telefonía. (Mártil, s. f.)

#### **b) Satélite**

Debido a su gran altura, las transmisiones por satélite pueden cubrir una amplia área sobre la superficie de la tierra. Esto puede ser muy útil para los usuarios que se encuentran en zonas remotas o islas donde no hay cables submarinos en servicio. Cada satélite está equipado con varios transpondedores los cuales constan de un transceptor y una antena. La señal entrante se amplifica y luego es retransmitida en una frecuencia diferente. («REDES INALÁMBRICAS», s. f.)

### **2.1.3. Elementos inalámbricos**

#### **2.1.3.1. Antenas**

Constituyen la parte fundamental de los dispositivos inalámbricos, puesto que se encargan de enviar o recibir las ondas electromagnéticas con los datos. Según la forma de señal que cubren, pueden clasificarse en tres tipos (García, s. f.):

**a) Omnidireccionales:** Radian la señal en todas direcciones.

**b) Direccionales o unidireccionales:** Concentran la señal en una sola dirección (o en dos direcciones, en las bidireccionales) y

cubren cierto ángulo alrededor de la dirección a la que se apunta.

- c) **Sectoriales:** Es un tipo mixto, que intenta juntar lo mejor de los dos anteriores. Por una parte, emite una señal más amplia que una direccional, pero menor que la omnidireccional. En cuanto a la intensidad (alcance) es mayor que la omnidireccional, pero algo menor que la direccional.

#### **2.1.3.2. Adaptadores inalámbricos**

Se trata de tarjetas inalámbricas integradas en todos los dispositivos inalámbricos denominadas estaciones, como son los clientes móviles, por ejemplo notebook, netbook, smartphones, tablets o ultrabooks, sin olvidar clientes fijos, como ordenadores de sobremesa, que pueden tener diferentes maneras de conectarse (PCI, PCMCIA y USB), y hasta los elementos de interconexión inalámbricos (puntos de acceso, puentes y enrutadores Wi-Fi) que los llevan incrustados. (García, s. f.)

#### **2.1.3.3. Puntos de acceso**

Las redes Wi-Fi tienen una topología sin organización, con uno o varios dispositivos emisores y receptores denominados «puntos de acceso» (AP), conectados a una red troncal. Se trata de un elemento clave dentro de estas redes, ya que dirige el tráfico y permite o no la circulación de los datos. Los puntos de acceso se crearon para adaptar la señal al medio y dar cobertura, si bien al mismo tiempo realizan la función de concentrador inalámbrico, ya que transmiten las tramas recibidas a través de cable u ondas de radio. De ahí que todos dispongan al menos de una conexión RJ45. En la actualidad se distinguen cuatro tipos de puntos de acceso («Despliegue de redes inalámbricas», s. f.):

- a) **Para redes de alto rendimiento:** como empresas, que requieren el mayor ancho de banda posible en cada momento.

- b) **Para redes de entornos de radiofrecuencia (RF) complicados:** como almacenes o zonas de producción en fábricas.
- c) **Para redes de interior:** muy indicados a la hora de cubrir los espacios interiores de edificios de oficinas.
- d) **Para redes malladas:** donde todos los elementos inalámbricos están interconectados siguiendo una topología de malla en que cualquier nodo sirve como repetidor o destino de la información.

#### **2.1.3.4. Puentes inalámbricos**

Se trata de los mismos puntos de acceso vistos anteriormente, aunque configurados para funcionar como puentes con la idea de unir dos segmentos de red en una o más sedes de una misma organización. El administrador de la red indica en qué modo ha de funcionar de acuerdo con las necesidades de cada momento. Para conseguirlo, se le puede indicar que trabaje en modo punto a punto o en modo punto a múltiples puntos. En ambos casos, solo puede existir un puente principal o raíz (root bridge) que se encargará de encaminar el tráfico, mientras que los otros tendrán la función de no-raíz (non-root bridge). («Despliegue de redes inalámbricas», s. f.)

#### **2.1.3.5. Routers inalámbricos**

En la actualidad, debido a la demanda de este tipo de dispositivos, los fabricantes de routers les han añadido un adaptador Wi-Fi para que puedan funcionar también como puntos de acceso. Basta con disponer de una conexión para acceder, mediante un navegador y la IP correspondiente, al panel de opciones y configurar la parte específica del acceso inalámbrico. Por lo general, la configuración se lleva a cabo tras introducir el nombre de usuario y la contraseña correspondiente. A partir de ese momento, podremos obtener

información del aparato y configurar todos los parámetros. («El rendimiento del WiFi continúa mejorando», 2018)

#### **2.1.4. Seguridad en redes inalámbricas**

La seguridad es uno de los puntos débiles de las WLAN. Al utilizar el aire como medio de transmisión para enviar datos a través de las ondas de radio, cualquier persona puede captarlas. A grandes rasgos, existen tres niveles de seguridad (García, s. f.):

- a) **Cero (no recomendable):** suele aplicarse cuando se considera que la información transmitida no es importante. Se da en los sistemas abiertos sin seguridad que permiten un acceso WLAN gratuito a Internet.
- b) **Básica (configuración por defecto):** Los elementos de interconexión suelen estar preconfigurados con algoritmos básicos de cifrado fáciles de romper. Se da en los sistemas WEP y WPA personales.
- c) **Avanzada:** habitual en aquellos casos en que debe manejarse información muy importante. Se emplea en los sistemas WPA profesionales, ya que se considera inadmisibles que una persona ajena a una organización determinada pueda acceder a documentación confidencial.

##### **2.1.4.1. WEP**

Suele ser la opción por defecto suministrada por los fabricantes para preconfigurar los routers, ya que es compatible con todos los dispositivos y estándares Wi-Fi existentes. Utiliza solo una clave única compartida (PSK) de seguridad para cifrar todas las comunicaciones entre los dispositivos, que deben conocerla. («Tipos de contraseña y cifrado para red WiFi: WEP, WPA, WPA2, TKIP, AES», s. f.)

#### 2.1.4.2. WPA/WPA2

Tanto WPA como WPA2 pueden considerarse variantes mejoradas de WEP que aumentan la seguridad de una clave compartida única con claves dinámicas (TKIP) y protegen las identidades de los usuarios o las máquinas mediante la autenticación con clave compartida (PSK), diversos certificados (PKI), como DNI-e, OpenID, etc., y servidores de autenticación RADIUS (802.1X), con los que utilizar diferentes versiones del Protocolo de Autenticación Extensible (EAP), como EAP-MD5, EAP-OTP, EAP-SIM, EAP-TLS (PKI), LEAP (Cisco), PEAP, etc. Aunque todas estas medidas han mejorado el grado de seguridad de las redes inalámbricas, también son vulnerables a ataques por fuerza bruta, si bien se requiere una gran potencia de cálculo para llevarlos a cabo. («Tipos de contraseña y cifrado para red WiFi: WEP, WPA, WPA2, TKIP, AES», s. f.)

#### 2.1.5. Ventajas y desventajas de las redes inalámbricas

**Ventajas** («características de una red inalámbrica», s. f.):

- a) **Flexibilidad:** Dentro de la zona de cobertura de la red inalámbrica los nodos se podrán comunicar y no estarán atados a un cable para poder estar comunicados.
- b) **Poca planificación:** A diferencia de las redes cableadas, sólo nos tenemos que preocupar de que el edificio o las oficinas queden dentro del ámbito de cobertura de la red.
- c) **Diseño:** Los receptores son bastante pequeños y pueden integrarse dentro de un dispositivo y llevarlo en un bolsillo, etc.
- d) **Robustez:** Ante eventos inesperados que pueden ir desde un usuario que se tropieza con un cable o lo desenchufa, hasta un pequeño terremoto o algo similar.

**Desventajas** («Desventajas de las redes inalámbricas - Redes Inalámbricas», s. f.):

- a) **Calidad de Servicio:** Las redes inalámbricas ofrecen una peor calidad de servicio que las redes cableadas. Estamos hablando de velocidades que no superan habitualmente los 10 Mbps, frente a los 100 Mbps que puede alcanzar una red normal y corriente. Por otra parte hay que tener en cuenta también la tasa de error debida a las interferencias.
- b) **Soluciones Propietarias:** Como la estandarización está siendo bastante lenta, ciertos fabricantes han sacado al mercado algunas soluciones propietarias que sólo funcionan en un entorno homogéneo y por lo tanto estando atado a ese fabricante. Esto supone un gran problema ante el mantenimiento del sistema, tanto para ampliaciones del sistema como para la recuperación ante posibles fallos.
- c) **Restricciones:** Estas redes operan en un trozo del espectro radioeléctrico, este está muy saturado hoy día y las redes deben amoldarse a las reglas que existan dentro de cada país.
- d) **Seguridad:** Por una parte seguridad e integridad de la información que se transmite, por otra parte, este tipo de comunicación podría interferir con otras redes de comunicación (policía, bomberos, hospitales, etc.) y esto hay que tenerlo en cuenta en el diseño.

## 2.2. Cableado estructurado

Las telecomunicaciones de datos y de voz continúan aumentando en complejidad; actualmente, las telecomunicaciones incluyen transmisión de voz, datos, fax y video, al igual que los sistemas de automatización para edificios, como por ejemplo alarmas contra incendios, alarmas de seguridad, vigilancia por video, controles de audio y controles ambientales. Los medios de comunicaciones pueden incluir fibras ópticas, cableado de cobre de datos, microondas y radio. El cableado estructurado es un sistema que tiene en cuenta todas las necesidades de cableado del cliente y después las combina en un solo paquete de cableado. (Toro, s. f.)





**Figura 2:** Cableado estructurado.

## **2.2.1. Estándares de cableado estructurado**

### **2.2.1.1. ISO/IEC**

Establecida en 1947, la Organización Internacional de Normalización (ISO) es una organización internacional integrada por organizaciones nacionales de estandarización de más de 140 países. ISO tiene un número de estándares informáticos importantes, y el más relevante de ellos podría ser el modelo de interconexión de sistemas abiertos (OSI), una arquitectura estandarizada para el diseño de redes. («Las Normas ISO. Herramientas para Todas las Organizaciones | Cemiot Internacional. Las Normas ISO. Herramientas para Todas las Organizaciones», 2012)

Por otro lado, el Comité Internacional Electrotécnico (IEC), fundado en 1906, es la organización global que prepara y publica estándares internacionales para todas las tecnologías de electricidad, electrónica y aquellas relacionadas. La misión del IEC es promover, a través de sus miembros, la cooperación internacional en todas las cuestiones relacionadas con electrotecnologías, como electrónica, magnetismo y electromagnetismo, electroacústica, multimedia, telecomunicación

y producción y distribución de energía, entre otras, así como disciplinas generales afines como terminología y símbolos, compatibilidad electromagnética, medición y rendimiento, seguridad de funcionamiento, diseño y desarrollo, seguridad y medio ambiente. (Quintero, s. f.)

#### **2.2.1.2. IEEE 802**

En febrero de 1980, el IEEE establece un comité para desarrollar estándares de networking, en particular, para el cableado y la transmisión de datos. El comité se conoció como comité 802 (802 hace referencia al año [1980] y al mes [febrero]). (Rodríguez, s. f.)

#### **2.2.1.3. IEEE 802.3 (Ethernet)**

En IEEE 802.3 se definen especificaciones de networking basadas en Ethernet. Este estándar describe la serie de bits digitales que viajan por el cable. IEEE 802.3 y sus variantes obtienen el uso del cable al competir por él. Este sistema se denomina Acceso múltiple con detección de portadora y detección de colisiones (CSMA/CD, Carrier Sense Multiple Access with Collision Detection). (Cruz, s. f.)

