CAPÍTULO 1

PRESENTACION DEL PROYECTO

I.- Capítulo I: Presentación del proyecto

I.1.- Presentación del proyecto

Título del Proyecto: Mejoramiento de la gestión de tráfico de datos de la red LAN de comunicación del "Servicio Departamental de Salud SEDES-Tarija" en el área de trabajo PAI utilizando VLANS y servicios de administración de redes

Nombre del Postulante: Natalia Alexandra Duran Díaz

Celular: 69309978

Carrera: Departamento de Informática y Sistemas

Facultad: Ciencias y Tecnología

Institución/Centro Cooperante: Servicio Departamental de Salud “SEDES” Tarija

Duración del Proyecto: 8 meses

Área/línea de investigación priorizada: Redes

I.2.- Perfil del proyecto

I.2.1.- Introducción

Las instituciones públicas o privadas que cuentan con una estructura de red que brindan servicios tecnológicos tienen muchas veces un problema en común: suelen brindar estos servicios de manera poco eficiente y esto resulta en la insatisfacción y el reclamo constante por parte de los usuarios ya sean operativos y/o administrativos de la misma institución, así como también por parte de los usuarios externos que en ambos casos buscan otras alternativas tecnológicas para cumplir con las tareas rutinarias que se les encomienda

También considerando la nueva normalidad que se ha generado donde muchos de los procesos se han automatizado y/o digitalizado el uso de una estructura de red que funcione de manera óptima se ha vuelto un requisito y una necesidad. Los motivos mencionados anteriormente provocan otras

inconformidades aparte de las ya dichas como el mal uso de la infraestructura a falta de actualización y mantenimiento preventivo de los equipos de computación y de la red.

En el Servicio de Salud Departamental (SEDES), no se realizaron nuevas adquisiciones en cuanto a equipos tecnológicos actualizados y equipos de comunicación en las últimas gestiones lo que ha llevado a continuar usando tecnologías obsoletas por parte de los responsables encargados del funcionamiento de la red a su vez que se debe analizar la factibilidad económica, técnica y operativa, para ver si el proyecto es viable

Por los motivos expuestos es que, se pretende analizar las necesidades de la institución bajo el marco de elaboración denominado (Especificación de requerimientos de configuración) y realizar una reestructuración de los servicios de comunicación con los recursos físicos de computación y comunicación disponibles para lo cual se comenzara con un análisis tecnológico de la situación actual del Servicio de Salud Departamental (SEDES) específicamente en el área de trabajo PAI (Programa Ampliado de Inmunización) que será en el cual el proyecto se enfocara y su conexión con el área del centro de datos de la misma institución, aplicando la metodología Top-Down que ayudara a implementar diferentes marcos de trabajo que nos servirá como guía para avanzar hacia una reestructuración y organización de los equipos de comunicación como también de los equipos de computación del área en la cual se trabajara.

I.2.2.- Descripción del proyecto

I.2.2.1.- Antecedentes

I.2.2.2.-Antecedentes de la institución

El servicio Departamental de Salud es una institución pública rectora y gestora de la salud del departamento, desconcentrada administrativa y funcionalmente del gobierno Autónomo

departamental de Tarija, regula e implementa políticas, planes, programas de salud, promueve la participación de todos los sectores públicos, privados y sociales que brinda servicios a la sociedad

El Servicio Departamental de salud Tarija, se constituye en la cabeza del sector salud en el departamento bajo la tuición del gobierno autónomo del departamento, cuyo propósito fundamental es adecuar y articular la política nacional de salud en el departamento; de esta manera busca contribuir al desarrollo humano, a través de un sistema de salud accesible, con equidad de género, basado en la salud familiar, comunitaria e intercultural que atiende con intersectorialidad, generando capacidades individuales para la atención integral a la población del departamento de Tarija.

En el estudio de los antecedentes la institución se logró recabar información sobre la estructura de red actual y su funcionamiento que si bien hasta ahora la entidad mencionada los ha venido utilizando de manera regular no se cuenta con registros de haber tenido ninguna reestructuración en los últimos años debido a esto y a la demanda que se tiene hoy en día se busca otras alternativas para mejorar la velocidad del envío y recepción de datos. A continuación, citaremos algunas tesis o proyectos que podrían relacionarse con el presente trabajo.

I.2.2.3.-Antecedentes de trabajos similares

En el presente trabajo de los autores **Gino John Cordero Paredes y Ximena Juliana Marcillo Espinoza (2018)** en el trabajo de grado realizado "Propuesta de diseño del data center y reestructuración de la red de datos" en la universidad estatal de Bolívar en Quito se basa en una propuesta de diseño de red de datos y de data center utilizando la norma 802.11ac para mejorar la conectividad

Otro de los trabajos que mencionaremos será el de los autores **Gema Katherine Chavez Zambrano y Lady Geomar Tuarez Anchundia(2016) "**Propuesta de red de datos para la gestión de los servicios de red " en el campus politécnico de la ESPAM MFL el cual trata acerca de diseñar un prototipo de administración centralizada para el manejo apropiado de una Red de datos sobre plataformas de tecnología libre y el uso del Estándar 802.11s, y así tener un control necesario de los dispositivos que conformen la infraestructura física, para la gestión de los mismos, como por ejemplo monitorización de la red, determinar el ancho de banda por usuario, incluso gestión de los usuarios a través del su portal cautivo

Del mismo modo tenemos el trabajo de grado de **Jessica Briggeth Borja Cáceres y Kevin Fernando Plazarte Falcon (2023)** "Propuesta de rediseño de la topología en la infraestructura de la red de comunicaciones de la fundación Tainate" de la universidad politécnica saleciana sedes Quito el cual habla sobre el realizar el diseño e implementación de una red de datos, así como también implementar un sistema de video vigilancia sobre IP

Por ultimo mencionamos la tesis de **Edgar Alfredo Von Quednow Mancilla (2006)** "Diseño e implementación de una red inalámbrica de área metropolitana, para distribución de internet en medios suburbanos, utilizando el protocolo IEEE 802.11B" en la universidad de San Carlos en Guatemala se trata de desarrollar los conocimientos necesarios para el diseño y la implementación de una red inalámbrica de área metropolitana (WLAN) como un medio práctico y de bajo costo para la distribución Internet.

I.2.3.- Justificación del proyecto

I.2.3.1.- Tecnológico

En el aspecto tecnológico se analiza que las instituciones que brindan servicios necesitan del uso de una red de datos fiable son los principales responsables de garantizar tecnologías que abastezcan

esas necesidades, así como también equipos actualizados listos para ser utilizados en la medida que sea conveniente para la institución, considerando que los beneficios serán por ambas partes por un lado la institución que provee una mejora sus prestaciones tecnológicas y por el otro lado los usuarios que recibirán servicios de red óptimos para desempeñar sus labores.

I.2.3.2.- Económico

El Servicio de Salud Departamental SEDES- Tarija se verá beneficiado en el ahorro de recursos puesto que el objetivo del proyecto es de implementar y reutilizar los equipos de computación que se encuentren disponibles de modo que la reestructuración no implique un elevado coste de adquisición de los equipos para la institución

Al contar con las plataformas de tecnología actualizadas, así como también con los servicios actualizados se ahorrará en el coste de adquisición de algunos recursos tecnológicos y esto permitirá controlar mejor los gastos económicos de la institución esto se verá con el análisis de factibilidad económica

I.2.3.3.- Social

El presente proyecto tendrá un impacto social puesto que afectara tanto a los usuarios directos que son todo el personal de la institución SEDES y en el área PAI como a los usuarios indirectos que tengan relación con las áreas mencionadas siendo que ambas partes podrán beneficiarse de un servicio de red mejorado que les permitirá mayor facilidad al momento de desempeñar sus respectivas labores.

I.2.3.4.- Desarrollo sostenible

El Servicio Departamental de Salud SEDES como institución tiene los recursos humanos para arrancar sin ningún impedimento con el desarrollo del presente proyecto

I.2.3.5.-Medio ambiental

Una vez que el Servicio de Salud Departamental mejore su calidad de servicios podrá brindar una atención optima sin inconvenientes a toda la población, como también el porcentaje de energía se verá reducido en un porcentaje debido a que algunas plataformas obsoletas dejaran de funcionar con la actualización a las diferentes tecnologías

I.2.4.- Planteamiento del problema

Deficiencia de la conectividad en el segmento de red centralizada LAN de comunicación en el área PAI dentro del "Servicio Departamental de Salud SEDES - Tarija"

I.2.5.- Análisis del cuadro de involucrados

Grupo	Intereses	Problemas	Recursos/Mandatos
Director general	Brindar una estructura de conexión en sus ambientes y dispositivos a través de una red confiable Fortalecimiento y satisfacción de parte del personal responsable en cuanto al uso de la red	Escasa y limitada señal de la red para las instalaciones en distancias amplias Limitado personal preparado para el manejo de la red	Reglamento interno del servicio departamental de salud SEDES Normativas y estatutos Recursos económicos

	Realizar una renovación de la red existente Mejorar el acceso a la red	Instalaciones de red obsoletas y anticuadas Ambientes con una arquitectura antigua	
Personal Administrativo	Recibir ambientes con una red de datos estructurada correctamente y funcional Contar equipos de computación adecuados Tener acceso a la red para la conexión de	Insuficiencia de dispositivos y equipos de computación Equipos de computación desactualizados y obsoletos	Reglamento interno del servicio departamental de salud SEDES Normativas y estatutos

	los equipos de computación y dispositivos Personal capacitado en el uso y manejo de los servicios requeridos	Ausencia de una conexión de red estable	
Personal Medico	Recibir ambientes con una red de datos estructurada correctamente y funcional Disponer de acceso a la red para la conexión de las máquinas y dispositivos	Equipos de computación carentes de mantenimiento regular Ausencia de una conexión de red estable	Reglamento interno del servicio departamental de salud SEDES Normativas y estatutos

Personal responsable de la red	Contar con una red cuya conectividad y señal sean eficientes Contar con las herramientas y dispositivos necesarios para el manejo de la red Recibir ambientes con una red de datos estructurada correctamente y funcional	Conexión de red inestable Herramientas y dispositivos insuficientes para el manejo de la red	Reglamento interno del servicio departamental de salud SEDES Normativas y estatutos

Tabla 1. Cuadro de involucrados

I.2.6.- Árbol de problemas

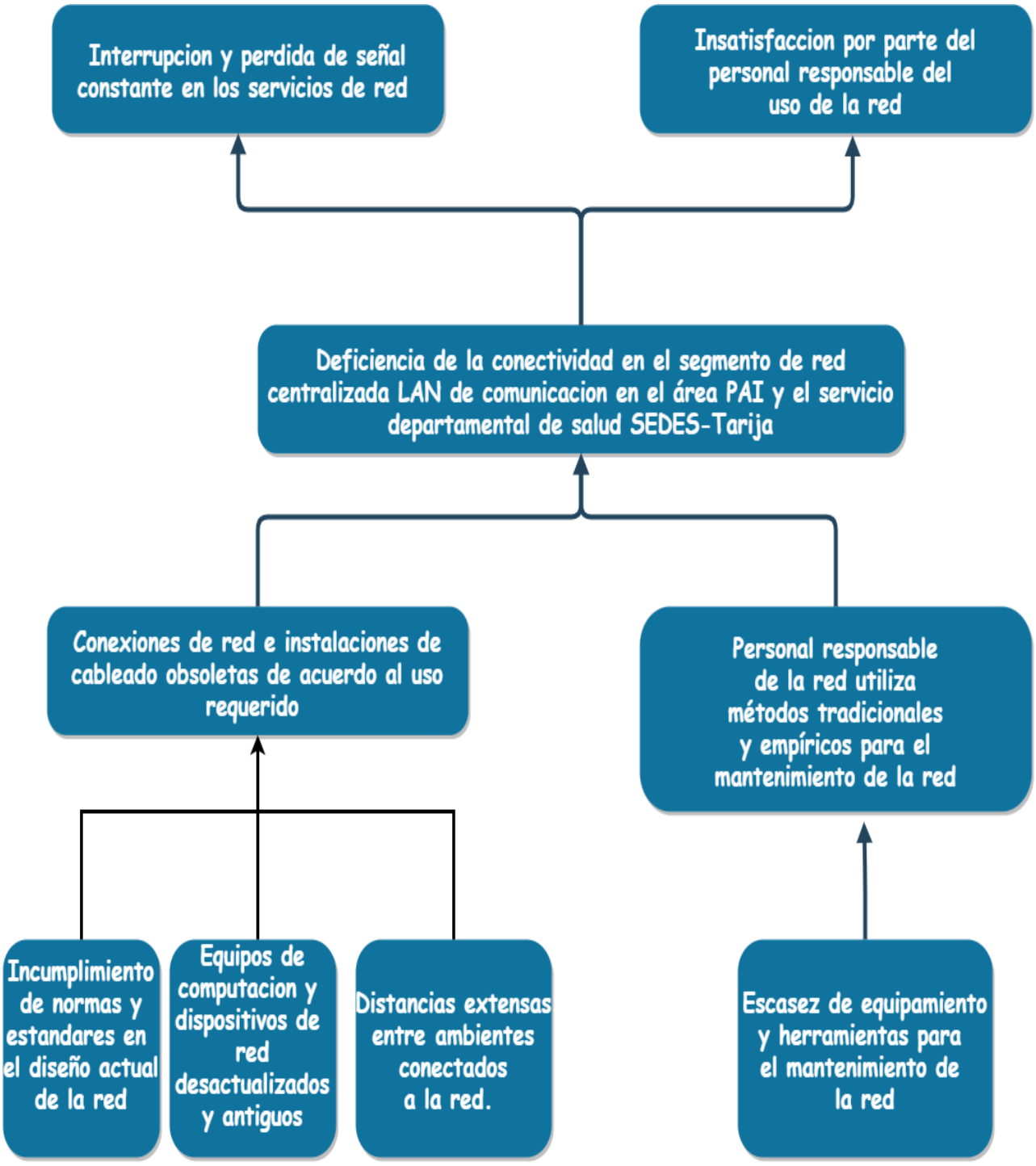


Figura 1. Árbol de problemas

I.2.7.- Árbol de objetivos

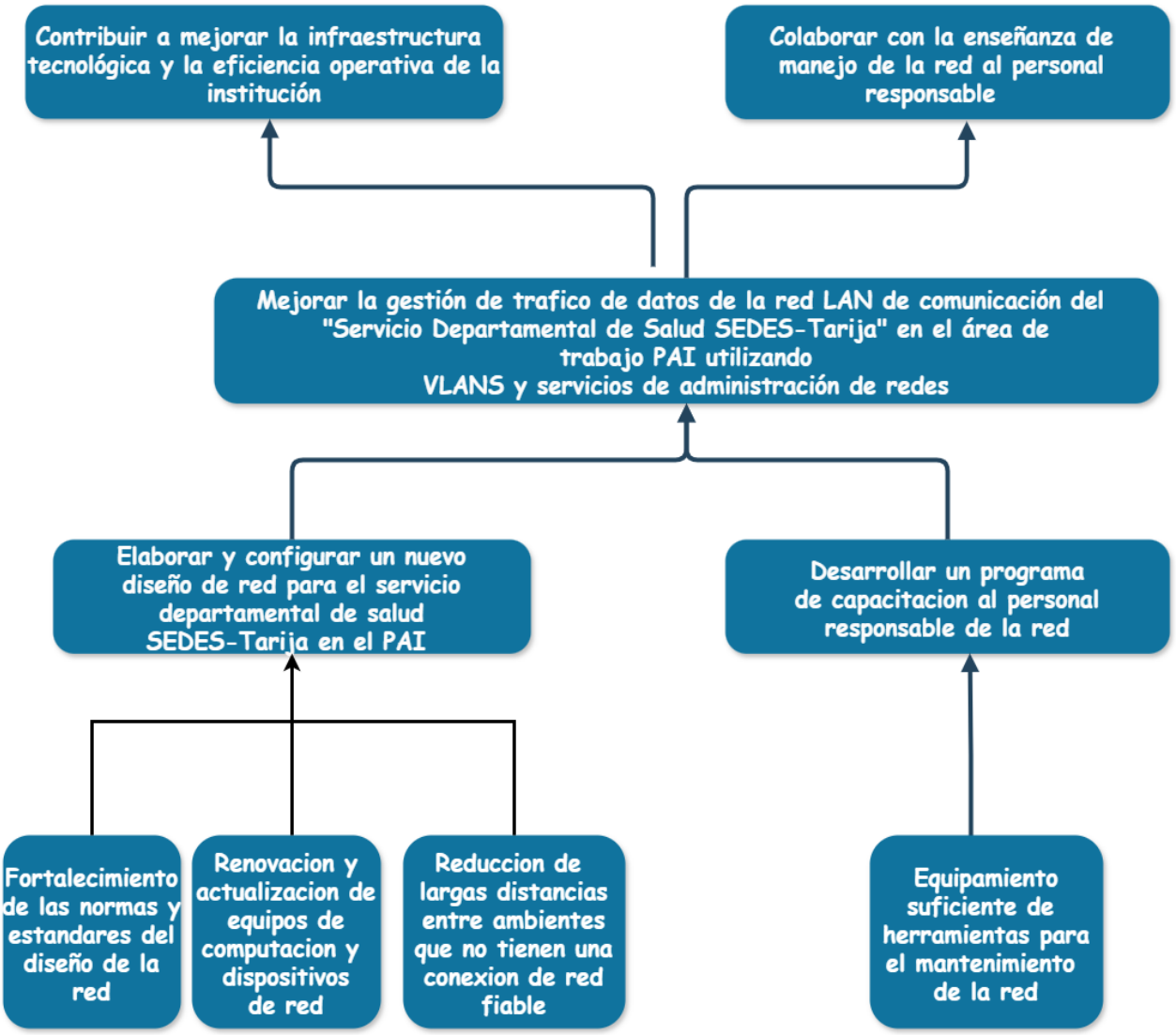


Figura 2. Árbol de objetivos

I.2.8.- Objetivos

I.2.8.1.- Objetivo general

Mejoramiento de la gestión de tráfico de datos de la red LAN de comunicación del "Servicio Departamental de Salud SEDES-Tarija" en el área de trabajo PAI utilizando VLANS y servicios de administración de redes

I.2.8.2.- Objetivos específicos

- Elaborar un nuevo diseño de red para el servicio departamental de salud SEDES-Tarija en el área de trabajo PAI
- Desarrollar un programa de capacitación al personal responsable de administrar la red

I.2.9.- Análisis de alternativas

ESTRATEGIA	**CRITERIO 1** **ECONOMICO**	**CRITERIO 2** **TECNOLOGICO**	**CRITERIO 3** **SOCIAL**
Utilizar un nuevo diseño de red implementando cableado estructurado, servicios de configuración de red para el servicio departamental de salud SEDES-Tarija y el área de trabajo PAI	Es una opción con un costo propio dependiendo de la complejidad el tiempo y el equipamiento necesario	Diseño basado en tecnologías más modernas que permite también actualizar equipos y servicios de red ya obsoletos	Brindaría una mejor señal de red y una conectividad óptima para el personal
Utilizar un diseño de red en base a antenas	Si bien es una opción viable es considerablemente	Diseño tradicional apto para ambientes	Permitiría que el personal cuente con

inalámbricas para el servicio departamental de salud SEDES-Tarija y el área de trabajo PAI	mucho más costosa que el proyecto planteado	con grandes distancias	una conexión a la red eficiente

Tabla 2. Cuadro de involucrados

I.2.10.- Matriz de marco lógico (MML)

Resumen Narrativo del Proyecto	Indicadores	Medios de Verificación	Supuestos
Fin Contribuir a mejorar la infraestructura tecnológica y la eficiencia operativa de la institución SEDES Colaborar con la enseñanza de manejo de la red al personal responsable	Al año de concluir el proyecto, se puede observar que el Servicio de salud Departamental SEDES mantendrá estables y disponibles al menos un 80% de los servicios por medio de red suyos y los que brinda en el área de trabajo PAI	Informe técnico por parte de la institución mostrando el grado de satisfacción con la propuesta de diseño de la red	Los usuarios se adaptan de manera rápida a la reestructuración de la red realizada en el área de trabajo PAI y el Servicio Departamental de Salud SEDES
Propósito		Cuadro comparativo entre el promedio de latencia actual, y el promedio de latencia	El personal encargado del Servicio Departamental SEDES muestra interés y

Gestión mejorada del tráfico de datos de la red LAN de comunicación del "Servicio Departamental de Salud SEDES-Tarija"	Al finalizar el proyecto, se ha reducido el tiempo promedio de latencia de la red LAN del SEDES y el área PAI, en un 80%	simulado con la nueva red LAN, avalado por el docente de Taller III	participa activamente en la definición de requerimientos y entrega de manera oportuna la información solicitada para la realización del rediseño de la red
Componentes Diseño de infraestructura de red escalable y segura, elaborada. Programa de capacitación implementado, en el uso y mantenimiento adecuado de la red,	Al finalizar el proyecto se logró completar un 90% del diseño de red propuesto, así como también con los servicios disponibles de acuerdo a la ANSI*/TIA-568, la IEEE 802.11 y la IEEE 802.1Q*	Carta por parte del técnico responsable del seguimiento que expresa la realización del diseño y la realización de la capacitación correspondiente.	Existencia del hardware necesario para realizar la reestructuración física de los equipos de computación y equipos de red de la institución

para el personal encargado del SEDES.	Al finalizar el proyecto el personal responsable de administrar la red será capacitado en cuanto a la configuración y uso de la misma	Lista de participantes de la capacitación	Disponibilidad por parte del personal responsable para asistir a las capacitaciones
Actividades Componente 1: Diseño de infraestructura de red escalable y segura, elaborada. Las actividades a realizar son las propuestas en la metodología TOP-DOWN • Analizar requerimientos • Desarrollar diseño lógico • Desarrollar diseño físico • Probar, optimizar y documentar diseño	**Resumen presupuesto** Investigaciones 1000.00 S. básicos 360.00 E. computación 4000.00 **Total** **5360.00 Bs**	Calendario propuesto para el proyecto se cumple Documentación de la realización del diseño de los servicios y las VLANs Material que avale la realización de la capacitación pertinente	Apoyo para el desarrollo y realización del proyecto por parte del personal El Servicio Departamental de Salud como institución cuenta con el presupuesto necesario para la correcta implementación de la propuesta del diseño de la

• Implementar y probar la red • Monitorear y optimizar la red Componente 2: Programa de capacitación implementado, en el uso y mantenimiento adecuado de la red, para el personal encargado del SEDES. • Cronograma de capacitacion al personal • Realizacion de la capacitacion al personal		Revisiones por parte del docente de la materia Taller III	reestructuración de su red y la del área de trabajo PAI

I.2.11.- Metodología para el desarrollo del proyecto

I.2.11.1.- Top Down

Esta metodología de la compañía Cisco tiene como propósito el de diseñar una red en un modelo jerárquico y de integración que proporciona un proceso donde se puede identificar subprocesos y aislar problemas para su resolución, de este modo es necesario cumplir con requisitos técnicos para una mayor funcionalidad, disponibilidad, escalabilidad, accesibilidad y seguridad de la red

Fase 1: Analizar requerimientos

En esta fase inicial se evalúa el estado y la situación actual de la infraestructura en base a la información obtenida de la red y los requisitos técnico que se necesitan

- Analizar metas del negocio
- Analizar metas técnicas
- Analizar red existente
- Analizar tráfico existente

Fase 2: Desarrollar diseño lógico

En la segunda fase se muestra la estructura lógica del diseño de red en base a la información obtenida de la primera fase. En esta etapa se presenta el diseño de la topología de la red y los datos más importantes de los protocolos de red que se utilizaron

- Diseñar topología de red
- Diseñar modelos de direccionamiento y hostnames
- Seleccionar protocolos para Switching y Routing
- Desarrollar estrategias de seguridad

- Desarrollar estrategias de administración de red

Fase 3: Desarrollar diseño físico

En la tercera fase se propone la estructura física y tecnológica de los equipos que van a ser utilizados en el diseño

- Seleccionar tecnologías y dispositivos para redes de campus
- Seleccionar tecnologías y dispositivos para redes empresariales

Fase 4: Probar, optimizar y documentar diseño

En esta fase se debe realizar un plan de pruebas donde se pueda verificar fallas en el diseño con el fin de corregirlas y documentarlo en el diseño final

- Simular el diseño de red
- Probar el diseño de red
- Optimizar el diseño de red
- Documentar el diseño

Fase 5: Implementar y probar la red

En esta fase se debe implementar y probar la red que se viene diseñando en las fases anteriores

- Realizar cronograma de implementación
- Implementación del diseño de red (final)
- Realizar pila de pruebas

Fase 6: Monitorear y optimizar la red

En la última fase se debe monitorear y optimizar la red implementada para verificar su funcionamiento

- Operación de la red en producción
- Monitoreo de la red
- Optimización de la red

I.2.12.- Resultados esperados

Servicios de red óptimos y minimización de la perdida de señal

Personal responsable del uso de la red satisfecho en cuanto al nuevo diseño propuesto

Se espera que el diseño y desarrollo de la realización de la reestructuración de la red satisfaga las necesidades de los funcionarios en cuanto a accesos a internet como también los sistemas administrativos en la red

Se espera que el personal responsable del funcionamiento de la red una vez haya concluido la capacitación sea capaz de administrar correctamente la nueva implementación, además de ser capaces de responder a los incidentes informáticos

I.2.13.- Beneficiarios

I.2.13.1.- Beneficiarios Directos

Los beneficiarios directos son tanto el personal administrativo como el médico y también el personal que está a cargo de la parte tecnológica del Servicio Departamental de Salud SEDES específicamente en el área de programa ampliado de inmunización (PAI).

I.2.13.2.-Beneficiarios indirectos

Los beneficiarios indirectos son todo el personal administrativo y medico de las áreas que tienen relación o están directamente conectadas al área PAI del Servicio Departamental de Salud SEDES

I.2.14.- Cronograma de Actividades

Nº	Actividad	Nº días	Fecha inicio	Fecha Final	M1	M2	M3	M4	M5	M6	M7	M8
1	Realización de la configuración de la red	**125**	**15/04/23**	**19/08/23**	**X**	**X**	**X**	**X**				
1.1	Recopilar información actual de los equipos de computación así como también del diseño actual de la red	**15**	**15/04/23**	**30/04/23**	**X**							
1.2	Realizar un diagnóstico con una solución recomendada	**20**	**2/05/23**	**21/05/23**		**X**						
1.3	Aplicar una solución a los equipos de computación y a los servicios de la red	**40**	**22/05/23**	**30/06/23**		**X**	**X**					

1.4	Diseñar la distribución de los servicios	**25**	**1/07/23**	**25/07/23**				**X**				
1.5	Implementar los servicios requeridos	**25**	**26/07/23**	**19/08/23**				**X**	**X**			
2	Capacitación al personal responsable del manejo de la red	**29**	**21/08/23**	**20/09/23**					**X**	**X**		
2.1	Definición de medios y estrategias	**15**	**21/08/23**	**4/09/23**					**X**	**X**		
2.2	Capacitación para el manejo de la nueva infraestructura tecnológica	**7**	**5/09/23**	**11/09/23**						**X**		

Tabla 3. Cronograma de actividades

I.2.15.- Presupuesto general

PARTIDA	**FINALIDAD**				
2000	**Consultor**				
#	**Recurso**	**Aporte UAJMS**	**Aporte institucional**		**TOTAL (Bs)**
1	Retribución por investigación y desarrollo	0.00	1000.00		1000.00
Subtotal componente					1000.00

PARTIDA	**FINALIDAD**				
4000	**Útiles y Materiales eléctricos**				
#	**Recurso**	**Aporte UAJMS**	**Aporte institucional**	**Cantidad**	**TOTAL (Bs)**
1	Tarjetas de red	0.00	207.00	15	3105.00

2	Kit de montaje en pared	0.00	70.00	4	280.00
3	Cable cat6 caja de 305 metros	0.00	185.00	1	185.00
4	Canaletas	0.00	3.00	10	30.00
Subtotal componente					3600.00

PARTIDA	**FINALIDAD**				
4500	**Equipos de computación**				
#	**Recurso**	**Aporte UAJMS**	**Aporte institucional**	**Cantidad**	**TOTAL (Bs)**
1	Computadoras de escritorio	0.00	2939.00	15	44085.00
Subtotal componente					44085.00

PARTIDA	**FINALIDAD**				
1000	**Equipos de comunicación**				
#	**Recurso**	**Aporte UAJMS**	**Aporte institucional**	**Cantidad**	**TOTAL (Bs)**
1	Enrutador wifi Internet Tigo	0.00	480.00	1	480.00
2	Access point	0.00	242.00	2	968.00
Subtotal componente					1448.00

PARTIDA	**FINALIDAD**				
2500	**Equipos de seguridad y protección contra incendios**				
#	**Recurso**	**Aporte UAJMS**	**Aporte institucional**	**Cantidad**	**TOTAL (Bs)**
1	Pulsador de Pánico	0.00	**20.00**	5	100.00

2	Central contra incendios	0.00	**105.00**	1	105.00
3	Sirena con luz estroboscópica	0.00	**61.00**	5	305.00
4	Sensor fototérmico	0.00	**120.00**	5	600.00
5	Extintores	0.00	**250.00**	5	1250.00
Subtotal componente					2360.00

Tabla 4. Presupuesto del proyecto

Condiciones

- El presupuesto tiene una duración de un año
- Sujeto a variación de precios por aumento en costos nivel nacional e internacional
- Equipos sujetos a Stock
- Equipos sujetos a Cambio por actualización de modelos
- Entrega de equipos en 120 días

CAPITULO II

MARCO TEORICO

II.- Capitulo II: Marco teórico

II.1.- Marco Teórico

II.1.1.- Introducción

En el presente capítulo se tiene como objetivo profundizar el concepto de lo que es una red para que sirve y porque es necesaria actualmente en la institución.

A su vez se mencionarán los diferentes componentes hardware (Dispositivos de red y componentes necesarios para instalación de la red) y las diferentes herramientas software que se utilizaron en el desarrollo del proyecto, además que se explicara las fases de la metodología TOP-DOWN que fue la seleccionada para el diseño y desarrollo del proyecto.

Una red es la combinación de dos o más sistemas y los enlaces de conexión de los mismos. Una red física es el hardware (equipo como adaptadores, cables y líneas de teléfono) que compone la red. El software y el modelo conceptual componen la red lógica. Existen distintos tipos de redes y emuladores que proporcionan funciones diferentes.

Las características de una red de comunicación son:

Infraestructura de la red

Son los dispositivos de red subyacentes que ayudan a interconectar los dispositivos de red. Los dispositivos que componen la infraestructura de red incluyen conmutadores de red, routers, cortafuegos, servidores, módems, etc.

Seguridad de la red

La seguridad de la red es la protección de la red contra cualquier acceso o ataque no autorizado. Incluye la prevención de software malicioso, virus y otros ataques a la red. La seguridad de la red

es importante para toda red informática porque protege los datos de la organización y la red informática.

Fiabilidad de la red

La fiabilidad de la red mide el tiempo que la red puede mantenerse en servicio sin ninguna interrupción o fallo. Lo que hay que saber es que hay muchos factores que pueden afectar a la fiabilidad de la red. Entre ellos se encuentran los desastres naturales, las catástrofes provocadas por el hombre y los problemas con el hardware y el software de la red.

Capacidad de la red

La capacidad de la red es la cantidad de datos o servicios que la red puede manejar al mismo tiempo. Hay que asegurarse de que la capacidad de la red informática es suficiente para manejar las necesidades actuales y futuras de la organización.

Velocidad y rendimiento de la red de comunicación

La velocidad de la red informática es la tasa de transmisión de datos a través de la red. También determina el tiempo que se tarda en transmitir los datos por la red. El rendimiento de la red es la cantidad de tiempo que se tarda en realizar una determinada tarea.

Escalabilidad de la red

La escalabilidad de la red es la capacidad de crecer y expandirse con el crecimiento del negocio. La red debe ser capaz de manejar las necesidades actuales y futuras de la organización. La red debe ser lo suficientemente escalable como para acomodar el creciente número de usuarios, datos y servicios.

Disponibilidad de la red

La disponibilidad de la red es el porcentaje de tiempo de actividad o de inactividad de la red. La disponibilidad de la red debe ser lo más cercana posible al 100%. Cuanto mayor sea la disponibilidad de la red, mejor será para la empresa.

Mantenimiento de la red

El mantenimiento de la red es el coste incurrido para el mantenimiento de la red. El mantenimiento incluye la supervisión, la resolución de problemas y la reparación de la red cuando sea necesario. Es importante mantener la red para proteger los datos y los recursos de las amenazas, y para que la red funcione sin problemas.

II.1.2.- Modelos de protocolos

Las personas se comunican y transmiten información a otras haciendo uso de protocolos de comunicación y para que esta sea posible deben existir tres elementos fundamentales: origen, destino y medio o canal, siempre que se envía o transmite información es importante identificar quien lo hace, hacia donde se envía y tener un método de comunicación acordado.

Los modelos que veremos a profundidad serán el TCP/IP y el modelo OSI.

II.1.2.1.- Modelo OSI

la Organización Internacional de Estandarización (ISO) desarrolló un modelo llamado OSI (Open Systems Interconnection, Interconexión de sistemas abiertos), el cual es usado para describir el uso de datos entre la conexión física de la red y la aplicación del usuario final. Este modelo es el mejor conocido y utilizado para describir los entornos de red.

Se compone en siete capas para las actividades de red. Cada capa tiene asociados uno o más protocolos. Las capas representan las operaciones de transferencia de datos comunes a todos los tipos de transferencias de datos entre las redes de cooperación

Si se dividen las funciones de la red en estas capas se obtienen las siguientes ventajas:

- Divide la comunicación de red en partes más pequeñas y sencillas.
- Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.
- Permite a los distintos tipos de hardware y software de red comunicarse entre sí.
- Impide que los cambios en una capa puedan afectar las demás capas, para que se puedan desarrollar con más rapidez.

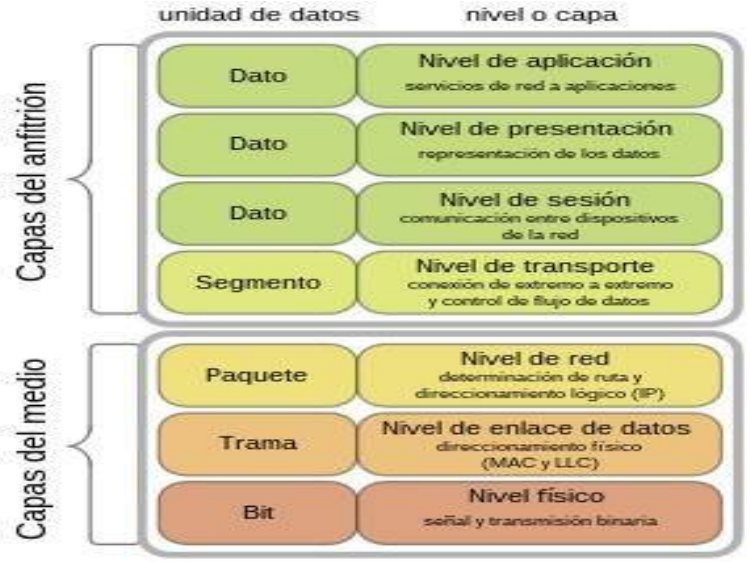


Figura 3. Modelo OSI

II.1.2.2.-Modelo TCP/IP

Si se dividen las funciones de la red en estas capas se obtienen las siguientes ventajas:

- Divide la comunicación de red en partes más pequeñas y sencillas.
- Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.
- Permite a los distintos tipos de hardware y software de red comunicarse entre sí.
- Impide que los cambios en una capa puedan afectar las demás capas, para que se puedan desarrollar con más rapidez.

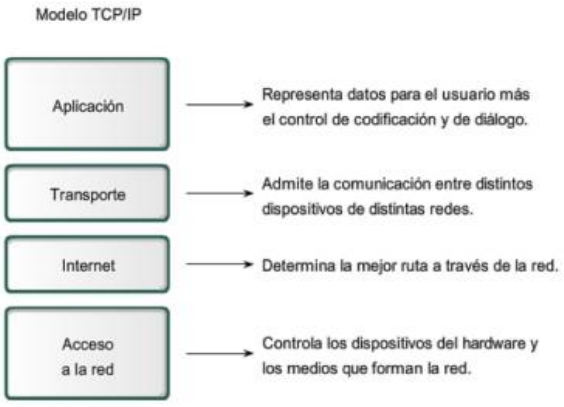


Figura 4. Modelo TCP/IP

II.1.2.3.-Diferencias entre modelo OSI y modelo TCP/IP

La capa de aplicación del modelo TCP/IP es similar a las capas 5, 6, 7 combinadas del modelo OSI, el modelo TCP/IP no tiene una capa de sesión. La capa de transporte de TCP/IP abarca las responsabilidades de la capa de transporte OSI y algunas de las responsabilidades de la capa de sesión OSI. La capa de acceso a la red del modelo TCP/IP abarca el enlace de datos y las capas físicas del modelo OSI

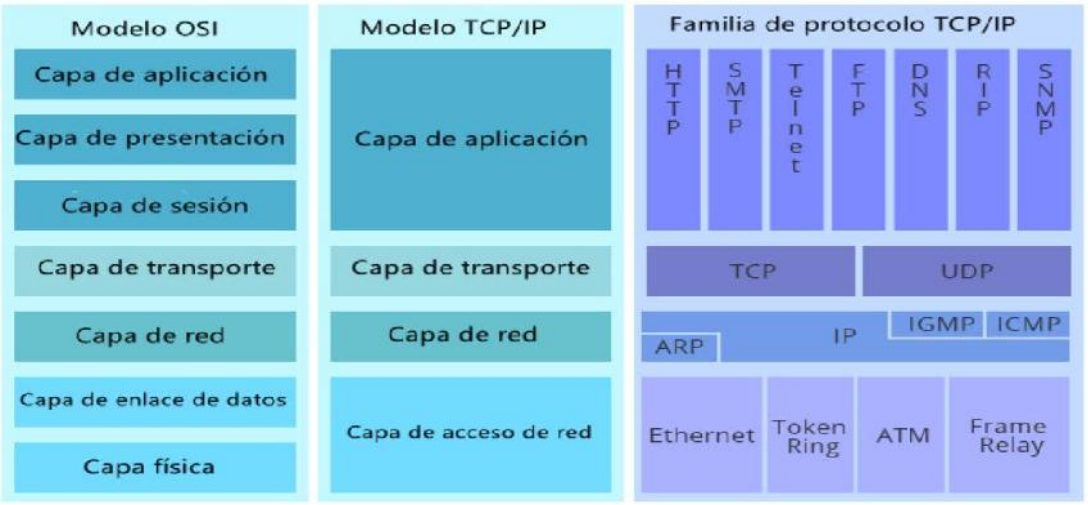


Figura 5. Diferencias entre OSI y TCP/IP

II.1.3.-Tecnologías de red

II.1.3.1.- Redes de área local LAN

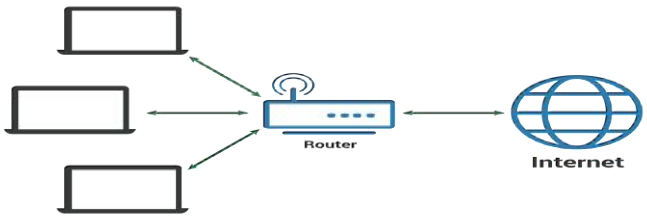


Figura 6. Redes LAN

Son redes de propiedad privada que se encuentran en un sólo edificio o campus de pocos kilómetros de longitud. Se utilizan ampliamente para conectar computadores personales, estaciones de trabajo impresoras y otros equipos de red, los cuales compartirán recursos e información. En este tipo de redes se deberán considerar tres aspectos: tamaño, tecnología de transmisión y topologías.

Sus ventajas son:

- Posibilidad de compartir equipos periféricos tales como impresoras, módems, fax,etc.

- Posibilidad de compartir información a través de bases de datos centralizadas en servidores
- Reduce y elimina la duplicidad de trabajos
- Permite mejorar la seguridad y control de la información

II.1.4.- Topología de una red

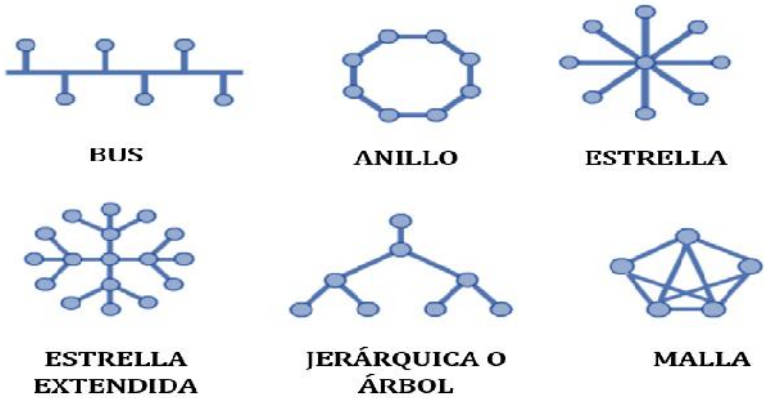


Figura 7. Topologia de red

La topología define la estructura de una red. Una parte de la definición topológica es la topología física, que es la disposición real de los cables o medios. La otra parte es la topología lógica, que define la forma en que los hosts acceden a los medios para enviar datos. Las topologías físicas más comúnmente usadas son las siguientes:

- **La Topología de Bus** usa un solo cable backbone que debe terminarse en ambos extremos todos los hosts se conectan directamente a este backbone.
- **La Topología de Anillo** conecta un host con el siguiente y al último host con el primero. Esto crea un anillo físico de cable.
- **La Topología en Estrella** conecta todos los cables con un punto central de concentración.