En la práctica, el CSMA/CD requiere que cada host que desea utilizar el cable primero lo escuche para determinar si está limpio. Cuando está limpio, el host puede transmitir. Debido a que existe la posibilidad de que otra estación haya realizado una transmisión simultáneamente, cada estación que transmite escucha el cable a medida que envía la primera parte de su mensaje. Si no escucha ninguna otra señal, continúa hasta que el mensaje finaliza, y luego comienza el proceso nuevamente para el mensaje siguiente. Si la estación escucha otra señal mientras todavía está transmitiendo, detiene la transmisión. Después, la estación envía una señal de atascamiento. Todas las estaciones que escuchan la señal de atascamiento borran el paquete recibido parcialmente y, esperan un período aleatorio antes de volver a comenzar la transmisión. («El IEEE 802.3 (Estándar de Ethernet) - Redesbasico150», s. f.)

#### **2.2.1.4. IEEE 802.11 (Wi-Fi)**

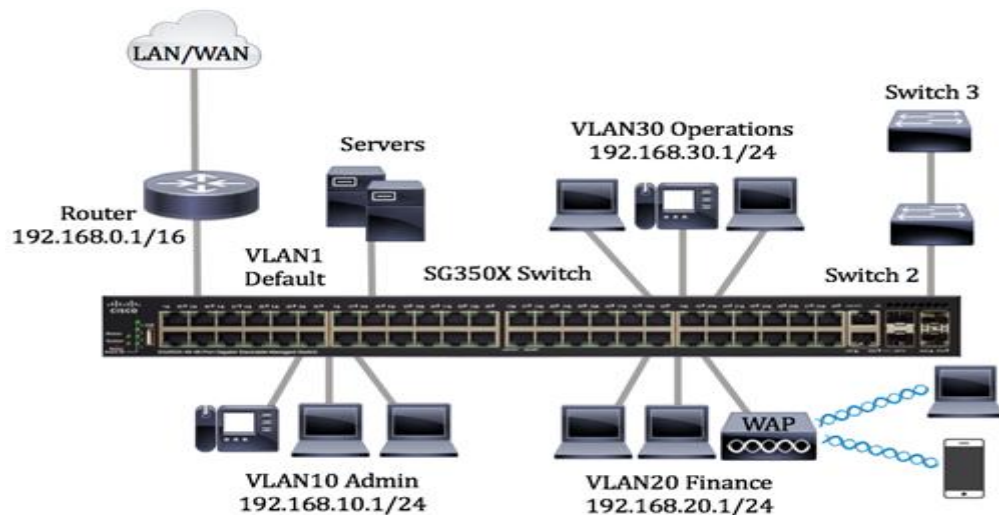
El 802.11b es una extensión de Ethernet alámbrica para medios inalámbricos. En principio se utiliza para TCP/IP, pero también puede soportar otras formas de tráfico de networking, como AppleTalk. La especificación IEEE 802.11b permite la transmisión inalámbrica de datos a distancias en interiores hasta de varios cientos de pies, y a distancias en exteriores hasta de miles de pies en bandas sin licencia en la región de las microondas. Los equipos que cumplen el estándar pueden transportar datos a aproximadamente 11 Mbps, aunque los avances actuales muestran que este límite se puede extender todavía más. («IEEE 802.11 (WiFi) - Redesbasico150», s. f.)

#### **2.2.1.5. Estándares TIA EIA**

La Asociación de Industrias Electrónicas (EIA, Electronic Industries Alliance) y la Asociación de la Industria de las Telecomunicaciones (TIA, Telecommunications Industry Association) son asociaciones de comercio que desarrollan y publican juntas una serie de estándares que abarcan el cableado estructurado de voz y datos para las LAN. («Estándares TIA EIA - Redesbasico150», s. f.)

### **2.3. VLANs**

Una VLAN (acrónimo de virtual LAN, «red de área local virtual») es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLANs pueden coexistir en un único conmutador físico o en una única red física. Consiste en una red de ordenadores que se comportan como si estuviesen conectados al mismo conmutador, aunque pueden estar en realidad conectados físicamente a diferentes segmentos de una red de área local. Los administradores de red configuran las VLANs mediante software en lugar de hardware, lo que las hace extremadamente flexibles. («Redes de área local virtuales (VLAN)», s. f.)



**Figura 3:** VLANs.

### 2.3.1. Tipos de VLANs

#### 2.3.1.1. VLAN de datos

Está configurada para enviar sólo tráfico de datos generado por el usuario. Una VLAN podría enviar tráfico basado en voz o tráfico utilizado para administrar el switch, pero este tráfico no sería parte de una VLAN de datos. Es una práctica común separar el tráfico de voz y de administración del tráfico de datos. La importancia de separar los datos del usuario del tráfico de voz y del control de administración del switch se destaca mediante el uso de un término específico para identificar las VLAN que sólo pueden enviar datos del usuario: una "VLAN de datos". A veces, a una VLAN de datos se la denomina VLAN de usuario. («Tipos de VLAN», s. f.)

#### 2.3.1.2. VLAN predeterminada

Todos los puertos de switch se convierten en un miembro de la VLAN predeterminada luego de su arranque. Hacer participar a todos los puertos de switch en la VLAN predeterminada los hace a todos parte del mismo dominio de broadcast. Esto admite cualquier dispositivo conectado a cualquier puerto de switch para comunicarse con otros dispositivos en otros puertos de switch. (Hdez, s. f.)

#### **2.3.1.3. VLAN nativa**

Una VLAN nativa está asignada a un puerto troncal 802.1Q, este admite el tráfico que llega de muchas VLAN (tráfico etiquetado) como también el tráfico que no llega de una VLAN (tráfico no etiquetado). El puerto de enlace troncal 802.1Q coloca el tráfico no etiquetado en la VLAN nativa. El tráfico no etiquetado lo genera una computadora conectada a un puerto de switch que se configura con la VLAN nativa. Las VLAN se establecen en la especificación IEEE 802.1Q para mantener la compatibilidad retrospectiva con el tráfico no etiquetado común para los ejemplos de LAN antigua. («Una VLAN nativa se asigna a un puerto de enlace troncal 802.1Q En la topología», s. f.)

#### **2.3.1.4. VLAN de administración**

Es cualquier VLAN configurada para acceder a las capacidades de administración de un switch. La VLAN 1 serviría como VLAN de administración si no se definió proactivamente una VLAN única para que sirva como VLAN de administración. Se puede manejar un switch mediante HTTP, Telnet, SSH o SNMP. (Medina, s. f.)

#### **2.3.1.5. VLAN de voz**

Se necesita una VLAN separada para admitir la Voz sobre IP (VoIP). Si se está recibiendo una llamada de urgencia, la calidad de la transmisión se distorsiona tanto que no se puede comprender lo que está diciendo la persona que llama. (Walton, 2017)

El tráfico de VoIP requiere (Walton, 2017):

- a) Ancho de banda garantizado para asegurar la calidad de la voz.
- b) Prioridad de la transmisión sobre los tipos de tráfico de la red.
- c) Capacidad para ser enrutado en áreas congestionadas de la red.
- d) Demora de menos de 150 milisegundos (ms) a través de la red.

# **DISEÑO DE LA RED**

## **CAPITULO III**

### **3.1. Estado situacional**

Actualmente, en el HNERM existe un modelo de CORE COLAPSADO, con 1 CORE modelo Alcatel de capa 03 y 12 cuchillas de Switches de capa 2, de donde parte la distribución a todos los gabinetes del hospital.

Sin embargo, existen 03 deficiencias:

#### **a) Estructura de la Red**

Al existir muchos tipos de usuarios y necesidades de seguridad, el hospital cuenta con distintos tipos de segmentos los cuales poseen diferentes tipos de permisos y seguridades para los usuarios.

El HNERM utiliza VLANs para la conexión de equipos y teléfonos con una sola red cableada.

#### **b) Cableado Estructurado**

La institución posee un sistema de cableado estructurado que fue diseñado con el fin de transportar datos, voz e imágenes. Los segmentos de red se interconectan por medio de VLAN. Por este motivo, la conexión entre los diferentes gabinetes se realiza a través de enlaces en cascada por gabinete a fin de transportar los servicios.

En el HNERM la red está constituida por cableado UTP categoría 6 TIA/EIA 568-B, tanto para el cableado vertical como para el horizontal, esto debido a que la cantidad de tráfico que transporta no es muy alta y además no se supera las distancias máximas de 100 metros permitidas. La única excepción es el segmento de imagen que utiliza fibra multimodo 1000BASE-SX.

Las zonas que se pretenden coberturar, actualmente cuentan con un cableado UTP CAT 6 SIEMONS que pasa mediante un canaleteo horizontal en la parte superior del frontis de los auditorios (ver Figuras 4, 5, 6 y 7).



**Figura 4:** Auditorio 2 - Entrada de cable.



**Figura 5:** Auditorio 3 - Entrada de cable.





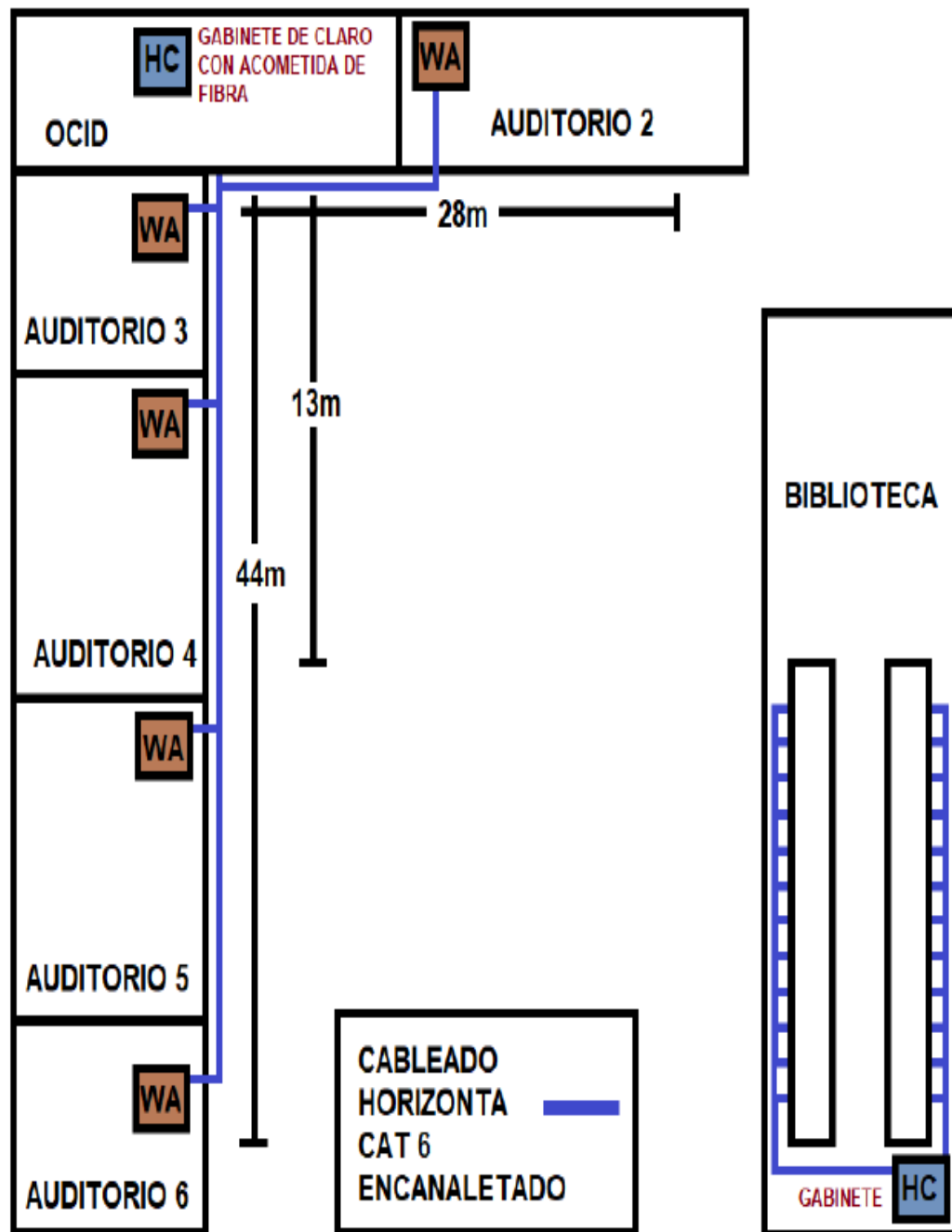
**Figura 6:** Auditorio 4 - Entrada de cable.



**Figura 7:** Auditorio 5 - Entrada de cable.

En la biblioteca, el cableado cubre 22 computadoras en cableado horizontal a piso, este viene desde un gabinete instalado dentro del ambiente.

Toda esta distribución se puede observar en la Figura 8. En la sección de Anexos se encuentra el plano en AutoCAD.



**Figura 8:** Distribución de cableado en los exteriores de la OCID.

### c) Red inalámbrica

Actualmente, el HNERM no cuenta con una red inalámbrica.

### **3.2. Requerimientos para la propuesta de solución**

Según los objetivos planteados, la propuesta de solución requiere las siguientes características técnicas:

- La red debe ser convergente y su arquitectura deberá proporcionar: seguridad, tolerancia a fallos, escalabilidad y calidad de servicio.
- La red debe contar con un Modelo de Diseño de Red Modular Cisco Systems.

#### **3.2.1. Cableado estructurado**

El cableado estructurado requiere las siguientes características técnicas:

- Será desplegado bajo los estándares ANSI/TIA 568-D, ANSI/TIA 569.D, ANSI/TIA 606.C.
- Deberá soportar el mínimo de pérdidas de señal.

#### **3.2.2. Red inalámbrica**

La red inalámbrica requiere las siguientes características técnicas:

- Deberá ser de un modo infraestructura.
- Soportará un traspaso/roaming que permita desplazarse de un área a otra.
- Deberá tener una gestión centralizada que provea servicios de seguridad, DHCP y administración de los puntos de acceso.
- Usar el mínimo de licencias y/o permisos de redes de telecomunicaciones.
- Los puntos de acceso (Access Point) deberán soportar PoE (Power Over Ethernet) para evitar el cableado eléctrico.

### **3.3. Análisis de la topología**

La topología está relacionada con la ubicación de cada punto que se intercomunicará con la red.

En cada auditorio sólo se dará acceso como máximo a 03 computadoras por medio de cableado y a 100 dispositivos de forma inalámbrica.

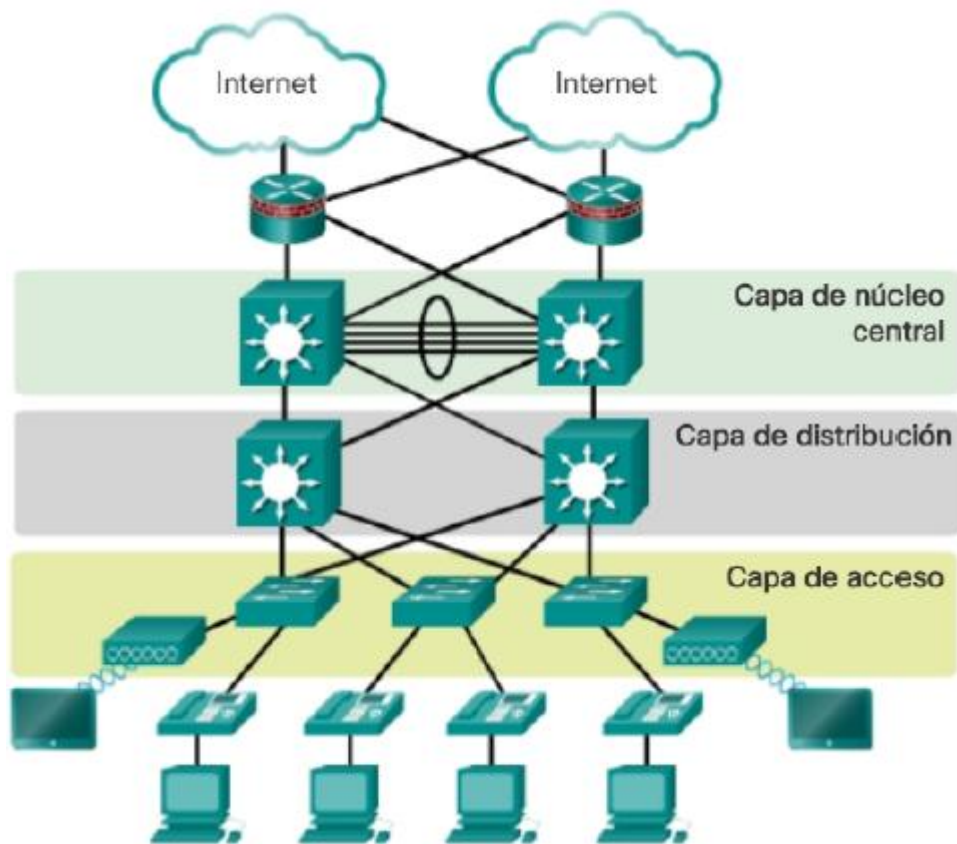
En la biblioteca se tendrá la misma consideración, pero con un máximo de 30 computadoras cableadas.

La distribución de los puntos obliga a que se tenga una topología tipo árbol pensando en la escalabilidad de la red.

### 3.4. Análisis de arquitectura

Para cumplir con los requisitos de la red, se debe establecer un modelo de diseño jerárquico que sea convergente y que proporcione: seguridad, tolerancia a fallos, escalabilidad y calidad de servicio.

El modelo de diseño jerárquico referido por Cisco Systems opera en las tres primeras capas del modelo OSI. Este permite a cada capa implementar funciones específicas, lo que simplifica el diseño de red y, por lo tanto, la implementación y administración de la red. Un diseño de red LAN jerárquico incluye las siguientes tres capas, como se muestra en la Figura 9.



**Figura 9:** Modelo de diseño jerárquico.

El modelo de diseño jerárquico cuenta con las siguientes capas:

- Capa de acceso.
- Capa de distribución.
- Capa principal o de núcleo.

La capa de acceso otorga a los puntos de acceso y a los usuarios acceso directo a la red. La capa de distribución agrega capas de acceso y brinda conectividad a los servicios. Por último, la capa principal ofrece conectividad entre las capas de distribución para entornos de LAN grandes.

El diseño de una red convergente está definido por el uso de dos medios de acceso: cableado e inalámbrico. Su despliegue en la red debe tener un buen desempeño, para lo cual es necesario segmentar la red en 03 subredes: DATOS, ACCESS-POINT, y ADMINISTRACIÓN, esta última para tener una administración remota centralizada de todos los dispositivos intermediarios.

Para asegurar la seguridad de la red, se tiene que aplicar políticas de control de acceso como: Listas de Acceso a nivel de Capa 02 o asegurarse con la adquisición de un Firewall de Red que permita el acceso por usuario hacia internet.

Una red robusta debe soportar tolerancia a fallos que pueden ocurrir en el funcionamiento, para eso se diseña una arquitectura que admita redundancias estableciendo enlaces de backup que funcionen con protocolos de redundancia como STP tanto a nivel de capa principal como de capa de distribución.

### **3.5. Análisis de usuarios y de medios**

De acuerdo con la información levantada mediante una visita al área y a la entrevista con el Jefe de Oficina, se requiere brindar acceso a un máximo de 03 computadoras por cada auditorio y un ACCESS POINT que cuente con un alcance de 100 usuarios, esto pensando en el crecimiento de la red (escalabilidad).

En cuanto a la biblioteca, se requiere un máximo de 30 computadoras operativas conectadas a un ACCESS POINT que cuente con un alcance máximo de 100 usuarios, esto pensando en el crecimiento de la red (escalabilidad).

**Tabla 1:** Número de usuarios y distancias de cableado.

Work Area	Computadoras	Dispositivos inalámbricos	Distancia (m)
AUDITORIO 02	03	50	28
AUDITORIO 03	03	50	10
AUDITORIO 04	03	100	13
AUDITORIO 05	03	100	39
AUDITORIO 06	03	50	44
BIBLIOTECA	30	100	47
TOTAL	45	450	181

Para la interconexión de los equipos intermediarios de red se evalúa la distancia entre áreas de trabajo (auditorios y biblioteca). De acuerdo a la norma ANSI/TIA – 568, la distancia límite para cableado CAT 6 es de 100 metros para enlace canal, superando esta distancia se deberá usar fibra óptica multimodo con un alcance de hasta 100 metros para 10 Gbps.

Las buenas prácticas exigen que la solución cableada deba soportar al menos un cambio tecnológico a futuro, es por eso que se debe prevenir el tema de interferencias así como la concentración de calor provocado por dispositivos PoE. La solución integraría un sistema de puesta a tierra o usar la tecnología Matrix Tape.

El cableado deberá ser de cobre unifilar para el Data Center y multifilar para el usuario. Deberá tener un revestimiento mínimo del tipo LSZH-1 incorporado con retardante de llama según los estándares IEC 61034 y IEC 60754.

De acuerdo a los datos de la Tabla 3.1, se determina que el cableado deberá ser implementado con cable F/UTP CAT 6 con tecnología Matrix Tape, la cual cuenta con revestimiento LSZH-3 para asegurar la prevención contra incendios, usando conectores Plug para dispositivos de campo y conectores Cat 6 estandarizados para computadoras. Los conectores deberán ser Cat 6A de una marca que garantice su aplicación (Panduit o Siemons).

Para la instalación de equipos de campo como Access Point o cámaras, es recomendable usar conectores Plug Terminal de Campo, estos resisten mejor las condiciones ambientales que los conectores simples de Cat 6.

Finalmente, los dispositivos deberán tener un etiquetado bajo la norma 606.C.

### 3.6. Análisis de ancho de banda

Estimamos las siguientes velocidades de descarga de acuerdo al número de usuarios, según la Tabla 2.

**Tabla 2:** Análisis de ancho de banda.

Servicio	Velocidad (Kbps)	Host requeridos	Total (Mbps)
Datos	192	30	5,76
Wireless	120	100	12
Teleconferencia	512	05	25,6
Total	824	642	43,36

Estimamos el ancho de banda con 50 Mbps con una línea dedicada para asegurar el rendimiento.

### 3.7. Análisis de seguridad LAN

Es necesario que la red cuente con un filtro de seguridad para protegerla ante ciberataques que puedan vulnerar la privacidad de los usuarios finales.