- **La Topología en Estrella Extendida** conecta estrellas individuales entre sí mediante la conexión de hubs o switches. Esta topología puede extender el alcance y la cobertura de la red.

II.1.5.- Medios físicos de transmisión

En la actualidad, numerosas empresa e instituciones educativas requieren una infraestructura de cableado estructurado para suplir las necesidades de transporte de información, con este propósito el cableado estructurado es la opción más relevante para el diseño de la red.

II.1.5.1.- Cable de Cobre o Par Trenzado

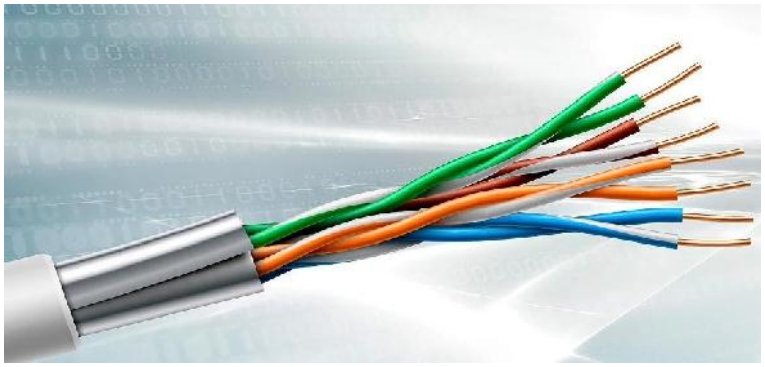


Figura 8. Cable de cobre

El cable de cobre es uno de los más utilizados en la actualidad junto con la fibra óptica, este cable está formado por hilos de cobre, estos están trenzados entre sí para mantener sus propiedades eléctricas y que están se mantengan estables con el tiempo y con el uso además para evitar interferencias. Cada uno de estos pares se identifica mediante un color, siendo los colores asignados y las agrupaciones de los pares de la siguiente forma:

Par 1: Blanco-Azul/Azul

Par 2: Blanco-Naranja/Naranja

Par 3: Blanco-Verde/Verde

Par 4: Blanco-Marrón/Marrón

El cable trenzado se blinda de acuerdo a la forma de blindaje se clasifican en varios tipos como:

Cable UTP: Es un cable de par trenzado que no está blindado. Es muy sensible a interferencias, es muy flexible.

Cable STP: Es un cable de par trenzado blindado individualmente, cada par se envuelve en una malla conductora y otra general que recubre todos los pares. Es inmune al ruido y bastante rígido

Cable FTP: Es un cable de par trenzado blindado globalmente, los cables se recubren de una malla conductora global en forma trenzada. Es poco sensible a las interferencias y tiene una rigidez intermedia.

Dependiendo la velocidad de transmisión ha sido divida en diferentes categorías como:

Categoría 1: Este tipo de hilo de par trenzado solamente está contemplado para su uso en comunicaciones por voz y telefónicas. Transmite a frecuencias en torno a 1 MHz, no llegando a dar una calidad suficiente para datos.

Categoría 2: Este cable actualmente tampoco es adecuado para efectuar transmisión de datos en una red, ya que es capaz de transmitir a una velocidad de hasta 4 Mbps. Fue utilizado en redes anteriores como Token Ring, no cuenta con blindaje y en él encontramos cuatro pares trenzados.

Categoría 3: En esta categoría tenemos ya un cable capacitado para transmitir datos en una red, implementándose en antiguas redes Ethernet 10BASE-T. Esto significa que ofrece un ancho de banda de 10 Mbps con una frecuencia de 16 MHz, por lo que ya no es de uso para las redes actuales.

Categoría 4: Este tipo de cable todavía no está blindado, aunque admite anchos de banda un poco más interesantes con hasta 20 Mbps de velocidad a una frecuencia de 20 MHz. Tampoco es de habitual uso, ya que las redes LAN actuales operando todas por encima de los 100 Mbps.

Categoría 5: Este cable aún está considerado de bajas prestaciones, ya que no tiene blindaje. Soporta transmisiones Fast Ethernet (100BASE-T) a 100 Mbps y a una frecuencia de 100 MHz.

Categoría 5e: Este será el cable típico y más económico que podríamos comprar hoy día en una tienda. Esta categoría cuenta con cables que pueden o no tener blindaje y serán capaces de brindar anchos de banda de 1000 Mbps (1000BASE-T) o Gigabit Ethernet operando en frecuencia de 100 MHz.

Categoría 6: Este cable es de uso generalizado en redes LAN internas, ya que ofrece velocidades de 1000 Mbps como el anterior, pero soportando frecuencias de 250 MHz al ser blindado. Esto implica que su estructura interna soporta mejor las interferencias y la diafonía.

Categoría 6e: Aquí tenemos ya un cable de bastante buena calidad entre las manos, estando construido para operar en redes hasta de 10 Gbps (10GBASE-T). Su mejor calidad de construcción le permite operar en frecuencia de hasta 500 MHz, cubriendo distancias superiores a los 50 m.

Categoría 7: Un cable poco habitual entre los usuarios domésticos pero que sí se utiliza en los centros de datos, al menos hasta la llegada de la fibra óptica. Cuenta con blindado, lo que permite operar en frecuencias de 600 MHz y a velocidades de 10 Gbps a una distancia de 100 m.

Categoría 7a: Otra variante de la categoría anterior para cables que sean capaces de transmitir a frecuencias de 1000 MHz y velocidades de entre 10 y 40 Gbps. Porque efectivamente, hay cables Ethernet capaces de superar los 10 Gbps.

Categoría 8: La última categoría listada se trata de la más potente en la actualidad, con cables par trenzado capaces de llegar a los 40 Gbps y operar en frecuencias de 2000 MHz.

II.1.5.2.-Cable Coaxial

Figura 9. Cable coaxial

Un cable compuesto por un hilo de cobre en la parte central rodeada por una malla metálica y separados ambos elementos conductores por un aislante, envuelto todo por una cubierta exterior. La malla metálica proporciona un apantallamiento para las interferencias. El cable coaxial es menos susceptible a interferencias y ruidos que el cable de par trenzado y puede ser usado a mayores distancias que éste. Puede soportar más estaciones en una línea compartida.

Existen dos tipos de cable utilizados para implementar redes LAN, los cuales son:

- Grueso, su grosor es de 1,27 cm y capacidad para transportar la señal a más de 500 m. Es bastante grueso se hace difícil su instalación.
- Fino, su grosor es de 0,64 cm y capacidad para transportar una señal hasta 185 m. Es flexible y de fácil instalación.

II.1.5.3.-Fibra Óptica

Figura 10. Fibra optica

El cable de fibra óptica consiste en un centro de cristal rodeado de varias capas de material protector. Por el centro de cristal se transmite luz, no señales eléctricas por lo tanto se elimina la problemática de las interferencias. Es ideal para entornos en los que haya gran cantidad de interferencias eléctricas. También se utiliza mucho en la conexión de redes entre edificios debido a su inmunidad a la humedad y a la exposición solar. Existen dos tipos de fibra óptica:

- Multimodo: Los diferentes haces que salen de la fuente de luz son contables. Eso significa que la fuente de luz no genera un haz disperso y continuo dentro de la fibra, sino que la luz entra solo en un número entero de ángulos diferentes.
- Monomodo: Su principal ventaja ancho de banda prácticamente ilimitada, sólo se propaga un modo por lo que se evita la dispersión modal, debida a la diferencia de velocidad de propagación de los modos que se transmiten por la fibra.

II.1.5.4.-Conector RJ45

Figura 11. Conector RJ45

Es una interfaz física comúnmente usada para conectar redes de cableado estructurado, (categorías 4, 5, 5e y 6). RJ es un acrónimo inglés de Registered Jack que a su vez es parte del Código Federal de Regulaciones de Estados Unidos. Posee ocho "pines" o conexiones eléctricas, que normalmente se usan como extremos de cables de par trenzado.

Es utilizada comúnmente con estándares como TIA/EIA-568-B, que define la disposición de los pines o wiring pinout.

Una aplicación común es su uso en cables de red Ethernet, donde suelen usarse 8 pines (4 pares). Otras aplicaciones incluyen terminaciones de teléfonos (4 pines o 2 pares) por ejemplo en Francia y Alemania, otros servicios de red como RDSI y T1 e incluso RS-232.

II.1.5.5.-Conectores de Fibra Óptica

Figura 12. Conectores fibra optica

Los conectores más comunes usados en la fibra óptica para redes de área local son los conectores ST y SC.

El conector SC (Straight Connection) es un conector de inserción directa que suele utilizarse en conmutadores Ethernet de tipo Gigabit. El conector ST (Straight Tip) es un conector similar al SC, pero requiere un giro del conector para su inserción, de modo similar a los conectores coaxiales.

II.1.6.- Cableado Estructurado

II.1.6.1.- Introducción

El cableado estructurado es un conjunto de cables, conectores, canalizaciones y dispositivos que componen la infraestructura de telecomunicaciones interior de un edificio o recinto. Que tiene como función transportar señales desde unos dispositivos (emisores) a otros (receptores) con el objetivo de crear la red de área local del mismo.

Esta estructura contiene una combinación de cables trenzados (UTP/STP/FTP), fibras ópticas (FO) y/o cables coaxiales que deben cumplir ciertos estándares universales para que puedan ser fácilmente entendidos por instaladores, administradores de redes.

II.1.6.2.- Organismos y normas

II.1.6.2.1.- Organismos:

ANSI: American National Standards Institute. Organización Privada sin fines de lucro fundada en 1918, la cual administra y coordina el sistema de estandarización voluntaria del sector privado de los Estados Unidos.

EIA: Electronics Industry Association. Fundada en 1924, desarrolla normas y publicaciones sobre las principales áreas técnicas: los componentes electrónicos, electrónica del consumidor, información electrónica y telecomunicaciones.

TIA: Telecommunications Industry Association Fundada en 1985 después del rompimiento del monopolio de AT&T. Desarrolla normas de cableado industrial23 voluntario para muchos productos de las telecomunicaciones y tiene más de 70 normas preestablecidas.

ISO: International Standards Organization. Organización no gubernamental creada en 1947 a nivel Mundial, de cuerpos de normas nacionales, con más de 140 países.

IEEE: Instituto de Ingenieros Eléctricos y de Electrónica. Principalmente responsable por las especificaciones de redes de área local como 802.3 Ethernet,802.5 Token Ring, ATM y las normas de Gigabit Ethernet.

II.1.6.2.2.-Normas

ANSI/TIA/EIA-568-B: Cableado de Telecomunicaciones en Edificios Comerciales. (Cómo instalar el Cableado)

TIA/EIA 568-B1 Requerimientos generales

TIA/EIA 568-B2 Componentes de cableado mediante par trenzado balanceado

TIA/EIA 568-B3 Componentes de cableado, Fibra óptica

ANSI/TIA/EIA-569-A: Normas de Recorridos y Espacios de Telecomunicaciones en Edificios Comerciales (Cómo enrutar el cableado)

ANSI/TIA/EIA-570-A: Normas de Infraestructura Residencial de Telecomunicaciones

ANSI/TIA/EIA-606-A: Normas de Administración de Infraestructura de Telecomunicaciones en Edificios Comerciales

ANSI/TIA/EIA-607: Requerimientos para instalaciones de sistemas de puesta a tierra de Telecomunicaciones en Edificios Comerciales.

II.1.6.3.-Longitud del cable

La longitud total del cable que se requiere para conectar un dispositivo incluye todos los cables desde los dispositivos finales del área de trabajo hasta el dispositivo intermediario en el centro de datos (generalmente un switch). Esto incluye el cable desde los dispositivos hasta el enchufe de

pared, el cable a través el edificio desde el enchufe de pared hasta el punto de conexión cruzada, o patch panel, y el cable desde el patch panel hasta el switch.

Si el switch se ubica en los cuartos de telecomunicaciones en diferentes pisos de un edificio o en diferentes edificios, el cable entre estos puntos debe incluirse en la longitud total.

Para las instalaciones UTP, el estándar ANSI/TIA/EIA-568-B especifica que la longitud combinado total del cable que abarca las cuatro áreas enumeradas anteriormente se limita a una distancia máxima de 100 metros por canal. Este estándar establece que se pueden utilizar hasta 5 metros de patch cable para interconectar los patch pannels.

II.1.6.4.- Cableado Horizontal

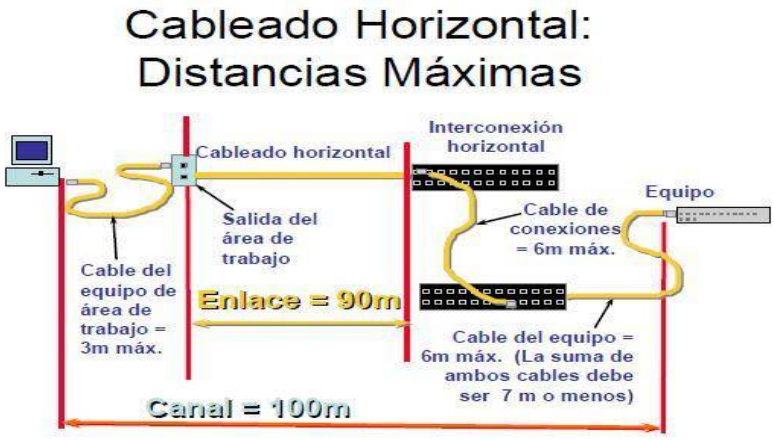


Figura 13. Cableado horizontal

La norma del EIA/TIA568A define el cableado horizontal de la siguiente forma: El sistema de cableado horizontal es la porción del sistema de cableado de telecomunicaciones que se extiende del área de trabajo al centro de datos o viceversa. El cableado horizontal consiste de cuatro elementos básicos: rutas y espacios verticales (también llamado "sistemas de pasada de datos horizontal"). Las rutas y espacios horizontales son utilizados para distribuir y soportar cable

horizontal y conectar hardware entre la salida del área de trabajo y el centro de datoss. Estas rutas y espacios son los "contenedores" del cableado horizontal.

El cableado horizontal incluye:

Las salidas (cajas/placas/conectores) de telecomunicaciones en el área de estudio.

Cables y conectores de transición instalados entre las salidas del área de estudio y el centro de datos.

Paneles (patch panel) y cables de empalme utilizados para configurar las conexiones de cableado horizontal en el centro de datos.

El cableado horizontal distribuye y da alcance a los dispositivos de la red para la interconexión y transmisión y recepción de la información a los equipos finales computadores, impresoras, entre otros.

II.1.6.5.-Cableado Vertical o Backbone

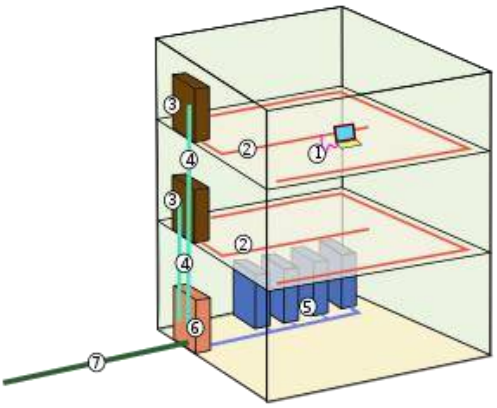


Figura 14. Cableado vertical

El sistema de cableado vertical proporciona interconexiones entre cuartos de entrada a servicios de edificio, cuartos de equipo y cuartos de telecomunicaciones. El cableado del backbone incluye la conexión vertical entre pisos en edificios de varios pisos. El cableado del backbone incluye medios

de transmisión (cables), puntos principales e intermedios de conexión cruzada y terminaciones mecánicas. El cableado vertical realiza la interconexión entre los diferentes gabinetes de telecomunicaciones y entre estos y la sala de equipamiento. En este componente del sistema de cableado ya no resulta económico mantener la estructura general utilizada en el cableado horizontal, sino que es conveniente realizar instalaciones independientes para la telefonía y datos

II.1.6.6.-Cuarto de Entrada de Servicios

En cables, accesorios de conexión, dispositivos de protección, y demás equipos es necesario para conectar el edificio a servicios externos. Puede contener el punto de demarcación. Ofrecen protección eléctrica establecida por códigos eléctricos aplicables. Deben ser diseñadas de acuerdo a la norma EIA/TIA-569-A. Los requerimientos de instalación son:

- Precauciones en el manejo del cable UTP
- Evitar tensiones en el cable
- Los cables no deben en distribuirse en grupos muy apretados
- Utilizar rutas de cable y accesorios apropiados 100 ohmios UTP y STP

II.1.6.7.-Centro de datos

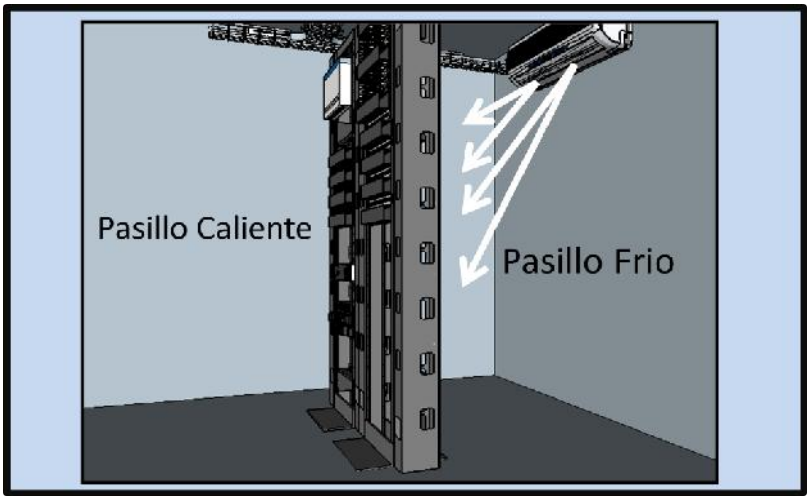


Figura 15. Centro de datos

El centro de datos es el espacio utilizado exclusivamente para alojar los elementos de terminación del cableado estructurado y los equipos de telecomunicaciones. El diseño de cuartos de telecomunicaciones debe considerar, además de voz y datos, la incorporación de otros sistemas de información del edificio tales como televisión por cable (CATV), alarmas, seguridad, audio y otros sistemas críticos. Todo edificio debe contar con al menos un centro de datos o cuarto de equipo. No hay un límite máximo en la cantidad de cuartos de telecomunicaciones que pueda haber en un edificio.

Cuando son redes de datos de gran tamaño por lo general se requieren de varios

cuartos de telecomunicaciones, cuando se presenta este fenómeno uno de los armarios

de distribución de cableado se escoge como MDF (Armario de Distribución

Principal) y los demás se rotulan con el título de IDF's (Armarios de Distribución

Intermedios).

II.1.6.8.-Gabinete de Telecomunicaciones

Los gabinetes protegen sus equipos de posibles daños, polvo y acceso de personal sin autorización garantizando la seguridad y administración de la red. 25 Ofrecen fácil acceso para el mantenimiento o instalación de equipos.

Rack: Es uno de los elementos imprescindibles de toda infraestructura de comunicaciones. Está diseñado para alojar, físicamente, todos los elementos necesarios para un sistema de cableado o comunicaciones. Consiste en una estructura metálica sencilla, pero resistente, que nos permite organizar todos los sistemas de telecomunicaciones. En estos armarios rack podremos alojar servidores, Switches, ordenadores, sistemas de redes o telefonía.

Gabinete: Para Instalación en la Pared está diseñado para alojar equipos de rack de 19" compatibles con la norma EIA en gabinetes de cableado de redes, tiendas minoristas, salones de clases, áreas administrativas y otras áreas con espacio limitado donde el equipo debe estar seguro, organizado y fuera del paso. Fabricado en acero para uso pesado con un duradero acabado en color negro de pintura en polvo, el gabinete tiene una capacidad máxima de carga de 91 kg [200 lb]. Los paneles laterales y la puerta frontal tienen cerradura para evitar daños, manipulación indebida o robos Los paneles del frente, arriba, abajo y laterales removibles tienen ventilación, lo que permite que fluya aire libremente para mantener al equipo fresco.

II.1.6.9.-Canalización del Cableado

El sistema de canalización interna del cableado estructurado está compuesto por las rutas y espacios horizontales que se utilizan para distribuir y soportar el cableado horizontal y conectar el equipo entre la salida del área de trabajo y el centro de datos. Estas rutas y espacios son críticas para el buen desempeño del sistema de cableado estructurado.

II.1.6.10.-Puesta a Tierra

El sistema de puesta a tierra para cableado estructurado está diseñado para la seguridad de la vida de los usuarios y asegurar una misma referencia eléctrica para todos los sistemas electrónicos contenidos en los diferentes espacios de un edificio o un data center. Este sistema está normado por el estándar ANSI/J/STD-607-A

II.1.7.- Dispositivos de red

II.1.7.1.- Switch (Conmutador)

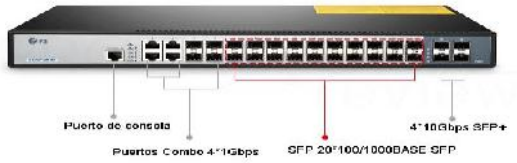


Figura 16. Dispositivo de red

Es un dispositivo electrónico de interconexión de redes de ordenadores que opera en

la capa 2 (nivel de enlace de datos) del modelo OSI (Open Systems Interconnection).

Un Switch (conmutador) interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas en la red.

Los Switches o conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las LANs (Local Area Network- Red de Área Local).

Los switches Ethernet están llegando a ser soluciones para conectividad de uso difundido porque, al igual que los puentes, los switches mejoran el rendimiento de la red al mejorar la velocidad y el ancho de banda.

Las siguientes son las dos operaciones básicas que realizan los switches:

Conmutación de tramas de datos: Los switches reciben tramas en una interfaz, seleccionan el puerto correcto por el cual enviar las tramas, y entonces envían la trama de acuerdo a la selección de ruta.

Mantenimiento de operaciones de switch: Los switches elaboran y mantienen las tablas de envío. Los switches también elaboran y mantienen una topología sin bucles en toda la LAN.

Existen ahora switches de capa 3 los cuales son dispositivos de alta capacidad y ejecución para el ruteo de las redes. Los switches de capa 3 no se diferencian mucho de los routeadores. Un Switch de capa 3 puede dar soporte a los mismos protocolos de ruteo que los routers de red. Ambos inspeccionan paquetes entrantes y hacen decisiones dinámicas de ruteo basados en las direcciones de fuente y destino que estos paquetes incluyen.

Los switches de capa 3 fueron concebidos como una tecnología para mejorar el rendimiento de los routers usados en LANs como Intranets corporativas. La diferencia fundamental entre los switches de capa 3 y los routers es la tecnología usada para construir la unidad. El hardware dentro de un Switch de capa 3 reúne las capacidades de un Switch y un router, reemplazando parte de la lógica del software de router con hardware para decisiones más rápidas y mejor ejecución en ciertos casos. En todo caso switches de capa 3 cuestan menos que los routers tradicionales y están diseñados para uso de redes locales LAN o metropolitanas MANs

Switches en la Capa de Distribución

Los switches de la capa de distribución son los puntos de totalización de múltiples switches de la capa de acceso. El switch debe poder adecuarse al monto total del tráfico desde los dispositivos de la capa de acceso.

El switch de la capa de distribución debe tener un alto rendimiento, dado que es un punto en el cual se encuentra delimitado el dominio de broadcast. La capa de distribución combina el tráfico VLAN y es un punto focal para las decisiones de política sobre flujo de tráfico. Por estas razones, los

switches que residen en la capa de distribución operan tanto en la Capa 2 como en la Capa 3 del modelo OSI. Los switches en esta capa se conocen como switches multicapa. Estos switches multicapa combinan las funciones de un router y de un switch en un dispositivo. Están diseñados para conmutar el tráfico a fin de obtener un rendimiento mayor que el de un router estándar.

II.1.7.2.- Routers

Figura 17. Router

Los Routers o enrutadores, son equipos utilizados para la interconexión de redes de computadores (LAN) permiten asegurar el enrutamiento de paquetes entre diferentes redes o determinar la ruta que debe tomar un determinado paquete de datos en función de la dirección 19 destino. Opera en capa de red del modelo OSI o internet en Modelo TCP/IP. Existen variedad de modelos fabricantes y tipos de conexión e incluso aplicaciones específicas que permiten un tratamiento específico sobre los paquetes a direccionar. Se pueden segmentar en dos grandes grupos los utilizados en empresas donde se requiere un tratamiento y manejo de volúmenes altos de información como CPD, ISP. Tienen variedad de interfaces para conexiones (RJ45, Serial, Fibra) siendo capases de pertenecer a varias redes incluso de diferentes tipos (Ethernet, ATM, X25, etc.) así comunicarlas entre sus interfaces y reglas de enrutamiento. La función principal de estos es hacer NAT, es decir, que el equipo de una LAN con direccionamiento interno privado salga a internet usando una sola dirección IP pública proporcionada por el ISP.

II.1.7.3.-Wi-Fi

Wi-Fi es el nombre comercial mediante el cual conocemos a una de las tecnologías de comunicación inalámbrica que se utilizan en la actualidad. También se conoce como WLAN (Wireless LAN, red inalámbrica) o estándar IEEE 802.11. Este estándar si inició en 1997 en el IEEE, con la especificación técnica 802.11 regace (1ª generación) y su evolución en el proceso de estandarización ha estado unido siempre a la demanda por parte de los usuarios. Algunos de los estándares más destacados son los siguientes:

802.11g (tercera generación) (2003)

802.11n (cuarta generación) (2009)

802.11ac (quinta generación) (2013)

II.1.7.4.-Access Point

Los AP o WAP (Access point o Wireless Access point) También conocidos como puntos de acceso. Son dispositivos para establecer una conexión inalámbrica entre equipos y pueden formar una red inalámbrica externa (local o internet) con la que interconectar dispositivos móviles o tarjetas de red inalámbricas. Esta red inalámbrica se llama WLAN (Wireless local área network) y se usan para reducir las conexiones cableadas. Usos que tiene:

- Crear un acceso inalámbrico LAN de un lugar de trabajo.
- Dar acceso a una red inalámbrica a los clientes.
- Llevar una conexión a internet a donde no había antes, sin perder ancho de banda con repetidores.
- Cubrir grandes áreas con una conexión de calidad, reduciendo el uso de cableado.

- Permite interconexiones entre dispositivos convencionales y inalámbricos si se conecta el AP a un switch.

ventajas de un punto de acceso:

Permite la conexión de dispositivos inalámbricos a la WLAN como móviles u ordenadores portátiles.

Se basan en emisiones de ondas de radio, capaces de traspasar muros, por lo que son perfectos para conectar edificios cercanos dentro de la misma red, con antenas potentes es posible crear una red WLAN de hasta a un kilómetro de distancia. Tienen un radio de acción de entre 30 metros a 100 metros. Proporciona información del estado de red y descongestionan la red dividiendo las redes y enviando la información de manera paralela más rápidamente que de forma convencional.

Si dispone de conexiones PoE es posible con un único cable Ethernet RJ-45 dar acceso a internet sin la necesidad de conectarlo a un enchufe convencional y permite más usuarios conectados, al mismo tiempo.

II.1.7.5.-VoIP

El término VoIP significa Voz sobre Protocolo de Internet, y se trata de un método con el que puedes hacer llamadas de voz a través de la red. Para eso, se toman el audio de lo que estás diciendo por el micrófono y se convierte en datos digitales, que se transmiten por la red a otro dispositivo donde se interpretan para que se escuche de nuevo la voz.

Esto quiere decir que es una alternativa a las llamadas telefónicas convencionales. Con la VoIP no se depende de la señal de las antenas o del cable del teléfono, sino que se depende de la cobertura de Internet que tengas para poder transmitir las llamadas. Esto tiene una parte negativa, y es que si hay una mala cobertura la llamada también perderá calidad.

El término de VoIP realmente se refiere a los protocolos que facilitan estas llamadas, aunque popularmente usamos el nombre para referirnos a las llamadas en sí. Estas pueden realizarse a través de cualquier tipo de conexión, desde las redes LAN domésticas hasta las redes de datos móviles. Vamos, que puedes llamar tanto desde el ordenador como desde el móvil o una tableta, siempre y cuando tengas una app que lo permita.

En cuanto a las aplicaciones, como te hemos dicho, prácticamente todas las principales de mensajería ofrecen hoy en día esta opción, incluyendo WhatsApp, Telegram, Skype o Messenger. En las apps identificas estas llamadas porque tienen el mismo icono del teléfono de la aplicación de llamadas convencionales. Sin embargo, al realizarse a través de la app móvil son llamadas VoIP.

También sirve para el teléfono fijo

Esta tecnología de llamadas por Internet es muy común sobre todo en aplicaciones móviles, pero también puede utilizarse en los teléfonos fijos. Hay varias opciones disponibles para este fin, y en todas ellas se hace que la voz que envías desde el teléfono se digitalice y envíe por Internet.

II.1.8.- Realimentación y protección eléctrica

El plantel cuenta con energía eléctrica suministrada por el proveedor, que no tiene como backup ningún tipo de energía alternativa como plantas eléctricas, energía solar y demás, los que nos indica implementar una o varias UPS en línea por área de trabajo (aula), con el fin de que los equipos no se queden sin energía y poder salvaguardar la información de trabajo en el momento de un corte de energía, las UPS tienen una autonomía de alrededor de 15 minutos lo cual es perfecto para salvar la información mientras se restablece el servicio de energía.

II.1.9.- Firewall

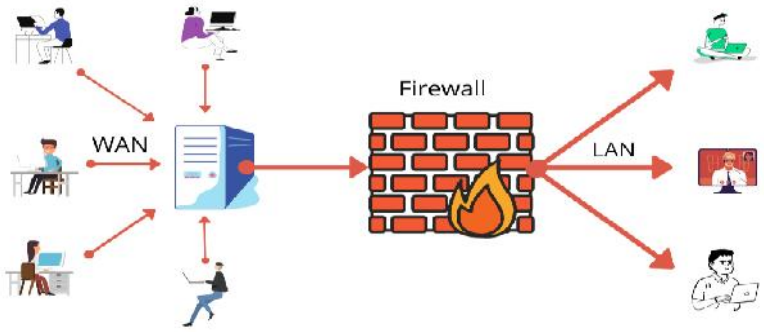


Figura 18. Firewall

Un firewall, también conocido como cortafuegos, es un elemento informático que trata de bloquear el acceso, a una red privada conectada a Internet, a usuarios no autorizados. Por tanto, el cortafuego se centra en examinar cada uno de los mensajes que entran y salen de la red para obstruir la llegada de aquellos que no cumplen con unos criterios de seguridad, al tiempo que da vía libre a las comunicaciones que sí están reglamentadas.

La función de un firewall es muy importante, ya que, de no ser por él, un ordenador –o red de ordenadores– podría ser atacado e infectado con bastante frecuencia. Además de los cortafuegos que, en la mayoría de casos, tenemos la ocasión de activar desde el sistema operativo del dispositivo, algunas compañías de antivirus también ofrecen protección firewall adicional para mejorar el sistema de defensa y frenar la entrada e instalación de un código malicioso.

La función de un firewall, como ya hemos comentado, no es otra que la de registrar el tráfico en internet de un dispositivo con el objeto de proteger una red informática privada impidiendo el acceso de usuarios no autorizados a ella, para que no se produzca el robo de información confidencial o se instale un virus en la computadora. Por consiguiente, un cortafuego sirve, en esencia, para preservar la seguridad y privacidad de los navegantes, proteger una red empresarial o doméstica de malévolos ataques y salvaguardar la información y los archivos en un buen estado.

Por lo que se refiere a su funcionamiento, el cortafuego está programado para diferenciar entre las conexiones permitidas y las sospechosas, aplicando diferentes procedimientos en función de cómo califique a la conexión.

Los diferentes procedimientos pueden ser:

Políticas de cortafuegos: suspendiendo las peticiones de comunicación que no provengan de la misma red o sistema, y disfrazando detrás de una IP los recursos internos.

Filtrado de contenido: identifica los contenidos que pueden dar problemas, teniendo el usuario la última palabra sobre si se bloquea o no el acceso.

Servicios antimalware: algunos cortafuegos pueden también detectar virus y evitar su expansión.

Servicios de DPI: los procedimientos de Inspección Profunda de Paquetes añaden una segunda capa de seguridad al sistema, revisando en profundidad los paquetes de información que se reciben.

II.1.10.- DHCP

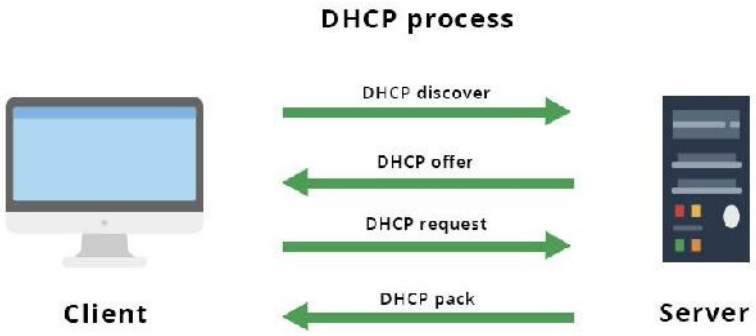


Figura 19. Protocolo DHCP

El protocolo DHCP (Protocolo de configuración dinámica de host) o también conocido como «Dynamic Host Configuration Protocol «, es un protocolo de red que utiliza una arquitectura cliente-servidor. Por tanto, tendremos uno o varios servidores DHCP y también uno o varios

clientes, que se deberán comunicar entre ellos correctamente para que el servidor DHCP brinde información a los diferentes clientes conectados. Este protocolo se encarga de asignar de manera dinámica y automática una dirección IP, ya sea una dirección IP privada desde el router hacia los equipos de la red local, o también una IP pública por parte de un operador que utilice este tipo de protocolo para el establecimiento de la conexión.

Cuando tenemos un servidor DHCP en funcionamiento, todas las direcciones IP que ha proporcionado a diferentes clientes se guardan en un listado donde se relaciona la IP que se le ha proporcionado (dirección lógica) y la dirección MAC (dirección física de la tarjeta de red). Gracias a este listado, el servidor DHCP se asegura de no proporcionar a dos equipos diferentes la misma dirección IP, lo que ocasiona un caos en la red local. A medida que el servidor va asignando direcciones IP, también tiene en cuenta cuándo pasa un determinado tiempo y caducan, quedando libres para que otro cliente pueda obtener esta misma dirección IP. El servidor DHCP sabrá en todo momento quién ha estado en posesión de una dirección IP, cuánto tiempo ha estado, y cuándo se ha asignado a otro cliente.

El protocolo DHCP incluye varias formas de asignación de direcciones IP, dependiendo de la configuración que realicemos y el escenario, podremos usar una forma de asignación u otra:

Manual o estática: el servidor DHCP nos permitirá configurar un listado de parejas IP-MAC con el objetivo de que siempre se le proporcione a un cliente una determinada dirección IP, y que esta dirección no cambie nunca.

Automática: el servidor DHCP se encarga de proporcionar una dirección IP al cliente que realiza la solicitud, y estará disponible para este cliente hasta que la libere. Existen routers que internamente están configurados para proporcionar direcciones IP privadas de forma secuencial,

sin embargo, hay firmwares que están diseñados para proporcionar una dirección IP específica dentro del rango y que no es secuencial, en base a un algoritmo interno y la dirección MAC que se haya conectado.

Dinámica: este método permite reutilización dinámica de las direcciones IP.

Aunque el protocolo DHCP es muy conocido por proporcionar la dirección IP, máscara de red y la puerta de enlace, tres parámetros básicos y fundamentales, también es capaz de proporcionar otra información de cara a los clientes, como los siguientes parámetros que son configurables y opcionales:

Servidor DNS primario y secundario.

Nombre DNS.

MTU para la interfaz.

Servidor y dominio NIS.

Servidores NTP.

Servidor de nombre WINS para Windows.

Otras opciones avanzadas.

Un aspecto muy importante es que, si un sistema Windows no es capaz de obtener una dirección IP a través del cliente DHCP en una red, se inicia un proceso llamado APIPA (Automatic Private Internet Protocol Addressing). Este proceso APIPA que usan los sistemas operativos cuando no se puede obtener una dirección IP por DHCP, este protocolo se encarga de asignar una dirección IP privada de clase B en el rango 169.254.0.0/16 con su correspondiente máscara de subred 255.255.0.0. Este bloque de direccionamiento se conoce como «link-local» para redes IPv4.

Aunque los sistemas operativos se autoconfigure esta dirección IP privada, cada 5 minutos volverán a consultar si hay un servidor DHCP en la red para que les proporcione una dirección IP privada de clase A, B o C habitual. Cuando no funciona el servidor DHCP o no lo tenemos configurado, podéis comprobar la dirección IP que se configura automáticamente si consultamos la IP privada que tenemos en nuestro equipo.

II.1.10.1.- Administrador de DHCP

El Administrador de DHCP es una herramienta de interfaz gráfica de usuario (GUI) que puede utilizar para llevar a cabo todas las tareas de administración asociadas al servicio DHCP. Puede utilizarlo para administrar el servidor y los datos que utiliza. Debe ser superusuario para ejecutar el Administrador de DHCP. Puede utilizar el Administrador de DHCP para:

Configurar y desconfigurar el servidor DHCP

Iniciar, detener y reiniciar el servidor DHCP

Desactivar y activar el servicio DHCP

Personalizar la configuración del servidor DHCP

El Administrador de DHCP permite administrar las direcciones IP, las macros de configuración de red y las opciones de configuración de red de los modos siguientes:

Agregar y eliminar redes en la administración de DHCP

Ver, agregar, modificar, eliminar y liberar direcciones IP en la administración de DHCP

Ver, agregar, modificar y eliminar macros de configuración de red

Ver, agregar, modificar y eliminar opciones de configuración de red que no sean estándar

El Administrador de DHCP permite administrar los almacenes de datos DHCP de los modos siguientes:

Convertir datos a un nuevo formato de almacén de datos

Mover los datos de DHCP de un servidor DHCP a otro exportándolos del primer servidor y luego importándolos en el segundo.

El Administrador de DHCP incluye una amplia ayuda en línea sobre los procedimientos que permite realizar la herramienta.

II.1.10.2.-Diferencias entre servidores Windows y Linux

Se realizó un nuevo diseño para la red primeramente se quiso realizar el uso de un servidor DHCP para configurar los equipos de computación con un sistema operativo Windows 10 pero después de observarlo mejor se tomó la decisión de realizar la configuración a través del sistema operativo Linux Debian.

Porque lo elegimos, veamos la tabla de diferencias entre Linux y windows:

	Windows	**Linux**
Costes	Costes de licencia por usuario	Sin costes de licencia
Uso estándar	Interfaz gráfica de usuario	Líneas de comandos
Acceso remoto	Servidor de terminales; el cliente tiene que instalarse y configurarse	Solución integrada (terminal y Shell)
Software y características	Soporta programas habituales; posibilidad de utilizar aplicaciones de Microsoft.	No ofrece portabilidad para todos los programas.
Seguridad	Elevado potencial de actualizaciones; interfaz integrada como posible punto de ataque	Los usuarios habituales no tienen acceso a los ajustes básicos del sistema.
Asistencia	Asistencia a largo plazo para todas las versiones	La asistencia varía en función de la distribución y de la versión
Documentación	El sistema y sus aplicaciones están muy bien documentadas, algo que difiere de los componentes de la API y de los formatos de los datos	Se conoce el código fuente completo del sistema, las API, las bibliotecas y las aplicaciones; la mayoría de manuales y de páginas informativas están en inglés

Figura 20. Diferencias entre Windows y Linux

II.1.10.3.-Ventajas de los servidores Linux

Las que tomamos en cuenta para nuestro uso de servidor DHCP es:

Estabilidad: Linux es capaz de manejar cantidades colosales tanto de datos como de procesos de una manera muy fluida y sin presentar ningún tipo de fallo. Aunque Windows en un principio ofrece la misma fluidez, con el paso del tiempo requiere de diversas acciones para volver a ser ágil, como la desfragmentación del disco duro.

Actualización: Linux puede lanzar una o dos actualizaciones anuales. En cambio, Windows es un sistema operativo muchísimo más abierto y cerrado pueden existir actualizaciones cada mes e incluso cada 2 semanas depende que problemas desea solucionar.

Seguridad: Windows al estar con Microsoft ofrece un entorno muy seguro, la compañía reacciona de una forma demasiado ágil ante cualquier tipo de agujero de seguridad con los 34 parches en las actualizaciones. En cambio, ante cualquier fallo relacionado con la seguridad del servidor, Linux actúa rápidamente. Además, hay que tener en cuenta que Linux es un sistema operativo de código abierto. Por lo tanto, cualquier usuario que tenga los conocimientos necesarios para solucionar ese fallo puede corregirlo y ponerlo a disposición del resto de usuarios de manera inmediata. **Libertad de uso:** Los servidores con Linux ofrecen una gran libertad de uso; los usuarios pueden utilizar y modificar todo aquello que deseen para satisfacer sus necesidades. En cambio, el servidor Windows es un entorno más cerrado, con algunas cláusulas que limitan la libertad de movimiento de los usuarios.