Con tal objetivo es obligatorio instalar un firewall de altas prestaciones que garantice un buen desempeño con las siguientes características:

- Configuración de redes.
- NAT.
- VPN.
- Políticas de seguridad: Filtro de contenidos, Filtro de Aplicaciones, Ips.

### 3.8. Red inalámbrica

#### 3.8.1. Análisis de frecuencia

El estándar IEEE 802.11 publica en sus versiones el uso de 04 tipos de frecuencia.

Para seleccionar el estándar a utilizar, se debe tomar en cuenta la velocidad de transmisión que se desea tener, así como el número de usuarios que puede soportar cada estándar. Al ser un requisito del proyecto la utilización de WiFi, se revisarán los estándares IEEE para comunicaciones

inalámbrica. Entre los estándares existentes se encuentran: 802.11a, 802.11b, 802.11g y 802.11n. Las diferencias entre los mismos se pueden observar de manera resumida en Tabla 3.

**Tabla 3:** Estándares IEEE 802.11.

<b>Parámetro</b>	<b>802.11a</b>	<b>802.11b</b>	<b>802.11g</b>	<b>802.11n</b>
Frecuencia	5 GHz	2.4 GHz	2.4 GHz	2.4 y 5 GHz
Ancho de banda	200 MHz	83.2 MHz	83.2 MHz	83.2 MHz - 2.4 GHz y 200 MHz - 5GHz
Modulación	OFDM	DSSS	OFDM	OFDM
Canales Utilizables	08	03	03	02 con MIMO
Ancho de banda por canal	20 MHz	22 MHz	22 MHz	20 y 40 MHz
Tasa de transmisión máxima	54 Mbps	11 Mbps	54 Mbps	600 Mbps
Cobertura interior	30 m	50 m	30 m	70 m
Cobertura exterior	50 m	150 m	50 m	250 m
Usuarios simultáneos	64	32	50	32

De acuerdo al diseño, el estándar elegido es el 802.11n debido al número de usuarios que soporta y la velocidad de transmisión, idónea para el rápido acceso a los servicios.

### 3.8.2. Análisis de dimensionamiento

Después que se ha justificado que la banda de frecuencia que se va a utilizar del estándar IEEE 802.11, es el 802.11n, el cual ofrece una velocidad máxima teórica de 600 Mbps, se procede a determinar el número total de puntos de acceso (AP's) necesarios para satisfacer las propias necesidades. Este número dependerá del número de usuarios y del área a cubrir.

Si se quiere ofrecer un valor añadido, la capacidad del sistema debería ofrecer a cada usuario potencial, una tasa de transferencia mínima de 01



Mbps. Para determinar la capacidad total necesaria en la red, será necesario estimar el número de posibles usuarios existentes conectados a la vez en cada una de las plantas del edificio.

El número de puntos de acceso que aquí se determinan, no serán en principio el número de puntos de acceso definitivos, ya que podría ser necesaria una cantidad superior de puntos de acceso para cubrir posibles zonas sin cobertura. En este caso, el número de puntos de acceso vendrían impuestos por el estudio de cobertura.

Para llevar a cabo dicho análisis se debe tener en cuenta los siguientes parámetros de partida:

- **Ce:** Capacidad efectiva de un punto de acceso. De los 600 Mbps totales, 160 Mbps son los efectivos para la transmisión y recepción de datos.
- **N:** Número máximo de usuarios potenciales por cada planta.
- **Fs:** Factor de simultaneidad. Número máximo de usuarios que están usando la red inalámbrica simultáneamente. Se utilizará un factor de simultaneidad del 50 por ciento.
- **Cg:** Capacidad garantizada por usuario. Tasa de transferencia mínima que se le garantiza a un usuario en el caso de que Fs sea máximo. En nuestro caso tomaremos 01 Mbps.
- **Fe:** Factor de escalabilidad. Debido a un previsible aumento de la demanda de usuarios conectados a la red, se utilizará un factor de escalabilidad del 10 por ciento.
- **C:** Capacidad necesaria por cada planta.

De acuerdo a los análisis, concluimos que basta un ACCESS POINT (AP) para la propagación de la señal inalámbrica entre los 05 auditorios y la biblioteca para cubrir la demanda de hasta 100 usuarios con un factor de escalabilidad del 50 por ciento. Estos cálculos están evidenciados en las Tablas 4 y 5.

**Tabla 4:** Cálculo de capacidad en Mbps.

<b>Tipo de usuario</b>	<b>Cg</b>	<b>N</b>	<b>Fs</b>	<b>Nº de usuarios</b>	<b>C</b>
Personal asistencial	01 Mbps	100	0,5	$100 \times 0,5 = 50$	$100 \times 1 = 50$ Mbps

**Tabla 5:** Cálculo del número de AP.

<b>Capacidad Total (C)</b>	50 Mbps
<b>Tasa de transmisión real de 802.11n (Mbps)</b>	160 Mbps
<b>Factor de Escalabilidad (Fe)</b>	1.1
<b>Número de Puntos de Acceso</b>	$50 \times (1.1/160) = 01$ aprox.

Además, es necesario para una administración centralizada el uso de un WIRELESS LAN CONTROLLER (WLAN CONTROLLER), el cual es un dispositivo de administración de Wi-Fi centralizado que administra todos los puntos de acceso en la red.

### 3.8.3. Análisis de tráfico

El tráfico de la red estará asociado a las aplicaciones y al tipo de acceso que se muestra en la Tabla 6.

**Tabla 6:** Trafico de red.

<b>Aplicación por caso de uso</b>	<b>Rendimiento nominal</b>
Web – casual	500 Kbps
Web: instructivo	01 Mbps
Audio – Casual	100 Kbps
Audio	01 Mbps
On-demand o Streaming Video – Casual	01 Mbps
On-demand o Streaming Video	02-04 Mbps
Impresión	01 Mbps
Uso compartido de archivos- Casual	01 Mbps
Uso compartido de archivos- Instructivo	02-08 Mbps
Copias de seguridad del dispositivo	10- 50 Mbps

### 3.8.4. Análisis de seguridad

La seguridad debe ser tal que no sea muy complejo para los usuarios acceder a la red y que tenga restricciones de acceso a equipos o redes no autorizadas que sean difíciles de superar para los intrusos. En varias de estas VLANs es necesario que se ingresen los datos de autenticación por única vez, ya que sería molesto para los usuarios realizar este proceso a diario generando quejas y fallas de ingreso.

En la Tabla 7 se examinarán los métodos de seguridad y su nivel de cumplimiento de los requerimientos del proyecto, para determinar la elección del método de seguridad.

**Tabla 7:** Análisis de opciones de seguridad.

REQUERIMIENTOS	WEP	WPA	RADIUS
Nivel de Seguridad	BAJO	MEDIO	ALTO
Implementación	FÁCIL	FÁCIL	DIFÍCIL
Configuración	FÁCIL	FÁCIL	DIFÍCIL
Costo de implementación	BAJO	MEDIO	ALTO

La mejor opción que está acorde a los requerimientos es WPA (Wi-Fi Protected Access). La selección de este método de seguridad se da por la vulnerabilidad a ataques por parte de WEP, lo que no puede permitirse en la red de la institución. Se descarta RADIUS por la complejidad de la implementación y porque representaría una inversión mayor.

## 3.9. Ingeniería de red

### 3.9.1. Distribución de direcciones IP

Para asegurar la convergencia y garantizar el buen desempeño de la red, una buena práctica usada por los administradores de redes es segmentar la red en subredes para tener una mejor administración.

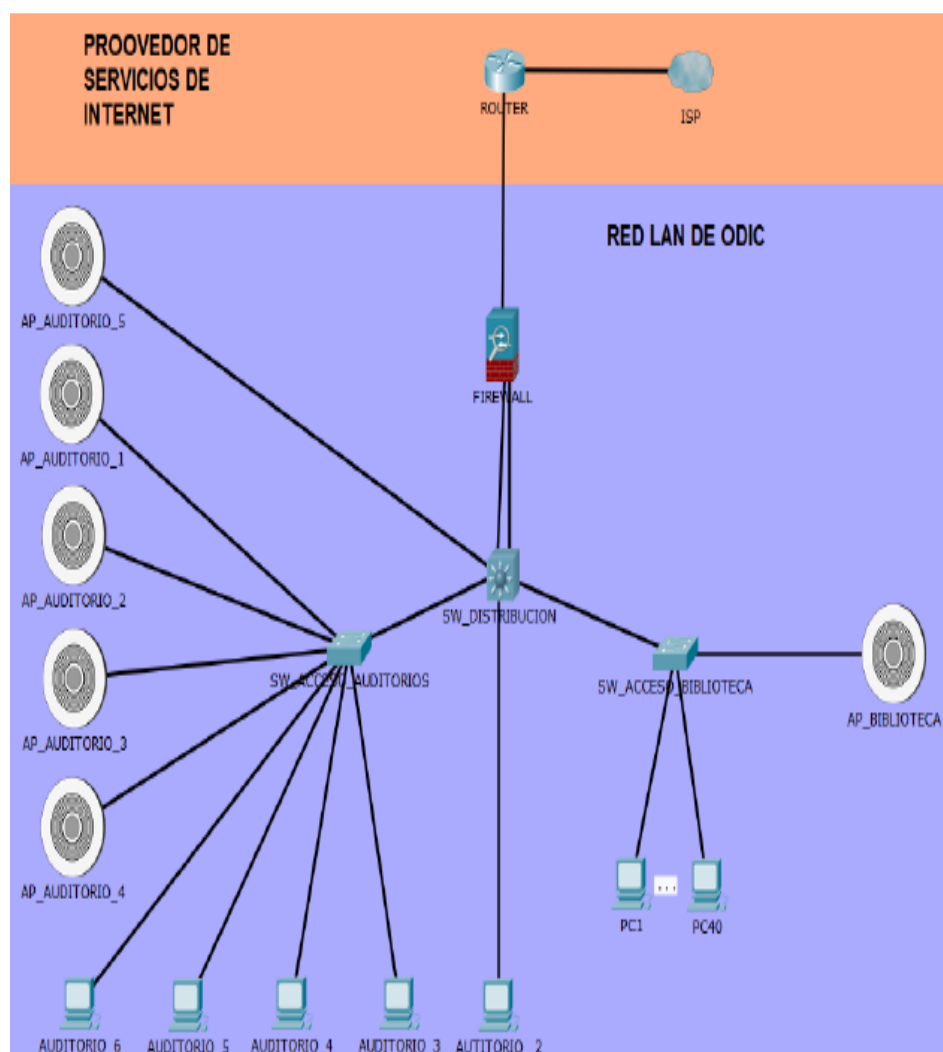
En este caso, como ya se mencionó anteriormente, se crearán 03 subredes como se muestra en la Tabla 8.

**Tabla 8:** Distribución de direcciones IP.

SERVICIO	HOST	SUBNET	BROADCAST	MASK	SUBNET SIZE	VLAN
Administración	07	10.1.1.0	10.1.1.255	255.255.255.0	254	99
Datos	30	10.1.10.0	10.1.11.255	255.255.254.0	512	10
Wireless	100	10.1.12.0	10.1.13.255	255.255.254.0	512	12
Videoconferencia	05	10.1.14.0	10.1.12.31	255.255.255.128	128	14

### 3.9.2. Diseño de arquitectura

La arquitectura de red queda determinada en un modelo de dos niveles (core colapsado y acceso). Para la red WiFi utilizaremos un Access Point y un WLAN Controller, distribuidos tal y como se muestra en la Figura 10.



**Figura 10:** Arquitectita de la red.

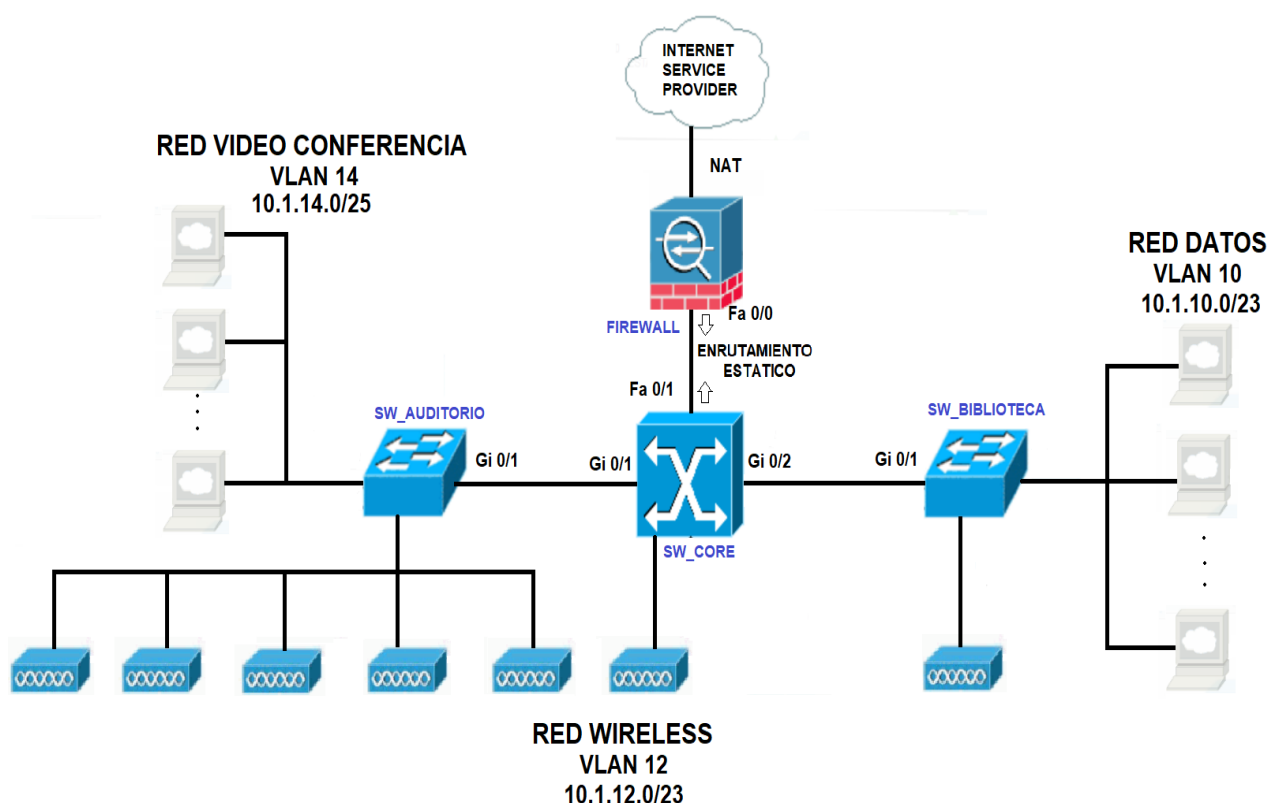
Entre los dispositivos tenemos:

- 01 Firewall.
- 01 Switch de Distribución de 24 puertos.
- 01 Switch de Acceso de Capa 02 de 24 puertos para los auditorios.
- 01 Switch de Acceso de Capa 02 de 48 puertos para la biblioteca.
- 06 Access Point.

El FIREWALL de red está diseñado para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas, este se conecta al SWITCH CORE que nos permite tener una administración centralizada de los SWITCHS DE ACCESO, a su vez permite la segmentación permitiendo cumplir con los requerimientos planteados.

### 3.9.3. Simulación de la red

En este diagrama lógico se muestra un escenario de creación y ruteo entre VLAN integrando un firewall de red que se encargará de realizar el NAT hacia la nube del proveedor de internet, entre otras funciones de seguridad.



**Figura 11:** Arquitectita para simulación de la red.

Los elementos que interconectan la LAN (Switch core, Switch acceso, Access Point, computadoras, equipos inalámbricos) están por cable de cobre UTP a una conexión Fast Ethernet como se muestra en la Figura 11.

Configuración:

a) Switch Core

- Configuración inicial del switch, este incluye:
  - o Nombre del equipo
  - o Mensaje de Bienvenida
  - o Claves de: Consola, usuario privilegiado
  - o Creación de usuarios
  - o Habilitar SSH v2
- Creación de VLAN.
- Creación de interfaces.
- Asignación de puertos troncales y acceso.
- Habilitación del servicio DHCP.
- Enrutamiento estático con el Firewall.

b) Switch Acceso

- Configuración inicial del switch, este incluye:
  - o Nombre del equipo
  - o Mensaje de Bienvenida
  - o Claves de: Consola, usuario privilegiado
  - o Creación de usuarios
  - o Habilitar Telnet
- Creación de VLAN.
- Asignación de puertos troncales y acceso.

c) Access Point

- Nombre del equipo.
- Creación de SSDI.
- Elección de cifrado para contraseñas.
- Creación de contraseñas.

- d) Computadoras
  - Habitación de DHCP.
- e) Firewall
  - Configuración inicial del switch, este incluye:
    - o Nombre del equipo
    - o Creación de interfaces.
    - o Enrutamiento Estático.
    - o NAT.

Resultados:

- a) Switch Core
  - Acceso SSH

```
C:\>ssh -l admin 10.1.1.1

Password:

SW_CORE_CAPACITACION#
SW CORE CAPACITACION#
```

**Figura 12:** Acceso SSH.

Se verifica el acceso por SSH al switch core para poder ser administrado remotamente. La encriptación es RSA por usuario y contraseña.

- VLAN

```
SW_CORE_CAPACITACION#show vlan

VLAN Name                Status    Ports
-----
1    default                active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                           Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                           Fa0/11, Fa0/12, Fa0/13, Fa0/15
                                           Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                           Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                           Fa0/24
10   Datos                  active
12   Wireless              active    Fa0/10
14   Videoconferencia       active    Fa0/14
77   Enlace_firewall        active    Fa0/1
99   Administracion         active
1002 fddi-default          active
1003 token-ring-default    active
1004 fddinet-default       active
1005 trnet-default         active
```

**Figura 13:** VLAN's.

Se verifica la creación de las VLAN de datos, wireless, videoconferencia, administración y la VLAN 77 exclusiva para el enrutamiento con el firewall.

#### - Interfaces

FastEthernet0/24	unassigned	YES	NVRAM	down	down
GigabitEthernet0/1	unassigned	YES	NVRAM	up	up
GigabitEthernet0/2	unassigned	YES	NVRAM	up	up
Vlan1	unassigned	YES	unset	administratively down	down
Vlan10	10.1.10.1	YES	manual	up	up
Vlan11	unassigned	YES	unset	down	down
Vlan12	10.1.12.1	YES	manual	up	up
Vlan14	10.1.14.1	YES	manual	up	up
Vlan77	192.168.77.1	YES	manual	up	up
Vlan99	10.1.1.1	YES	manual	up	up
SW_CORE_CAPACITACION#					

**Figura 14:** Interfaces.

Se verifica la creación de interfaces IP a cada VLAN que funcionarán como puerta de enlace predeterminada para los host que se conecten a cada subred.

#### - Creación de puertos troncales

```
interface FastEthernet0/24
!
interface GigabitEthernet0/1
 switchport trunk native vlan 99
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet0/2
 switchport trunk native vlan 99
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

**Figura 15:** Creación de puertos troncales.

Se verifica que los puertos Gi0/1 y Gi0/2 son puertos troncales con VLAN nativa 99 que van hacia los switch de acceso pasando las VLAN.

#### - Creación de puertos de acceso

```
interface FastEthernet0/10
 switchport access vlan 12
 switchport mode access
 switchport nonegotiate
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
 switchport access vlan 14
 switchport mode access
 switchport nonegotiate
!
```

**Figura 16:** Creación de puertos de acceso.



Se verifica que los puertos finales donde son conectados los host son del tipo acceso y están configurados de acuerdo a la VLAN que le corresponde.

#### - DHCP

```
SW_CORE_CAPACITACION#show ip dhcp pool

Pool vlan14 :
Utilization mark (high/low)      : 100 / 0
Subnet size (first/next)         : 0 / 0
Total addresses                   : 126
Leased addresses                  : 6
Excluded addresses                : 4
Pending event                     : none

1 subnet is currently in the pool
Current index      IP address range      Leased/Excluded/Total
10.1.14.1          10.1.14.1 - 10.1.14.126  6 / 4 / 126

Pool vlan12 :
Utilization mark (high/low)      : 100 / 0
Subnet size (first/next)         : 0 / 0
Total addresses                   : 510
Leased addresses                  : 3
Excluded addresses                : 4
Pending event                     : none

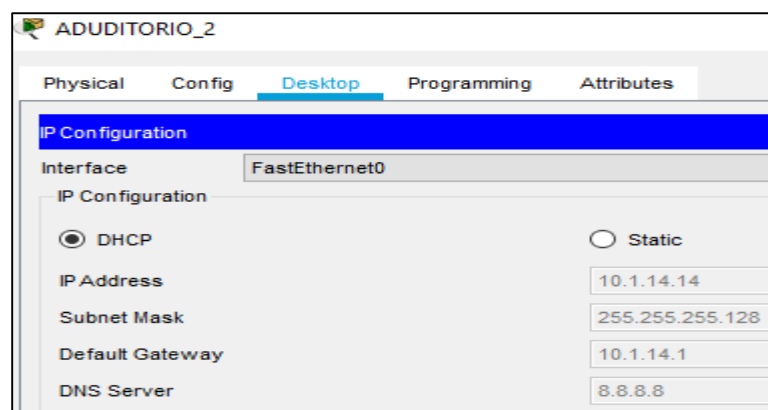
1 subnet is currently in the pool
Current index      IP address range      Leased/Excluded/Total
10.1.12.1          10.1.12.1 - 10.1.13.254  3 / 4 / 510

Pool vlan10 :
Utilization mark (high/low)      : 100 / 0
Subnet size (first/next)         : 0 / 0
Total addresses                   : 510
Leased addresses                  : 4
Excluded addresses                : 4
Pending event                     : none

1 subnet is currently in the pool
Current index      IP address range      Leased/Excluded/Total
10.1.10.1          10.1.10.1 - 10.1.11.254  4 / 4 / 510
SW_CORE_CAPACITACION#
```

**Figura 17: DHCP.**

Se verifica que se ha levantado el servicio DHCP según el direccionamiento IP (ver Tabla 8).



**Figura 18: DHCP en host finales.**

- Enrutamiento estático por defecto

```
SW_CORE_CAPACITACION#SHOW IP Route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is 192.168.77.2 to network 0.0.0.0

    10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
C       10.1.1.0/24 is directly connected, Vlan99
C       10.1.10.0/23 is directly connected, Vlan10
C       10.1.12.0/23 is directly connected, Vlan12
C       10.1.14.0/25 is directly connected, Vlan14
        192.168.77.0/30 is subnetted, 1 subnets
C       192.168.77.0 is directly connected, Vlan77
S* 0.0.0.0/0 [1/0] via 192.168.77.2
```

**Figura 19:** Enrutamiento estático.

Se verifica el enrutamiento estático por defecto desde el SW CORE hasta el firewall.

- b) Switch de Acceso

- Acceso Telnet y Banner Modt

```
C:\>telnet 10.1.1.2
Trying 10.1.1.2 ...Open#####ACCESO RESTRINGIDO####

User Access Verification

Username: admin
Password:
SW_AUDITORIO#
```

**Figura 20:** Acceso Telnet y Banner Modt.

Se verifica el acceso telnet desde un host hasta el switch de acceso.

- Creación de VLAN

```
SW_AUDITORIO#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/2
10	Datos	active	
12	Wireless	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10
14	Videoconferencia	active	Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20

**Figura 21:** Creación de VLAN's.

Se verifica la creación de las VLAN en el switch de acceso SW\_AUDITORIO.