Por esta razón elegimos Linux ya que podremos configurar el uso del servidor para DHCP en cambio en windows debemos instalar otro software de manera externa para hacerlo funcionar como servidor.

II.1.11.- Pruebas de la red

II.1.11.1.- Probar la conectividad de la red

También es posible utilizar el comando ping para probar la capacidad de comunicación de un host en la red local. Por lo general, esto se realiza haciendo ping a la dirección IP del gateway del host.

II.1.11.2.- Prueba de Dispositivos

La prueba de red es un proceso que se utiliza para medir cuantitativa o cualitativamente el rendimiento de una infraestructura de TI. Es un nivel primitivo de identificación de fallas

II.1.11.3.- Pruebas funcionales

Las pruebas funcionales se llevan a cabo para comprobar las características críticas para el negocio, la funcionalidad y la usabilidad. Las pruebas funcionales garantizan que las características y funcionalidades del software se comportan según lo esperado sin ningún problema. Los tipos de pruebas funcionales incluyen pruebas unitarias, pruebas de interfaz, pruebas de regresión, además de muchas.

II.1.11.4.- Prueba de las comunicaciones

La prueba de las comunicaciones es normalmente más detallada y rigurosa que la verificación. Se requiere para asegurar que cada componente de un sistema esté operando como debe y que el sistema esté funcionando de acuerdo con los requerimientos locales específicos.

Un programa de prueba integral y bien estructurado es aquel que asegura que todos los componentes del sistema sean probados. Entre las medidas de prueba que se pueden considerar figuran las siguientes:

- Desarrollar un conjunto de criterios para la prueba.
- Aplicar pruebas funcionales para determinar si se han satisfecho los criterios de prueba.

- Aplicar evaluaciones de calidad para determinar si se han satisfecho los criterios de prueba.
- Conducir pruebas en condiciones de "laboratorio" y en una variedad de condiciones "reales".
- Conducir pruebas durante un periodo prolongado, para cerciorarse que los sistemas pueden funcionar de manera consistente.
- Conducir "pruebas de carga", simulando tanto como sea posible una variedad de condiciones reales utilizando o excediendo los volúmenes de información que se pueden esperar en una situación concreta.
- Verificar que lo que entra es lo que sale, introduciendo información conocida y verificando que el resultado sea consecuente con ella.

II.1.12.- Monitoreo de la red

Monitoreo de red describe el uso de un sistema que constantemente monitoriza una red de computadoras en busca de componentes defectuosos o lentos, para luego informar a los administradores de redes mediante correo electrónico, mensáfono u otras alarmas. Como herramientas para el monitoreo de la red tenemos:

II.1.12.1.- Solarwinds

Es una de las herramientas de monitoreo de redes más conocidas. Destaca por su mapeo de redes y nodos automático, sin necesidad de acciones manuales. Posee un interfaz gráfico bastante potente en el que se puede ver con facilidad la topología de red y el estado de la misma. Solarwinds permite integrar máquinas virtuales en su monitorización.

Es una muy buena opción para empresas medianas, aunque deben poder permitirse el precio de sus licencias (de las más caras del mercado).

II.1.12.2.- GlassWire

Esta aplicación facilita el monitoreo del uso de datos móviles, los límites de datos y la actividad de la red Wifi.

II.1.12.3.-Manage Engine / OPManager

ManageEngine pertenece a Zoho Group, el gigantesco conglomerado de empresas indio, y es una de las herramientas de monitoreo de redes

II.1.13.- Optimización de la red

La optimización de la red es una tecnología utilizada para mejorar el rendimiento de la red para un entorno determinado. Se considera un componente importante de la gestión eficaz de los sistemas de información. La optimización de la red desempeña un papel importante ya que la tecnología de la información está creciendo a tasas exponenciales con usuarios comerciales que producen grandes volúmenes de datos y, por lo tanto, consumen anchos de banda de red más grandes. Si no se cuenta con la optimización de red adecuada, el crecimiento continuo puede agregar tensión a la arquitectura de red del entorno u organización en cuestión

II.1.13.1.- Calidad de servicio

La **calidad de servicio (QoS)** es el uso de mecanismos o tecnologías que funcionan en una red para controlar el tráfico y garantizar el rendimiento de aplicaciones críticas con capacidad de red limitada. Permite a las organizaciones ajustar su tráfico de red general al priorizar aplicaciones específicas de alto rendimiento.

La QoS generalmente se aplica a redes que transportan tráfico para sistemas con uso intensivo de recursos. Los servicios comunes para los que se requiere incluyen televisión por protocolo de Internet (IPTV), juegos en línea, medios de transmisión, videoconferencias, video a pedido (VOD) y voz sobre IP (VoIP).

La tecnología de redes de QoS funciona al marcar paquetes para identificar tipos de servicios y luego configurar enrutadores para crear colas virtuales separadas para cada aplicación, según su prioridad. Como resultado, el ancho de banda se reserva para aplicaciones críticas o sitios web a los que se les ha asignado acceso prioritario.

Las tecnologías de QoS proporcionan la capacidad y la asignación de manejo a flujos específicos en el tráfico de redes. Esto permite al administrador de red asignar el orden en el que se manejan los paquetes y proporcionar la cantidad adecuada de ancho de banda a cada aplicación o flujo de tráfico.

II.1.14.- Protección contra incendios

La protección contra el fuego es vital, por los daños materiales y sobre todo por las pérdidas humanas que puede ocasionar, por lo que un sistema de prevención contra el fuego tiene que ser eficaz para que se pueda prevenir, detectar y extinguir el incendio en su fase inicial. Para cumplir con este fin un sistema contra incendios involucra varias áreas de diseño que deben considerarse: hidráulica, eléctrica, mecánica, etc. Las características se basan ciertas normativas reconocidas alrededor del mundo como por ejemplo la NFPA (Asociación Nacional de Protección contra el Fuego) cuyos códigos y normas son ampliamente adoptados debido a que son generados a través de un proceso abierto y consensuado.

II.1.14.1-Sistemas de detección y alarma de incendios

Existe actualmente una oferta amplia de sistemas de detección y alarma contra incendios, con diversos fabricantes y sistemas muy completos. Dependiendo del tipo de sistema que se requiera instalar los precios también cubren un amplio margen, desde cientos a miles de dólares. Se encuentra también fabricantes especializados en dispositivos específicos como sensores de gas, sensores de humo, parlantes, sirenas, etc. Que pueden ser acoplados a un sistema general.

II.1.14.2.-Tipos de Sistemas

Convencionales: Son aquellos que están compuestos por dispositivos iniciadores y anunciadores que cumplen con las características requeridas sin que necesariamente cuenten con un panel de control que especifique el lugar o zona donde se genere la alarma o el tipo de alarma.

Inteligentes: Son aquellos sistemas que permiten identificar en un panel central el lugar donde se origina la alarma del incendio, dan la alarma respectiva a los dispositivos anunciadores correspondientes y usan dispositivos programables para activar bombas o ventiladores.

Ubicación de los detectores: El montaje de sensores puntuales está basado en ubicar o localizar los detectores en el centro de un rectángulo 9x9 metros. La distancia del centro del detector a cualquier extremo no deberá de exceder 6.4 metros

II.1.14.3.- Extintores

Los extintores son elementos portátiles destinados a la lucha contra fuegos incipientes. Sirven para dominar o extinguir cualquier tipo de fuego generado para evitar así su transformación en incendios mayores. Existe un tipo de extintor recomendado para cada tipo de incendio y hoy desde Soler Prevención desglosaremos los tipos de extintores existentes y las recomendaciones específicas para sus usos.

Tipos de fuegos extintores

Para poder entender mejor la funcionalidad de cada tipo de extintor, es necesario saber primero qué tipos de fuegos existen:

• Clase A: fuegos con combustibles sólidos como madera, cartón, plástico, etc.

• Clase B: fuegos donde el combustible es líquido como por ejemplo el aceite, la gasolina o la pintura.

• Clase C: en este caso el combustible son gases como el butano, propano o gas ciudad.

• Clase D: en este tipo de fuegos el combustible es un metal: el magnesio, el sodio o el aluminio

II.1.15.- Tecnologías utilizadas

II.1.15.1.- Packet tracer

Figura 21. Software pack tracer

¿Qué es Cisco Packet Tracer?

Cisco Packet Tracer es una herramienta de simulación multiplataforma, diseñada por Cisco Systems, que te va a permitir crear distintas simulaciones del funcionamiento o instalación de redes de telecomunicaciones e informáticas de Cisco.

Este software permite a los usuarios simular distintos tipos de configuraciones para routers o conmutadores de Cisco mediante una interfaz de comandos simulada. En su interfaz, Cisco Packet Tracer emplea un sistema intuitivo y sencillo de usar que consiste en arrastrar y soltar, lo que permite que podamos añadir y quitar dispositivos de red como mejor nos parezca.

Packet Tracer permite a los estudiantes diseñar redes grandes y complejas, lo que a menudo no es factible con hardware físico debido a los costes derivados de él.

Algunas de sus funciones son las siguientes:

- Diseñar y construir una red desde el principio.
- Trabajar sobre proyectos ya elaborados, a partir de distintos ejemplos ya incluidos.
- Probar nuevos diseños y topologías de redes cisco.
- Probar cambios en la red antes de ponernos a aplicarlos.
- Examinar el flujo de datos a través de una red.
- Hacer simulaciones con Internet of Things (IoT)

II.1.15.2.- GNS3

Figura 22. Software GNS3

GNS3 (Graphical Network Simulator-3) es un simulador de redes de computadoras que permite a los usuarios diseñar, construir y simular redes complejas. Es una herramienta de software libre que se utiliza para simular redes de computadoras en un ambiente de laboratorio virtual.

GNS3 se basa en el software Dynamips, que simula los dispositivos Cisco IOS en un ambiente de software, permitiendo a los usuarios crear y simular topologías de redes complejas. Con GNS3, los usuarios pueden simular dispositivos de red, como routers, switches y servidores, así como configurar protocolos de red y probar escenarios de fallos.

GNS3 permite emular una amplia variedad de redes, como redes de computadoras, redes de comunicaciones, redes de servicios, entre otras. Algunos ejemplos de las redes que pueden ser emuladas en GNS3 incluyen:

Redes Cisco: GNS3 es especialmente popular entre los profesionales de Cisco debido a su capacidad para emular dispositivos Cisco, como routers y switches.

Redes de computadoras: GNS3 permite emular una variedad de protocolos de red, como TCP/IP, OSPF, EIGRP, entre otros.

Redes de servicios: GNS3 puede emular servicios de red, como firewalls, servicios de VPN, servicios de seguridad, entre otros.

Redes de comunicaciones: GNS3 permite emular dispositivos de comunicaciones, como gateways y PBX.

II.1.15.3.- VMWare

Figura 23. Software VMWare

VMWare es una empresa de software que se especializa en virtualización y computación en la nube. La virtualización consiste en la creación de una representación de algo a través de un software, como un servidor, para que se pueda acceder a él y utilizar independientemente de las restricciones de su hardware físico.

II.1.15.4.- Netspot

Figura 24. Netspot

NetSpot es un programa para sistemas operativos Microsoft Windows y macOS, que nos va a permitir analizar todas las redes Wi-Fi que hay a nuestro alrededor, mostrándonos una gran cantidad de información sobre ellas. Por ejemplo, podremos ver la señal que recibimos, los canales utilizados por las diferentes redes inalámbricas, si hay interferencias, ruido, y mucha más información con el objetivo de optimizar la red Wi-Fi para tener la mejor señal Wi-Fi posible.

Principales Características de NetSpot

NetSpot tiene un «modo descubrir «, cuyo objetivo es visualizar todos los detalles de las redes Wi-Fi de nuestro alrededor, presentándonos los datos como una tabla interactiva. Todos los datos que recibimos son en tiempo real, si redes Wi-Fi nuevas aparecen, en el programa también se verán reflejados estos cambios. Vamos a poder ver la configuración individual de cada uno de los AP, gráficos en tiempo real, e incluso es compatible con la banda de 2.4GHz y 5GHz de manera simultánea (es obligatorio tener una tarjeta Wi-Fi doble banda, de lo contrario no veremos 5GHz). También vamos a poder comparar fácilmente los diferentes AP en cuanto a señal recibida, e incluso exportar la información a formato CSV para su posterior análisis.

Este programa también tiene un modo «análisis Wi-Fi«, donde tendremos la posibilidad de subir un plano de planta y ubicar físicamente los diferentes puntos de acceso, para comprobar si vamos

a tener cobertura inalámbrica por todo nuestro hogar. En los mapas de calor, vamos a poder crear múltiples zonas en un único proyecto, además, vamos a poder ver información detallada de todas las redes Wi-Fi disponibles, crear instantáneas para compararlas posteriormente con otras configuraciones, recomendaciones adhoc para mejorar la red configurada, y también podremos exportar los datos a PDF o CSV.

Algunas características muy interesantes de esta herramienta, es que tiene compatibilidad con el nuevo Wi-Fi 6, o también conocido como 802.11ax, por lo que si cuentas con un router o punto de acceso con esta tecnología, y una tarjeta de red inalámbrica Wi-Fi con Wi-Fi 6, podrás realizar un análisis en profundidad y aprovechar todas las nuevas características. También han incorporado soporta para el protocolo de cifrado WPA3, un nuevo protocolo fundamental para asegurar la confidencialidad de nuestras comunicaciones.

Se han incorporado en la interfaz gráfica de usuario nuevos idiomas, entre los que se incluye el español, por tanto, no tendremos que usarlo en inglés nunca más, también se permite la exportación activa de todos los datos del escaneo en formato CSV, y, además, podremos ver el fabricante de los routers y APs con la nueva lista actualizada de direcciones MAC.

Por último, NetSpot ha mejorado y optimizado la creación de mapas de calor para ver dónde se encuentran las zonas de mayor y menor cobertura, gracias a estas características, podremos saber con mucho más detalle la cobertura que recibimos.

II.1.15.5.- Glaswire

Figura 25. Software Glaswire

GlassWire es una plataforma de seguridad y supervisión de redes que proporciona a las empresas diversas herramientas, como supervisión de redes en tiempo real, firewall integrado, funciones de seguridad de Internet, alertas, supervisión de la utilización del ancho de banda, supervisión de servidores y más. También ofrece una aplicación para Android que permite a los usuarios supervisar las redes sobre la marcha con cualquier dispositivo Android con Internet.

Con las herramientas de supervisión de red visual dentro de GlassWire, las empresas pueden ver la actividad pasada y presente de la red y obtener información detallada sobre qué aplicaciones utilizan más ancho de banda. Todos los datos se presentan en gráficos e informes visuales y fáciles de interpretar para ayudar a los usuarios a comprender mejor cómo se utiliza la red. Se puede realizar un seguimiento de la utilización de la red por una hora, día, semana o mes específicos mediante la vista de línea de tiempo.

Las empresas pueden usar GlassWire para realizar un seguimiento de qué aplicaciones se están comunicando con la red, cuánto ancho de banda se está utilizando, qué aplicaciones están compartiendo datos, quién está utilizando una red o conexión WiFi específica y más. Se pueden activar alertas para notificar a los usuarios cuando se producen cambios en la red o cuando se detectan amenazas

II.1.15.6.- Fortigate

Figura 26. Firewall Fortigate

Los Firewall Fortinet (también conocidos como firewalls de próxima generación NGFW o simplemente FortiGate) son dispositivos de seguridad que permiten la creación de redes seguras y proporcionan una protección amplia, integrada y automatizada contra amenazas emergentes y sofisticadas.

Características de un FortiGate

Cabe destacar que los FortiGate son bien conocidos tanto por su rendimiento como por su eficacia de seguridad, para tener más claro esto, veamos las siguientes características avanzadas con las que cuentan:

Control de aplicaciones: Permite crear políticas rápidamente para permitir, denegar o restringir el acceso a aplicaciones o categorías completas de aplicaciones.

Prevención de intrusiones: Protege contra intrusiones en la red mediante la detección y el bloqueo de amenazas antes de que lleguen a los dispositivos de red.

Antivirus: Efectivo contra virus, software espía y otras amenazas a nivel de contenido.

Filtrado de URL: Bloquea el acceso a sitios web maliciosos, pirateados o inapropiados.

Sandboxing: Es una solución avanzada de detección de amenazas para protegernos identificando malware previamente desconocido.

Inspección SSL: Obtén visibilidad del tráfico cifrado y previene el malware.

Por otro lado, también existen algunas características que siguen siendo constantes como, por ejemplo:

La mayoría de los productos Fortinet están impulsados por los servicios de seguridad FortiGuard, garantizando que los clientes tengan la visibilidad y protección más recientes.

Solo hay un sistema operativo en todas las plataformas Fortigate: nivel de entrada, gama media y alta.

Todos los dispositivos se pueden monitorear y administrar con facilidad usando FortiManager un único panel de administración.

CAPITULO III

COMPONENTES

III.- Capitulo III: Componentes

III.1.- Componente I: Elaborar un diseño de red para el "Servicio Departamental de Salud SEDES-Tarija" y el área de trabajo PAI

III.1.2.- Metodología para diseño de red top Down

La metodología que se utilizara para el diseño de red de la institución "Servicio departamental de salud SEDES y su programa ampliado de inmunización PAI" es la metodología Top-Down.

Esta metodología también se utiliza para en otras disciplinas como desarrollo de software, gestión de proyectos. Para aplicarlo a redes se tiene que analizar los requerimientos que se utiliza para realizar los protocolos y la topología que se utilizará. La metodología Top-Down consta de 6 fases las cuales son:

Fase 1: Analizar Requerimientos

Fase 2: Desarrollar Diseño Lógico

Fase 3: Desarrollar Diseño Físico

Fase 4: Probar, optimizar y documentar diseño

Fase 5: Implementar y probar la red

Fase 6: Monitorear y Optimizar la Red

De las 6 fases mencionadas se planea realizar todas las fases que son 6 la última es fase de monitorear y optimizar la red.

III.1.2.1.- Fase 1: Análisis de requerimientos

III.1.2.1.1- Análisis de metas del negocio

III.1.2.1.1.1.- Organigrama de la institución

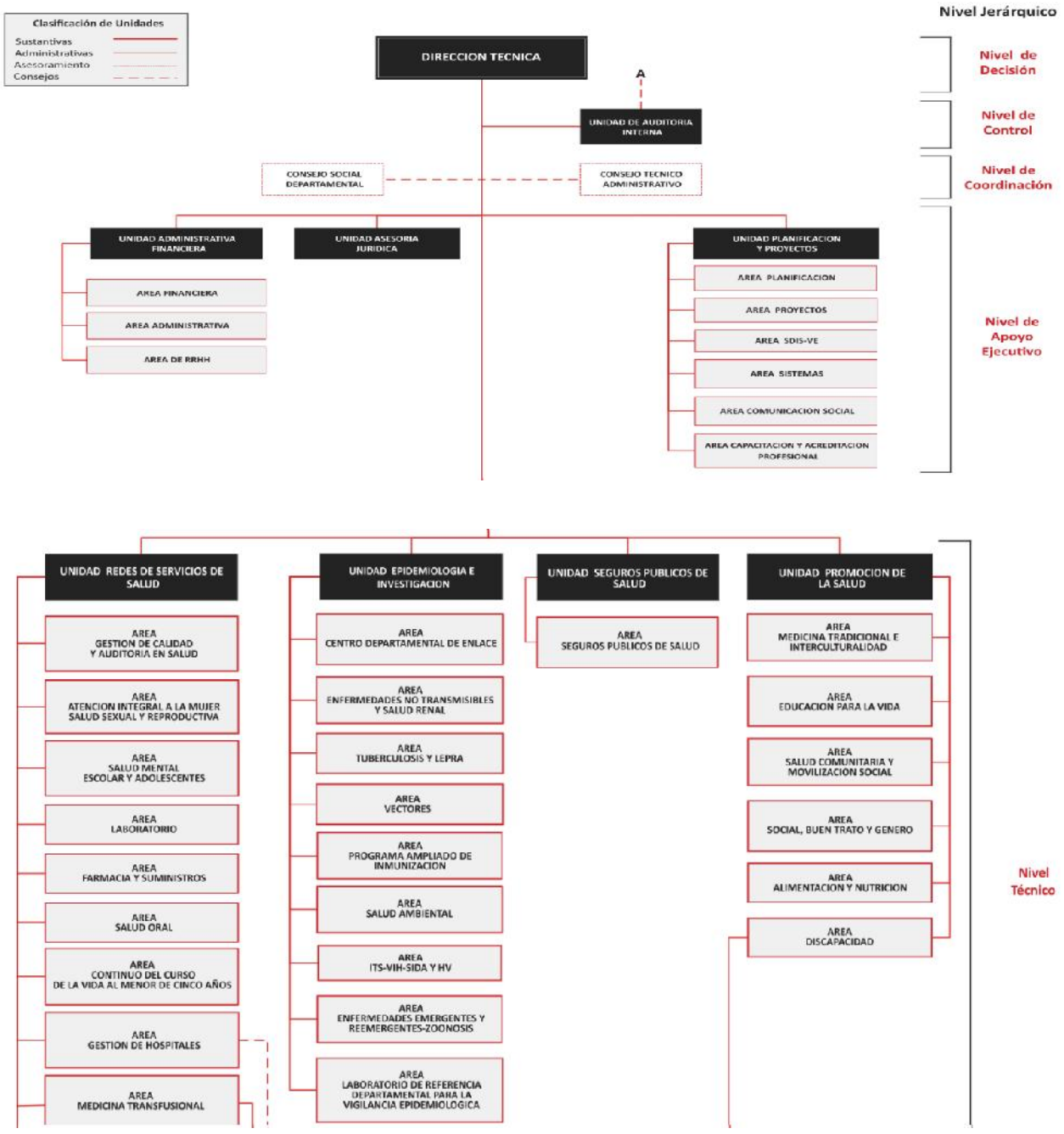


Figura 27. Organigrama de SEDES

III.1.2.1.1.2.-Organización del PAI a nivel nacional

Figura 28. Organigrama del PAI a nivel nacional

III.1.2.1.1.3.-Organización del PAI a nivel departamental

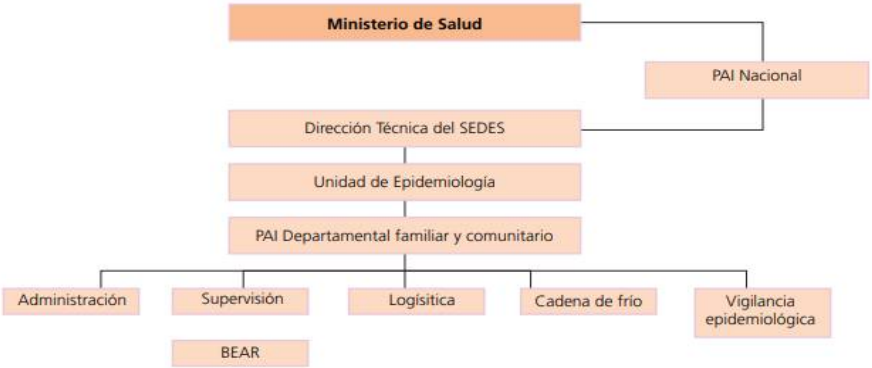


Figura 29. Organización del PAI a nivel departamental

III.1.2.1.1.4.- Estructura organizacional del PAI

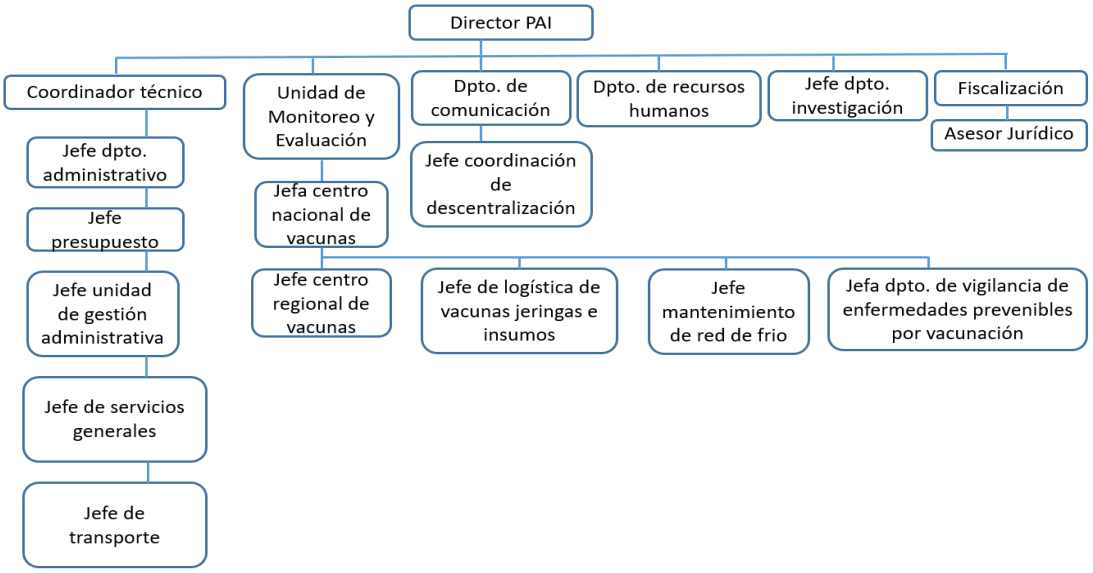


Figura 30. Estructura organizacional del PAI

III.1.2.1.2.- Análisis de metas técnicas

La organización SEDES y su programa PAI buscan renovar su red de comunicaciones actual esto con el objetivo de ofrecer un servicio óptimo a sus usuarios internos y por consecuente a la población, así como también buscan capacitar al personal en el uso correcto de los equipos y la red

III.1.2.1.3.- Analizar red existente

El servicio de salud SEDES cuenta con una red cuyo proveedor de servicios de internet es TIGO por cable UTP y por conexión inalámbrica al cual acceden mediante el centro de datos principal el cual cuenta con un rack y un servidor que actualmente no se está usando y 2 switch y este es el responsable de brindar a todos sus programas internet entre ellos el programa al cual nosotros diseñaremos nuestra nueva estructura para su red que es el PAI

En SEDES se cuenta con 30 usuarios aproximadamente y en el PAI con 26 usuarios y en la red actualmente se encuentra sin ningún tipo de cableado estructurado ni ninguna norma ni orden

El programa ampliado de inmunización (PAI) cuenta con una red cuyo proveedor de servicio de internet es TIGO por cable utp y conexión inalámbrica al cual acceden desde el centro de datos principal que está ubicado en el edificio de al lado que es SEDES

En cuanto a la administración de la red es básica la cual contiene solamente los dispositivos de manera rudimentaria y sin ningún tipo de orden no se cuenta con documentación de la red y la seguridad con la que se cuenta es una intranet o bloqueador de páginas para evitar que los usuarios entren a paginas no deseadas

El servicio departamental de salud SEDES cuenta con un total de 30 trabajadores en el área de administración y cuenta con un total de:

- 26 equipos de computación
- 10 impresoras
- 4 laptops

El programa ampliado de inmunización PAI cuenta con un total de 30 trabajadores junto al demás personal de los demás programas manejados por SEDES y el programa cuenta con un total de:

- 24 equipos de computación
- 7 impresoras
- 2 laptops

Conexión a internet por medio del proveedor de servicios de internet Tigo

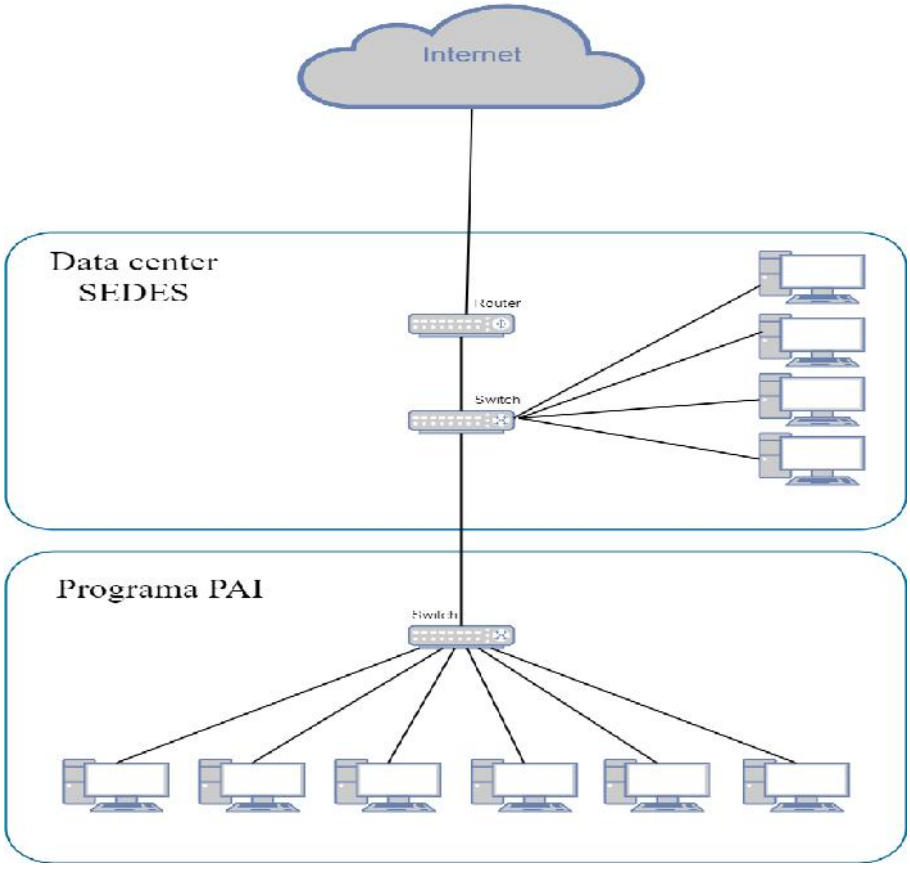


Figura 31 Conexión a internet

Distribución de energía y conectividad en el MDF

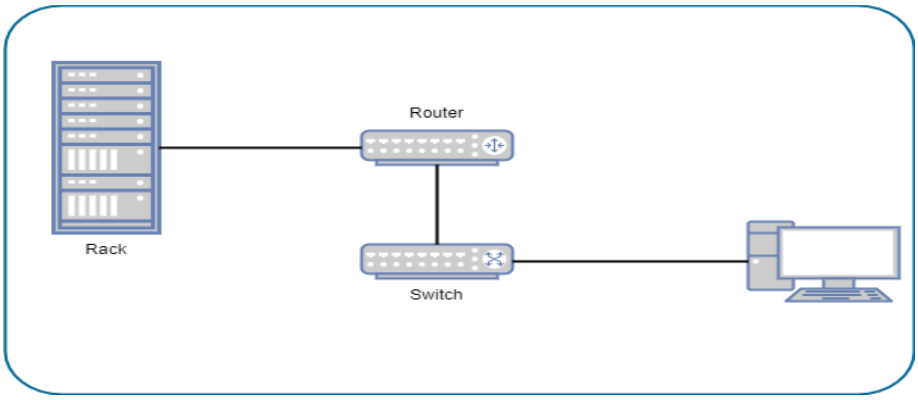


Figura 32.Distriucion de energía y conectividad en el MDF

MDF ubicado en el data center de SEDES

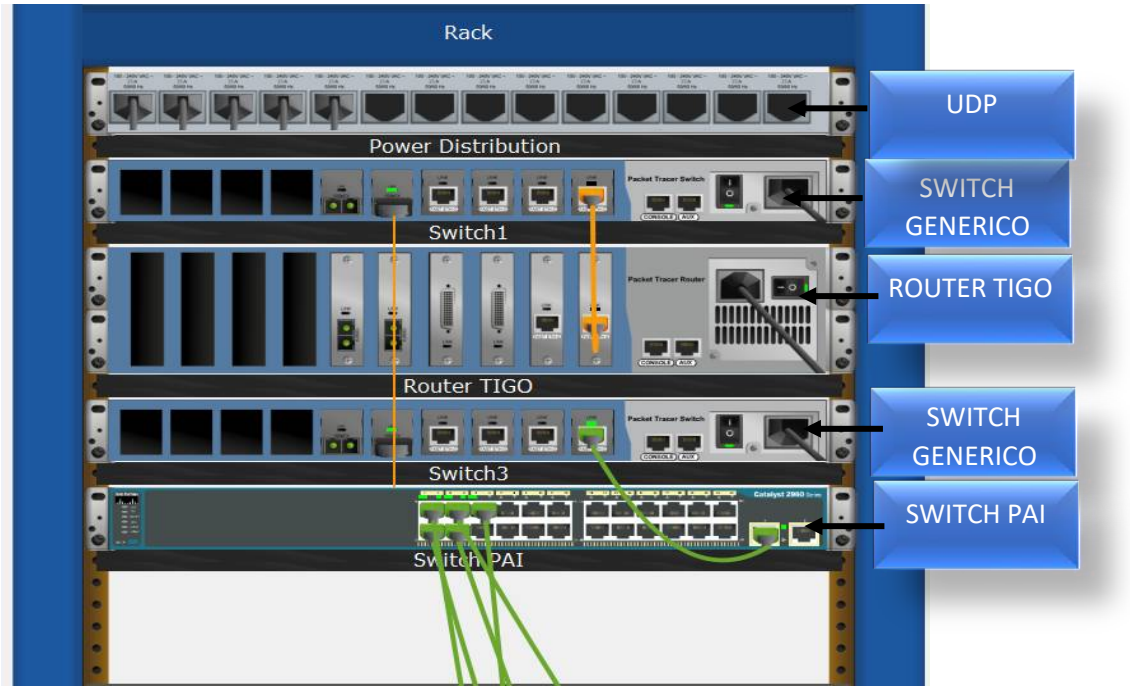


Figura 33. MDF ubicado en la data center

Topología actual de la red

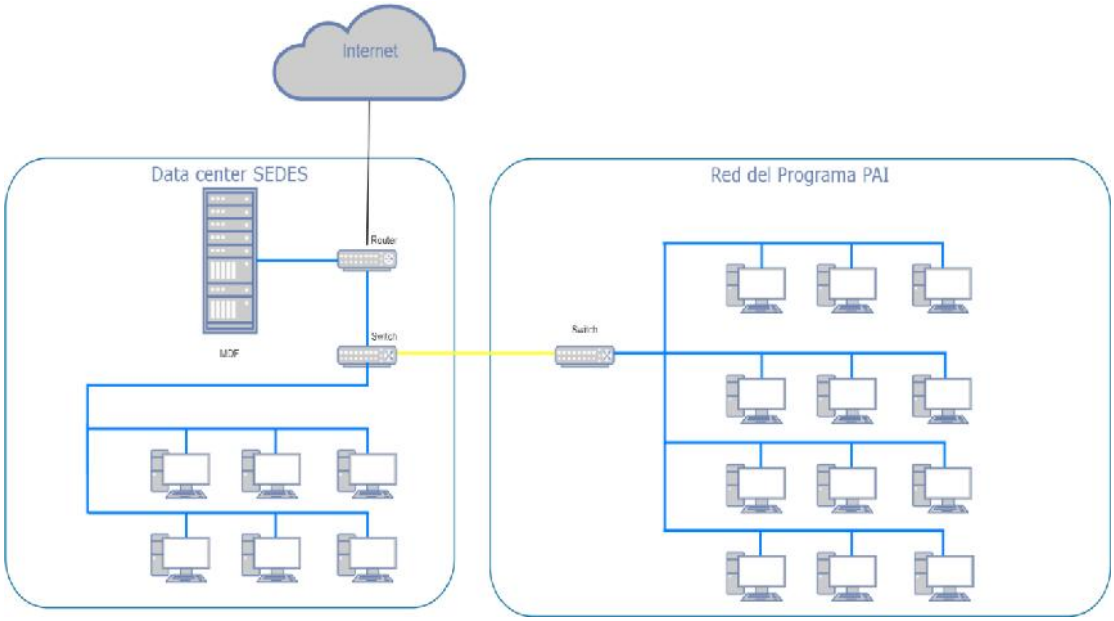


Figura 34. Topología actual de la red

Equipos y dispositivos de la red

Equipos	Marca	Cantidad
Computadoras	DELL	50
Impresoras	HP	17
Laptops	ASUS	6
Servidor	CISCO	1
Rack	S/M	1
Switches	CISCO	2
Cable utp cat5	S/M	200mts

Tabla 5. Equipos y dispositivos de la red

III.1.2.1.3.1.- Direccionamiento actual de los equipos

La red tiene asignada el segmento de red clase A con la red 10.160.1.0 y están asignadas de manera estática

III.1.2.1.3.1.1.- Direccionamiento IP maquinas PC

Nro.	Equipo	Dirección IP	Mascara de red	Puerta de enlace
1	PC1	10.160.1.10	255.0.0.0	10.160.1.1
2	PC2	10.160.1.11	255.0.0.0	10.160.1.1
3	PC3	10.160.1.12	255.0.0.0	10.160.1.1
4	PC4	10.160.1.13	255.0.0.0	10.160.1.1
5	PC5	10.160.1.14	255.0.0.0	10.160.1.1
6	PC6	10.160.1.15	255.0.0.0	10.160.1.1
7	PC7	10.160.1.16	255.0.0.0	10.160.1.1
8	PC8	10.160.1.17	255.0.0.0	10.160.1.1
9	PC9	10.160.1.18	255.0.0.0	10.160.1.1
10	PC10	10.160.1.19	255.0.0.0	10.160.1.1

11	PC11	10.160.1.20	255.0.0.0	10.160.1.1
12	PC12	10.160.1.21	255.0.0.0	10.160.1.1
13	PC13	10.160.1.22	255.0.0.0	10.160.1.1
14	PC14	10.160.1.23	255.0.0.0	10.160.1.1
15	PC15	10.160.1.24	255.0.0.0	10.160.1.1
16	PC16	10.160.1.25	255.0.0.0	10.160.1.1
17	PC17	10.160.1.26	255.0.0.0	10.160.1.1
18	PC18	10.160.1.27	255.0.0.0	10.160.1.1
19	PC19	10.160.1.28	255.0.0.0	10.160.1.1
20	PC20	10.160.1.29	255.0.0.0	10.160.1.1
21	PC21	10.160.1.30	255.0.0.0	10.160.1.1
22	PC22	10.160.1.31	255.0.0.0	10.160.1.1
23	PC23	10.160.1.32	255.0.0.0	10.160.1.1
24	PC24	10.160.1.33	255.0.0.0	10.160.1.1
25	PC25	10.160.1.34	255.0.0.0	10.160.1.1
26	PC26	10.160.1.35	255.0.0.0	10.160.1.1
27	PC27	10.160.1.36	255.0.0.0	10.160.1.1
28	PC28	10.160.1.37	255.0.0.0	10.160.1.1
29	PC29	10.160.1.38	255.0.0.0	10.160.1.1
30	PC30	10.160.1.39	255.0.0.0	10.160.1.1
31	PC31	10.160.1.40	255.0.0.0	10.160.1.1
32	PC32	10.160.1.41	255.0.0.0	10.160.1.1
33	PC33	10.160.1.42	255.0.0.0	10.160.1.1
34	PC34	10.160.1.43	255.0.0.0	10.160.1.1
35	PC35	10.160.1.44	255.0.0.0	10.160.1.1
36	PC36	10.160.1.45	255.0.0.0	10.160.1.1
37	PC37	10.160.1.46	255.0.0.0	10.160.1.1
38	PC38	10.160.1.47	255.0.0.0	10.160.1.1
39	PC39	10.160.1.48	255.0.0.0	10.160.1.1

40	PC40	10.160.1.49	255.0.0.0	10.160.1.1
41	PC41	10.160.1.50	255.0.0.0	10.160.1.1
42	PC42	10.160.1.51	255.0.0.0	10.160.1.1
43	PC43	10.160.1.52	255.0.0.0	10.160.1.1
44	PC44	10.160.1.53	255.0.0.0	10.160.1.1
45	PC45	10.160.1.54	255.0.0.0	10.160.1.1
46	PC46	10.160.1.55	255.0.0.0	10.160.1.1
47	PC47	10.160.1.56	255.0.0.0	10.160.1.1
48	PC48	10.160.1.57	255.0.0.0	10.160.1.1
49	PC49	10.160.1.58	255.0.0.0	10.160.1.1
50	PC50	10.160.1.59	255.0.0.0	10.160.1.1

Tabla 6. Direccionamiento IP maquinas PC

III.1.2.1.4.- Análisis del tráfico existente

Se realizó un análisis del tráfico de datos de la red del SEDES y del PAI cuyo proveedor de internet es TIGO y se cuenta con un solo punto de acceso por cada institución y el plan de internet que poseen actualmente es de 35 Mbps y tiene una velocidad de descarga de 10,4 Mbps y una velocidad de subida de 9,11 Mbps

Figura 35. Análisis de la velocidad de internet en SEDES

El momento de más alto tráfico ocurre según la información obtenida por el técnico es entre las horas de la mañana entre las 10:00 y las 12:00 y en la tarde de 15:00 a 18:00 y como se puede observar hay un gran tráfico de datos dado que se utilizan muchas aplicaciones en línea que requieren un mayor ancho de banda