- Asignación de puertos troncales y de acceso

```
interface FastEthernet0/20
  switchport access vlan 14
  switchport mode access
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
  switchport trunk native vlan 99
  switchport trunk allowed vlan 1-12,14-1005
  switchport mode trunk
!
```

**Figura 22:** Asignación de puertos troncales y de acceso.

Se verifica que la interfaz Gi0/1 funciona como puerto troncal que interconecta al switch core mediante la VLAN 99 como nativa.

#### c) Access Point

- Configuración de SSDI, CIFRADO Y NOMBRE



**Figura 23:** Configuración de cifrado WPA2-PSK.

Se verifica que se ha configurado el AP\_AUDITORIO\_1 con un cifrado WPA2-PSK.

d) Firewall

- Nombre del dispositivo y contraseña

```
FIREWALLODIC>
FIREWALLODIC>enable
Password:
FIREWALLODIC#config ter
FIREWALLODIC (config) #
```

**Figura 25:** Configuración de nombre y contraseña.

Se verifica que la configuración de la clave de acceso y el nombre del equipo.

- Creación de interfaces

```
interface Vlan1
 nameif outside
 security-level 0
 ip address 192.168.1.10 255.255.255.0
!
interface Vlan2
 no nameif
 no security-level
 ip address dhcp
!
interface Vlan77
 nameif inside
 security-level 100
 ip address 192.168.77.2 255.255.255.252
!
object network ADMIN
 subnet 10.1.1.0 255.255.255.0
object network DATOS
 subnet 10.1.10.0 255.255.254.0
object network VIDEOCONF
 subnet 10.1.14.0 255.255.255.128
object network VLAN77
 subnet 192.168.77.0 255.255.255.0
object network WIRELESS
 subnet 10.1.12.0 255.255.254.0
!
```

**Figura 26:** Creación de interfaces.

Se verifica la creación de objetos de red que representan las subredes, con los cuales se va trabajar para las configuraciones siguientes.

- Enrutamiento Estático

```
route inside 10.1.1.0 255.255.255.0 192.168.77.1 1
route inside 10.1.10.0 255.255.254.0 192.168.77.1 1
route inside 10.1.12.0 255.255.254.0 192.168.77.1 1
route inside 10.1.14.0 255.255.255.128 192.168.77.1 1
```

**Figura 27:** Enrutamiento estático.

Se verifica el enrutamiento estático para poder llegar a las subredes mediante la interfaz directamente conectada al SW CORE desde el FIREWALL.

- NAT

```
!
access-group nat_outside in interface outside
access-group nat_outside out interface outside
object network ADMIN
  nat (inside,outside) dynamic interface
object network DATOS
  nat (inside,outside) dynamic interface
object network VIDEOCONF
  nat (inside,outside) dynamic interface
object network VLAN77
  nat (inside,outside) dynamic interface
object network WIRELESS
  nat (inside,outside) dynamic interface
```

**Figura 28:** NAT.

Se verifica la configuración de NAT para la salida hacia la WAN del ISP.

### 3.9.4. Características técnicas y ubicación de los equipos

Los equipos de red tienen que cumplir con las siguientes especificaciones:

**FIREWALL:**

**Seguridad:**

- Proteger contra exploits conocidos, malware y sitios web maliciosos utilizando la inteligencia continua de amenazas proporcionada por los servicios de seguridad de los laboratorios de FortiGuard.

- Detectar ataques desconocidos utilizando un análisis dinámico y proporciona mitigación automatizada para detener ataques dirigidos.

#### **Redes:**

- Ofrecer grandes capacidades de enrutamiento, conmutación, control inalámbrico y VPN IPsec de alto rendimiento para consolidar la funcionalidad de red y seguridad.
- Permitir una implementación flexible como UTM y Secure SD-WAN.

#### **Rendimiento:**

- Proporcionar el mejor rendimiento de protección contra amenazas de la industria y latencia ultra baja utilizando la tecnología de procesador de seguridad (SPU) diseñada específicamente para este dispositivo.
- Proporcionar un rendimiento y protección líderes de la industria para el tráfico cifrado SSL.

#### **Administración:**

- La vista del Single Pane of Glass con el Centro de operaciones de red (NOC) debe proporcionar una visibilidad de 360 para identificar problemas de forma rápida e intuitiva.
- La lista de verificación de cumplimiento predefinida debe analizar la implementación y remarcar las prácticas recomendadas para mejorar la postura general de seguridad.

#### **Certificaciones:**

- Probadas de manera independiente y con la mejor eficacia y rendimiento de seguridad validados.
- Recibir certificaciones de terceros sin precedentes de NSS Labs, ICSA, Virus Bulletin y AV Comparatives.

**Tejido de seguridad:**

- Permite a los productos de los socios de Fortinet y Fabric-Ready integrarse de forma colaborativa
- y proporcionar seguridad de extremo a extremo en toda la superficie de ataque.

**SWITCH DE DISTRIBUCIÓN:****Características fiables de hardware y software:**

- Protección contra sobretensión de 6 kV para los puertos Ethernet.
- Reloj de tiempo real (RTC).
- Dying Gasp.
- Compatibilidad con fuente de alimentación redundante (RPS).

**Características avanzadas de conmutación:**

- VLAN trunking.
- VLAN mirroring.
- ISM VLAN.
- RSPAN.

**Características completas de seguridad:**

- Listas de control de acceso (ACL).
- Motor de seguridad D-Link.
- Protección contra ataques BPDU.
- Prevención de ataques DoS.
- Control de acceso basado en IEEE 802.1X.
- Control de acceso basado en MAC.
- Guest VLAN.

**Administración del sistema:**

- 802.1ag CFM.
- 802.3ah enlace Ethernet OAM.
- SNMP v1/v2c/v3.
- RMON v1/v2.

- LLDP/LLDP-MED.

## **SWITCH DE ACCESO:**

### **Características avanzadas:**

- Apilamiento físico de hasta 6 dispositivos a través de dos 10G puertos.
- Conmutación de protección de anillo de Ethernet (ERPS).
- Enrutamiento estático.
- VLAN de vigilancia automática.
- VLAN de voz automática.
- Detección de bucle invertido.
- LLDP / LLDP-MED.

### **Características de seguridad:**

- Lista de control de acceso (ACL).
- D-Link Safeguard Engine.
- Protección contra ataques BPDU.
- Prevención de suplantación de identidad ARP.
- Enlace de puerto IP-MAC
- DoS Attack Prevention.
- Control de acceso web / MAC sin cliente.

### **Gestión intuitiva:**

- Interfaz de usuario multilenguaje basada en web.
- MIB SNMP incorporada para red remota sistemas de gestión.
- Soporte integral de CLI.
- Capacidad de administración para ambos entornos IPv4 / IPv6.
- Soporte de imagen dual.
- Utilidad D-Link Network Assistant (DNA).
- Interfaz de consola para gestión fuera de banda.



## **ACCESS POINT:**

### **Estándares:**

- IEEE 802.11n.
- IEEE 802.11g.
- IEEE 802.3ab.
- IEEE 802.3af.
- IEEE 802.3u.
- IEEE 802.3.

### **Administración:**

- Telnet - Secure (SSH) Telnet).
- Interfaz de Navegador Web.
- HTTP - HTTP seguro (HTTPS).
- Compatibilidad con SNMP.
- Matriz de AP.

### **Seguridad:**

- WPA TM-Personal.
- WPA-Enterprise.
- WPA2 TM-Personal.
- WPA2-Enterprise.
- 64/128-bit WEP.
- SSID Broadcast Disable.
- Control de acceso: Dirección MAC.
- Detección de Rogue AP (AP Intruso).

### **Soporte VLAN / SSID:**

- Soporte 802.1q/Multiple SSID para hasta 8 VLAN.

### **Calidad de servicio (QoS):**

- 04 colas de prioridad.
- Prioridad WMM inalámbrico.

Los equipos irán ubicados en 03 gabinetes los cuales estarán ubicados estratégicamente con las especificaciones que se muestran en la Tabla 3.9.

**Tabla 9:** Ubicación de gabinetes y equipos (ver Anexos),

GABINETE	EQUIPOS	ESPECIFICACIONES	UBICACIÓN
GABINETE A	FIREWALL DISTRIBUCIÓN	<ul style="list-style-type: none"> <li>- Diseñado según la norma EIA-310D.</li> <li>- Altura útil de 8RU.</li> <li>- Fabricado con acero LAF de 1.2mm.</li> <li>- 02 rieles, tropicalizado, con perforaciones circulares, normalizados en 19"</li> <li>- Diseñado bajos procesos desengrasante, fosfatado y anti oxidante.</li> <li>- Resistencia cinco veces mayor al oxido y rallados.</li> <li>- Entrada y salida de cables a través del marco desmontable.</li> <li>- Puerta con centro de acrílico polarizado de 3mm.</li> </ul>	Interior de la OCID
GABINETE B	ACCESO	<ul style="list-style-type: none"> <li>- Diseñado según la norma EIA-310D.</li> <li>-Altura útil de 8RU.</li> <li>- Fabricado con acero LAF de 1.2mm.</li> <li>- 02 rieles, tropicalizado, con perforaciones circulares, normalizados en 19"</li> <li>- Diseñado bajos procesos desengrasante, fosfatado y anti oxidante.</li> <li>- Resistencia cinco veces mayor al oxido y rallados.</li> <li>- Entrada y salida de cables a través del marco desmontable.</li> <li>- Puerta con centro de acrílico polarizado de 3mm.</li> </ul>	Interior del Auditorio 04
GABINETE C	ACCESO	<ul style="list-style-type: none"> <li>- Diseñado según la norma EIA-310D.</li> <li>- Altura útil de 8RU.</li> <li>- Fabricado con acero LAF de 1.2mm.</li> <li>- 02 rieles, tropicalizado, con perforaciones circulares, normalizados en 19"</li> <li>- Diseñado bajos procesos desengrasante, fosfatado y anti oxidante.</li> <li>- Resistencia cinco veces mayor al oxido y rallados.</li> <li>- Entrada y salida de cables a través del marco desmontable.</li> <li>- Puerta con centro de acrílico polarizado de 3mm.</li> </ul>	Interior de la Biblioteca

# **SELECCIÓN DE EQUIPOS Y ANÁLISIS DE COSTOS**

## **CAPITULO IV**

#### 4.1. Selección de equipos

La red pasiva se refiere al cableado estructurado necesario para conectar los equipos de la red activa. Para estos elementos no se especifica una marca y se deja esta opción a las empresas que presenten cotizaciones.