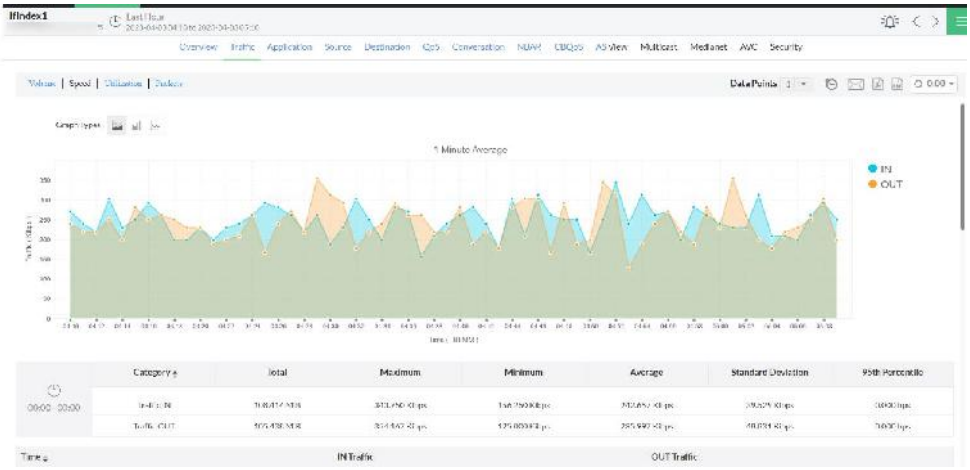


Figura 36. Nivel de tráfico de datos en horas pico

III.1.2.1.4.1.- Nivel de señal actual de SEDES

Figura 37. Nivel de señal actual del Access Point en SEDES

#	Nombre de la red	Canal	PHY	Nivel de señal máximo	Fabricante
1	ROG Rapture GT-AC2900, 2.4 GHz	1 (2.4 GHz)	ax	20 dBm	ASUS
2	ROG Rapture GT-AC2900, 5 GHz	36 (5 GHz)	ax	20 dBm	ASUS

Nivel de señal bajo de SEDES 2.4 GHz

Figura 38. Intensidad de señal baja

#	Nombre de la red	Canal	PHY	Nivel de señal máximo	Fabricante
1	ROG Rapture GT-AC2900, 2.4 GHz	1 (2.4 GHz)	ax	20 dBm	ASUS

Nivel de señal bajo 5 GHz

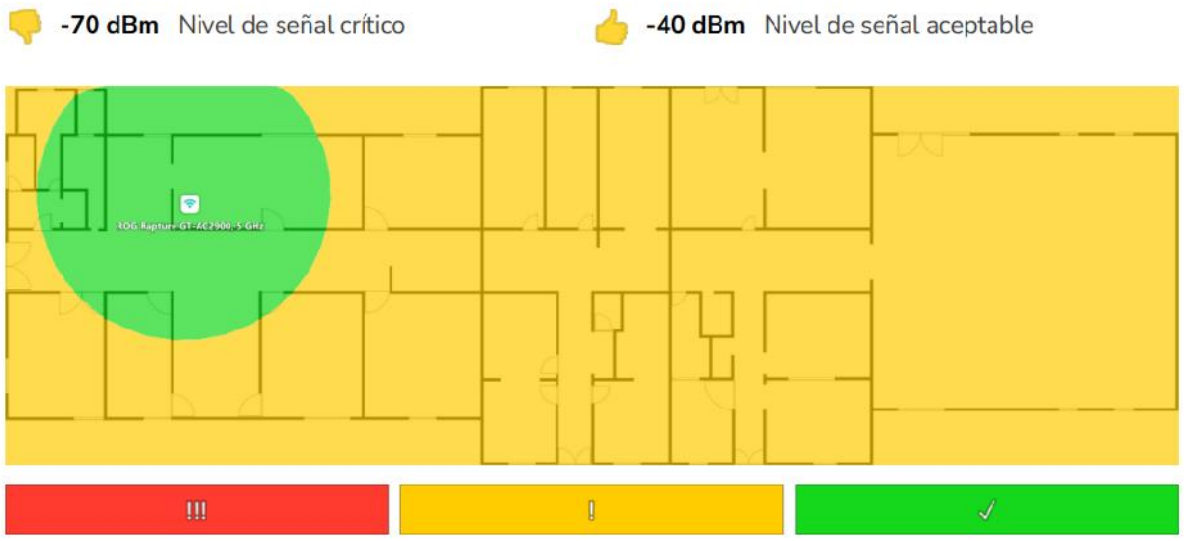


Figura 39. Intensidad de señal Baja 5GHz

#	Nombre de la red	Canal	PHY	Nivel de señal máximo	Fabricante
1	**ROG Rapture GT-AC2900, 5 GHz**	36 (5 GHz)	ax	**20 dBm**	ASUS

III.1.2.1.4.2.- Nivel de señal PAI

-96 dBm Nivel de señal mínimo -10dBm nivel de señal máximo

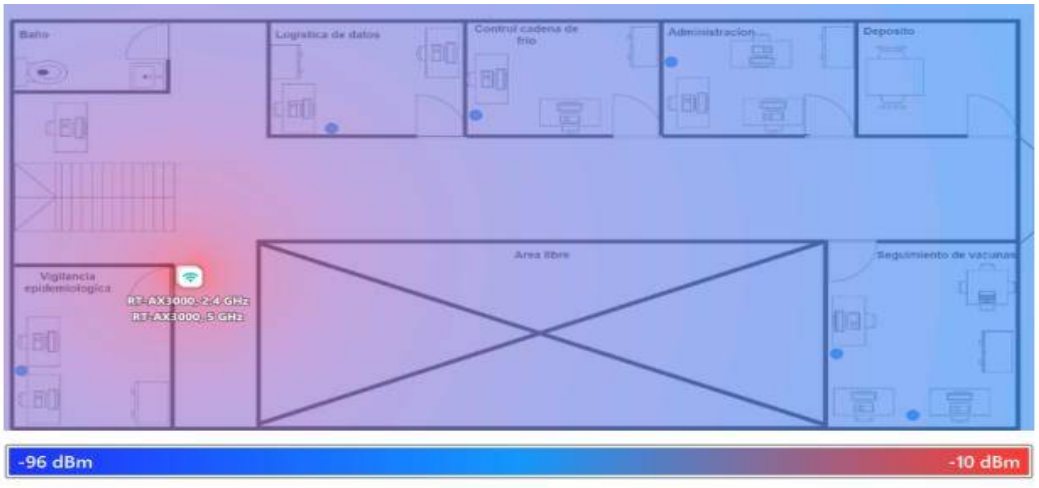


Figura 40. Nivel de señal en PAI primera planta

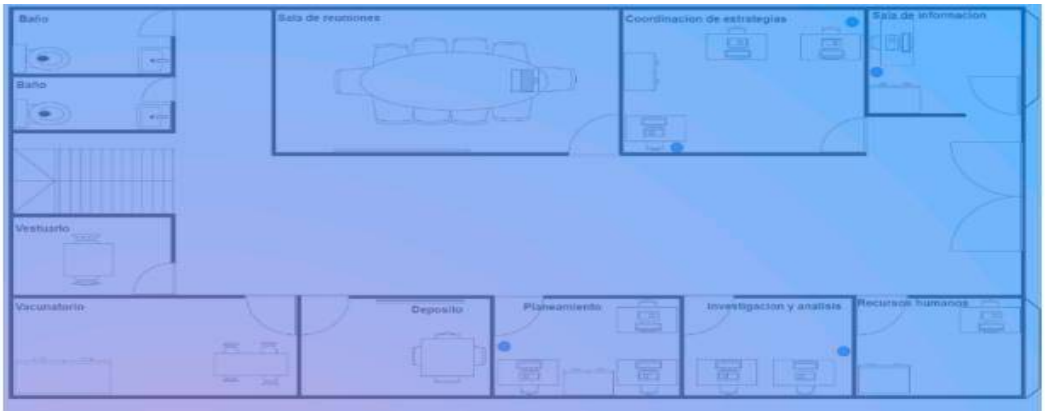


Figura 41. Nivel de señal en PAI planta baja

#	Nombre de la red	Canal	PHY	Nivel de señal máximo	Fabricante
1	**RT-AX3000, 2.4 GHz**	1 (2.4 GHz)	ax	**20 dBm**	ASUS
2	**RT-AX3000, 5 GHz**	36 (5 GHz)	ax	**20 dBm**	ASUS

Nivel de señal bajo

-70 dBm nivel de señal critico -40 dBm nivel de señal aceptable

Figura 42. Nivel de señal bajo en PAI

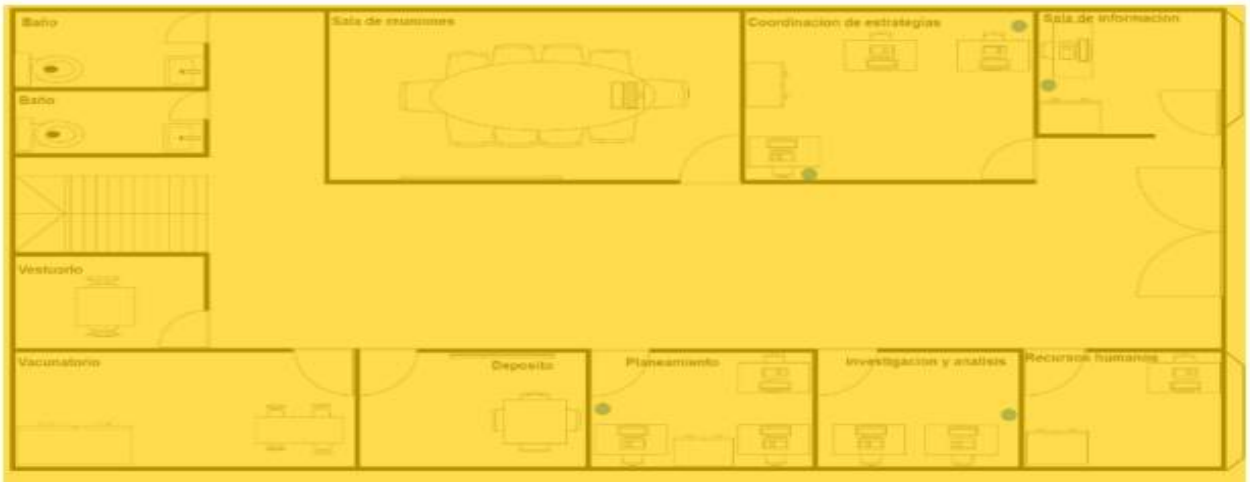


Figura 43. Nivel de señal bajo planta baja

El tráfico de red del programa ampliado de inmunización tiene los siguientes objetivos principales:

- Utilización eficiente del sistema
- Documentación y logística de datos
- Descarga de documentos
- Envió y recepción datos vacunados
- Reuniones virtuales
- Uso de aplicaciones en red

III.1.2.1.5.- Planos de la infraestructura general

III.1.2.1.5.1.- Planos de SEDES

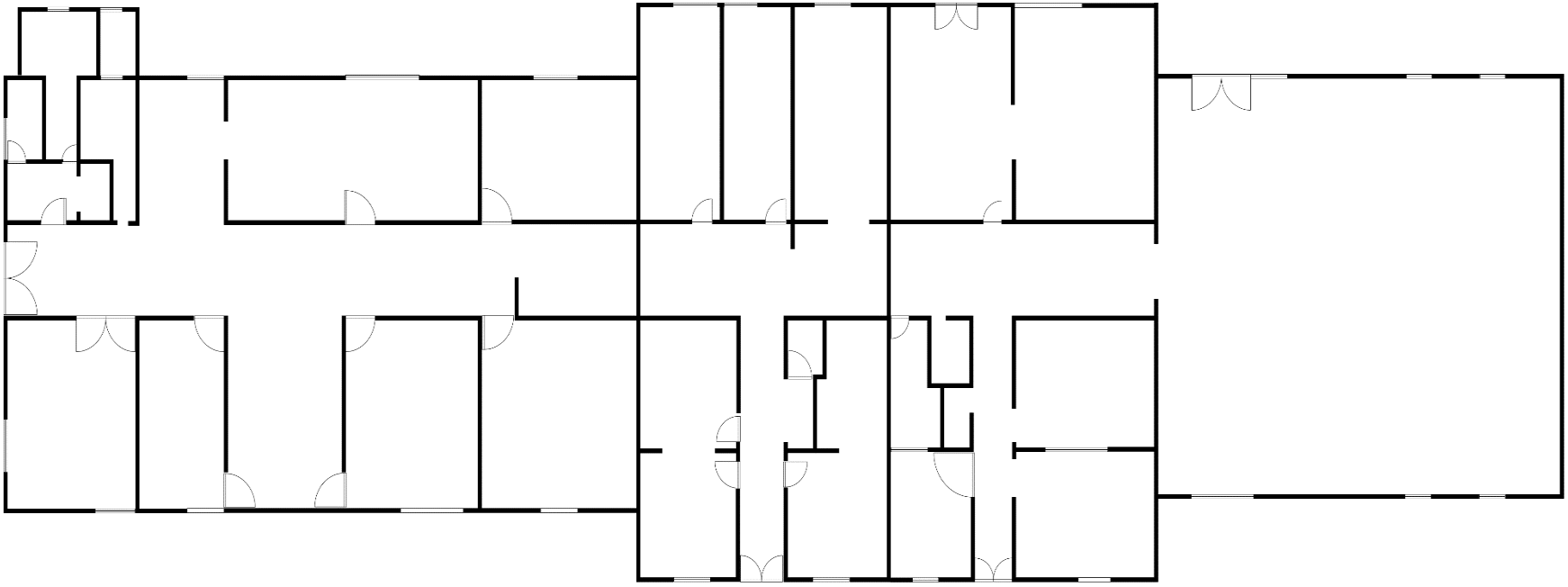


Figura 44. Planos de SEDES

III.1.2.1.5.2.- Planos del programa ampliado de inmunización PAI

Planos de infraestructura planta baja

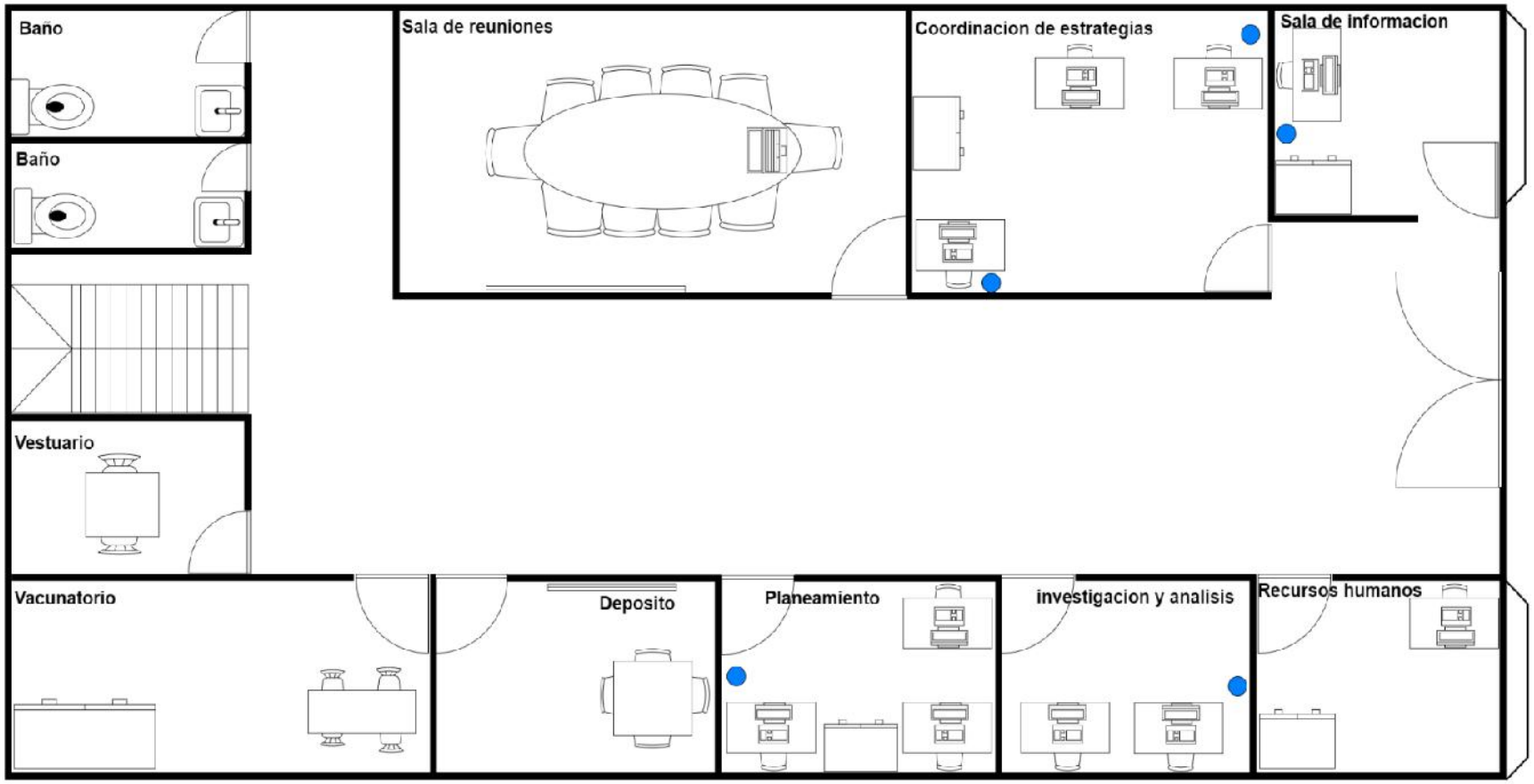


Figura 45. Planos de la infraestructura del PAI planta baja

Planos de infraestructura planta alta

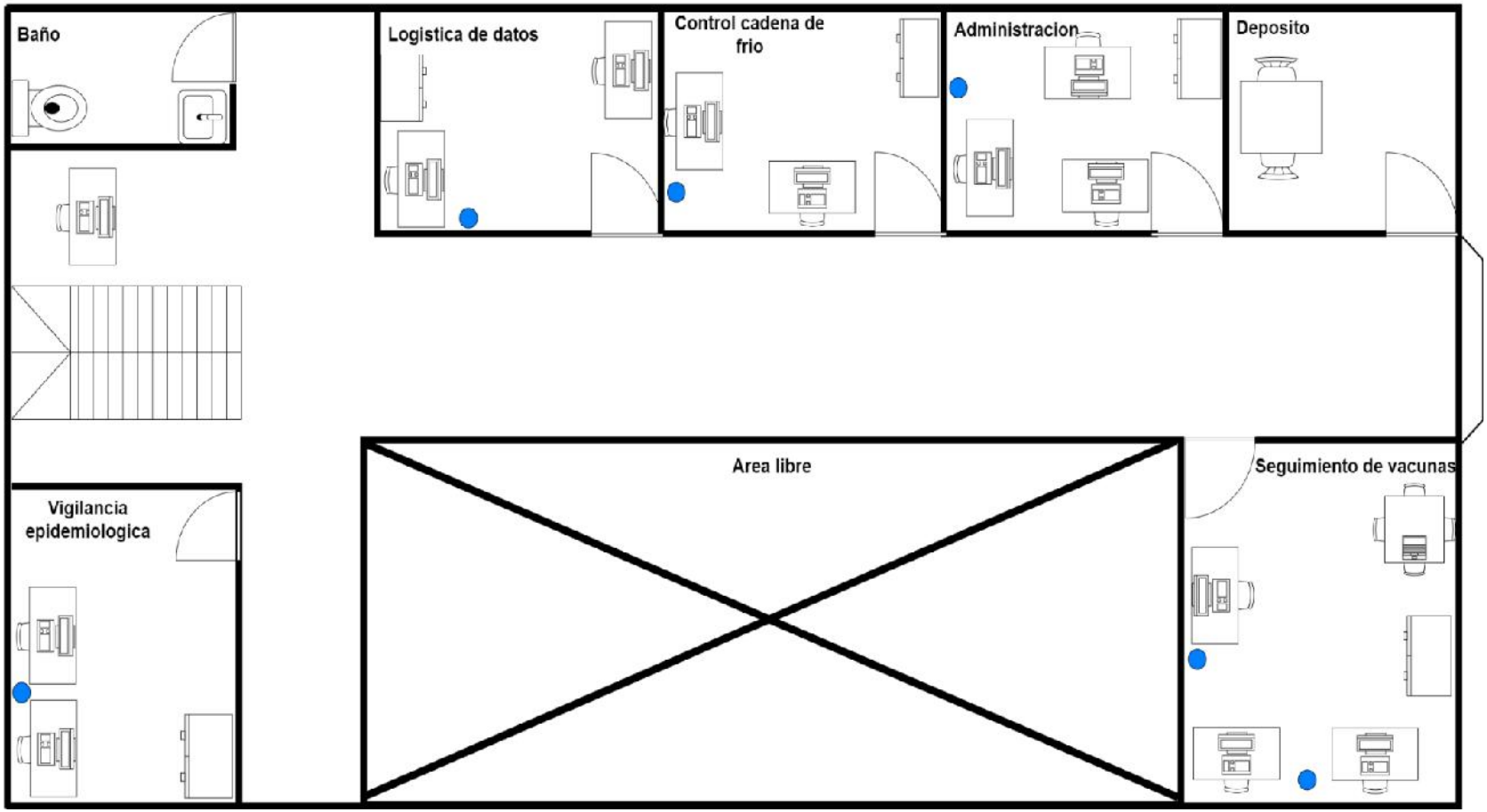


Figura 46. Planos del PAI infraestructura planta alta

III.1.2.1.5.3.-Estructura actual de la red en SEDES

Figura 47. Estructura actual de la red en SEDES

III.1.2.1.5.4.- Estructura actual de la red en PAI

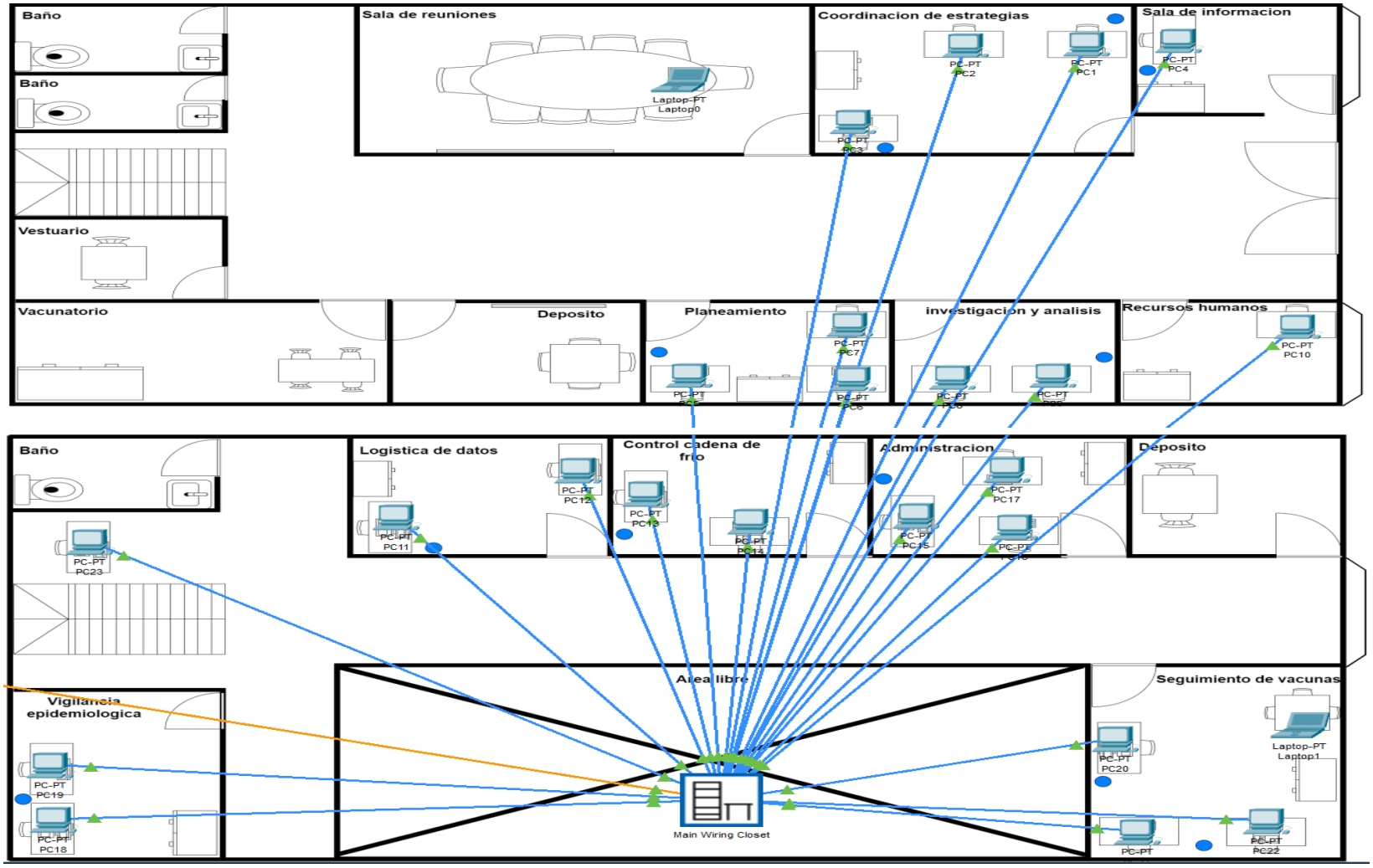


Figura 48. Estructura actual de la red en PAI

III.1.2.1.6.-Explicación de los planos

El servicio departamental de salud SEDES Tarija se encuentra ubicado en avenida potosí entre Junín y coronel delgadillo es de un solo piso y cuenta con 22 oficinas y el programa PAI se encuentra ubicado en la calle Junín al lado del banco de sangre y la iglesia de San Juan de Dios el PAI es un edificio de dos pisos en el que la planta baja tiene 10 oficinas y el primer piso tiene 6 oficinas

III.1.2.2.- Fase 2: Desarrollar diseño lógico

III.1.2.2.1.- Diseño de topología de red

Se realizará el diseño lógico de la red en base a los requerimientos identificados en el análisis de la red actual donde se debe recopilar información para presentar un modelo de diseño teniendo como objetivo principal brindar una alternativa que mejore el estado actual de la red del programa ampliado de inmunización permitiendo que se administre de una manera más eficaz y optima

Para esto primero analizamos el eje troncal de red y su topología existentes y verificamos si es necesario cambiarlas o trabajar con las mismas.

La institución tiene una topología estrella cuyo centro principal de conexiones MDF se encuentra en SEDES y de ahí se ramifica al PAI y a sus otros programas posteriormente se planea implementar el cableado estructurado debido a que el PAI no cuenta con uno y se implementara las medidas de seguridad básicas tanto para el MDF como para las conexiones de red del PAI

III.1.2.2.2.- Diseño del direccionamiento y host-name

Para realizar el diseño del direccionamiento se debe conocer el total de host que vamos a utilizar, por lo que tomaremos en cuenta todos los equipos que necesiten una dirección IP que son los siguientes:

- 50 computadoras de escritorio
- 6 laptops
- 17 impresoras
- 3 access point
- 10 telefonos IP
- 1 interface router
- 1 servidor

Una vez establecido que el total es de 88 dispositivos que se conectaran a la red se debe comenzar a realizar el diseño donde se dividirá en 2 redes principales: la red 1 que será la 192.168.1.0 y será utilizada para los servicios principales y la red 2 que será la 172.17.1.0 y servirá para la telefonía IP y finalmente las 3 redes logicas la 192.168.100.0 la 192.168.101.0 y la 192.168.102.0 que serán para las VLANs para lo cual debemos determinar el direccionamiento de cada host.

Se trabajará con 1 red con direcciones IP de clase C y una con dirección de clase B y para las redes que tienen VLANs utilizarán IPs de clase C que serán distribuidas de la siguiente forma:

Red	IP de red	Mascara	Primer Host	Ultimo Host	Broadcast
Red principal	192.168.1.0/24	255.255.255.0	192.168.1.1	192.168.1.254	192.168.1.255
Red SEDES-A	192.168.100.0/24	255.255.255.0	192.168.100.1	192.168.100.254	192.168.100.255
Red SEDES-B	192.168.101.0/24	255.255.255.0	192.168.101.1	192.168.101.254	192.168.101.255
Red PAI-A	192.168.102.0/24	255.255.255.0	192.168.102.1	192.168.102.254	192.168.102.255
Red-telefonia	172.17.0.0/16	255.255.0.0	172.17.0.2	172.17.0.254	172.17.0.255

Tabla 7. Division de redes

A continuación, se detallará para que será utilizada cada red:

La red principal será para los dispositivos de conexión que debe ser una red externa a las VLANs para que el DHCP pueda configurarse de manera correcta y estos serán el router y el servidor DHCP y los 3 Access point.

La red SEDES-A está diseñada para las oficinas del SEDES con la VLAN 10 para el centro de comunicaciones principal que cuenta con 13 equipos de escritorio 4 laptops 10 impresoras a los cuales serán asignadas las direcciones IP que tiene un rango de 30 hosts disponibles considerando que más adelante se añadan más equipos a la red

La red SEDES-B está diseñada para las oficinas del SEDES con la VLAN 20 que cuenta con 13 equipos de escritorio 2 laptops y 5 impresoras a los cuales serán asignadas las direcciones IP que tiene un rango de 30 hosts disponibles considerando que más adelante se añadan más equipos a la red

La red PAI-A está diseñada para la planta baja y el primer piso del PAI con la VLAN 30 que cuenta 24 equipos de escritorio con 1 laptop y 7 impresoras a los cuales serán asignadas las direcciones IP que tiene un rango de 40 hosts disponibles considerando que más adelante se añadan más equipos a la red

La red de telefonía IP serán para los 10 teléfonos que conectan SEDES y el PAI

III.1.2.2.2.1.- Host-name

Para el diseño del host-name se utilizará una estructura de nombre para asignar a los equipos:

III.1.2.2.2.1.1.- Host-name para oficinas de SEDES

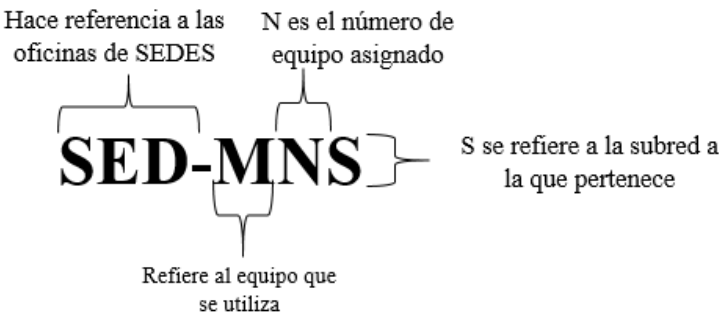


Figura 49. Host-name para máquinas de oficinas de SEDES

Figura 50. Host-name para laptops oficinas de SEDES

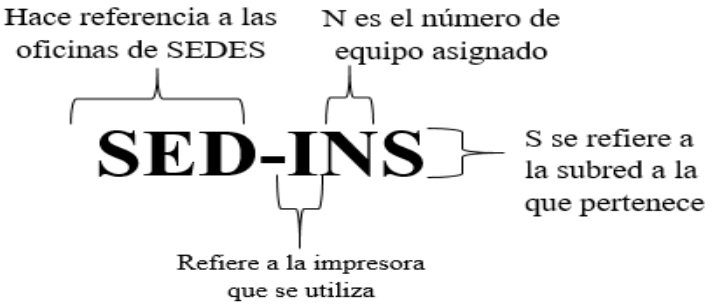


Figura 51. Host-name para impresoras oficinas de SEDES

III.1.2.2.2.1.2.- Host-name para planta baja del PAI

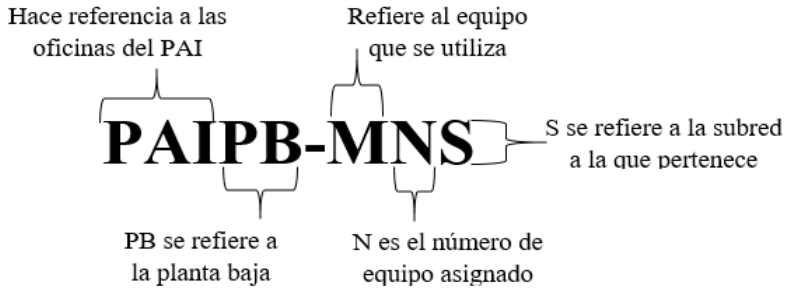


Figura 52. Host-name para maquinas planta baja del PAI

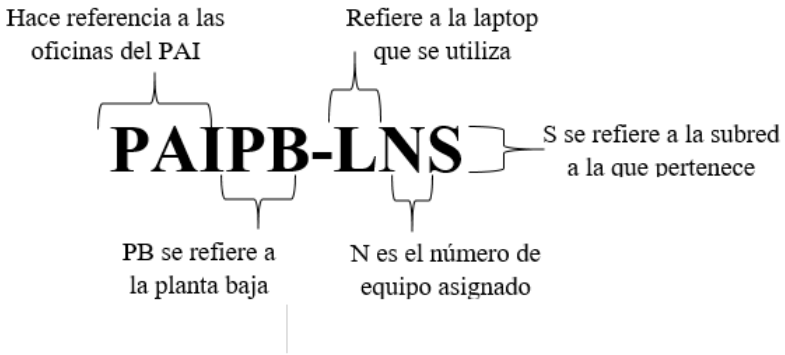


Figura 53. Host-name para laptops planta baja PAI

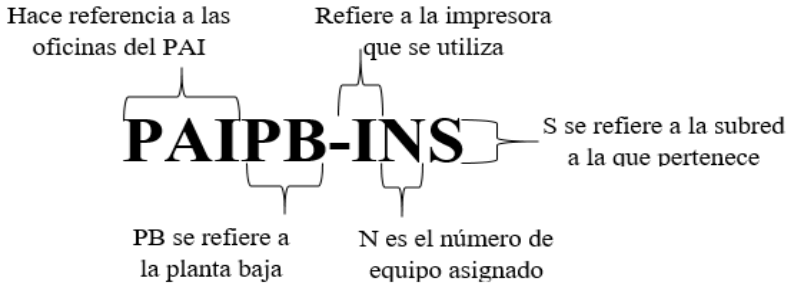


Figura 54. Host.name para impresoras planta baja PAI

III.1.2.2.2.1.3.- Host-name para primer piso del PAI

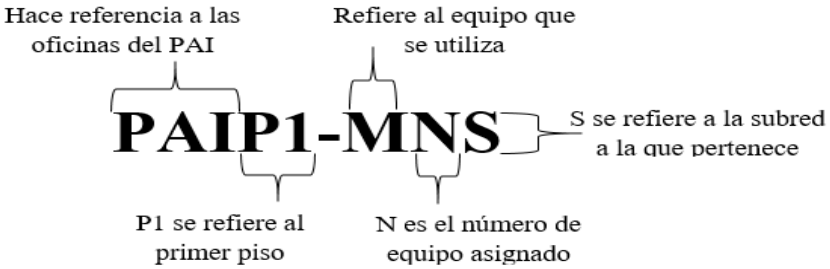


Figura 55. Host-name para maquinas primer piso PAI

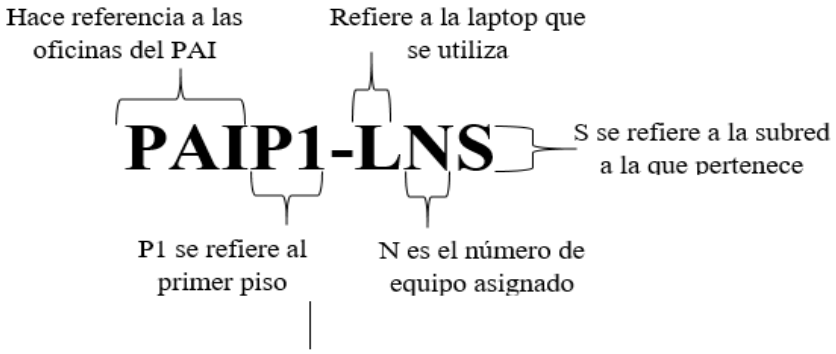


Figura 56. Host-name para laptops primer piso PAI

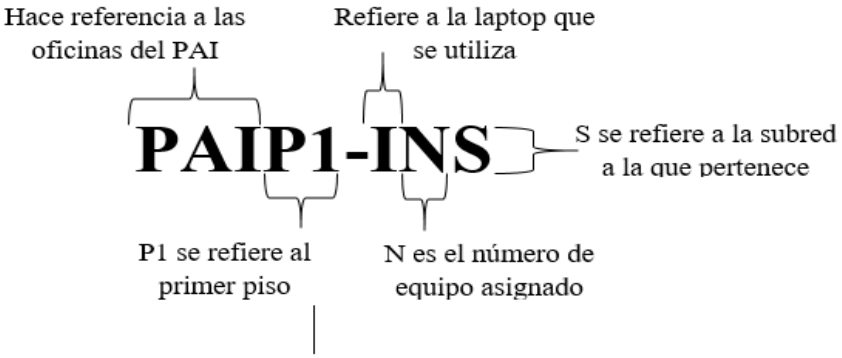


Figura 57. Host-name para impresoras primer piso PAI

III.1.2.2.2.1.4.- Host-name para los dispositivos de conexión de la red

Figura 58. Host-name para el Access point

Figura 59. Host-name para el servidor

Figura 60. Host-name para el switch

Figura 61. Host-name para el router

III.1.2.2.2.2.- Diseño del Direccionamiento

III.1.2.3.8.1.- Planificación de la distribución de las IP para la red principal

NOMBRES	DIRECCIONES
RED	**192.168.1.0/24**
SERVIDOR DHCP	**192.168.1.5**
MASCARA DE RED	**255.255.255.0**
PUERTA DE ENLACE	**192.168.1.1**

Tabla 8. Distribucion de las IPs en la red principal

Planificación de las IP para la vlan SEDES-A de SEDES

NOMBRES	DIRECCIONES
RED	**192.168.100.0/24**
SERVIDOR DHCP	**192.168.1.5**
MASCARA DE RED	**255.255.255.0**
AMBITO DE DHCP	**192.168.100.3 192.168.100.62**
PUERTA DE ENLACE	**192.168.100.1**

Tabla 9. Planificación de la distribución de IP para la vlan SEDES-A

Planificación de las IP para la vlan SEDES-B de SEDES

NOMBRES	DIRECCIONES
RED	**192.168.101.0/24**
SERVIDOR DHCP	**192.168.1.5**
MASCARA DE RED	**255.255.255.0**
AMBITO DE DHCP	**192.168.101.3 192.168.101.62**
PUERTA DE ENLACE	**192.168.101.1**

Tabla 10. Planificación de la distribución de IP para la vlan SEDES-B

Planificación de las IP para el PAI que tendrá la vlan PAI-A

NOMBRES	DIRECCIONES
RED	**192.168.102.0**
SERVIDOR DHCP	**192.168.1.5**
MASCARA DE RED	**255.255.255.0**
AMBITO DE DHCP	**192.168.102.3 192.168.102.94**
PUERTA DE ENLACE	**192.168.102.1**

Tabla 11. Planificación de la distribución de IP para la vlan PAI-A

Planificación de las IP para la telefonía IP

NOMBRES	DIRECCIONES
RED	**172.17.1.0**
SERVIDOR DHCP	**172.17.1.3**
MASCARA DE RED	**255.255.0.0**
AMBITO DE DHCP	**172.17.1.4 - 172.17.1.20**
PUERTA DE ENLACE	**172.17.1.1**

Tabla 12. Planificación de las IPs para la telefonía IP

Una vez definido el diseño dividimos y repartimos las direcciones IPs al lugar que le corresponde

Equipo	Interfaz	Dirección IP	Mascara	Gateway
R1	Fa0/0	192.168.1.1	255.255.255.0	No aplica
AP1	Port 0	No tiene	255.255.255.0	192.168.1.1
SERV1		192.168.1.5	255.255.255.0	192.168.1.1

Tabla 13. Direccionamiento equipos de red

Direccionamiento de IPs red SEDES-A en SEDES

Equipo	Interfaz	Dirección IP	Mascara	Gateway
SED-L1-A	NIC	DHCP	255.255.255.0	No aplica
SED-L2-A	NIC	DHCP	255.255.255.0	No aplica
SED-M1-A	NIC	DHCP	255.255.255.0	192.168.100.1
SED-M2-A	NIC	DHCP	255.255.255.0	192.168.100.1
SED-M3-A	NIC	DHCP	255.255.255.0	192.168.100.1
SED-M4-A	NIC	DHCP	255.255.255.0	192.168.100.1
SED-M5-A	NIC	DHCP	255.255.255.0	192.168.100.1
SED-M6-A	NIC	DHCP	255.255.255.0	192.168.100.1
SED-M7-A	NIC	DHCP	255.255.255.0	192.168.100.1
SED-M8-A	NIC	DHCP	255.255.255.0	192.168.100.1
SED-M9-A	NIC	DHCP	255.255.255.0	192.168.100.1

SED-M10-A	NIC	DHCP	255.255.255.0	192.168.100.1
SED-M11-A	NIC	DHCP	255.255.255.0	192.168.100.1
SED-M12-A	NIC	DHCP	255.255.255.0	192.168.100.1
SED-M13-A	NIC	DHCP	255.255.255.0	192.168.100.1
SED-I1-A	NIC	DHCP	255.255.255.0	192.168.100.1
SED-I2-A	NIC	DHCP	255.255.255.0	192.168.100.1
SED-I3-A	NIC	DHCP	255.255.255.0	192.168.100.1
SED-I4-A	NIC	DHCP	255.255.255.0	192.168.100.1
SED-I5-A	NIC	DHCP	255.255.255.0	192.168.100.1

Tabla 14. Direccionamiento red SEDES-A en SEDES

Direccionamiento de IPs red SEDES-B en SEDES

Equipo	Interfaz	Dirección IP	Mascara	Gateway
SED-L3-B	NIC	192.168.101.13	255.255.255.0	192.168.101.1
SED-L4-B	NIC	192.168.101.14	255.255.255.0	192.168.101.1
SED-M14-B	NIC	DHCP	255.255.255.0	192.168.101.1
SED-M15-B	NIC	DHCP	255.255.255.0	192.168.101.1
SED-M16-B	NIC	DHCP	255.255.255.0	192.168.101.1
SED-M17-B	NIC	DHCP	255.255.255.0	192.168.101.1
SED-M18-B	NIC	DHCP	255.255.255.0	192.168.101.1
SED-M19-B	NIC	DHCP	255.255.255.0	192.168.101.1
SED-M20-B	NIC	DHCP	255.255.255.0	192.168.101.1
SED-M21-B	NIC	DHCP	255.255.255.0	192.168.101.1
SED-M22-B	NIC	DHCP	255.255.255.0	192.168.101.1
SED-M23-B	NIC	DHCP	255.255.255.0	192.168.101.1
SED-M24-B	NIC	DHCP	255.255.255.0	192.168.101.1
SED-M25-B	NIC	DHCP	255.255.255.0	192.168.101.1
SED-M26-B	NIC	DHCP	255.255.255.0	192.168.101.1

SED-I6-B	NIC	DHCP	255.255.255.0	192.168.101.1
SED-I7-B	NIC	DHCP	255.255.255.0	192.168.101.1
SED-I8-B	NIC	DHCP	255.255.255.0	192.168.101.1
SED-I9-B	NIC	DHCP	255.255.255.0	192.168.101.1
SED-I10-B	NIC	DHCP	255.255.255.0	192.168.101.1

Tabla 15. Direccionamiento red SEDES-B en SEDES

Direccionamiento de IPs red PAI-A en el primer piso en PAI

Equipo	Interfaz	Dirección IP	Mascara	Gateway
AP2	G0/0	192.168.102.1	255.255.255.0	No aplica
PAIP1-M1-A	NIC	DHCP	255.255.255.0	192.168.102.1
PAIP1-M2-A	NIC	DHCP	255.255.255.0	192.168.102.1
PAIP1-M3-A	NIC	DHCP	255.255.255.0	192.168.102.1
PAIP1-M4-A	NIC	DHCP	255.255.255.0	192.168.102.1
PAIP1-M5-A	NIC	DHCP	255.255.255.0	192.168.102.1
PAIP1-M6-A	NIC	DHCP	255.255.255.0	192.168.102.1
PAIP1-M7-A	NIC	DHCP	255.255.255.0	192.168.102.1
PAIP1-M8-A	NIC	DHCP	255.255.255.0	192.168.102.1
PAIP1-M9-A	NIC	DHCP	255.255.255.0	192.168.102.1
PAIP1-M10-A	NIC	DHCP	255.255.255.0	192.168.102.1
PAIP1-M11-A	NIC	DHCP	255.255.255.0	192.168.102.1
PAIP1-M12-A	NIC	DHCP	255.255.255.0	192.168.102.1
PAIP1-M13-A	NIC	DHCP	255.255.255.0	192.168.102.1
PAIP1-L1-A	NIC	DHCP	255.255.255.0	192.168.102.1
PAIP1-I1-A	NIC	DHCP	255.255.255.0	192.168.102.1
PAIP1-I2-A	NIC	DHCP	255.255.255.0	192.168.102.1
PAIP1-I3-A	NIC	DHCP	255.255.255.0	192.168.102.1
PAIP1-I4-A	NIC	DHCP	255.255.255.0	192.168.102.1

Tabla 16. Direccionamiento red PAI-A en PAI primer piso

Direccionamiento de IPs red PAI-A planta baja en PAI

Equipo	Interfaz	Dirección IP	Mascara	Gateway
PAIPB-L1-A	NIC	DHCP	255.255.255.0	192.168.102.1
PAIPB-M14-A	NIC	DHCP	255.255.255.0	192.168.102.1
PAIPB-M15-A	NIC	DHCP	255.255.255.0	192.168.102.1
PAIPB-M16-A	NIC	DHCP	255.255.255.0	192.168.102.1
PAIPB-M17-A	NIC	DHCP	255.255.255.0	192.168.102.1
PAIPB-M18-A	NIC	DHCP	255.255.255.0	192.168.102.1
PAIPB-M19-A	NIC	DHCP	255.255.255.0	192.168.102.1
PAIPB-M20-A	NIC	DHCP	255.255.255.0	192.168.102.1
PAIPB-M21-A	NIC	DHCP	255.255.255.0	192.168.102.1
PAIPB-M22-A	NIC	DHCP	255.255.255.0	192.168.102.1
PAIPB-M23-A	NIC	DHCP	255.255.255.0	192.168.102.1
PAIPB-M24-A	NIC	DHCP	255.255.255.0	192.168.102.1
PAIPB-I1-A	NIC	DHCP	255.255.255.0	192.168.102.1
PAIPB-I2-A	NIC	DHCP	255.255.255.0	192.168.102.1
PAIPB-I3-A	NIC	DHCP	255.255.255.0	192.168.102.1

Tabla 17. Direccionamiento red PAI-A en PAI planta baja

III.1.2.2.3.- Seleccionar protocolos para switching y routing

En la selección de protocolos de switching y routing se consideraron los objetivos de la institución y los objetivos técnicos

Se decidió implementar el uso de VLANs para segmentar la red y poder administrar de manera más óptima el trafico existente de la red para esto se utilizará el protocolo IEEE 802.1Q

El protocolo IEEE 802.1Q se encarga del etiquetado de las tramas que es asociada inmediatamente con la información de la VLAN.

Se optó por este protocolo de switching para la institución debido a que en el análisis previo que se realizó a la red se observó que presenta un alto tráfico de datos sobre todo en el área de SEDES durante ciertas horas de la mañana entre las 10:00 y las 12:00 y en la tarde de 15:00 a 18:00 lo que ocasiona que la red congestione y su rendimiento no sea el óptimo para evitar esto lo que se propone es segmentar la red principal ya que ambas instituciones tienen diferente tráfico de datos en 3 redes lógicas ósea en 3 vlans las cuales estarán distribuidas 2 en la institución SEDES y 1 en el programa PAI

Se tendrá 5 switch el principal o trunkal ubicado en SEDES y los otros 4 serán los secundarios de esta forma el tráfico será distribuido y se evitará la congestión de datos en horas donde la red este en su mayor uso también de esta manera proporcionaremos seguridad a la red gestionando las vlans para el uso que estas tengan

VLAN	RED	IP
1	RED SEDES-A	192.168.100.0
2	RED SEDES-B	192.168.101.0
3	RED PAI-A	192.168.102.0

Tabla 18. Direccionamiento de las VLANs

Planificación de las VLANS

Planificación de las IP para la vlan SEDES-A de SEDES

NOMBRES	DIRECCIONES
RED	**192.168.100.0/24**
SERVIDOR DHCP	**192.168.1.5**
MASCARA DE RED	**255.255.255.0**
AMBITO DE DHCP	**192.168.100.3 192.168.100.62**
PUERTA DE ENLACE	**192.168.100.1**

Tabla 19. Planificación de la distribución de IP para la vlan SEDES-A

Planificación de las IP para la vlan SEDES-B de SEDES

NOMBRES	DIRECCIONES
RED	**192.168.101.0/24**
SERVIDOR DHCP	**192.168.1.5**
MASCARA DE RED	**255.255.255.0**
AMBITO DE DHCP	**192.168.101.3 192.168.101.62**
PUERTA DE ENLACE	**192.168.101.1**

Tabla 20. Planificación de la distribución de IP para la vlan SEDES-B

Planificación de la IP para el PAI que tendrá la vlan PAI-A

NOMBRES	DIRECCIONES
RED	**192.168.102.0**
SERVIDOR DHCP	**192.168.1.5**
MASCARA DE RED	**255.255.255.0**
AMBITO DE DHCP	**192.168.102.66 192.168.102.94**
PUERTA DE ENLACE	**192.168.102.1**

Tabla 21. Planificación de la distribución de IP para la vlan PAI-A

III.1.2.3.6.4 Diseño lógico de la red

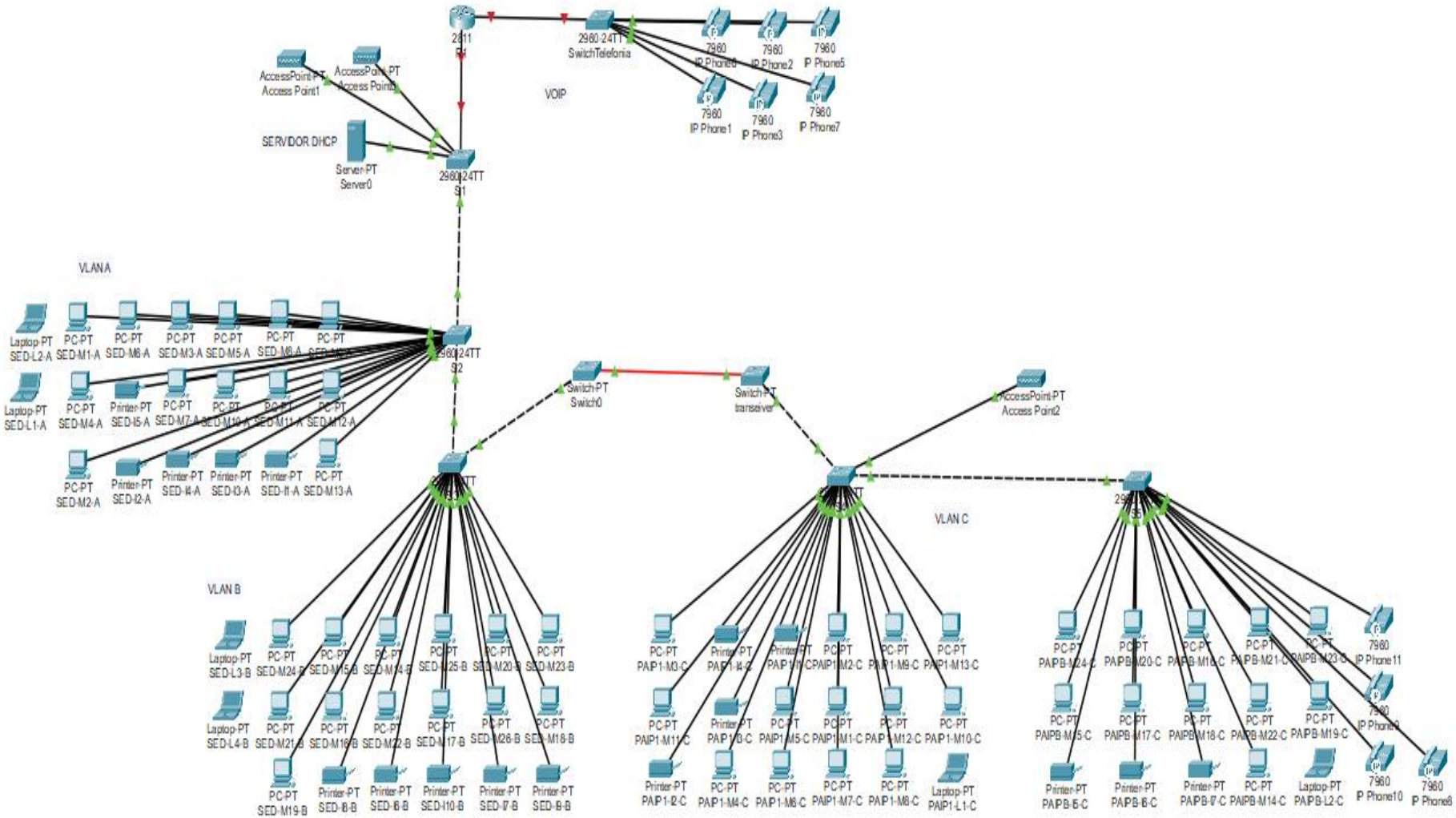


Figura 62. Diseño lógico de la red

III.1.2.2.4.- Desarrollo de estrategias de seguridad

Para el desarrollo de estrategias de seguridad de la red primeramente se contemplará un análisis de riesgos y posteriormente se propondrá un plan de seguridad

Lo esencial es proteger la información que maneja la institución que viene siendo los datos personales de los pacientes vacunados de cualquier tipo de intento de sustracción de información y o perdida de la misma previamente en el análisis de la red actual se pudo observar que esta posee vulnerabilidades debido a que no se cuenta con ningún tipo de seguridad por lo que se plantea tomar medidas de prevención y control para proteger la información que se maneja de riesgos y amenazas

III.1.2.2.4.1.- Desarrollar un plan de seguridad

Se propone:

Implementar un firewall Fortigate que permitirá que la red interna este protegido de redes externas el objetivo del software es detectar amenazas ocultas permitiéndonos ver nuestra actividad de red actual. También nos permite bloquear el acceso a Internet a programas que no deban hacerlo, y, además, detecta malware.

Implementar un software de monitoreo de la red GlassWire que permitirá supervisar la red y el tráfico de datos que se tiene

Implementar el uso de vlans de manera que divida el tráfico de la red por áreas evitando que se mezclen los diferentes tipos de tráfico esto también es una estrategia de seguridad

Bloqueo de páginas por medio de un software de filtrado web

En cuanto a la seguridad inalámbrica se propone lo siguiente:

Nosotros utilizaremos: WPA2-Personal, Filtrado de Mac y Cambio de SSID esto lo realizamos para evitar un ataque, necesita productos específicamente diseñados para proteger la red inalámbrica.

Cuentas de Usuario ID o SSID: El Router tendrá un nombre personalizado para que se puedan conectar las personas solo de la institución.

Autenticación: Se utilizará el Cifrado WPA2-Personal todas las oficinas estarán conectadas de este modo con este tipo de seguridad ambas instituciones tendrán contraseñas

Filtrado de Mac: Se realiza una lista con las Mac de los equipos de computación que se conecten de manera inalámbrica para que se puedan conectar al Access Point solo ese equipo.

III.1.2.2.5.- Desarrollo de estrategias de administración de red

En las estrategias de administración de redes nos enfocaremos en las contingencias que pueden presentarse, durante la puesta en marcha de la red de datos.

En la red se implementó las siguientes estrategias de administración de red

Lo primero que realizaremos para la administración de red será:

- Administración de las cuentas y contraseñas del personal
- Administración de los equipos por redes asignando host-name a cada uno
- Optimizar el ancho de banda por red
- Implementar protocolos en la implementación de vlans esta es otra forma de administrar la red debido a que se está implementando el protocolo IEEE 802.1Q
- Aplicar un modelo de direccionamiento, el direccionamiento es una función clave de los protocolos de capa de Red que permite la transmisión de datos entre hosts de la misma red

o en redes diferentes. El Protocolo de Internet versión 4 (IPv4) ofrece direccionamiento jerárquico para paquetes que transportan datos.

- Implementar Host-names a los equipos

III.1.2.3.- Fase 3: Desarrollar Diseño Físico

Descripción de las funciones de los edificios

SEDES cuenta con una sola planta baja mientras que su programa PAI cuenta con dos plantas, ambas instituciones están conectadas mediante el centro de datos

SEDES: Consta de 21 habitaciones 2 salas de reuniones secretaria farmacia jefe farmacia gerencia departamental, oficina sida, oficina, secretaria, deposito (oficina del director de sedes), sala de reuniones AIEPI, gerencia salud sexual y reproductiva, sala de disección oficina de salud sexual y reproductiva, administración aula, deposito

PAI planta baja: Consta de 7 habitaciones sala de información, coordinación de estrategias sala de reuniones, vacunatorio, planeamiento, investigación y análisis recursos humanos

PAI planta alta: Consta de 5 habitaciones logística de datos control de cadena de frio, administración, vigilancia epidemiológica, seguimiento de vacunas

III.1.2.3.1.- Situación actual del edificio

La estructura de cableado actualmente no cuenta con medios de canalización ni en los pasillos ni en los ambientes el cableado se encuentra expuesto por lo que se realizara una reestructuración utilizando algunos elementos que ya existen para la canalización del cableado de la red

SEDES: Se implementará a través del suelo del centro de datos ubicado en un cuarto improvisado que tiene la institución a las 20 oficinas que tendrá 30 equipos de escritorio y 3 laptops contando las conexiones inalámbricas se tienen un total de 35 usuarios conectados

PAI planta alta: Se implementará desde el centro de datos ubicado en SEDES hasta el rack de pared ubicado en la planta alta de PAI teniendo un aproximado de 12 equipos de escritorio y 1 laptop

PAI planta baja: Se implementará desde el rack de pared ubicado en la planta alta del PAI por la pared hacia los diferentes puntos de red teniendo un aproximado de 11 equipos de escritorio y 1 laptop

III.1.2.3.2.-Estimación total de la infraestructura física

Descripción detallada de la canalización cableado, conector rizado y rosetas

En primer lugar, veremos el tema del cableado se usará cable certificado UTP categoría 5e para transmisión de datos para que se mantenga estable con el tiempo y con el uso además para evitar interferencias.

Primero se debe determinar el tamaño de la infraestructura física esto con el fin de saber cuánto cableado deberemos instalar en cada planta los planos de cada una de las plantas tanto de SEDES como del PAI tienen una escala de 1:100 y los podremos encontrar en el documento, así como también la cantidad de cable en metros que se utiliza en el diseño que es un total de 868 metros en SEDES y 619 metros en PAI

El cálculo total de cada planta se especifica a continuación:

Distancia máxima:

SEDES: 60m x 15m

PAI planta alta: 35m x 12m

PAI planta baja: 35m x 12m

Distancia real:

SEDES: 57m x 12m

PAI planta alta: 32m x 11m

PAI planta baja: 32m x 11m

Cableado

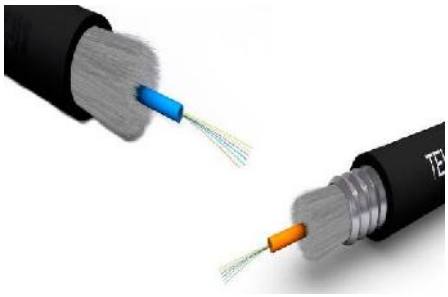
Se decidió utilizar el tipo de cableado UTP para la instalación de la red interna ya que su costo no supone una inversión muy grande dicho esto el tipo de cable es el siguiente:

Modelo de cable UTP cat 5e

- Número de pares: 4
- Conductor: cobre sólido (clase 1)
- Aislamiento: HDPE, PE, Poliolefina
- Alambre de drenaje: Cobre estañado
- Pantalla: Papel Al
- Revestimiento exterior: Polietileno de baja densidad (LDPE), LSZH, LSZH
- Color: Negro, Azul, Azul claro

Figura 63. Cable UTP cat5e

Para la conexión de ambas instituciones y para la conexión de internet se utilizará fibra óptica y dicho cable es el siguiente:



- Un núcleo central de fibra con un alto índice de refracción.
- Una cubierta que rodea al núcleo, de material similar, con un índice de refracción ligeramente menor.
- Una envoltura que aísla las fibras y evita que se produzcan interferencias entre fibras adyacentes, a la vez que proporciona protección al núcleo. Cada una de ellas está rodeada por un revestimiento y reforzada para proteger a la fibra

Latiguillos de parcheo

Latiguillo de parcheo de 4 pares sin apantallar (UTP). Desarrollado principalmente para la conexión entre los puestos de trabajo, o para la distribución entre repartidores. Soporta frecuencias de hasta 350 MHz y velocidades de hasta 1000 Mbps.

Supera las condiciones de Cat. 6 marcados por la norma.

Alta protección contra las interferencias electromagnéticas.

Baja propagación de retardo.

Altos valores ACR y error mínimo de velocidad.

Figura 64. Latiguillos de parcheo

Rosetas y conectores

Se instalarán las rosetas respetando el destrenzado menor de 13 mm, se evitará la perdida de categoría

Figura 65. Rosetas RJ45

El tipo de conectores que se utilizarán serán los conectores RJ45, que es un conector con ocho pines metálicos que se conectan con los pines del cable

Conectores RJ45

- Contactos: 8
- Nº de puertos: 1
- Categoría LAN: CAT 6A
- Chapado de los contactos: Oro
- Material de contacto: bronce

Figura 66. Conector RJ45

Canaleta PVC

Descripción: Canaleta plástica 27 mm de profundidad x 30 mm de ancho

Por medio de este irán los cables protegidos frente a incidencias exteriores, la canaleta dispondrá de una tapa desmontable para poder quitar o añadir para la instalación de los cables se colocará de dos tipos el de paredes que ira fijada con tornillo y el cable canal para piso

Figura 67. Canaleta PVC

Al escoger el tipo de cable se debe tener en cuenta una serie de características de los cables UTP. Los cables de datos tienen una resistencia de hasta 100Ω y están formados por cuatro pares.

Nombre	**Cantidad**	**Precio (Bs)**
Cable UTP categoría 5e certificado	5 cajas (305 metros por caja)	970 por caja
	1525 metros	4850 total

Patch cord	30 unidades	12,50 por unidad 375 total
RJ45	200 unidades	2 por unidad 400 total
Roseta RJ45	200 unidades	5 por unidad 1000
Conector 4 bocas hembra de pared de red RJ45 jack utp cat5e	25 unidades	48 por unidad 1200 total
Canaleta PVC	30 unidades	10 por unidad 300

Tabla 22. Componentes cableado

En las instituciones se realizará el cableado estructurado el cableado vertical será encargado de interconectar la acometida principal hacia afuera que vendría a ser el internet con el cuarto principal de conexión (centro de datos) y el armario de distribución (rack) intermedio la conexión entre estos será con fibra óptica y se mantendrá la topología estrella.

Debido a que en la institución PAI no se tiene un ambiente adecuado para los cables, accesorios de conexión y demás equipos se utilizará un gabinete de comunicaciones donde alojaremos el switch que estará conectado al centro de datos ubicado en el SEDES este nos permitirá organizar el sistema de comunicaciones

La canalización del cableado está compuesta por las rutas y espacios horizontales que se utilizan para distribuir y soportar el cableado horizontal y conectar el equipo entre la salida del área de trabajo estas rutas y espacios son críticas para el buen desempeño del sistema de cableado estructurado.

La puesta a tierra es un sistema para que el cableado estructurado este diseñado para la seguridad de la vida de los usuarios, la norma que usaremos es el estándar ANSI/J/STD-607-A.

III.1.2.3.3.- Descripción de armarios para el centro de datos

III.1.2.3.3.1.-Rack de distribución 32U

Gabinete de telecomunicaciones de alta durabilidad, flujo de aire óptimo y especialmente diseñado para gabinete de distribución intermedia (IDF) de una red de datos mediana o grande, permite el montaje de dispositivos como Switches, Routers, Firewall, NVR. Así mismo permite alojar elementos del cableado estructurado como patch panel y organizadores.

Características:

- Marca: TOTEN.
- Factor de forma: 32U, estándar de 19 pulgadas.
- Ancho: 600 mm.
- Profundidad: 600 m
- m.
- Color: Negro.
- Material principal: (SPCC) acero laminado en frío.
- Acabado: Desengrasado, decapado, recubierto en polvo.
- Puertas desmontables: Frontal vidrio, posterior microperforada y laterales rígidas.
- Entradas de cables: Superior e inferior.
- Grado de protección: IP20.
- Capacidad de carga: 800 Kg. de carga estática.
- Accesorios: Ruedas y pie de apoyo ajustable.
- Montaje: Piso.
- Estándares: ANSI/EIA RS-310-D, IEC297-2, DIN41494, ETSI.

Figura 68. Rack de 32U

III.1.2.3.3.2.-Gabinete para instalación en pared capacidad para 6U

Sus dimensiones normalizadas según la especificación EIA-310 permiten que sea compatible con equipos de cualquier marca o fabricante. Capacidad de carga de 60 Kg. La altura interna permite alojar dispositivos hasta completar 6U rack de 19".

Tiene un ventilador de 120 mm para su correcta refrigeración, una bandeja y una regleta eléctrica de 1U rack con 6 tomas.

Estructura de doble sección altamente resistente, fabricada en acero laminado en frío SPCC de 2,0 mm de grosor en los perfiles y con ligeras planchas de 1,0 mm para el resto de elementos

Figura 69. Rack de 6U

III.1.2.3.3.3.-Regleta de fuerza

Permite conectar y brindar energía a los equipos alojados en rack, así mismo brinda protección contra fugas de eléctrica y sobretensiones.

- Marca: TOTEN
- Modelo: PD.0601.9000X2
- Factor de forma: 1U, estándar de 19 pulgadas.
- Salidas: 6 tomas tipo nema.
- Corriente: 10A. 16AWG, 1150W
- Interruptor: Si.
- Longitud del cable: 3m
- Color: Negro.
- Carcasa: Aluminio

Figura 70. Regleta de fuerza

III.1.2.3.3.4.-Organizador de cableado

Sirven para organizar y eliminar la congestión de los cables

TOTEN Organizador horizontal para rack de 19" con tapa 1RU

Figura 71. Organizador de cableado

III.1.2.3.3.5.-Ventilador rack

La unidad de ventilación está diseñada para no ocupar espacio en el interior del armario ya que va fijada en el techo

Figura 72. Ventilador para rack

III.1.2.3.3.6.-Patch panel de 24 puertos

La función del patch panel será de hacer de conector intermediario entre las rosetas y el switch al que se conectan los dispositivos

Es un dispositivo de red eficaz y flexible para mantener organizado el centro de datos, así como para facilitar el traslado, la adición o el cambio de la infraestructura de cableado en el futuro

Cumple con los estándares ANSI/EIA/TIA 568-B.2-1 y ISO/IEC 11801

Etiquetado con códigos de color para esquemas de cableado T568A y T568B

Listo para Ethernet Gigabit de cobre 1000Base-T

Compatible con Cat Cableado de 3, 4, 5, 5e y 6

Figura 73. Patch panel

III.1.2.3.3.7.-UPS

La realimentación se toma en cuenta que el plantel cuenta con energía eléctrica suministrada por el proveedor (SETAR), que no tiene como backup ningún tipo de energía alternativa los que nos indica implementar una UPS con el fin de que los equipos no se queden sin energía y poder salvaguardar la información de trabajo en el momento de un corte de energía, las UPS tienen una autonomía de alrededor de 15 minutos lo cual es perfecto para salvar la información mientras se restablece el servicio de energía.

Figura 74. UPS

III.1.2.3.3.8.-Aire acondicionado

Para proteger los equipos de sobrecalentamiento es necesario contar con un equipo de refrigeración el cual estará ubicado de forma que el aire llegue justamente a los dispositivos

Figura 75. Aire acondicionado

Características

- Protección Blue Fin
- Control Wi-Fi Smart
- Compatible con Google Home y Alexa
- Clase energética A+

- Modo Ahorro de energía
- Función Turbo Cooling

III.1.2.3.3.9.- Componentes del rack

Componente	Tamaño	Unidades	Total
Regleta de fuerza	1U	1	1U
Organizador de cable	1U	2	2U
Ventilador	No ocupa un espacio	1	1U
Patch panel 24 puertos	1U	2	2U
UPS	No ocupa espacio	1	
Aire acondicionado	No ocupa espacio		

Tabla 23. Componentes del rack

III.1.2.3.3.10.-Descripción de dispositivos para el centro de datos

En el centro de datos o MDF se usara el servidor ya existente como servidor DHCP que permitirá asignar IPs de manera dinámica, así como también utilizaremos switchs para configurar las VLANs para segmentar la red y evitar congestión en la misma y un Firewall que permitirá tener una mayor seguridad de la información que manejan en cuanto a la administración de la red se diseñará y creará un direccionamiento de las IPs y los host-names para los equipos también se implementará medidas de seguridad físicas para los ambientes que serán los sensores de humo y extinguidores esto con el fin de proteger los equipos de posibles daños como incendios, polvo y el acceso de personal sin autorización garantizando la seguridad y administración de la red

Los equipos tecnológicos que utilizaremos son:

III.1.2.3.3.11.-Servidor

Un servidor que será configurado como servidor DHCP que lo que hará será repartir IPs de manera dinámica el que utilizaremos será el servidor Dell PowerEdge530

Figura 76. Servidor

III.1.2.3.3.12.-Switch de 24 puertos

Un switch es un dispositivo de interconexión que sirve para conectar todos los equipos en una red; incluidos los computadores, las consolas, las impresoras y los servidores

- Switch Web Smart PoE+ de 24 puertos a 10/100 Mbps
- 24 puertos PoE a 10/100 Mbps
- 4 puertos Gigabit
- 2 ranuras SFP compartidas
- Consumo PoE de 193 Vatios

Figura 77. Switch 24 puertos

III.1.2.3.3.13.-Access Point

El Access Point dispositivo que establecerá una conexión inalámbrica entre equipos y puedan formar una red inalámbrica externa (local o internet) con la que interconectar dispositivos

móviles o tarjetas de red inalámbricas sus características básicas son: Arris, US/DS, Online, Ethernet 1-2, Phone, Wireless.

Usos que tendrá:

- Dar acceso a una red inalámbrica a los usuarios que lo requieran.
- Llevar una conexión a internet a donde no había antes, sin perder ancho de banda con repetidores.
- Cubrir grandes áreas con una conexión de calidad, reduciendo el uso de cableado.
- Permite interconexiones entre dispositivos convencionales e inalámbricos si se conecta el AP a un switch

Figura 78. Router TIGO

III.1.2.3.4 Descripción de los equipos

DELL CORE i5 10MA GENERACION 15.6”

Figura 79. Laptop

Características:

- procesador: intel core i5-1035g1 cpu (1.19ghz)
- disco duro: ssd 256gb
- memoria ram: 8gb
- tarjeta de video: (c) 4107 mb uhd gráficos
- pantalla: 15.6’’ hd led antirreflejo wled (1920 x 1080)
- teclado: español y teclado numérico luminoso
- puertos: 1hdmi – 3usb 3.1 – lector memoria.
- webcam: cámara hd true visión. ranura para candado de seguridad.
- wifi:(802.11 a/b/g/n) conexión inalámbrica combo de wifi 802.11a/b/g/n/ac (1×1) inalámbrica de
- bluetooth® 4.2 con wi-di intel 3165 lan: 10 / 100 / 1000 mbps

Computadora de escritorio a12-9800e+monitor z1253-a

Figura 80. Computadora de escritorio

Características:

- Tarjeta madre: asus prime a320 hdmi-vga
- Procesador: amd pro a12-9800 r7 (3.10ghz)4p-4n

- Disco duro: m.2(nvme35x) 250gb + hdd 1tb (1000gb)
- Memoria ram: 8gb ddr4 (3200ghz) 2p
- Video integrado (c): 4316 r7 hd graphics
- Case: kit combo sure
- Teclado: usb
- Mouse: usb
- Parlante: oficina.
- Monitor: 20” lg hd hdmi-vga

Impresora

Epson EcoTank L3250

Figura 81. Impresora

Teléfono VoIP Cisco 7960G

- 2 puertos Ethernet (PoE).
- Pantalla LCD monocromática
- Protocolo SIP, MGCP, SCCP, H323
- Gestión de hasta 6 líneas
- Función manos libres
- Tecla mute
- Toma auricular.

- Altavoz.
- Navegador XML.
- Identificación de llamada

Figura 82. Telefono IP

ISP

El proveedor de servicios de internet será la empresa encargada de abastecer a sus clientes una conexión de banda ancha que en el caso de la institución es TIGO

III.1.2.3.5.- Identificación de la infraestructura física

III.1.2.3.5.1.- Etiquetado y documentación del sistema.

En el sistema de cableado estructurado, es necesario etiquetar todo el material que pueda causar confusión y permita facilitar el trabajo de una forma más eficaz y eficiente.

Además, permitirá mantener ordenada de una forma lógica la instalación.

La duración del etiquetado tiene que ser similar al del conexionado.

Los elementos que deben ser etiquetados en un sistema de cableado estructurado son:

Cableado horizontal y vertical. Como mínimo ambos extremos del cable, y si es

posible en tramos regulares.

Repartidores y switch.

Rosetas o tomas de usuario.

Espacios donde se localicen terminales.

III.1.2.3.5.2.- Abreviaturas para el PAI

- SR: Sala de reuniones
- CE: Coordinación de estrategias
- SI: Sala de información
- V: Vacunatorio
- P: Planeamiento
- IA: Investigación y análisis
- RH: Recursos humanos
- LD: Logística de datos
- CCF: Control cadena de frio
- A: Administración
- VE: Vigilancia epidemiológica
- SV: Seguimiento de vacunas
- SE: Secretaria

Nombre equipo	Puerto	Distancia (metros)	Roseta	Jack	RJ45
Vigilancia epidemiológica					
PAIP1-M1-C	1	18	1	1	**VE-1**
PAIP1-M2-C	2	15	1	3	**VE-2**
PAIP1-I1-C	3	10	1	2	**VE-3**
Secretaria					
PAIP1-M3-C	4	14	2	1	**SE-1**
TELEFONO-11	5	13	2	2	**SE-2**
Logística de datos					
PAIP1-M4-C	6	17	3	1	**LD-1**
PAIP1-M5-C	7	20	3	2	**LD-2**

PAIP1-I2	8	16	3	3	**LD-3**
AP-2	9	16			
Control cadena de frio					
PAIP1-M6-C	10	19	4	3	**CCF-1**
PAIP1-M7-C	11	11	4	2	**CCF-2**
TELEFONO-10	12	14	4	1	**CCF-3**
Administración					
PAIP1-M8-C	13	10	5	3	**A-1**
PAIP1-M9-C	14	12	5	1	**A-2**
PAIP1-M10-C	15	17	5	4	**A-3**
PAIP1-I3-C	16	23	5	2	**A-4**
Seguimiento de vacunas					
PAIP1-M11-C	17	13	6	1	**SV-1**
PAIP1-M12-C	18	19	6	4	**SV-2**
PAIP1-M13-C	19	25	6	3	**SV-3**
PAIP1-I4-C	20	25	6	2	**SV-4**
Vacunatorio					
PAIPB-M14-C	21	14	7	1	**V-1**
Coordinación de estrategias					
PAIPB-M15-C	22	30	8	4	**CE-1**
PAIPB-M16-C	23	20	8	2	**CE-2**
PAIPB-M17-C	24	19	8	1	**CE-3**
PAIPB-I5-C	25	32	8	3	**CE-4**
Sala información					
PAIPB-M18-C	26	10	9	1	**SI-1**
TELEFONO-8	27	10	9	2	**SI-2**
Recursos humanos					
PAIPB-M19-C	28	19	10	1	**RH-1**
PB-I6-C	29	14	10	2	**RH-2**
Investigación y análisis					
PAIPB-M20-C	30	9	11	2	**IA-1**
PAIPB-M21-C	31	19	11	1	**IA-2**
TELEFONO-9	32	19	11	3	**IA-3**
Planeamiento					
PAIPB-M22-C	33	24	12	2	**P-1**
PAIPB-M23-C	34	21	12	4	**P-2**
PAIPB-M24-C	35	14	12	1	**P-3**
PAIPB-I7-C	36	18	12	3	**P-4**

Tabla 24. Medidas del cableado SEDES

III.1.2.3.5.3.- Abreviaturas para SEDES

- Dirección tecnica
- Unidad administrativa financiera

- Unidad asesoría juridica
- Unidad planificación y proyectos
- Secretaria
- Recursos humanos
- Unidad redes de servicios de salud
- Unidad epidemiológica e investigación
- Área seguros públicos de salud
- Unidad promoción de la salud
- AIEPI
- Área sistemas
- Gerencia salud sexual y reproductiva
- Administración

Nombre equipo	Puerto	Distancia (metros)	Roseta	Jack	RJ45
Dirección técnica					
SED-M1-A	1	10	1	3	**DT-1**
SED-M2-A	2	7	1	1	**DT-2**
SED-M3-A	3	15	1	2	**DT-3**
SED-I1-A	4	6	1	4	**DT-4**
Unidad administrativa financiera					
SED-M4-A	5	39	2	2	**AF**
SED-M5-A	6	31	2	3	**AF**
SED-M6-A	7	15	2	1	**AF**
TELEFONO-6	8	14	2	4	**AF**
Unidad asesoría jurídica					
SED-M7-A	9	16	3	2	**AJ**
SED-I2-A	10	10	3	1	**AJ**
TELEFONO-7	11	12	3	3	**AJ**
Unidad planificación y proyectos					
SED-M8-A	12	15	4	1	**PP**
SED-M9-A	13	22	4	2	**PP**
Administración					
SED-M10-A	14	10	5	1	**A**

SED-I3-A	15	14	5	2	**A**
Secretaria					
SED-M11-A	16	10	6	1	**S**
SED-I4-A	17	10	6	2	**S**
Recursos humanos					
SED-M12-A	18	26	7	3	**RH**
SED-M13-A	19	33	7	1	**RH**
SED-I5-A	20	16	7	2	**RH**
TELEFONO-2	21	13	7	4	**RH**
Unidad redes de servicios de salud					
SED-M14-B	22	39	8	1	**SS**
SED-M15-B	23	21	8	3	**SS**
SED-M16-B	24	23	8	4	**SS**
SED-I6-B	25	16	8	2	**SS**
AP-0	**26**	**73**			
SNIS-VE					
SED-M17-B	27	33	9	1	**SN**
SED-M18-B	28	19	9	3	**SN**
SED-I7-B	29	13	9	2	**SN**
TELEFONO-5	30	15	9	4	**SN**
Unidad redes de servicios de salud					
SED-M19-B	31	11	10	1	**RS**
SED-M20-B	32	19	10	2	**RS**
SED-I8-B	33	12	10	3	**RS**
Unidad epidemiológica e investigación					
SED-M21-B	34	6	11	1	**EI**
TELEFONO-1	35	9	11	2	**EI**
Área seguros públicos de salud					
SED-M22-B	36	11	12	1	**SP**
SED-M23-B	37	21	12	3	**SP**
SED-M24-B	38	34	12	4	**SP**
SED-I9-B	39	19	12	2	**SP**
Área sistemas					
SED-M25-B	40	17	13	3	**AS**
SED-M26-B	41	21	13	1	**AS**
SED-I10-B	42	13	13	2	**AS**
TELEFONO-3	43	12	13	4	**AS**
AP-1	44	67			
TOTAL		868			

Tabla 25. Tabla de medidas del PAI

III.1.2.3.6.- Diseño de la red a implementar

Primeramente, indicamos la cantidad de máquinas y dispositivos que se utilizaran para el diseño de la implementación

SEDES:

- 26 equipos de escritorio
- 4 portátiles
- 10 impresoras
- 3 switch
- 2 Access point
- 1 interface router
- 1 transceiver
- 1 servidor

PAI:

- 24 equipos de escritorio
- 2 laptops
- 7 impresoras
- 2 switch
- 1 access point
- 1 transceiver

Serán distribuidos de la siguiente manera:

SEDES cuenta con 1 router 1 servidor 4 switchs, 2 Access point 1 transceiver y 26 equipos de escritorio 4 laptops y 10 impresoras

La planta baja del PAI cuenta con 11 equipos de escritorio 1 laptop y 3 impresoras

La primera planta del PAI cuenta con 2 switch 1 transceiver 13 equipos 1 laptop y 4 impresoras

En la simulación del diseño primeramente se configurara lo que es el centro de datos en SEDES con el router el servidor y los Access point y se utilizara las IPs desde la 192.168.1.1 hasta las 192.168.1.5 también se mostrará a SEDES con los 26 equipos de escritorio 4 laptops y 10 impresoras que serán configuradas para obtener una dirección IP por medio de DHCP la cual tendrá la dirección 192.168.1.5 y la asignación de IPs varía dependiendo cada vlan en la planta baja del PAI con los 11 equipos de escritorio 1 laptop y 3 impresoras las cuales configuraremos para que tengan una dirección IP por medio del servidor DHCP y dicha IP iniciara desde la 192.168.100.2, la primera planta del PAI con el access point los 13 equipos 1 laptop y 4 impresoras también obtendrán una dirección IP por medio de DHCP los Access point servirán para los dispositivos inalámbricos