Para la red activa existen múltiples posibilidades en el mercado con soluciones básicas hasta las más complejas que varían en cuanto a la marca y calidad de los equipos. Cisco es una marca reconocida por su garantía y trascendencia en el mercado por lo que es una de las primeras opciones a considerar, después tenemos proveedores como Mikrotic que ofrecen soluciones para pequeñas empresas y sus equipos soportan un límite de usuarios, pero para una red escalable no es lo recomendado.

A continuación, se recomiendan los equipos que se muestran en la Tabla 4.1.

**Tabla 10:** Recomendación de dispositivos.

EQUIPOS DE RED	FAMILIA	MODELO
FIREWALL	FORTINET 100	FORTIGATE 100E
SW DISTRIBUCIÓN	GAMA DGS-3000	DGS-3000-24P
SW ACCESO	GAMA DGS-1510	DGS-1510
ACCESS POINT	ACCESS POINT LINK	DAP-2660

#### 4.2. Análisis de costos

El costo final se observa en la Tabla 4.2.

**Tabla 11:** Costo total del proyecto.

Costo	Descripción y modelo	Cant.	Proveedor	P/unit. (\$)	P. total (\$)
RED ACTIVA	Firewall - FortiGare 100	01	AMAZONCOM	1,494.00	1,494.00
RED ACTIVA	Smart Switch -D - Link DGS-1510-52P	01	DELTRON	784.00	784.00
RED ACTIVA	Smart Switch - D - Link DGS-1210-28	01	DELTRON	395.36	395.00

RED ACTIVA	Access Point - D-Link DAP-2660	06	DELTRON	143.92	863.52
RED ACTIVA	306 metros de cable de red UTP - PANDUIT CAT 6	01	MERCADO LIBRE	450.00	450.00
RED ACTIVA	Canaleta 25 x 25 mm PVC Sin Adhesivo Blanco - Schneider Electric	25	SODIMAC	9.90	247.50
RED ACTIVA	Adhesivo Terokal Recordf 1/4 gl – Tekno	02	SODIMAC	18.00	36.00
RED ACTIVA	Gabinete de Pared 8 Ru 42x53x53 – SATRA	01	MERCADO LIBRE	241.00	241.00
RED ACTIVA	Gabinete de Pared 6 Ru 33x53 SATRA	01	MERCADO LIBRE	215.00	215.00
IMPLEMENTACIÓN	SUPERVISIÓN DE PROYECTO	01	-	600.00	600.00
IMPLEMENTACIÓN	CONFIGURACIÓN DE FIREWALL	01	-	460.00	460.00
IMPLEMENTACIÓN	CONFIGURACIÓN DE EQUIPOS DE LAN	03	-	50.00	150.00
IMPLEMENTACIÓN	CONFIGURACIÓN DE RED WIRELESS	06	-	50.00	300.00
IMPLEMENTACIÓN	CABLEADO	05	-	50.00	250.00
IMPLEMENTACIÓN	INSTALACIÓN DE GABINETES	03	-	50.00	150.00
<b>COSTO TOTAL</b>					6636.38

# CONCLUSIONES

## CONCLUSIONES

- 1) Se logró de diseñar una red de comunicaciones para la Oficina de Capacitación, Investigación y Docencia (OCID), ubicada en el Block G del HNERM, la cual permitirá al personal tener acceso seguro a internet y a la vez se aprovechará el medio para desplegar servicios de videoconferencia en los auditorios que forman parte de la OCID.
- 2) La red de comunicación, formada por una red cableada y una red inalámbrica, es escalable, segura, eficiente y tendrá la capacidad de coberturar inicialmente a un número máximo de 200 usuarios en las áreas de los auditorios y la biblioteca del HNERM.
- 3) De acuerdo al análisis de dimensionamiento para la red cableada, se determinó que el ancho de banda es de 50 Mbps, por lo que la elección del cable UTP Cat 6 (Panduit) es la opción más adecuada y económica en comparación con la Cat 6A y 7, las cuales tienen un precio más elevado y son utilizadas para anchos de banda superiores.
- 4) Para la red inalámbrica, el estándar elegido es el IEEE 802.11n debido a que el número de usuarios simultáneos que soporta y su velocidad de transmisión se ajustan a las condiciones de diseño de este proyecto y permitirá que el personal tenga un rápido acceso a los servicios.

# **BIBLIOGRAFÍA**



## REFERENCIAS BIBLIOGRÁFICAS

- *Características de una red inalámbrica. (s. f.). Recuperado 17 de junio de 2019, de web de duvanruales website:*  
*<http://duvanruales.jimdo.com/redes/caracteristicas-de-una-red-inalambrica/>*
- *Cruz, E. (s. f.). GoConqr - Estándares IEEE: 802.3, 802.5, 802.11, 802.15. Recuperado 17 de junio de 2019, de GoConqr website:*  
*<https://www.goconqr.com/flowchart/10797338/est-ndares-ieee-802-3-802-5-802-11-802-15->*
- *Despliegue de redes inalámbricas. (s. f.). Recuperado 12 de junio de 2019, de*  
*<https://www.mheducation.es/bcv/guide/capitulo/844818386X.pdf+%&cd=3&hl=es-419&ct=clnk&gl=pe&client=firefox-b-d>*
- *Desventajas de las redes inalámbricas - Redes Inalámbricas. (s. f.). Recuperado 17 de junio de 2019, de*  
*<https://sites.google.com/site/redesinalambricas04/home/desventajas-de-las-redes-inalambricas>*
- *El IEEE 802.3 (Estándar de Ethernet) - Redesbasico150. (s. f.). Recuperado 17 de junio de 2019, de*  
*<https://sites.google.com/site/redesbasico150/introduccion-a-los-estandares-de-cableado/el-ieee-802-3-estandar-de-ethernet>*
- *El rendimiento del WiFi continúa mejorando. (2018, junio 21). Recuperado 17 de junio de 2019, de Optical Networks website: <https://www.optical.pe/conoces-la-evolucion-del-wifi/>*
- *Estándares TIA EIA - Redesbasico150. (s. f.). Recuperado 17 de junio de 2019, de*  
*<https://sites.google.com/site/redesbasico150/introduccion-a-los-estandares-de-cableado/estandares-tia-eia>*

- *Garcia, J. (s. f.). WMAN Wireless (Metropolitan Area Network) WLAN Wireless (Local Area Network) Actividades WPAN Wireless (Personal Area Network) WPAN WLAN WMAN WWAN Estándares. Recuperado de [https://www.academia.edu/9410313/WMAN\\_Wireless\\_Metropolitan\\_Area\\_Network\\_WLAN\\_Wireless\\_Local\\_Area\\_Network\\_Actividades\\_WPAN\\_Wireless\\_Personal\\_Area\\_Network\\_WPAN\\_WLAN\\_WMAN\\_WWAN\\_Est%C3%A1ndares](https://www.academia.edu/9410313/WMAN_Wireless_Metropolitan_Area_Network_WLAN_Wireless_Local_Area_Network_Actividades_WPAN_Wireless_Personal_Area_Network_WPAN_WLAN_WMAN_WWAN_Est%C3%A1ndares)*
- *Guerrero, J. (s. f.). GUÍA PARA LA IMPLANTACIÓN DE TECNOLOGÍAS EN LA INDUSTRIA 4.0 (11a Parte). Recuperado 12 de junio de 2019, de <https://www.linkedin.com/pulse/gu%C3%ADa-para-la-implantaci%C3%B3n-de-tecnolog%C3%ADas-en-industria-joaquin-8>*
- *Hdez, M. (s. f.). REDES VLAN. Recuperado 18 de junio de 2019, de <https://prezi.com/y2u8zcugywfa/redes-vlan/>*
- *IEEE 802.11 (WiFi) - Redesbasico150. (s. f.). Recuperado 17 de junio de 2019, de <https://sites.google.com/site/redesbasico150/introduccion-a-los-estandares-de-cableado/ieee-802-11-wifi>*
- *Introducción a las Redes Inalámbricas. (s. f.). Recuperado 12 de junio de 2019, de <http://webcache.googleusercontent.com/search?q=cache:Uy0Ei3wF88IJ:bibing.us.es/proyectos/abreproy/11761/fichero/Volumen1%25252F5-Cap%25C3%25ADtulo1%2B-%2BIntroducci%25C3%25B3n%2Ba%2B%2Bredes%2Binal%25C3%25A1mblicas.pdf%2B+&cd=3&hl=es-419&ct=clnk&gl=pe&client=firefox-b-d>*
- *Las Normas ISO. Herramientas para Todas las Organizaciones | Cemiot InternacionalLas Normas ISO. Herramientas para Todas las Organizaciones. (2012, septiembre 18). Recuperado 17 de junio de 2019, de Cemiot*

*Internacional website: <http://www.cemiot.com/inicio/las-normas-iso-herramientas-para-todas-las-organizaciones/>*

- *Macanella, X. (s. f.). Tecnologías inalámbricas. Recuperado 12 de junio de 2019, de [https://www.academia.edu/34858741/Tecnolog%C3%ADas\\_inal%C3%A1mblicas](https://www.academia.edu/34858741/Tecnolog%C3%ADas_inal%C3%A1mblicas)*
- *Mártil, I. (s. f.). ¿Cómo funcionan las redes inalámbricas de telefonía móvil? – Un poco de ciencia, por favor. Recuperado 12 de junio de 2019, de <https://blogs.publico.es/ignacio-martil/2017/02/24/como-funcionan-las-redes-inalambricas-de-telefonía-movil/>*
- *Medina, P. (s. f.). VLAN. Recuperado 18 de junio de 2019, de [https://issuu.com/perlamedinaa/docs/practica\\_4.docx](https://issuu.com/perlamedinaa/docs/practica_4.docx)*
- *Quintero, M. (s. f.). Introduccion a los estandares del cableado by Marleni Quintero on Prezi. Recuperado 17 de junio de 2019, de <https://prezi.com/fmcxktm2tqwh/introduccion-a-los-estandares-del-cableado/>*
- *Redes de área local virtuales (VLAN). (s. f.). Recuperado 17 de junio de 2019, de [https://www.ibm.com/support/knowledgecenter/es/ssw\\_aix\\_72/com.ibm.aix.networkcomm/adapters\\_vlan.htm](https://www.ibm.com/support/knowledgecenter/es/ssw_aix_72/com.ibm.aix.networkcomm/adapters_vlan.htm)*
- *REDES INALÁMBRICAS. (s. f.). Recuperado 12 de junio de 2019, de [https://webcache.googleusercontent.com/search?q=cache:pDL8VHOIHHwJ:https://upcommons.upc.edu/bitstream/handle/2117/100918/LM01\\_R\\_ES.pdf+&cd=10&hl=es-419&ct=clnk&gl=pe&client=firefox-b-d](https://webcache.googleusercontent.com/search?q=cache:pDL8VHOIHHwJ:https://upcommons.upc.edu/bitstream/handle/2117/100918/LM01_R_ES.pdf+&cd=10&hl=es-419&ct=clnk&gl=pe&client=firefox-b-d)*
- *Redes Inalámbricas de Área Personal. (s. f.). Recuperado 12 de junio de 2019, de*

<http://webcache.googleusercontent.com/search?q=cache:NWAN5icxOs4J:bibing.us.es/proyectos/abreproy/11761/fichero/Volumen1%25252F6-Cap%25C3%25ADtulo2%2B-%2BRedes%2Binal%25C3%25A1mbricas%2Bde%2B%25C3%25A1rea%2Bpersonal%2B%2528WPAN%2529.pdf%2B+&cd=3&hl=es-419&ct=clnk&gl=pe&client=firefox-b-d>