III.1.2.3.6.1.- Diseño de la conexión de la red

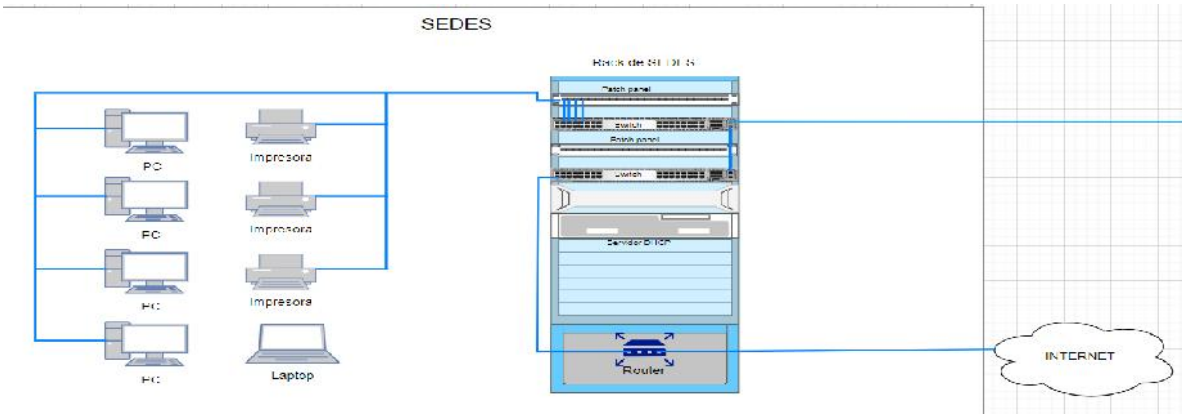


Figura 83. Diseño de la conexión de la red en SEDES

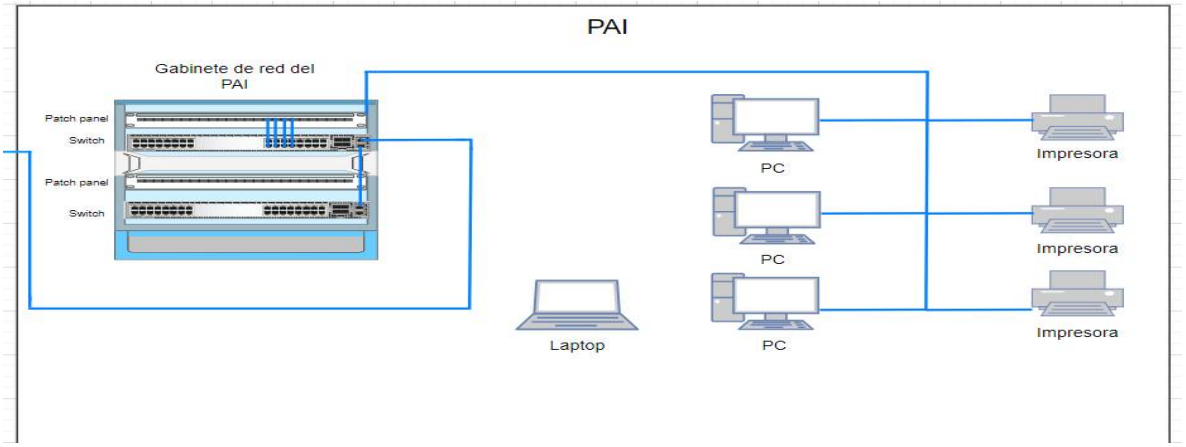


Figura 84. Diseño de la conexión de la red en PAI

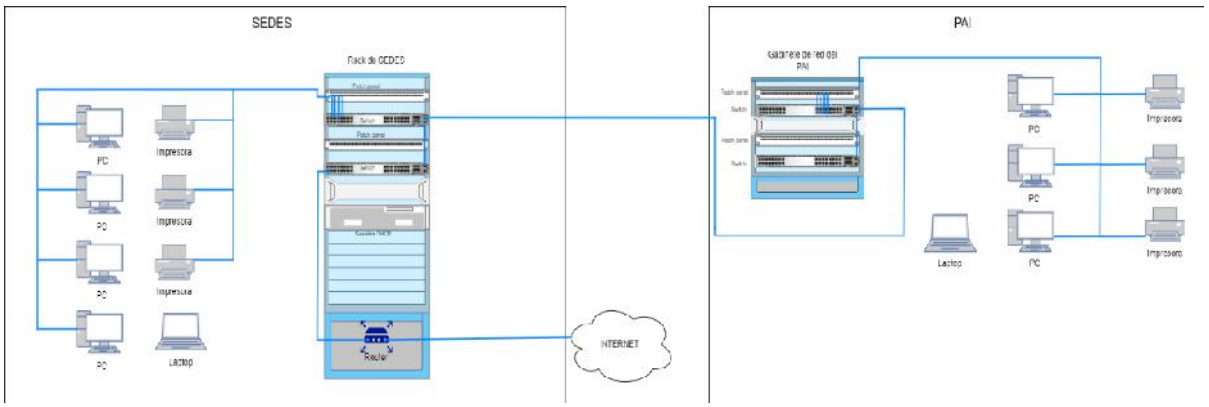


Figura 85. Diseño de la conexión de la red en SEDES y PAI

III.1.2.3.6.5.- Diseño de la conexión del rack en SEDES

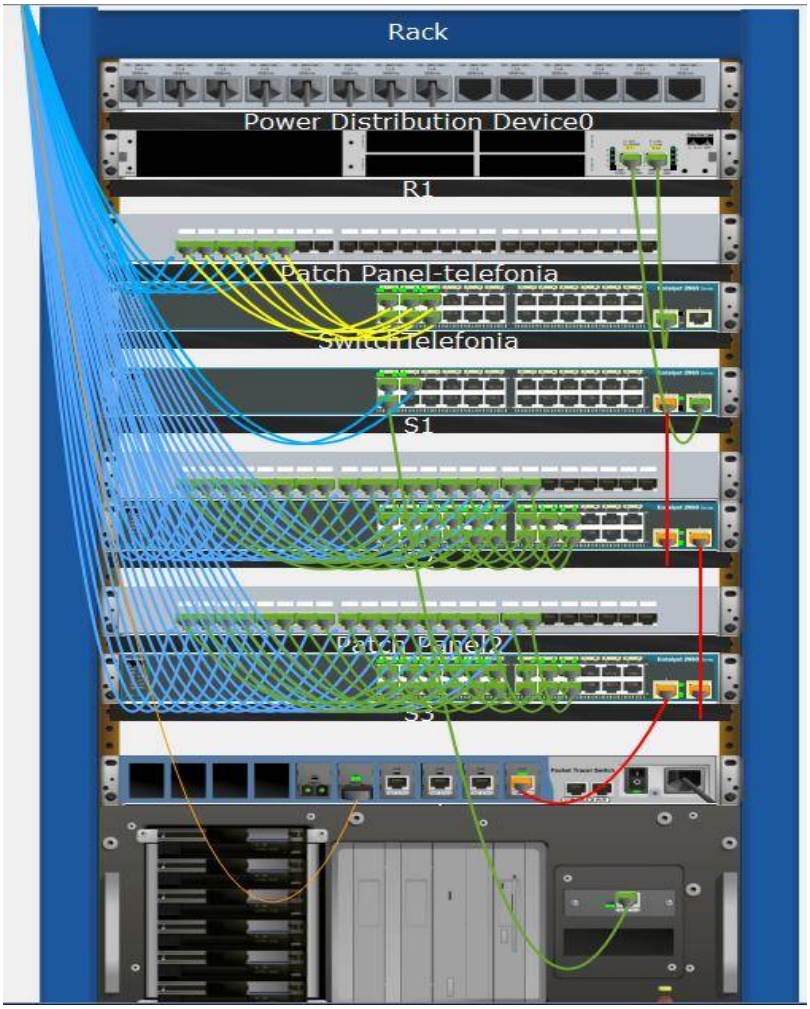


Figura 86. Diseño de la conexión del Rack en SEDES

III.1.2.3.6.6.- Diseño de la conexión del gabinete en PAI

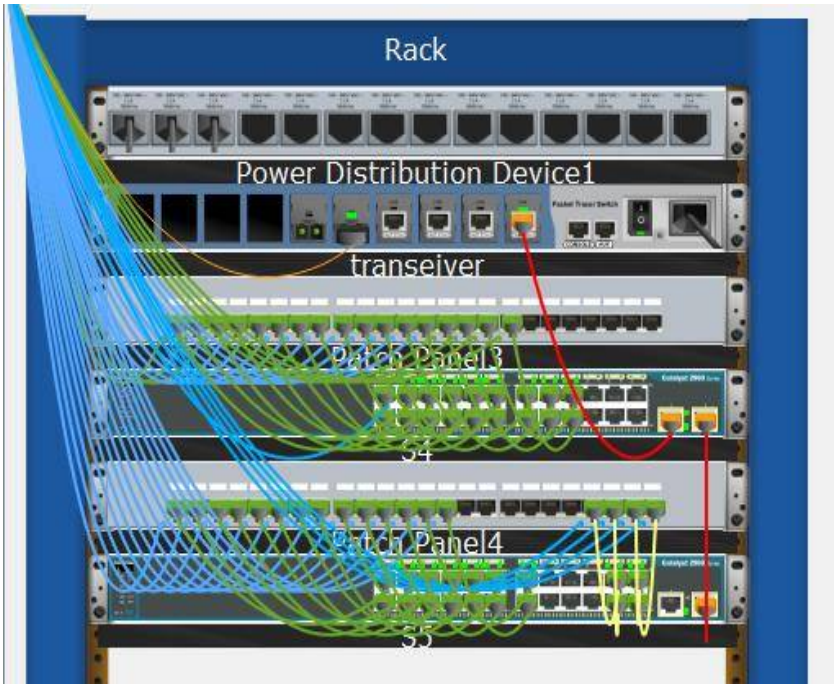


Figura 87. Gabinete ubicado en el PAI

III.1.2.3.7.- Diseño de seguridad física

III.1.2.3.7.1.- Sistema de prevención de incendios

Se diseñó un sistema de alarmas contra incendios con el objetivo de cubrir las necesidades de seguridad de la institución el cual cuentan con sensores de humo, detector de calor extinguidor, botón de pánico y panel de control.

El sistema trabaja de manera automática para la detección de eventos que puedan ocasionar un incendio, reciben una señal directamente desde el detector y logran pasarla al panel de control para que posteriormente el panel active el mecanismo de alarma

Tenemos n ambientes para los cuales utilizaremos n alarmas y n botones de pánico para el panel de control

La instalación de cada sensor se va realizar de acuerdo a la norma NFPA 72 con una separación de 12,8 metros la instalación de los pulsadores se realizará a una altura máxima de 1,5 metros en relación al piso. Las cuáles serán distribuidas en el área protegida de forma que no tengan ninguna obstrucción y sean de fácil acceso serán ubicadas en las salidas de cada bloque la separación entre estaciones manuales no debe superar los 61 metros medidos horizontalmente en el mismo piso

III.1.2.3.7.2.- Elementos

Sensor

Bosch D-273TH

Figura 92. Sensor

Funciona con sistemas comerciales de señalización de protección contra incendios y con sistemas domésticos de aviso de incendio. Detecta las partículas de humo producidas durante la combustión de madera, papel y tejidos usando una fuente de luz LED infrarroja (IR) y un fotodiodo de silicona para medir la luz en una cámara, cuando las mediciones del fotodiodo superan el umbral de alarma, el detector emite una señal que indica la presencia de una condición de alarma. Una delgada pantalla cubre la cámara para impedir el ingreso de insectos y reducir la acumulación de polvo, y así minimizar las falsas alarmas.

- Marca BOSCH
- D273TH Cuatro cables con sensor térmico de 57 °C (135 °F)

- Entrada de 12 VCC o 24 VCC
- Diseñados para el uso comercial o residencial
- Aplicación de cuatro cables
- Diodos electroluminiscentes (LED) que indican el estado de la cámara, la alimentación y la alarma
- Bloque de terminales extraíble para simplificar las conexiones de cableado
- Consumo de corriente (alarma) a 30 VCC 18 mA máximo
- Dimensiones (diámetro x altura) 12,7 cm x 5,1 cm
- Material de plástico ABS retardante de fuego y resistente a altos impactos

Pulsador de pánico

marca: maadok

modelo: maa-pb101

botón de pánico SOS inalámbrico 433mhz

Características

- Frecuencia: 433 MHz
- Alcance 100-150 metros (área abierta)
- Indicador de alarma LED rojo
- Indicador de batería baja LED rojo
- Dimensiones: 40mm x 70mm x 18 mm
- Peso: 50 gramos

Figura 93. Pulsador de panico

Sirena

marca: stv

modelo: st-fs106

Características

- Energía: DC12V
- Nivel de sonido 110dB
- LED de alarma Brillante
- Corriente nominal 90 mA
- Dimensiones: 13.5*11.5*5cm
- Peso: 200 g

Figura 88. Sirena

Central

La central contra incendios debe cuenta con las siguientes características:

Central base de 1 bucles

- Permite conectar 44 puntos por bucle
- Todos los puntos de los bucles son supervisados
- Capacidad de hasta 64 relés configurables
- Permite la programación de 44 zona por bucle
- Historial que almacena hasta 4095 eventos con fecha y hora
- Salida supervisada retardable de sirena general identificada como sirena
- Salida de alarma libre de tensión no supervisada identificada como Alarma
- Salida supervisada retardable de avería general identificada como Avería
- Pulsador de evacuación
- Display LCD retroiluminado de 4 líneas y 40 caracteres
- Incorpora tres idiomas por defecto
- Configurable y manejable mediante software
- Permite la conexión de hasta 15 repetidores
- Protección IP30
- Incluye dos baterías de 12v 7Ah

Figura 95. Central

Extintores

Los extintores son dispositivos portátiles especialmente diseñados para poder ser desplazados y extinguir un fuego en cualquier lugar. Los extintores suelen tener una masa de 20 kilos o incluso menor. Según la normativa los extintores deben ser rojos para facilitar su localización e identificación.

Los extintores deben estar colocados a una altura adecuada de forma que, como máximo, la parte superior del extintor esté situada a 1’20 metros del suelo. Deben estar debidamente señalizados con una señal homologada, y su vida útil ronda los 20 años.

Los extintores deben contar con un dispositivo de seguridad para evitar que se disparen de forma automática.

Figura 96. Extintor

III.1.2.3.7.3.- Requerimiento de sistema de prevención de incendios

Distribución de elementos de sistema de prevención de incendios

Bloque	Pulsadores	Sirenas	Sensores
Importaciones bloque abajo	4	4	6
Importaciones bloque alto	3	2	2

Tabla 26. Sistema de prevención de incendios

III.1.2.3.7.4.- Planos sistema de prevención de incendios

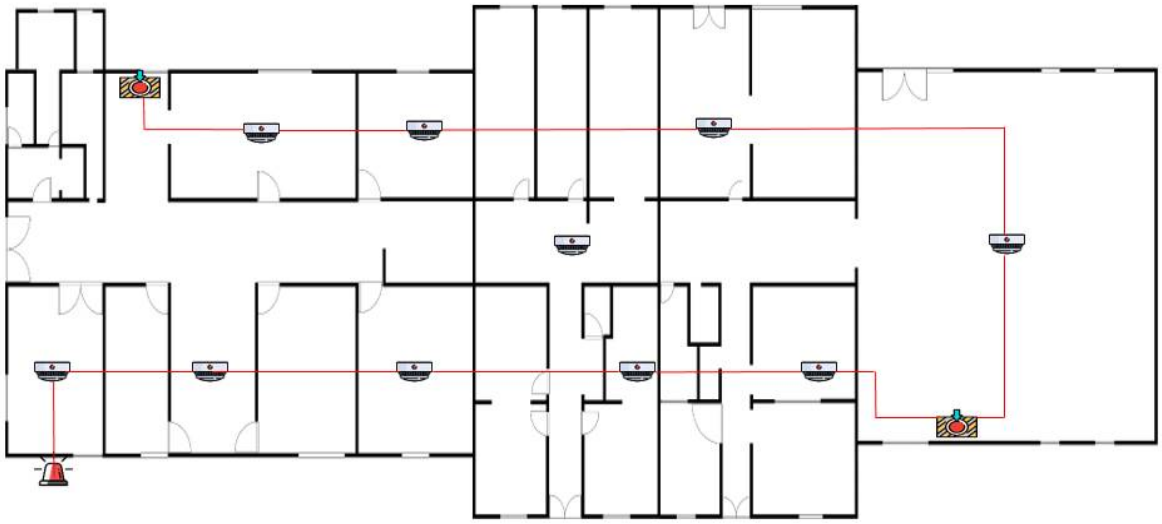


Figura 97. Sistema de prevencion SEDES

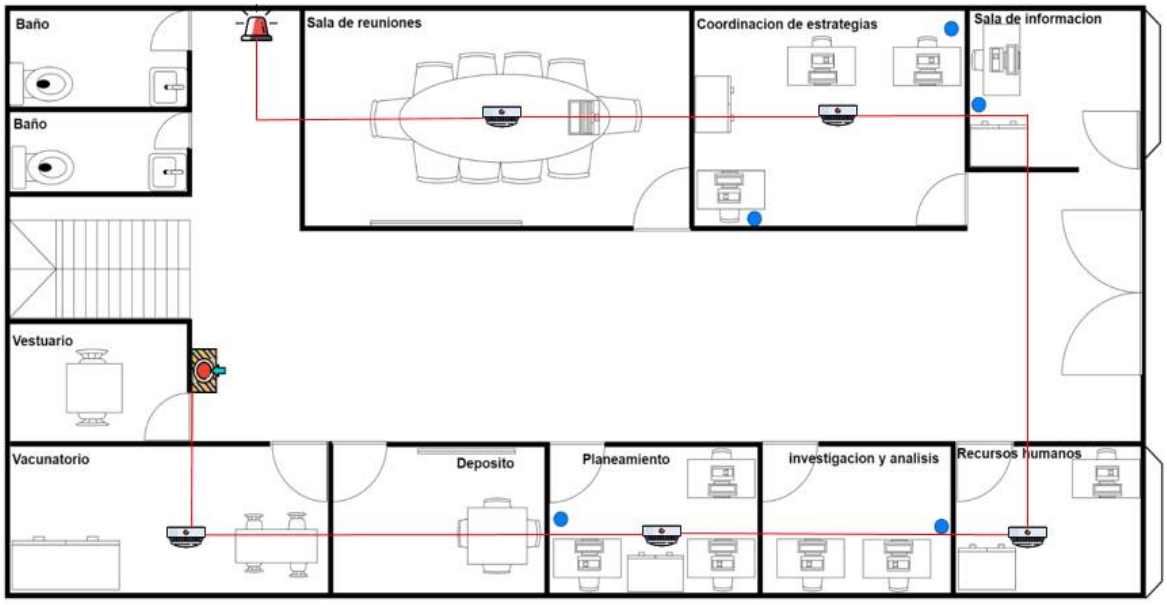


Figura 98. Sistema de prevención PAI planta baja

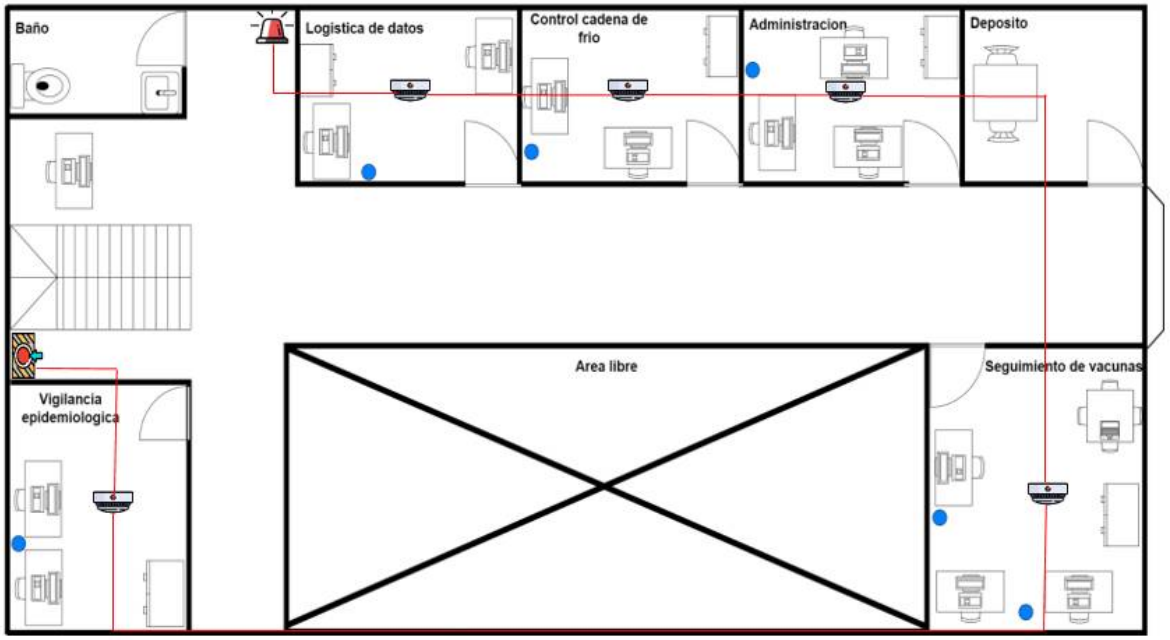


Figura 99. Sistema de prevención PAI primera planta

III.1.2.4.- Fase 4: Probar, optimizar y documentar el diseño

III.1.2.4.1.-Simulación del diseño

III.1.2.4.1.1.- Ubicación geográfica de la red de SEDES y PAI

Figura 100. Ubicación de las instituciones

III.1.2.4.1.2.- Diseño de la red de SEDES

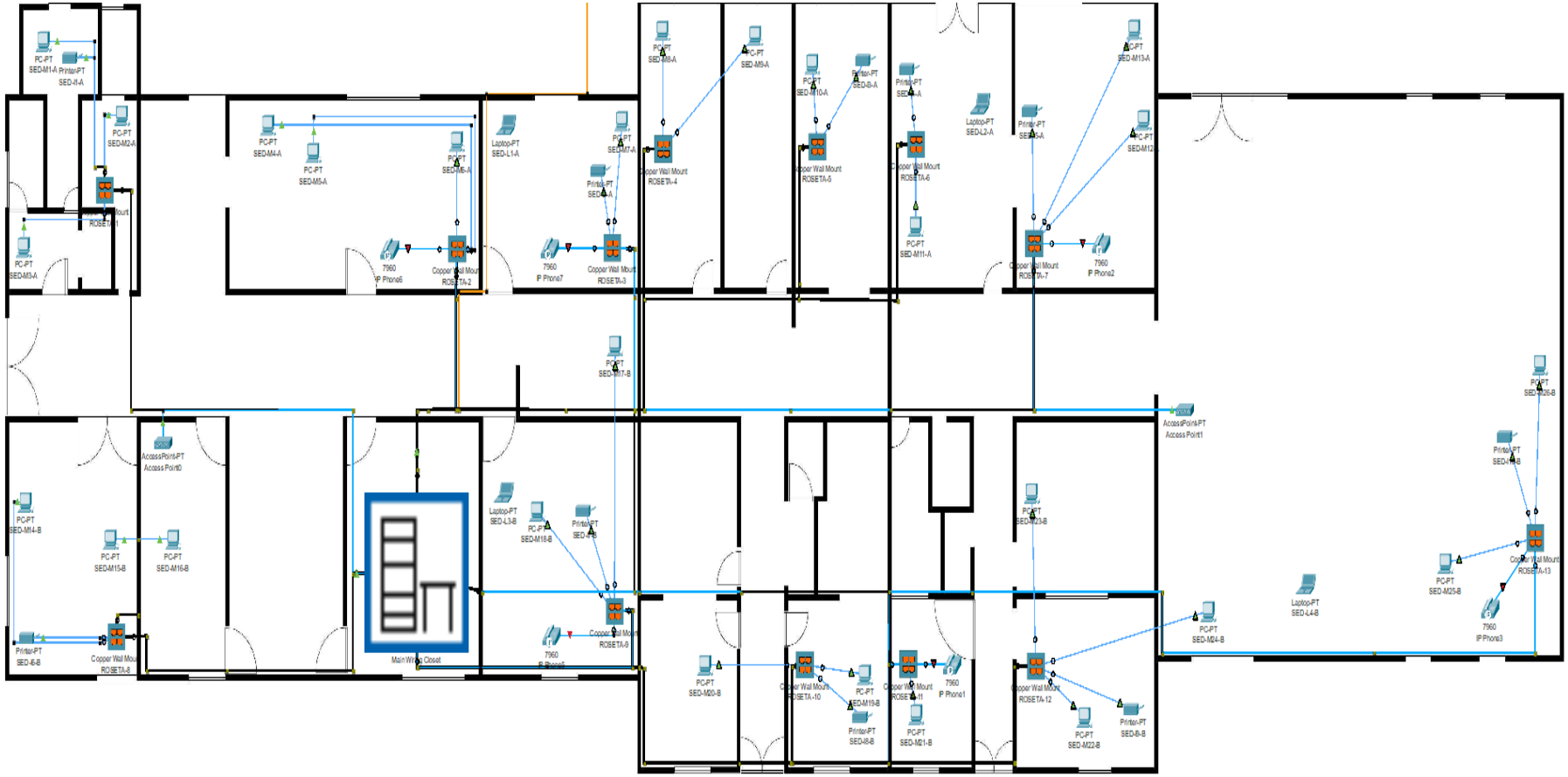


Figura 101. Estructura cableada de SEDES

III.1.2.4.1.3.- Diseño de la conexión del PAI

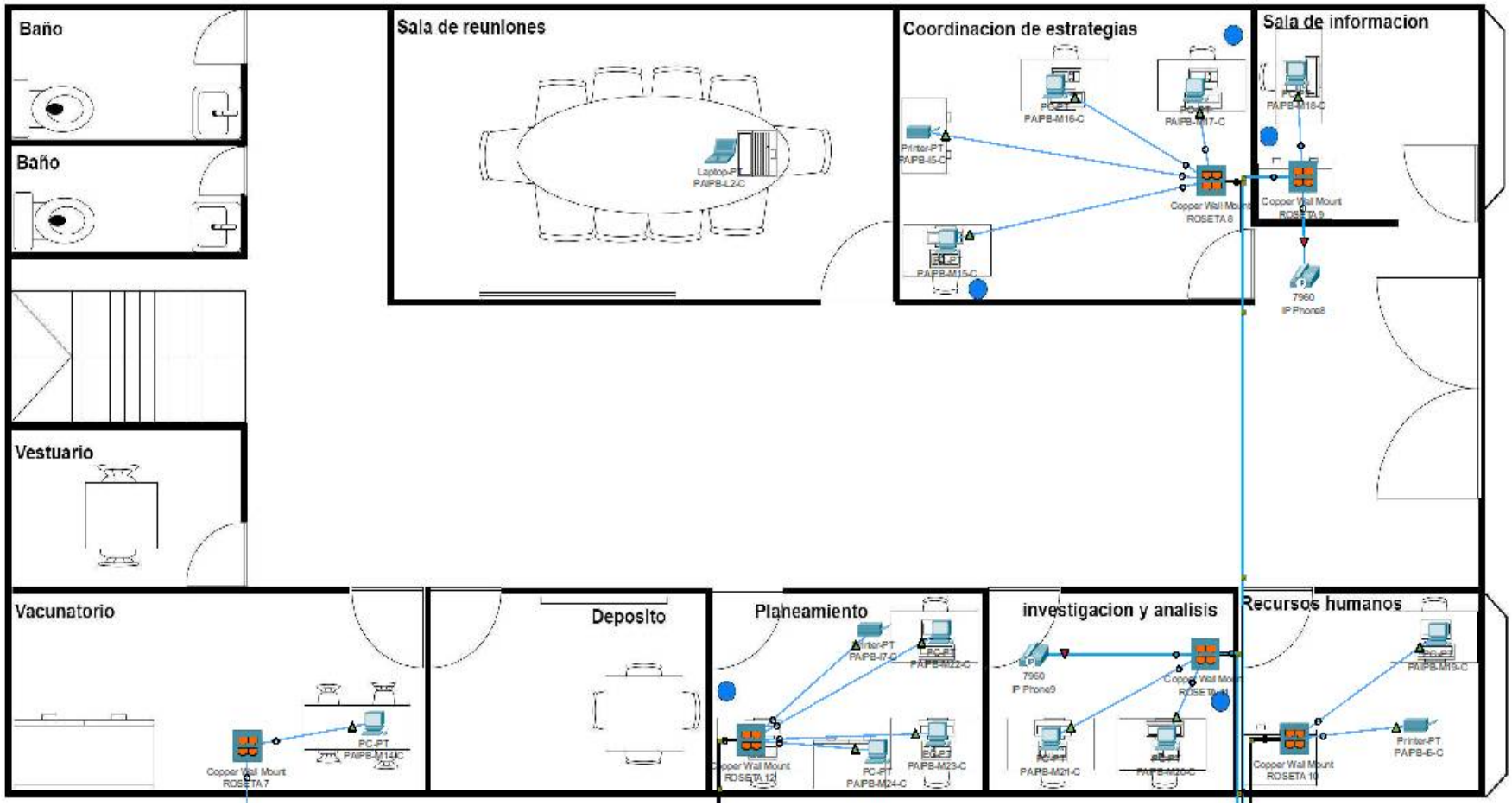


Figura 102. Estructura cableada PAI

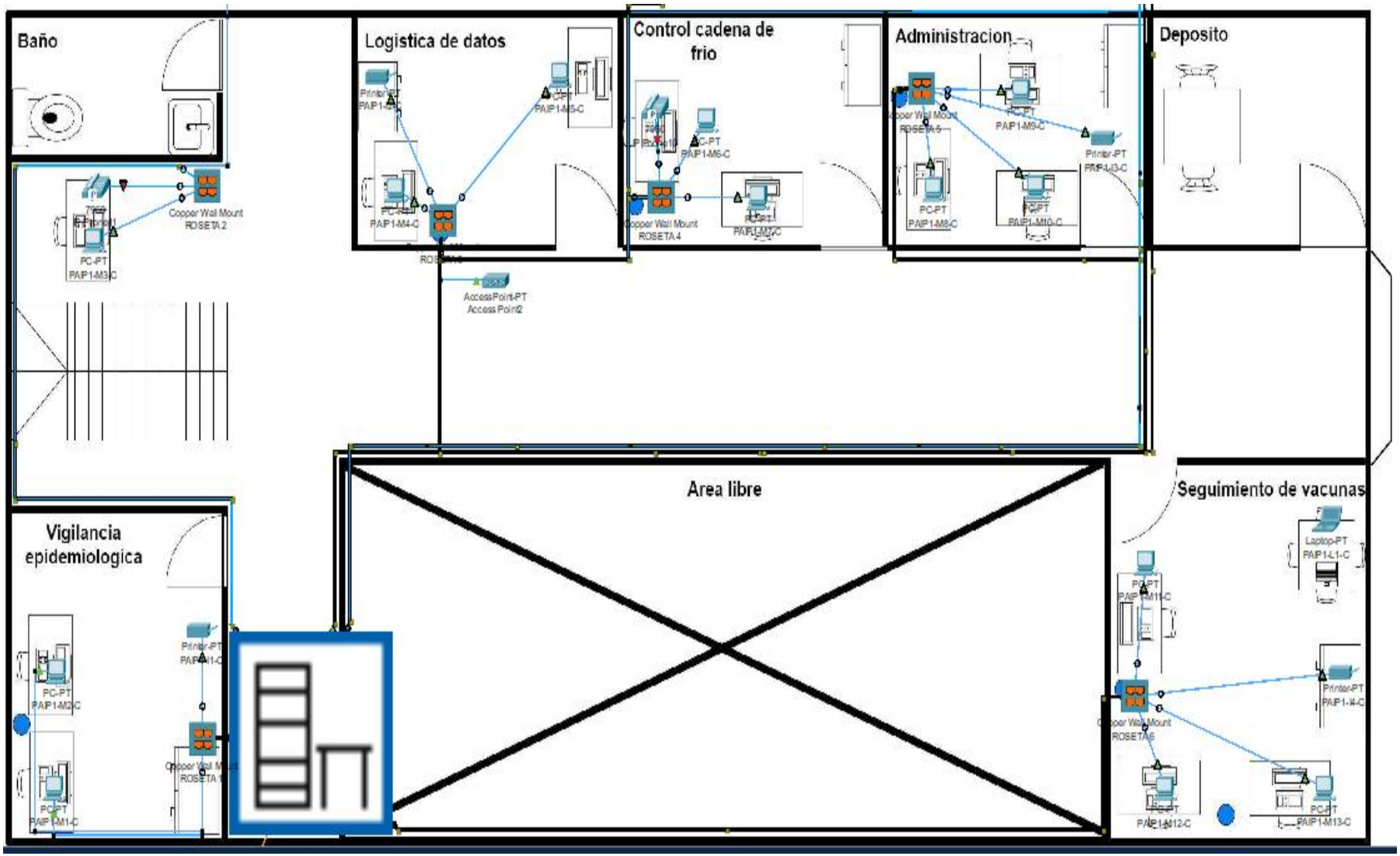


Figura 103. Estructura cableada y gabinete en PAI

En cuanto a la red inalámbrica se optó por cambiar el plan a uno de mayor megas en este caso el plan que se propone es el de 60 Mbp

III.1.2.4.1.4.- Nivel de señal en SEDES

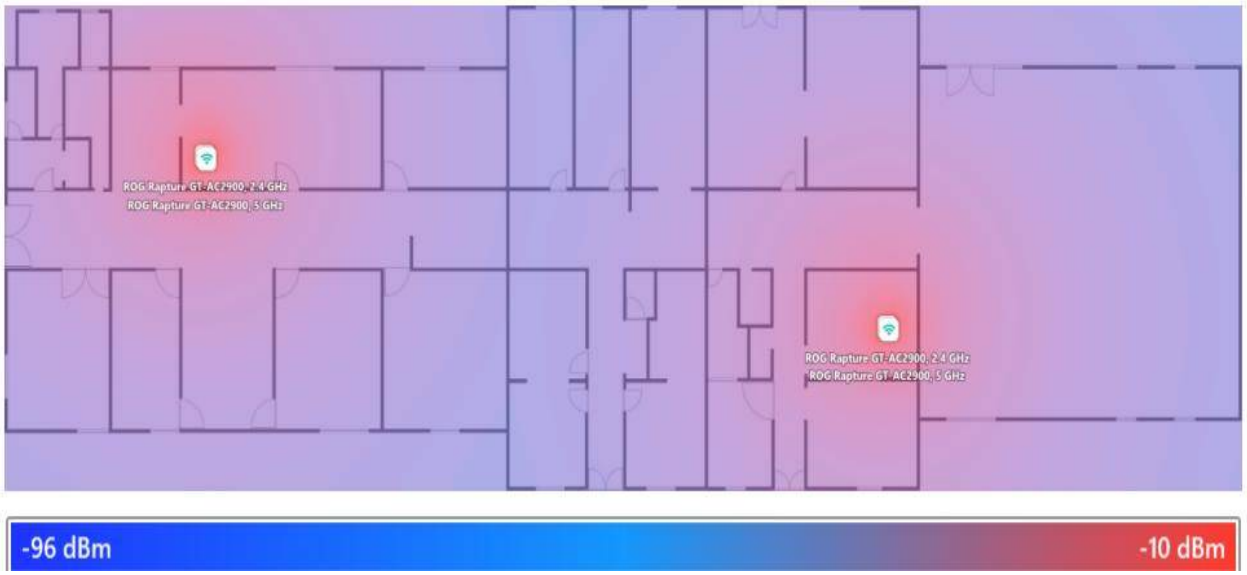


Figura 104. Nivel de señal nuevo SEDES

Nivel de señal mínimo: -96 dBm Nivel de señal máximo: -10dBm

#	Nombre de la red	Canal	PHY	Nivel de señal máximo	Fabricante
1	ROG Rapture GT-AC2900, 2.4 GHz	1 (2.4 GHz)	ax	20 dBm	ASUS
2	ROG Rapture GT-AC2900, 5 GHz	36 (5 GHz)	ax	20 dBm	ASUS
3	ROG Rapture GT-AC2900, 2.4 GHz	1 (2.4 GHz)	ax	20 dBm	ASUS
4	ROG Rapture GT-AC2900, 5 GHz	36 (5 GHz)	ax	20 dBm	ASUS

Nivel de señal bajo

Figura 105. Nivel de señal bajo nuevo SEDES

Nivel de señal mínimo: -70 dBm Nivel de señal máximo: -4

#	Nombre de la red	Canal	PHY	Nivel de señal máximo	Fabricante
1	ROG Rapture GT-AC2900, 2.4 GHz	1 (2.4 GHz)	ax	20 dBm	ASUS
2	ROG Rapture GT-AC2900, 5 GHz	36 (5 GHz)	ax	20 dBm	ASUS
3	ROG Rapture GT-AC2900, 2.4 GHz	1 (2.4 GHz)	ax	20 dBm	ASUS
4	ROG Rapture GT-AC2900, 5 GHz	36 (5 GHz)	ax	20 dBm	ASUS

Nivel de señal bajo 5GHz

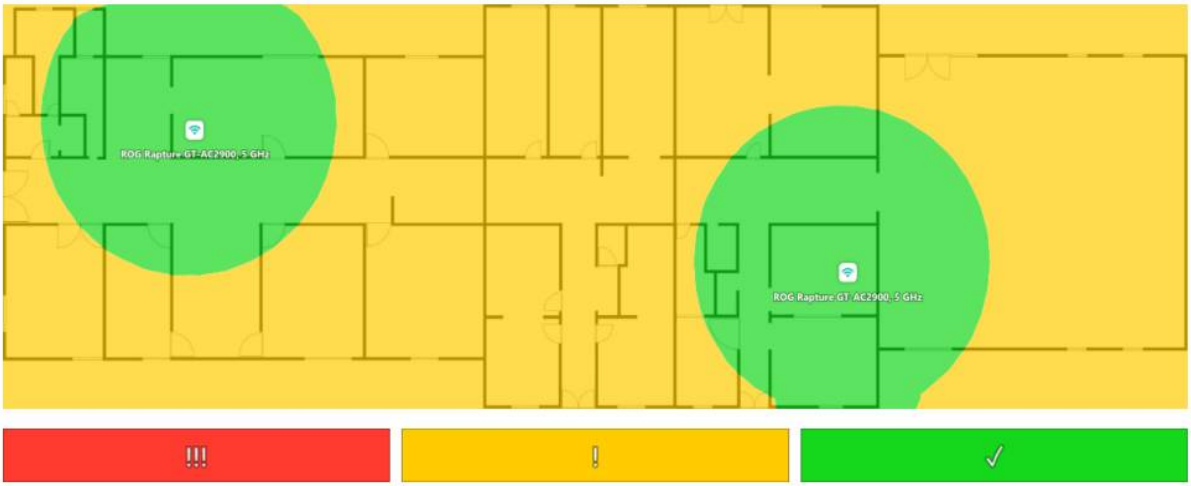


Figura 106. Nivel de señal 5GHz nuevo

Nivel de señal mínimo: -70 dBm Nivel de señal máximo: -40 dB

#	Nombre de la red	Canal	PHY	Nivel de señal máximo	Fabricante
1	**ROG Rapture GT-AC2900, 5 GHz**	36 (5 GHz)	ax	**20 dBm**	ASUS
2	**ROG Rapture GT-AC2900, 5 GHz**	36 (5 GHz)	ax	**20 dBm**	ASUS