- *Rodríguez, A. (s. f.). Introducción a los Estándares de Cableado. Recuperado 17 de junio de 2019, de Scribd website:*  
<https://es.scribd.com/presentation/62186514/Introduccion-a-los-Estandares-de-Cableado>
- *Tipos de contraseña y cifrado para red WiFi: WEP, WPA, WPA2, TKIP, AES. (s. f.). Recuperado 17 de junio de 2019, de*  
<https://www.testdevelocidad.es/wifi/wi-fi-diferentes-tipos-clave-debemos-elegir/>
- *Tipos de VLAN. (s. f.). Recuperado 18 de junio de 2019, de*  
<https://sites.google.com/site/modulovlan/3-1-presentacion-de-las-vlan/3-1-2-tipos-de-vlan?tmpl=%2Fsystem%2Fapp%2Ftemplates%2Fprint%2F&showPrintDialog=1>
- *TIPOS REDES INALÁMBRICAS. (s. f.). Recuperado 12 de junio de 2019, de*  
<http://utp-redesinalambricas.blogspot.com/2015/09/tipos.html>
- *Toro, M. (s. f.). Modulo 7 cableado estructurado. Recuperado 17 de junio de 2019, de Issuu website:*  
[https://issuu.com/martintoro5/docs/modulo\\_7\\_cableado\\_estructurado](https://issuu.com/martintoro5/docs/modulo_7_cableado_estructurado)
- *Una VLAN nativa se asigna a un puerto de enlace troncal 8021Q En la topología. (s. f.). Recuperado 18 de junio de 2019, de*

*<https://www.coursehero.com/file/p1f2dyf/Una-VLAN-nativa-se-asigna-a-un-puerto-de-enlace-troncal-8021Q-En-la-topolog%C3%ADa/>*

- Walton, E. por A. (2017, diciembre 26). *Segmentación de VLAN: Introducción.*

*Recuperado 18 de junio de 2019, de CCNA desde Cero website:*

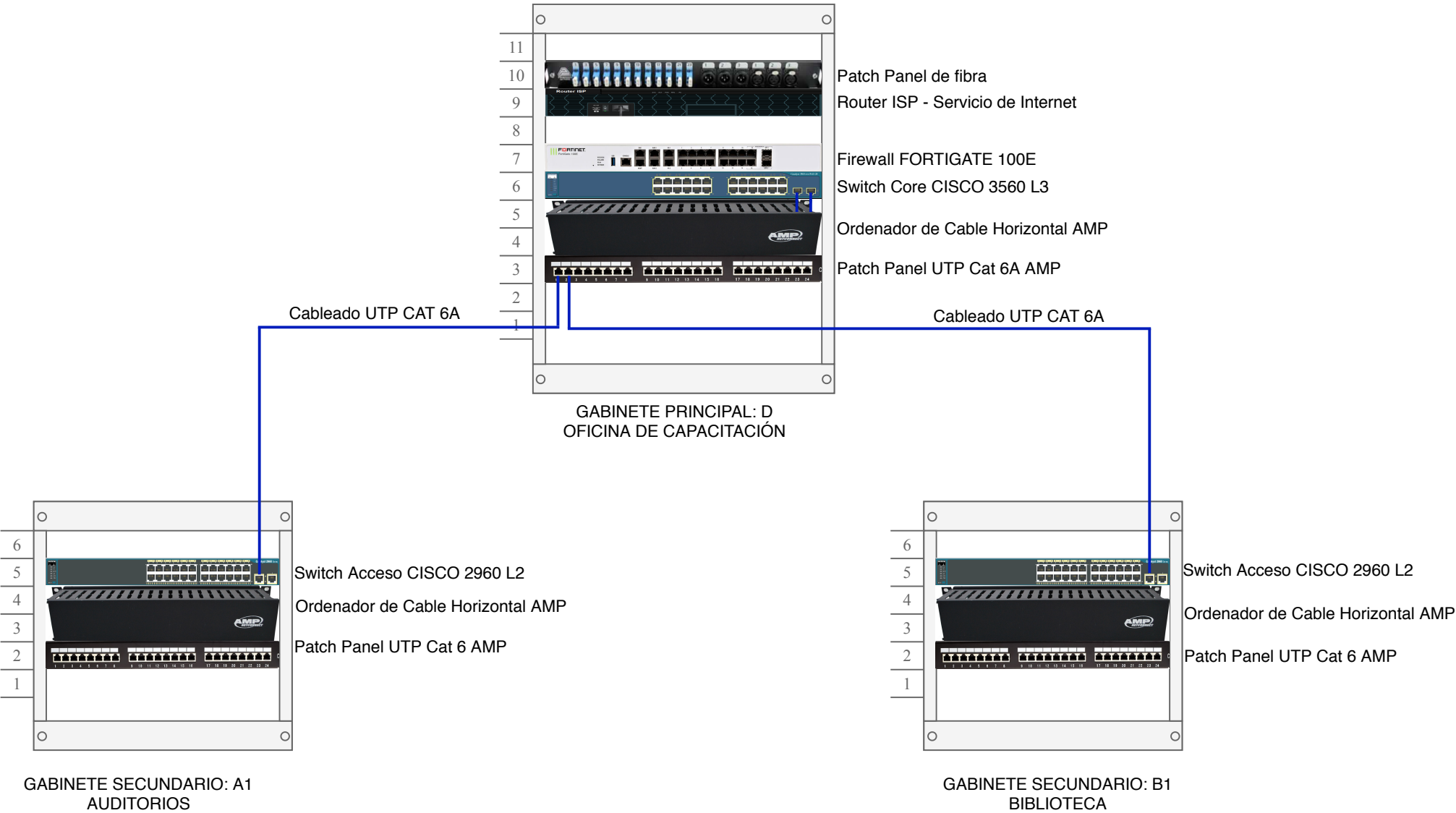
*<https://ccnadesdecero.es/segmentacion-de-vlan-definicion-y-tipos/>*

- WiFi - Wikitel. (s. f.). *Recuperado 12 de junio de 2019, de*

*<http://62.97.113.75/wiki/WiFi>*

# **ANEXOS**

# DISTRIBUCION DE EQUIPOS EN GABINETES Y CUARTO DE TELECOMUNICACIONES



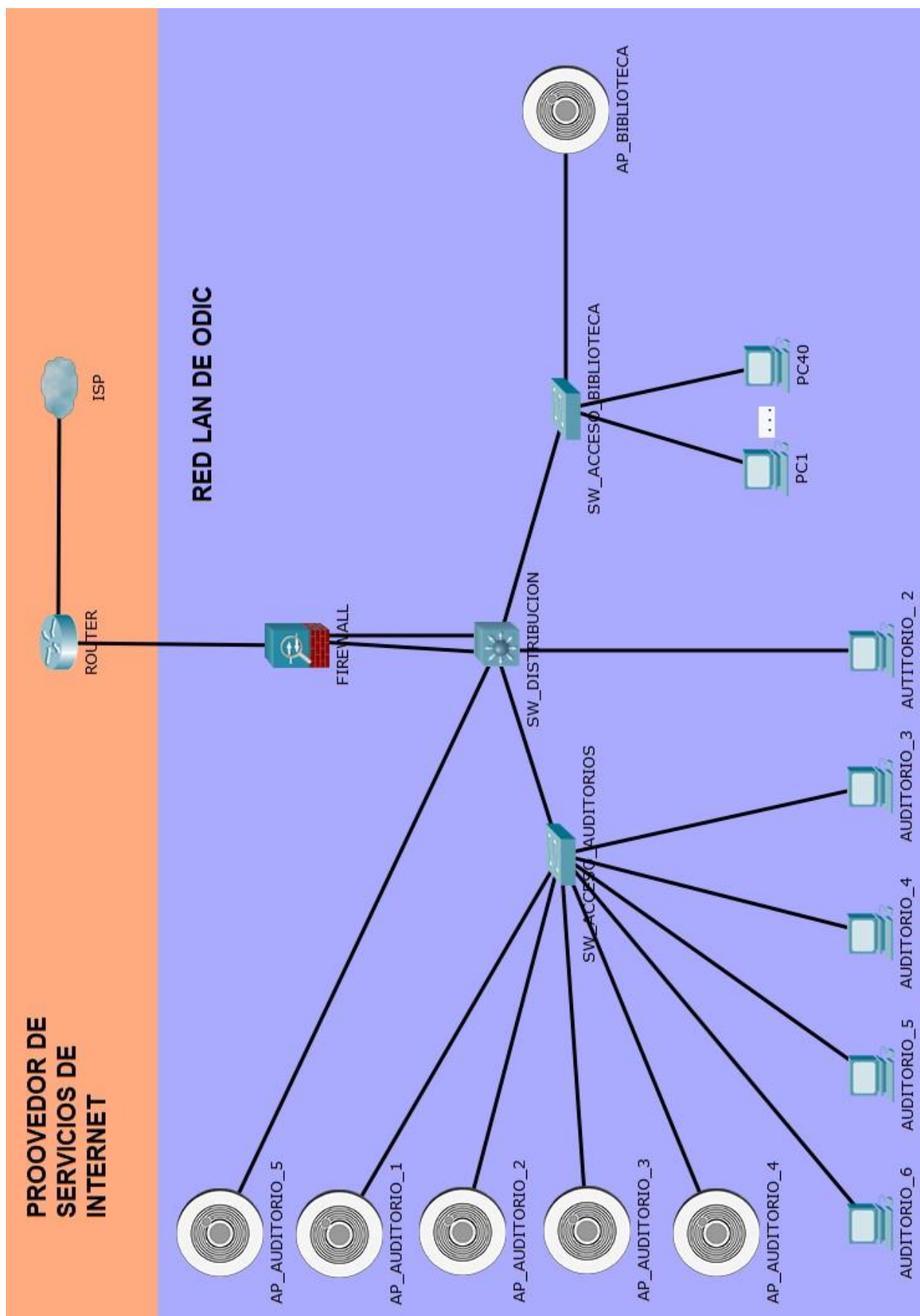
FICHA TECNICA DE GABINETES EN AMBIENTE DE COMUNICACIONES

N	TIPO	RU	MODELO	NOMBRE DE GABINETE	ENLACE	UBICACIÓN FÍSICA
1	PARED	10	GABINETE COMUNICACIONES	GABINETE D	PRINCIPAL	OFICINA DE CAPACITACION- SECRETARIA
2	PARED	6	RACK COMUNICACIONES	GABINETE A1	SECUNDARIO	AUDITORIO 3 INTERIOS
3	PARED	6	RACK COMUNICACIONES	GABINETE B1	SECUNDARIO	BIBLIOTECA INTERIOR

RELACION DE EQUIPOS

N	MARCA	MODELO	VELOCIDAD	CONFIGURACION	VLAN	CAPA	NUM DE PUERTOS	CANTIDAD
1	FORTINET	FORTIGATE 100E	10/100/1000	ADMINISTRABLE	SI	L4	24	1
2	CISCO	CATALYST 3960 - X	10/100/1000	ADMINISTRABLE	SI	L3	24	1
3	PARED	CATALYSY 2960 - X	10/100/1000	ADMINISTRABLE	SI	L2	24	2

## DISEÑO DE ARQUITECTURA





# Plano de la Oficina de Capacitación, Investigación y Desarrollo, auditorios y biblioteca del HNERM.