III.1.2.4.2.- Configuración de los dispositivos

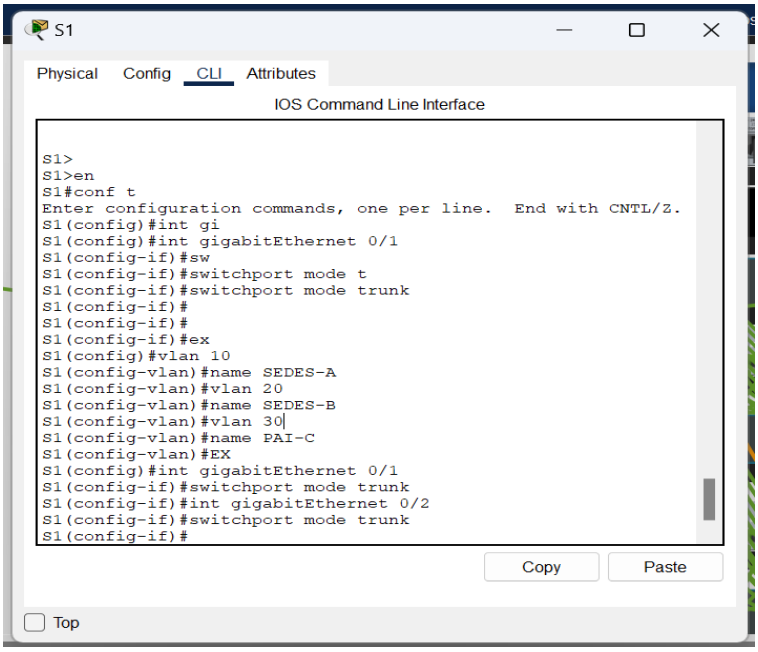


Figura 89. Configuración Switch 1

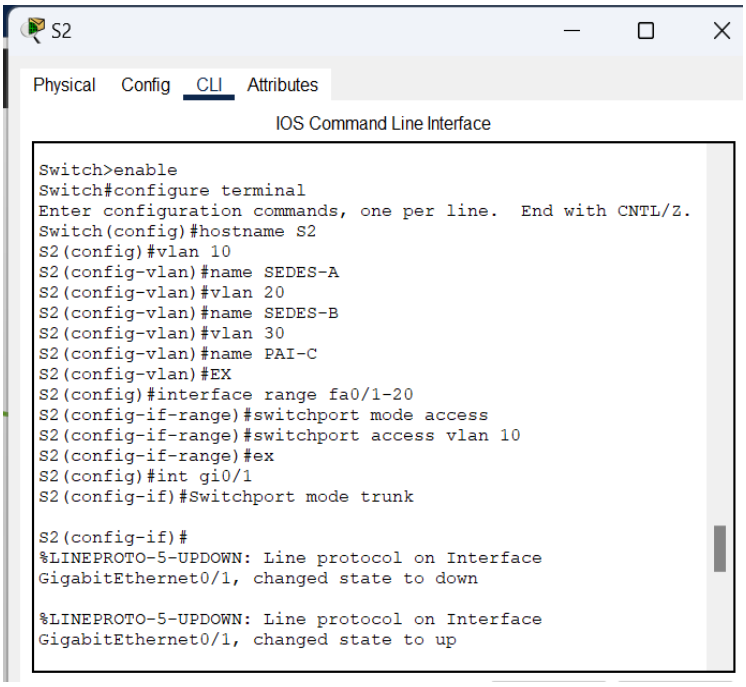


Figura 90. Configuración switch 2

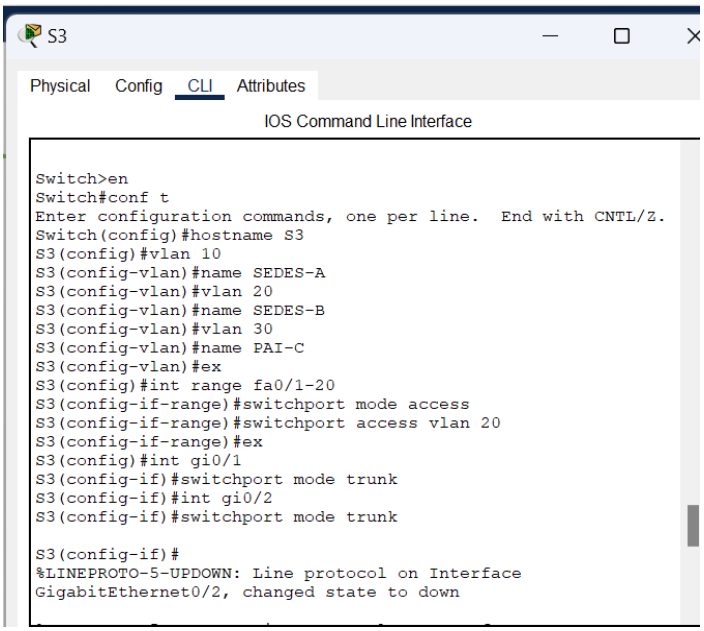


Figura 91. Configuración switch 3

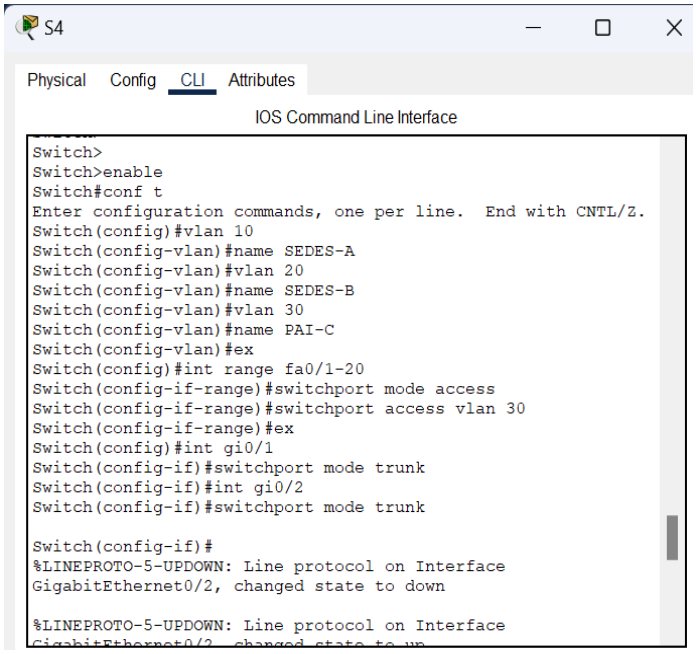


Figura 92. Configuración switch 4

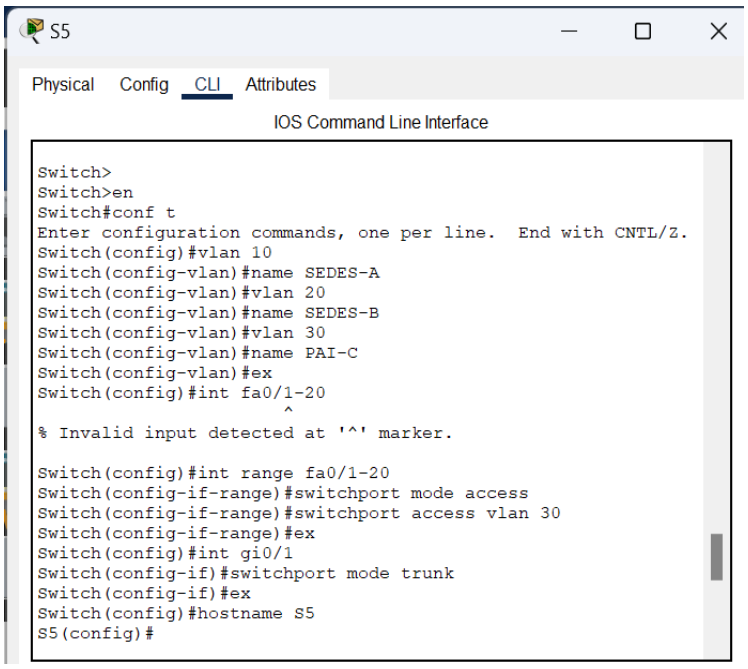


Figura 93. Configuración switch 5

III.1.2.4.2.1.- Configuracion del servidor para el DHCP

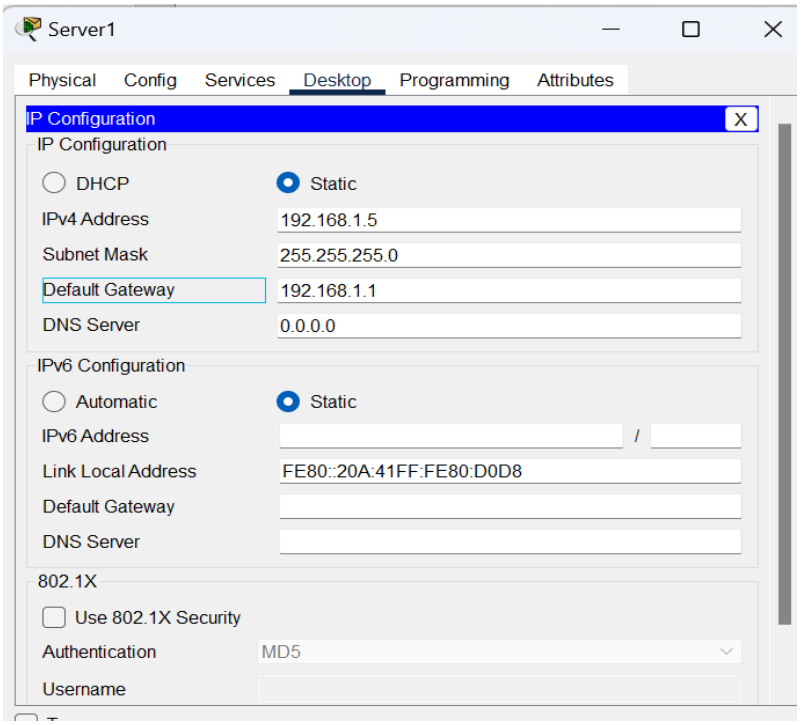


Figura 94. Configuración dirección IP del servidor

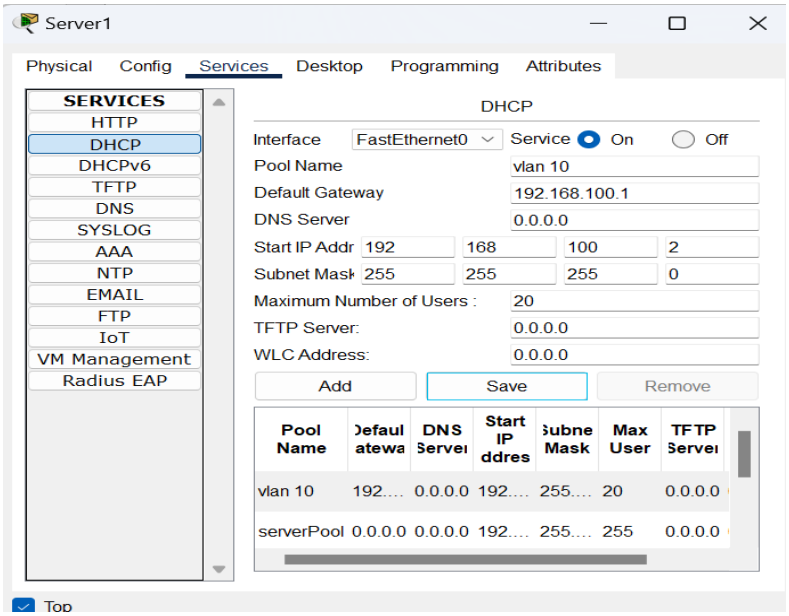


Figura 95. Configuración del DHCP para cada vlan

III.1.2.4.2.2.- Configuración del router para el encapsulamiento de las VLAN

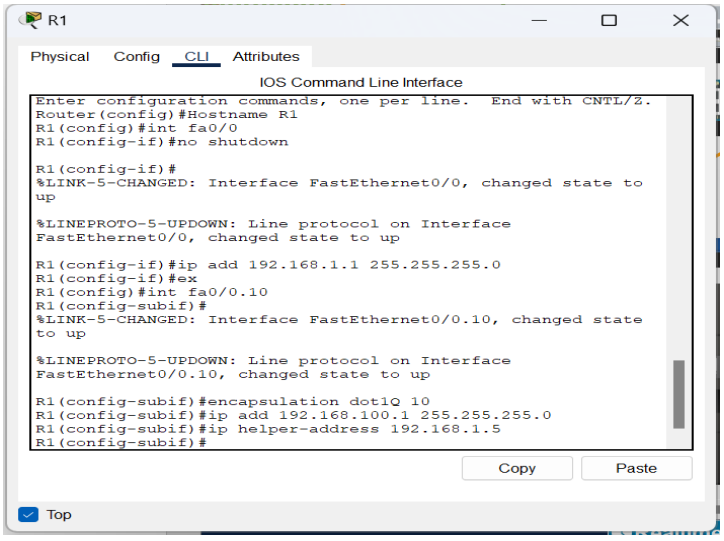


Figura 96. Configuración del router

III.1.2.4.2.3.- Configuración del bloqueo de comunicación entre vlans

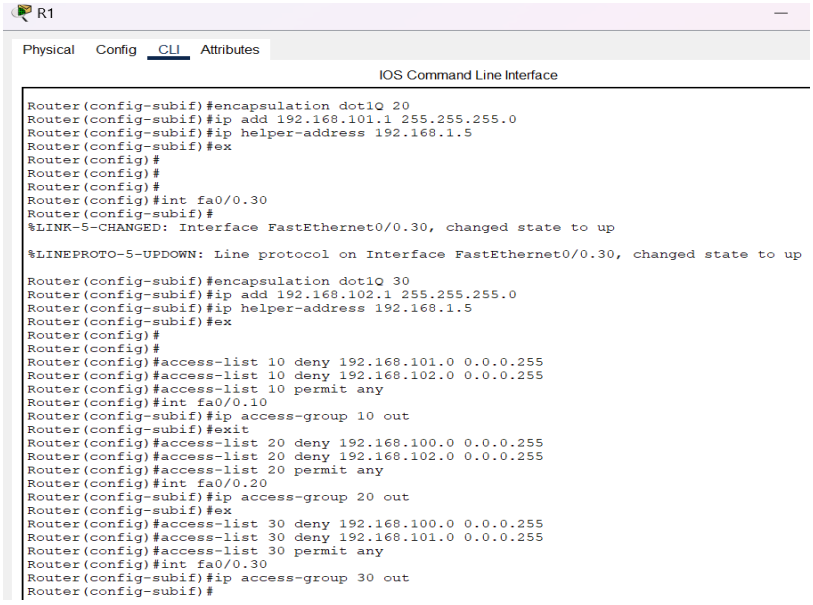


Figura 97. Bloqueo de VLANs

III.1.2.4.2.4.- Configuración del Access point para el acceso a la red de manera inalámbrica

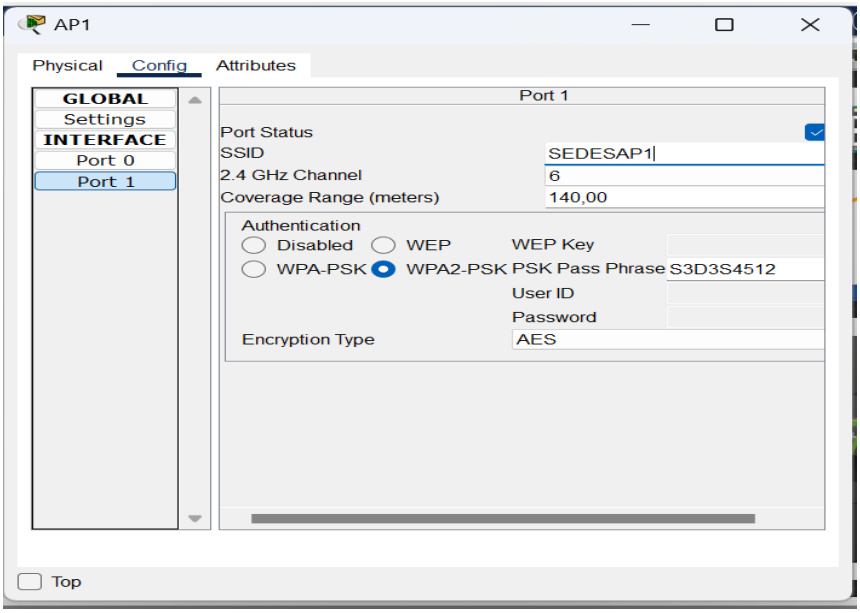


Figura 98. Configuración del Access point

III.1.2.4.2.5.- Configuración de la telefonía IP en el router

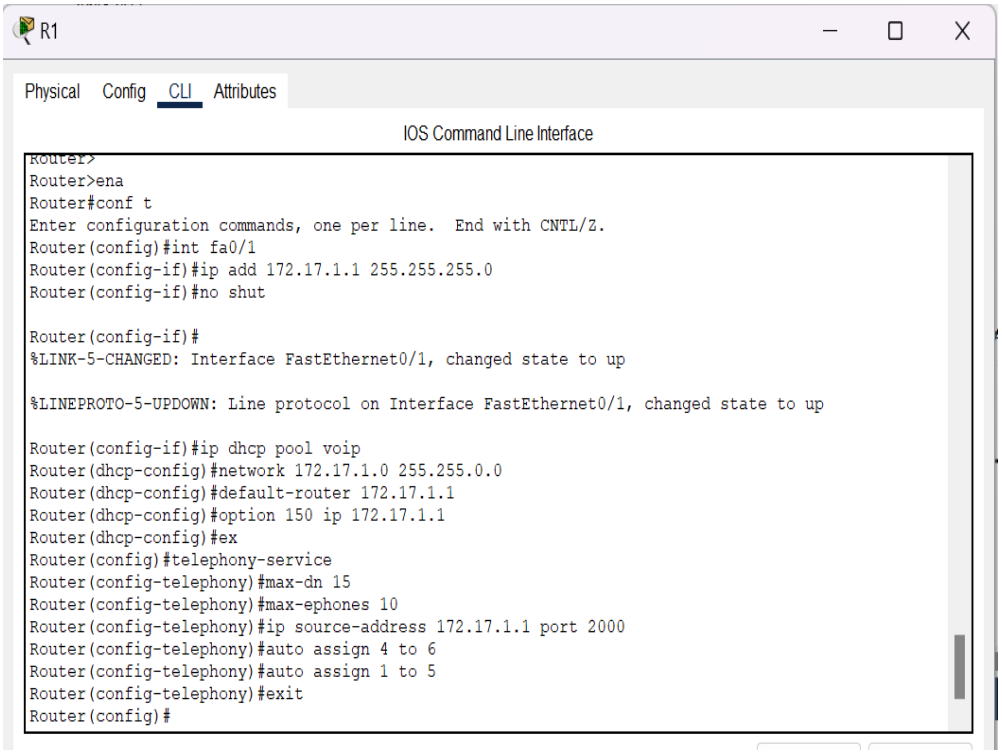


Figura 99. Configuracion VoIP

Figura 100. Asignacion de números e IPs

III.1.2.4.2.6.- Configuración de calidad de servicio QoS en el router

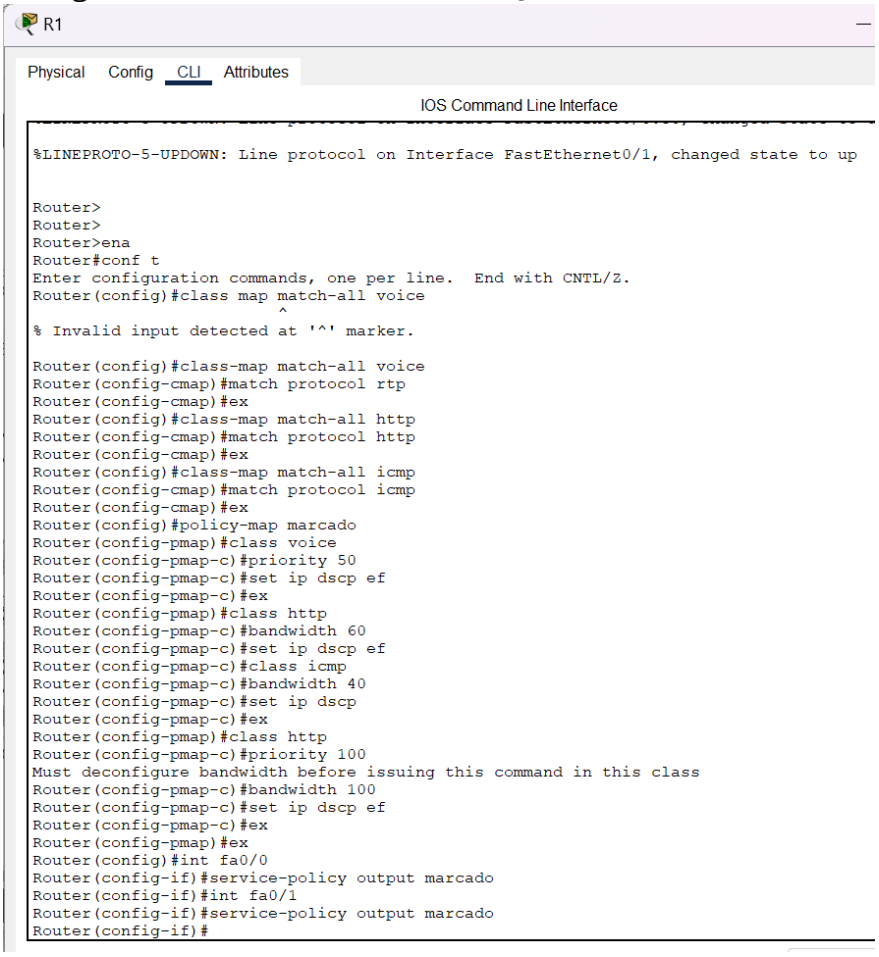


Figura 101. QoS

```
Router#
Router#
Router#show policy-map
  Policy Map marcado
    Class voice
      Strict Priority
      Bandwidth 50 (kbps) Burst 1250 (Bytes)
      set ip dscp ef
    Class http
      Bandwidth 100 (kbps) Max Threshold 64 (packets)
      set ip dscp ef
    Class icmp
      Bandwidth 40 (kbps) Max Threshold 64 (packets)
      set ip dscp default
Router#
Router#
```

Figura 102. Verificacion de la configuracion QoS

III.1.2.4.2.7.- Configuración del firewall Fortigate

III.1.2.4.2.7.1.-Diseño lógico

Figura 103. Diseño logico del firewall

Asignación de IP al Fortigate

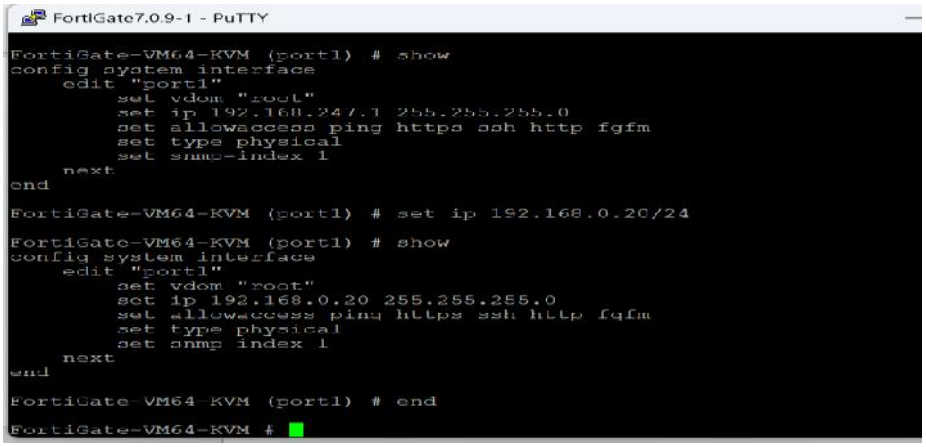


Figura 104. Asignación de dirección IP

Ingresamos a la interfaz grafica con la ip que asignamos

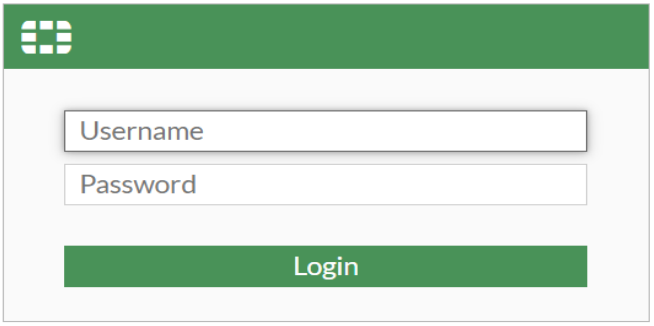


Figura 105. Interfaz gráfica de Fortigate

Configuramos el DHCP para poder configurar la red entramos a Network -> Interfaces

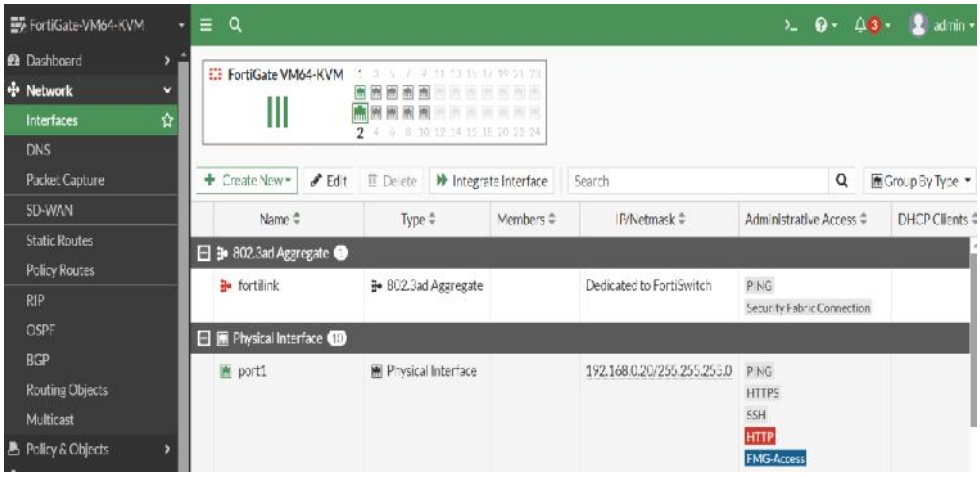


Figura 106. Configuración DHCP Fortigate

Ingresamos al puerto que conecta el Fortigate con el switch

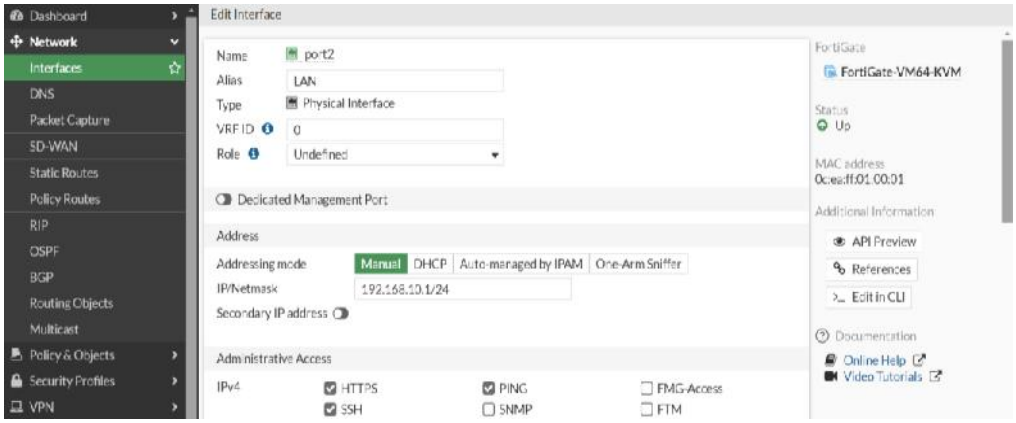


Figura 107. Configuración de la interfaz

Habilitamos el DHCP

Figura 108. rango de direcciones IP

Tenemos una IP externa y una interna

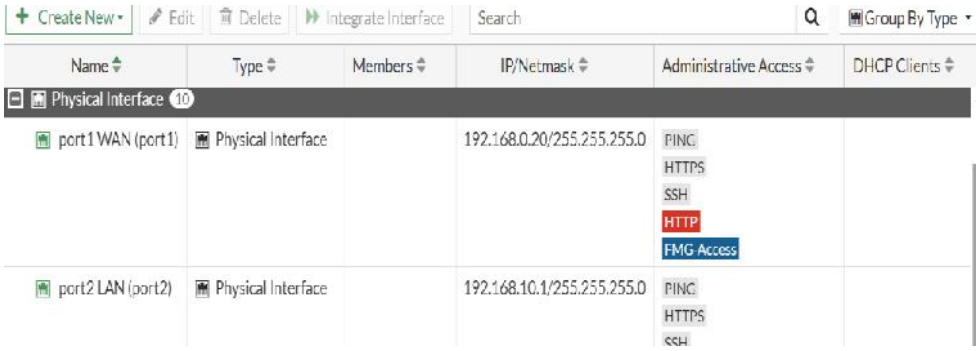
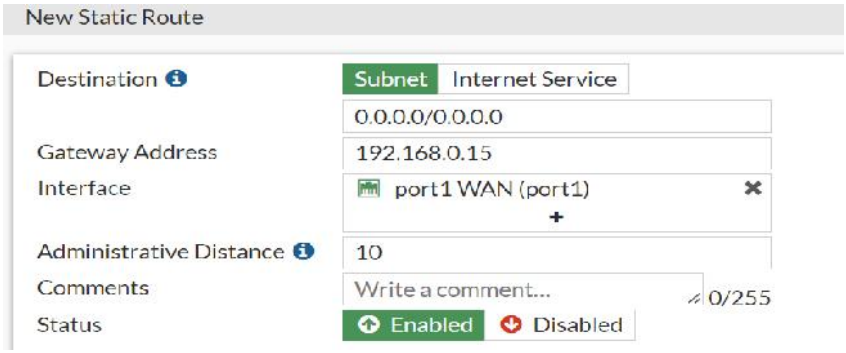


Figura 109. Interfaces físicas

Creamos una ruta estática



Ingresamos una nueva política en policy y object -> Crear addresses asignamos el rango de IPs que tendrán la política

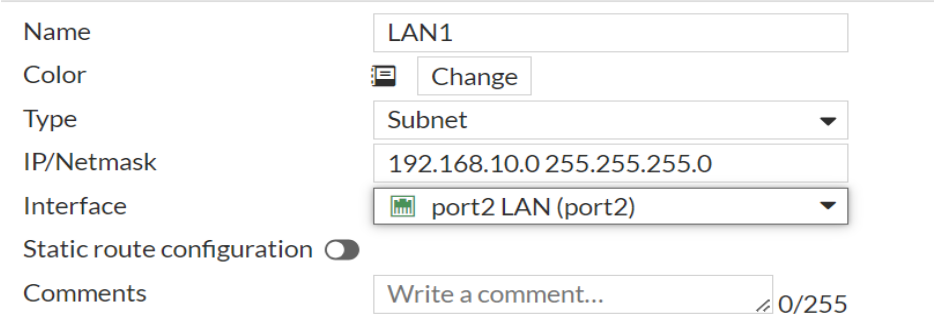


Figura 110. Configuración IP interna

Una vez asignado todas las configuraciones se tiene la siguiente pantalla

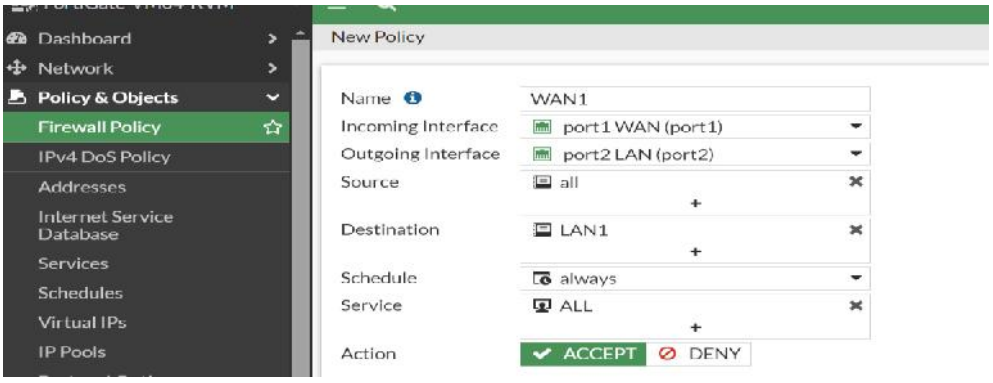


Figura 111. Configuración IP externa

Verificamos que se asigne las direcciones

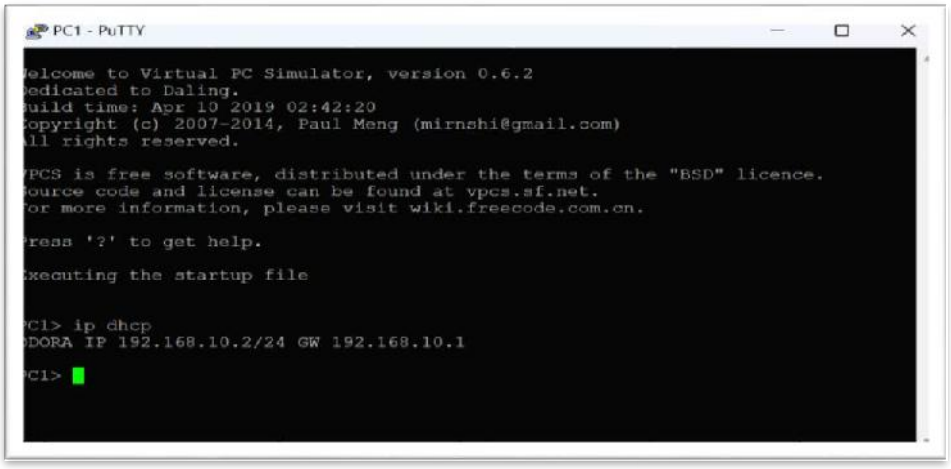


Figura 112. Asignación de dirección IP

Configuración para bloqueo de páginas web

Creamos una nueva política

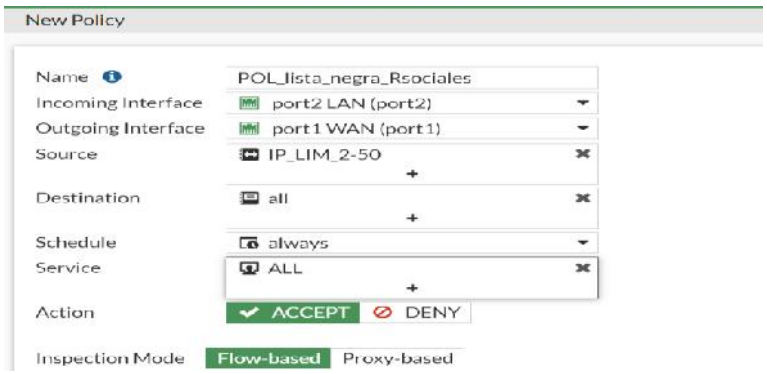


Figura 113. Política lista de bloqueo

Rango de IPs que tendrán bloqueadas las paginas

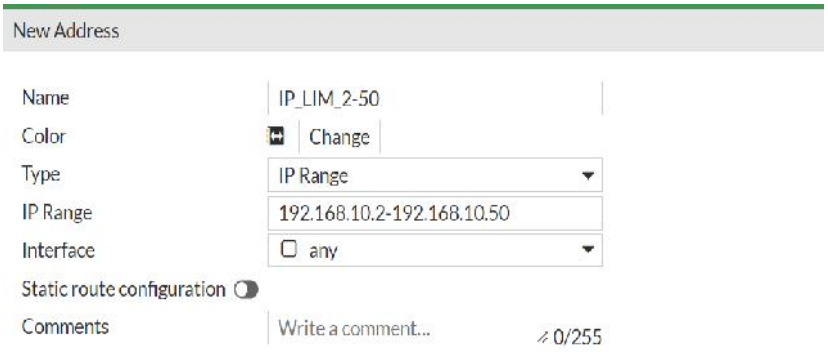


Figura 114. Lista negra de bloqueo de paginas

Previo esto debemos crear las reglas en security profiles el web filter y aplication control

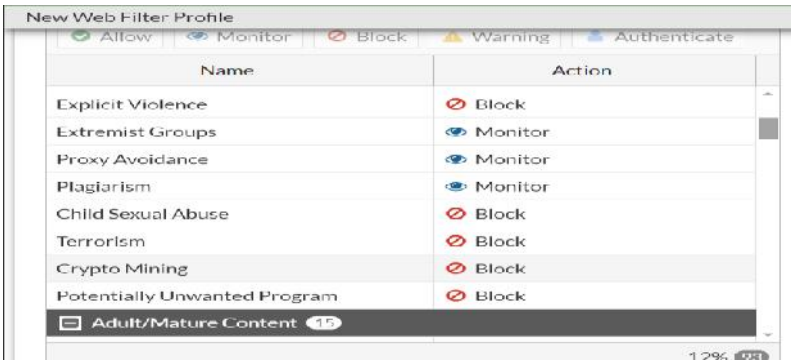


Figura 115. configuracion web filter

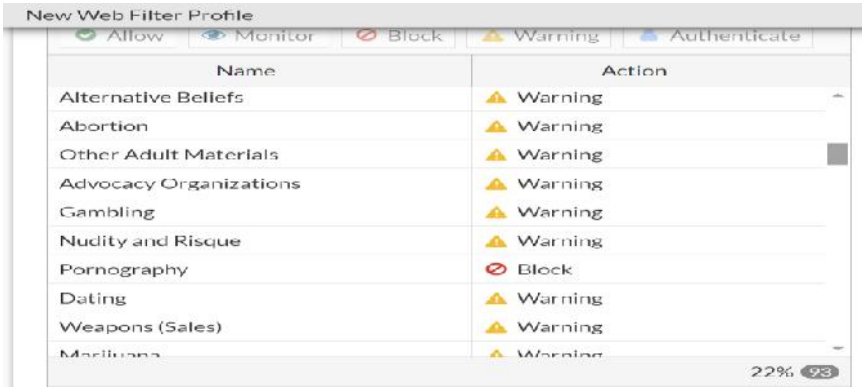


Figura 116. Configuración web filter

Realizamos el bloqueo por URL

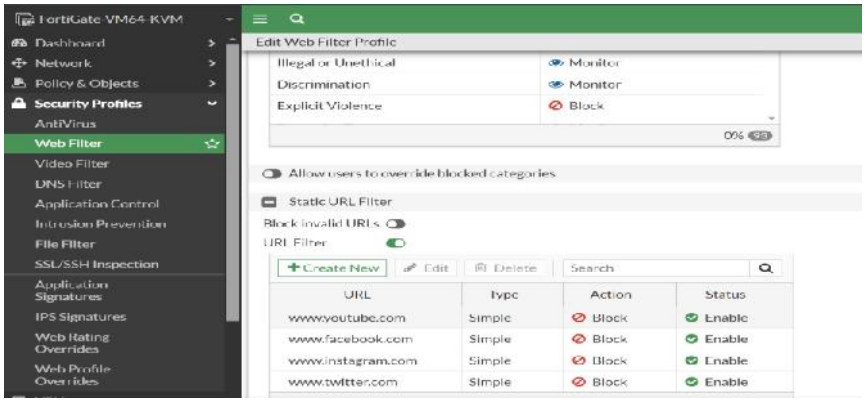


Figura 117. Bloqueo de URLs

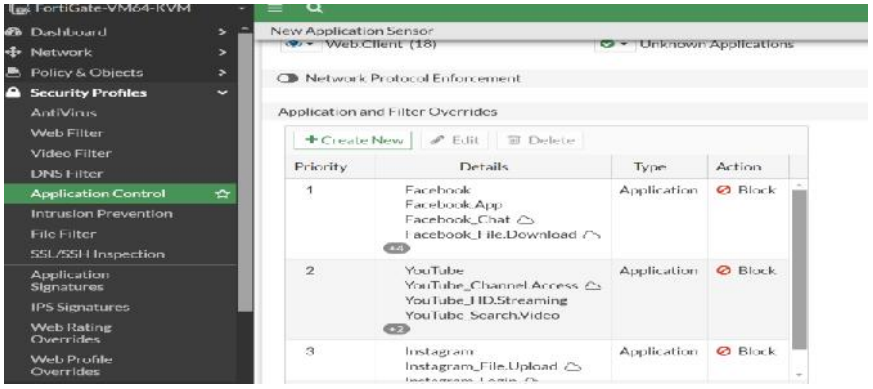


Figura 118. Control de aplicaciones

Una vez creado el web filter y el application control los asignamos a la política que creamos

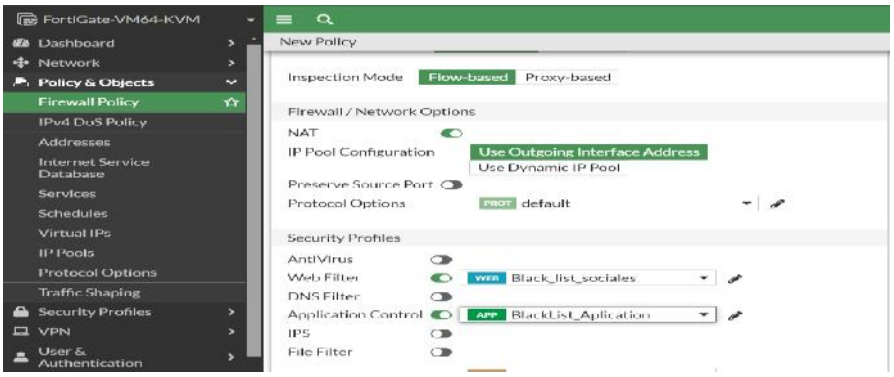


Figura 119. Asignación de filtros a la politica de bloqueo

Figura 120. politicas de bloqueo

III.1.2.4.2.8.- Configuración de los Access point

III.1.2.4.2.8.1.- Configuración del Access point en SEDES

Figura 121. Interfaz gráfica del Access point

III.1.2.4.2.8.2.- Configuración del Access point en PAI

Figura 122. Interfaz gráfica del Access point

III.1.2.4.2.9.- Configuración de un servidor DHCP en Linux debían

Se configuro el servidor como servidor DHCP para asignar direcciones IP a los equipos en cada VLAN el cual va proporcionarlas en el siguiente rango desde la 192.168.100.10 hasta la 192.168.100.40/24, con los siguientes parámetros de configuración:

- Tiempo de concesión = 1 día
- Máximo tiempo de concesión = 9 días
- Mínimo tiempo de concesión = 2 horas
- Red: 192.168.100.0
- Mascara de red: 255.255.255.0
- Puerta de enlace: 192.168.100.1

A continuación, se pondrá los pasos que se debe seguir para configurar el servidor DHCP

Paso 1: Instalar con el comando **apt install isc-dhcp-server** el servidor DHCP en el sistema operativo Linux debían

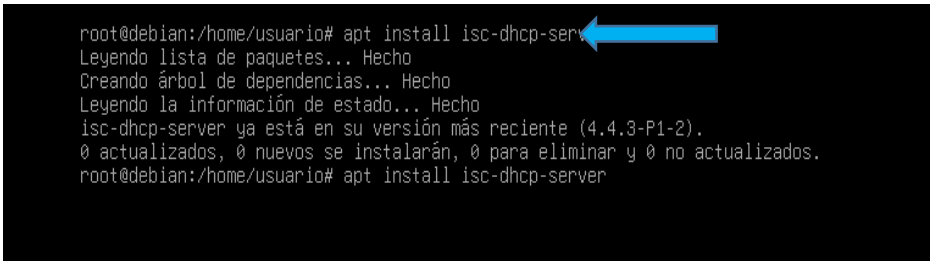


Figura 123. Instalación del servidor DHCP

Paso 2: Colocarle una dirección IP estática al servidor editando el archivo **/etc/networ k/interfaces** en este caso le colocaremos la 192.168.100.5

```
root@debian:/home/usuario# nano /etc/network/interfaces
```

Figura 124. Comando para ingresar al fichero

```
  GNU nano 7.2                                /etc/network/interfaces *
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
#allow-hotplug ens33
#iface ens33 inet dhcp

#Direccion IP estatica
auto ens33
iface ens33 inet static
        address 192.168.100.5
        netmask 255.255.255.0
        network 192.168.100.0
        broadcast 192.168.100.255
        gateway 192.168.100.1_
```

Figura 125. Configuración IP estática

Paso 3: Indicamos en que interface de red se va escuchar las peticiones DHCP, para lo cual primero verificamos cual es el nombre de la interface con el comando **ip address** luego entramos en el fichero **isc-dhcp-server** para editarlo en este caso está en la interface “ens33” como se muestra a continuación

```
root@debian:/home/usuario# ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:80:56:fc brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.100.5/24 brd 192.168.100.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe80:56fc/64 scope link
       valid_lft forever preferred_lft forever
root@debian:/home/usuario#
```

Figura 126. Verificacion interfaz de red

```
root@debian:/home/usuario# nano /etc/default/isc-dhcp-server
```

Figura 127. Ingreso al fichero

```
  GNU nano 7.2                          /etc/default/isc-dhcp-server *
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPDv4_PID=/var/run/dhcpd.pid
#DHCPDv6_PID=/var/run/dhcpd6.pid

# Additional options to start dhcpd with.
#       Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="ens33"
INTERFACESv6=""
```

Figura 128. Configuración de la interfaz de red como DHCP

Paso 4: Se debe editar el archivo de configuración **dhcpd.conf** para comenzar a configurar el servidor DHCP y configuramos todos los parámetros necesarios

```
root@debian:/home/usuario# nano /etc/dhcp/dhcpd.conf
```

Figura 129. Comando para ingresar al fichero

```
  GNU nano 7.2                                  /etc/dhcp/dhcpd.conf *

# This declaration allows BOOTP clients to get dynamic addresses,
# which we don't really recommend.

#subnet 10.254.239.32 netmask 255.255.255.224 {
#  range dynamic-bootp 10.254.239.40 10.254.239.60;
#  option broadcast-address 10.254.239.31;
#  option routers rtr-239-32-1.example.org;
#}

# A slightly different configuration for an internal subnet.
subnet 192.168.100.0 netmask 255.255.255.0 {
  range 192.168.100.10 192.168.100.40;
# option domain-name-servers ns1.internal.example.org;
# option domain-name "internal.example.org";
  option routers 192.168.100.1;
  option broadcast-address 192.168.100.255;
  default-lease-time 691200;
  max-lease-time 691200;
}
```

Figura 130. Parámetro de configuraciones del servidor DHCP

Explicando cada línea seria así:

- Subnet: se refiere a la red a la que pertenece la cual es la 192.168.100.0
- Range: es el rango en el cual se va repartir direcciones IP a los dispositivos
- Option routers: es la dirección de la puerta de enlace que en este caso es la 192.168.100.1
- Default-lease-time: mínimo tiempo de concesión, expresado en segundos
- Max-lease-time: máximo tiempo de concesión, expresado en segundos

Paso 5: Una vez realizadas todas las configuraciones necesarias se debe reiniciar el servidor para que este reconozca dichas configuraciones y empiece a funcionar como un servidor DHCP

```
root@debian:/home/usuario# /etc/init.d/isc-dhcp-server restart
```

Figura 131. Reiniciar el servidor DHCP

Paso 6: Comprobar que el equipo cliente reciba una concesión, es decir, que se le asigne una dirección IP correctamente

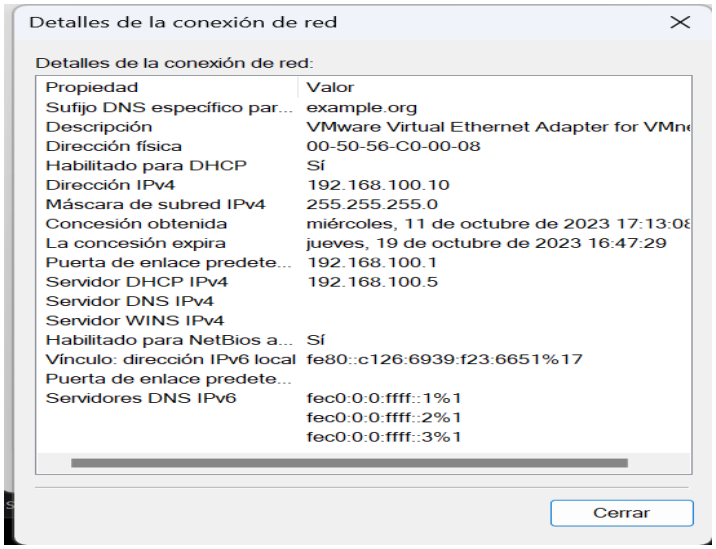


Figura 132. Verificación de IP cliente

III.1.2.4.3.- Detalles de los aspectos en que se realizan las mejoras tecnológicas

El diseño e implementación de cableado estructurado mejora la red en los siguientes aspectos:

- Administración eficaz y sencilla de la red
- Integración de varios servicios en la red en un mismo sistema
- Fácil mantenimiento ya que se hace seguimiento a una sola estructura de cableado de modo que reduce costos
- Alto rendimiento ya que tiene mayor velocidad de conexión de datos entre los equipos
- Visualmente se ve mejor al integrar todo en un mismo cableado, se reducen los espacios, logrando que todo se vea más ordenado y cuidado
- Se puede ampliar de tamaño si es necesario brindando seguridad y protección a los datos

Diseño de las Vlans mejora la red de la siguiente manera:

- Trasladar fácilmente las estaciones de trabajo en la LAN
- Agregar fácilmente estaciones de trabajo a la LAN
- Cambiar fácilmente la configuración de la LAN
- Controlar fácilmente el tráfico de red
- Mejorar la seguridad

Implementando servidor DHCP

- Facilita la administración de las direcciones IP
- Portabilidad y disponibilidad en la red

Seguridad implementando el Fortigate

- Protege el correo electrónico, el perímetro de la red, LAN, WLAN y acceso a la red, contra las amenazas más sofisticadas, mediante métodos potentes y automatizados.
- Funcionalidades: incluye las características principales de un firewall, como prevención de intrusiones, anti-malware y filtrado web. También incluye inspección SSL, protección contra amenazas y segmentación escalable.

Monitoreo

- Permite monitorear todos los aspectos de la red, como los dispositivos conectados a su red y el tráfico que pasa a través de ella
- Prevención del tiempo de inactividad (Down time)
- El monitoreo de red se usa principalmente para monitorear el rendimiento, pero también puede ayudar a descubrir amenazas de seguridad dentro de su sistema. Al monitorear continuamente la actividad inusual o sospechosa, puede detectar incluso pequeñas amenazas antes de que se conviertan en grandes
- Supervisar el uso de ancho de banda

Telefonía IP

- Atender múltiples llamadas de forma simultánea
- Múltiples usuarios hablando a la vez: evita las esperas al teléfono
- Trasferencia de las llamadas
- Tener múltiples teléfonos
- Usar el fijo desde aplicaciones en el móvil
- Bloquear números concretos de spam
- Se pueden atender llamadas en movilidad

Mejorar el centro de datos

- Reducir costos

- Mejorar la eficiencia
- Conexiones redundantes
- Seguridad física
- Escalabilidad
- Almacenamiento seguro
- Fiabilidad

III.1.2.4.4.- Probar el diseño

La fase de pruebas consiste en comprobar la correcta incorporación de todos los componentes de la red para que se demuestre que todo está funcionando bien, esta fase también es donde se identifican y se arreglan los defectos que se pueda encontrar en la red. Las pruebas se realizarán durante todo el proyecto y no solamente durante la fase de pruebas

Se utilizarán los siguientes métodos de prueba para la red:

III.1.2.4.5.- Optimizar el diseño de la red

Un punto importante en el diseño de la red es la transferencia de información por lo que para optimizarla se trabajara en un ancho de banda adecuado para la red de la institución que lo que se busca es mejorar los parámetros de disponibilidad de su red por lo que para este punto utilizaremos herramientas de tipo analítico:

Tester de velocidad de red: usaremos el tester del sitio web oficial de Tigo para medir la velocidad

Software de simulación para la configuración de red: Packet tracer

Software de monitoreo: Glaswire

Si se llega a tener retardo en tiempo de procesamiento en la red tenemos que buscar elementos de optimización en la transmisión de velocidad de la red en el router principal.

Los retardos en una red están normalmente presentes en:

- Elementos de conmutación de paquetes (Router, Switches)
- Paquetes por segundo de procesamiento del switch
- Capacidad del backplane
- Configuración de parámetros de seguridad pueden afectar el desempeño.
- Tiempos de propagación.
- Elementos de almacenamientos (buffers)
- Elementos de seguridad de la red (Firewalls, IPS)
- Velocidades de conexión.
- Protocolos de transporte.
    - Protocolo TCP
    - Protocolo UDP
    - Otros protocolos
    - IPSEC
    - H323
    - SIP

III.1.2.4.6.- Diseño de Arquitectura de red

La arquitectura de la red es de acuerdo de los requerimientos de la institución que se tenga o que se pida. El diseño incluye elementos tales como:

- Ubicación de los diferentes elementos de red
- Ancho de Banda requerido hacia Internet.
- Parámetros configuración
- Velocidad de las conexiones.

- Tiempo de respuesta aplicaciones
- Caracterización del trafico
- Protocolos usados por aplicaciones
- Tráfico generado por las aplicaciones
- Requerimientos promedio a las aplicaciones
- Paquetes por segundo requerido de procesamiento en la red.
- Definición de memoria de almacenamiento en dispositivos.
- Parámetros para manejo de memoria en los dispositivos de red

III.1.2.5. Fase 5: Implementar y probar la red

III.1.2.5.1. Cronograma de implementación de la red

Actividad	Nº días	Fecha inicio	Fecha fin	S1	S2	S3	S4	S5
Implementar los servicios requeridos	31	01/09/23	31/10/23	X	X	X	x	X
Configuración de los equipos de red (routers, switch, servidor DHCP y firewall)	5	01/09/23	05/09/23	X				
Instalación de los equipos de computación	2	06/09/23	07/09/23	X				
Conexión del cableado estructurado de la red	6	08/09/23	13/09/23	X	X			
Configuración de los equipos de computación a la red mediante cableado	3	14/09/23	16/09/23	X	X			
Configuración de las laptops de manera inalámbrica	3	17/09/23	19/09/23		X	X		

Instalación de programas hacia la red	5	20/09/23	24/09/23				X	
Pruebas de la red	7	25/09/23	31/09/23					X

Tabla 27. Cronograma de implementación

III.1.2.5.2. Implementación del diseño de red

III.1.2.5.2.1.- Diagrama de red principal

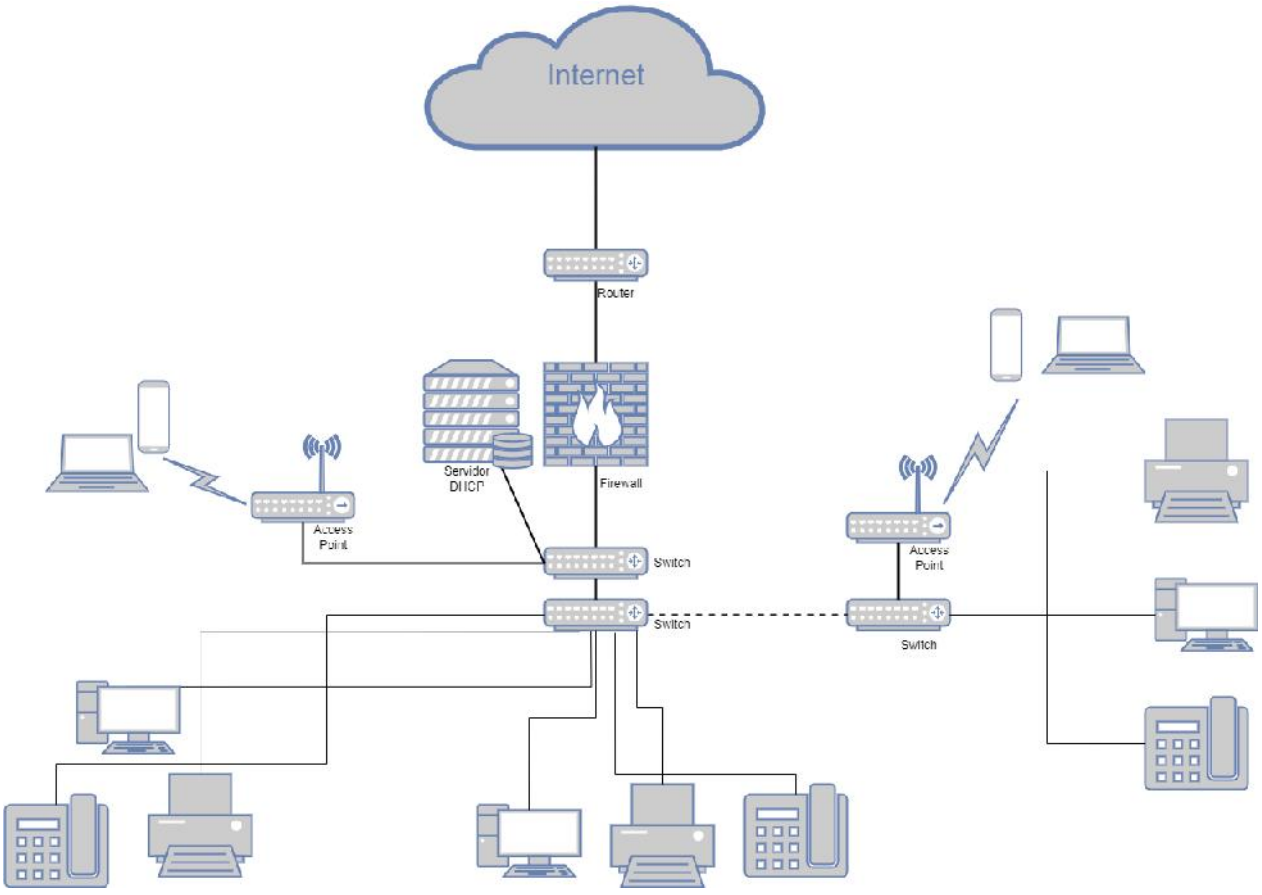


Figura 133. Red principal de toda la institución

III.1.2.5.2.2.-Diagrama de servidor DHCP

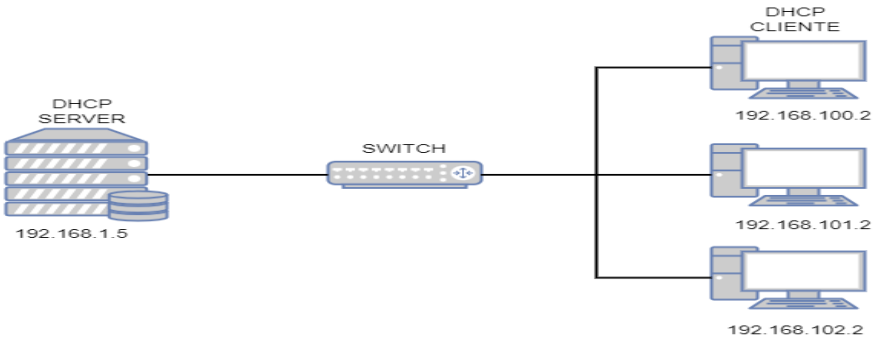


Figura 134. Direccionamiento IP

III.1.2.5.2.3.- Diagrama general de las VLAN

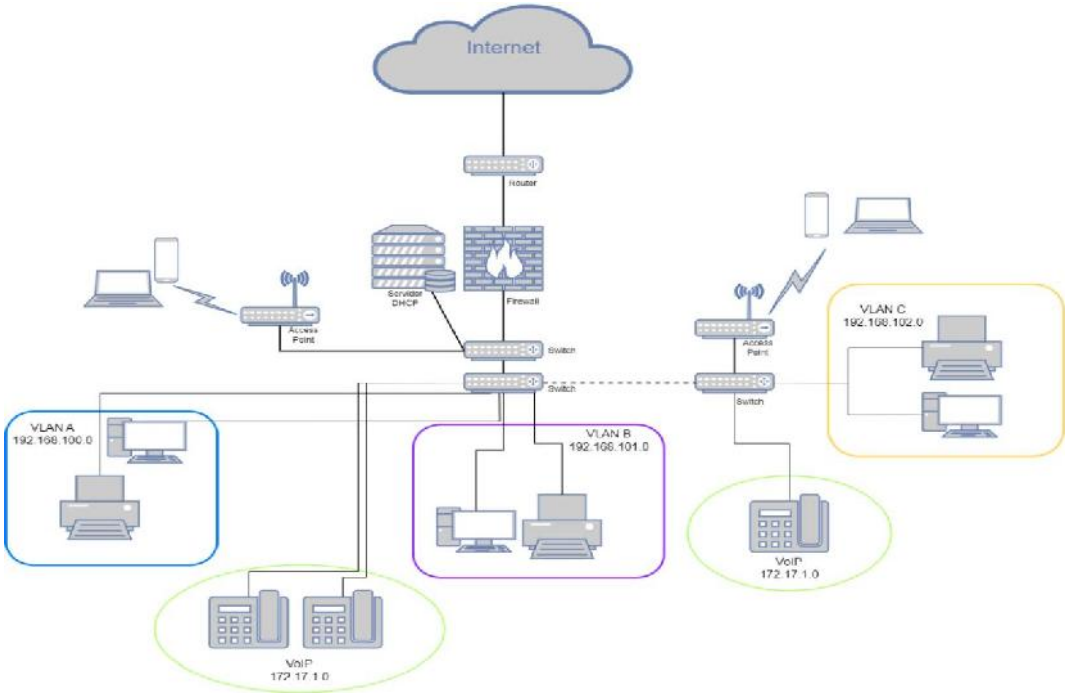


Figura 135. Diagramas de Vlans

III.1.2.5.2.3.1.- Diagrama de la conexión de la VLAN SEDES-A de la institución SEDES

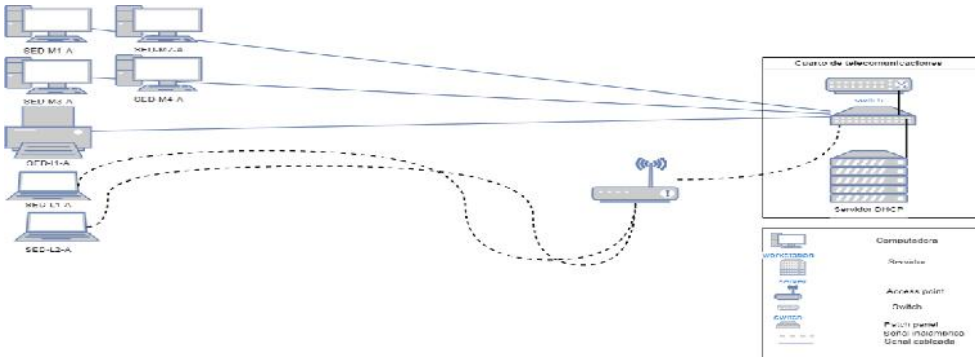


Figura 136. red SEDES-A institución SEDES

III.1.2.5.2.3.2.- Diagrama de la conexión de la VLAN SEDES-B de la institución SEDES

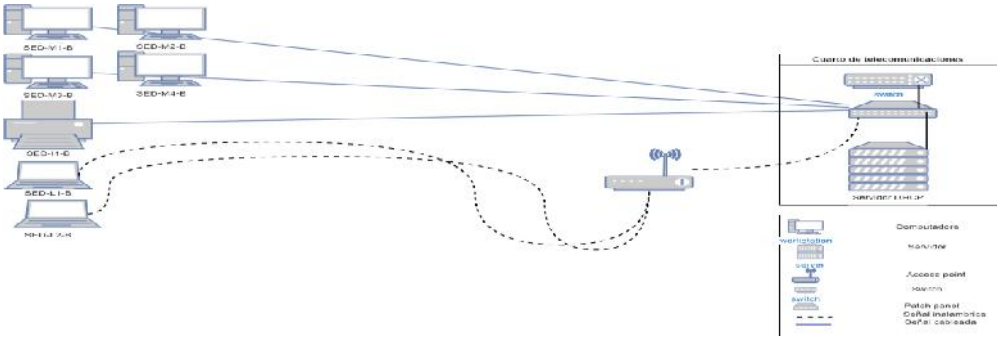


Figura 137. red SEDES-B institución SEDES

III.1.2.5.2.3.3.- Diagrama de la conexión de la VLAN PAI-A de la institución PAI

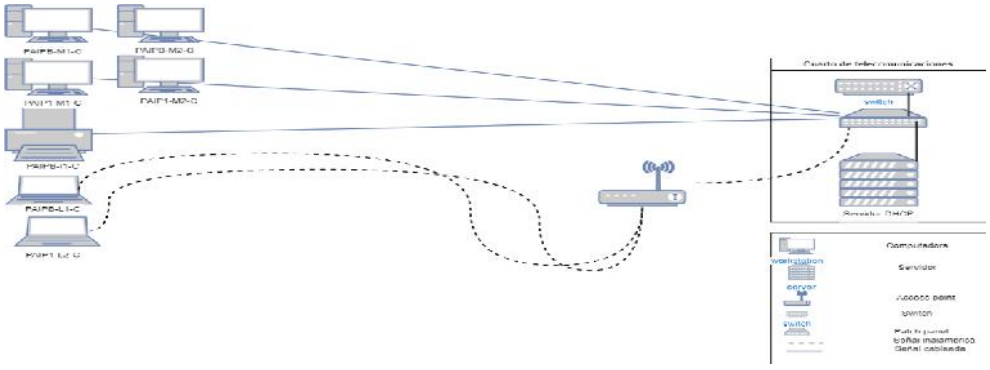


Figura 138. red PAI-A institución PAI

III.1.2.5.2.4.- Diagrama del cuarto principal de telecomunicaciones

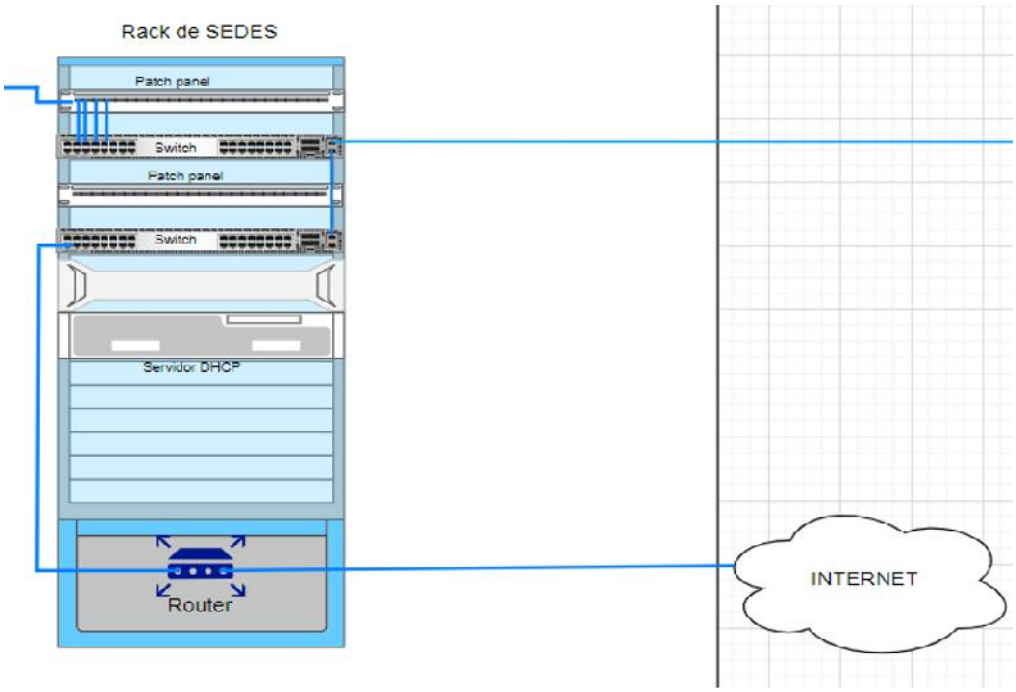


Figura 139. Cuarto principal de comunicación

III.1.2.5.2.5.- Diagrama de gabinete

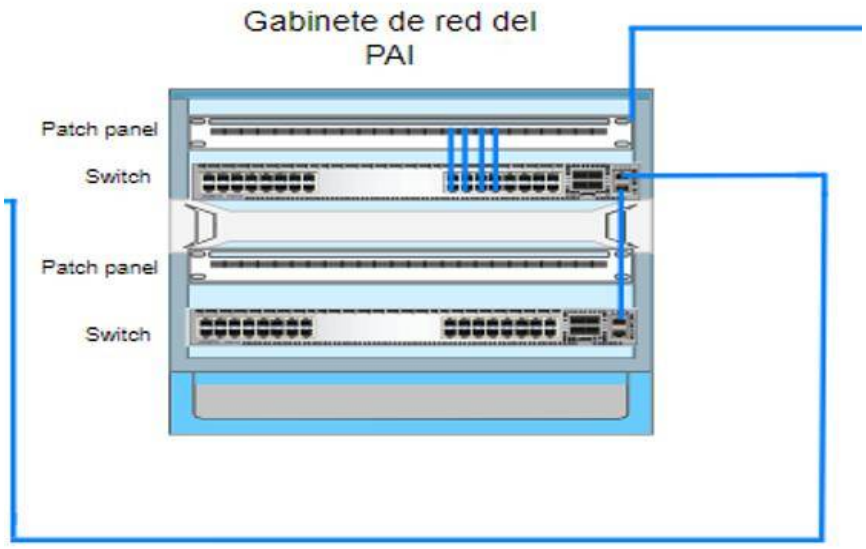


Figura 140. Gabinete de PAI

III.1.2.5.5. Cableado de electricidad y Cable UTP distancia

Para instalar el cableado de red se debe tener en cuenta el cableado de electricidad con la norma UNE-EN 50174-2 sobre la separación entre cableado de datos y cableado de red de alimentación:

A continuación, mostraremos los tipos de instalación

Tipo de instalación	Con divisor metálico o sin divisor
Cable de datos UTP y cable eléctrico no apantallado	200 mm
Cable de datos UTP y cable eléctrico apantallado	30 mm

Tabla 28. Instalación de cableado

Con la tabla mencionada decimos que la distancia requerida para la conexión del cable de red debe tener mínimamente 200 mm de distancia con el cable de corriente eléctrica

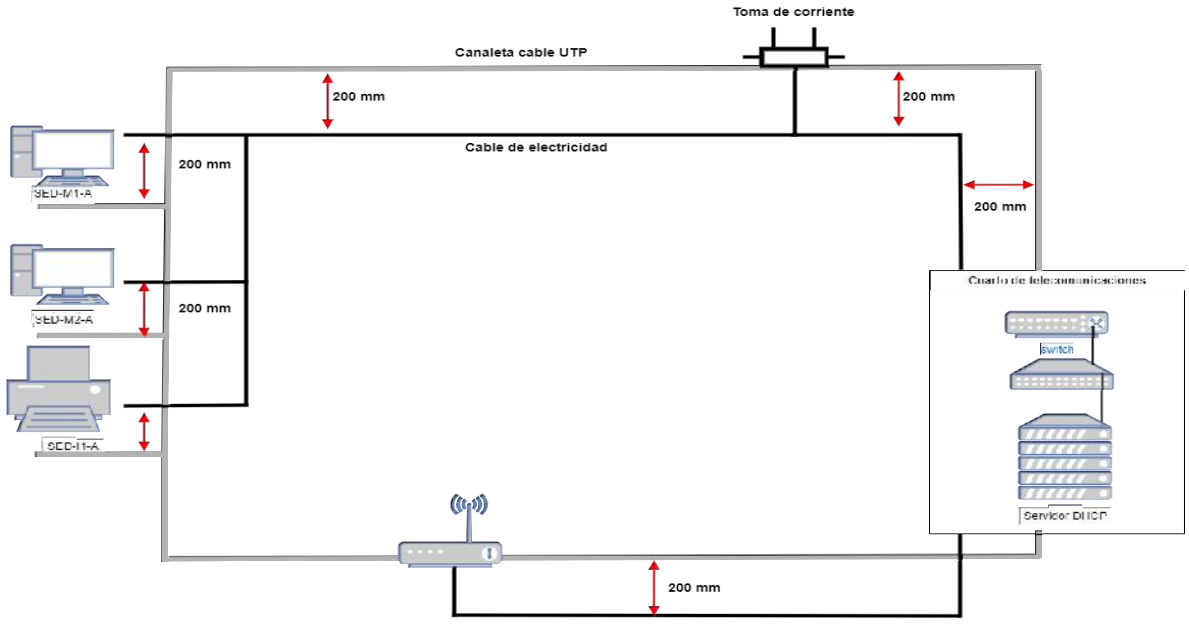


Figura 141. Distribución cableado eléctrico.

III.1.2.5.3.- Probar el diseño

La fase de pruebas consiste en comprobar la correcta incorporación de todos los componentes de la red para que se demuestre que todo está funcionando bien, esta fase también es donde se identifican y se arreglan los defectos que se pueda encontrar en la red. Las pruebas se realizarán durante todo el proyecto y no solamente durante la fase de pruebas

Se utilizarán los siguientes métodos de prueba para la red:

III.1.2.5.3.1.- Probar la conectividad de la red

En primer lugar, se realizará ping a los servicios web que utiliza la institución, así como también a sus respectivas paginas

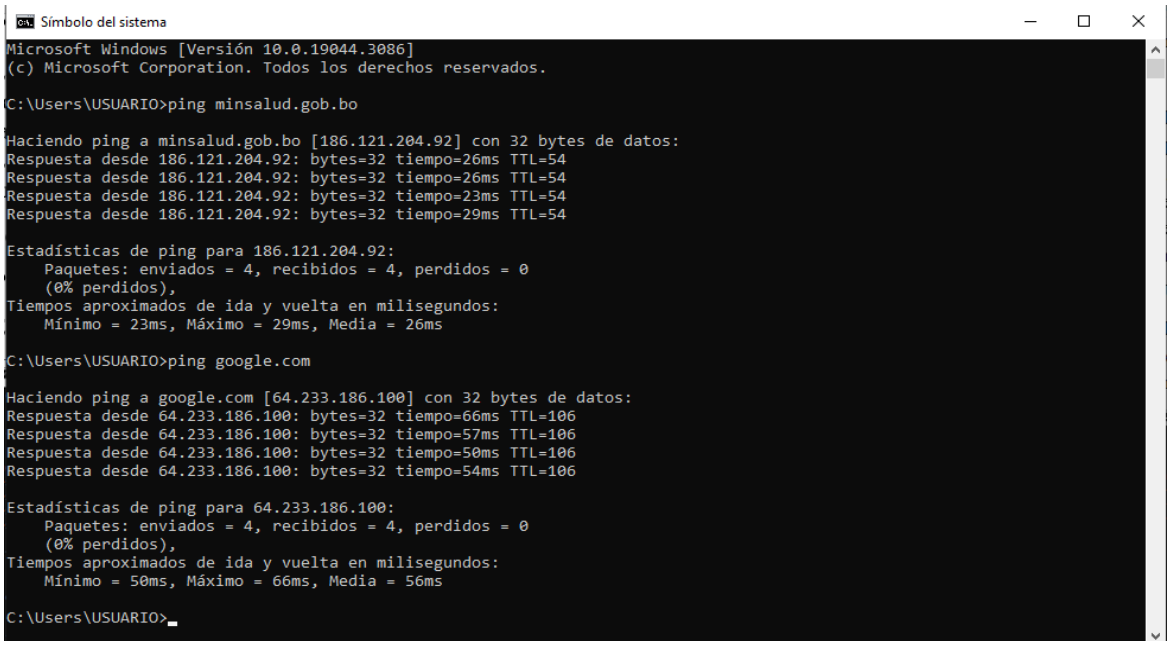


Figura 142. Ping a los servicios utilizados

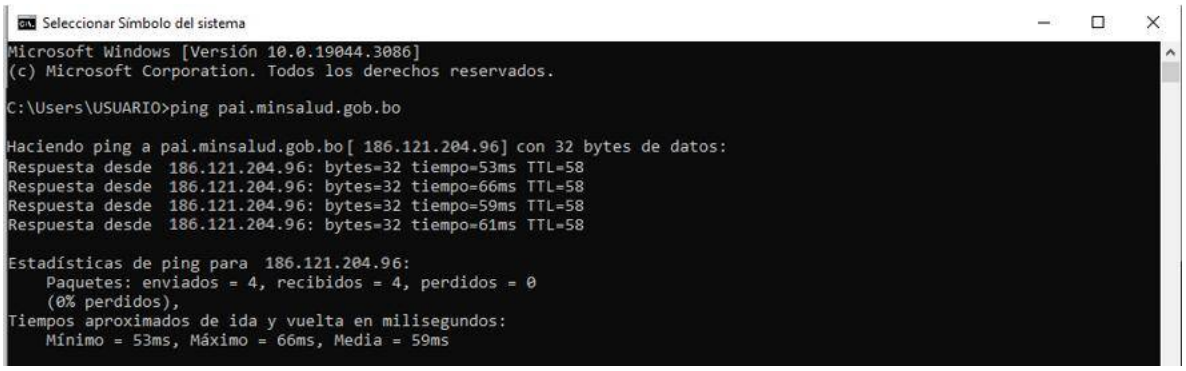


Figura 143. ping a los servicios requeridos

III.1.2.5.3.2.- Pruebas de los dispositivos

En este punto detallaremos las pruebas relacionadas a los dispositivos y a su funcionamiento en su respectiva área dichas pruebas se realizarán para verificar también el alcance de los dispositivos en cuanto a su comunicación.

El servidor DHCP asigno a los equipos de su respectiva VLAN una IP de manera dinámica por lo que probaremos la conectividad entre uno de los equipos de escritorio de la VLAN SEDES-A y una de sus impresoras en la institución de SEDES

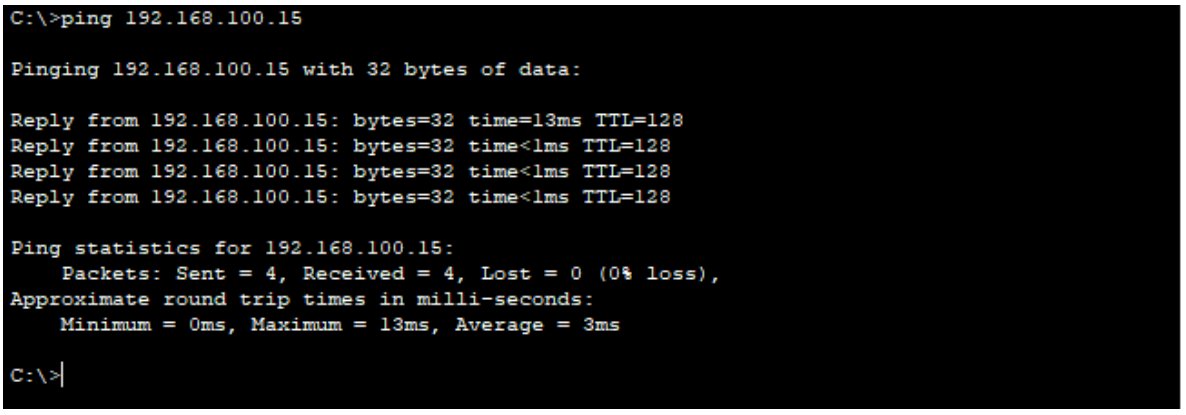


Figura 144. ping a la red SEDES-A

Probaremos la conectividad entre uno de los equipos de escritorio de la VLAN SEDES-B y una de sus impresoras en la institución de SEDES

```
C:\>ping 192.168.101.6

Pinging 192.168.101.6 with 32 bytes of data:

Reply from 192.168.101.6: bytes=32 time=3ms TTL=128
Reply from 192.168.101.6: bytes=32 time<1ms TTL=128
Reply from 192.168.101.6: bytes=32 time=1ms TTL=128
Reply from 192.168.101.6: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.101.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 1ms

C:\>
```

Figura 145. ping a la red SEDES-B

Probamos la conectividad entre un equipo de escritorio y una impresora en la institución PAI

```
C:\>ping 192.168.102.15

Pinging 192.168.102.15 with 32 bytes of data:

Reply from 192.168.102.15: bytes=32 time=13ms TTL=128
Reply from 192.168.102.15: bytes=32 time=24ms TTL=128
Reply from 192.168.102.15: bytes=32 time<1ms TTL=128
Reply from 192.168.102.15: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.102.15:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 24ms, Average = 9ms

C:\>
```

Figura 146. ping a la red PAI-A

III.1.2.5.3.3.- Nivel de señal actual

Figura 147. Nuevo nivel de señal

III.1.2.5.4.- Pruebas de funcionalidad

Uno de los requerimientos más importantes para los funcionarios de la institución es contar acceso a todos los programas necesarios a través de sus equipos de computación, así como también tener una buena conectividad a la red para así tener un buen rendimiento en sus funciones laborales

Se realizaron pruebas con el software de los usuarios en los dispositivos comprobando los siguientes programas:

- Sitio web de SEDES
- Sitio web de PAI
- Google Earth pro
- Google Maps
- Otras librerías de google
- Sitio web SNIS-VE

A continuación, se mostrarán los programas anteriormente mencionados funcionando correctamente.

Sitio web de SEDES

Figura 148. Sitio web SEDES

Sitio web de PAI

Figura 149. Sitio web PAI

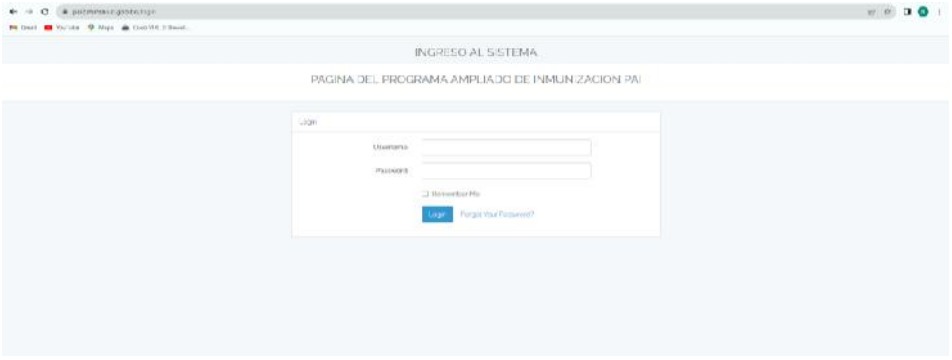


Figura 150. Ingreso al sistema PAI

Google Earth pro

Figura 151. Sitio web google earth

Google Maps

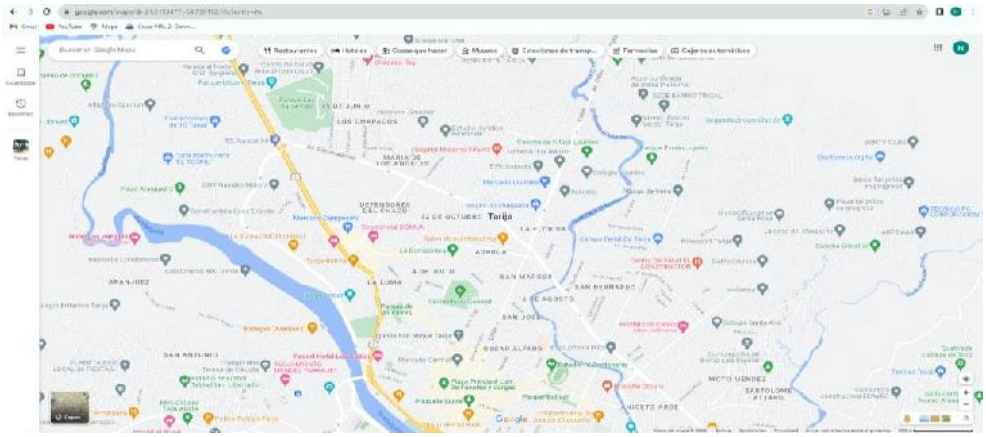


Figura 152. Sitio web google maps

SNIS-VE

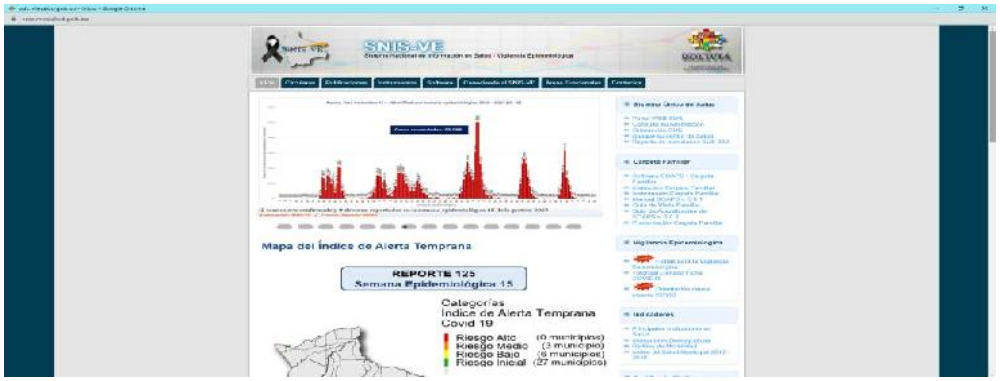


Figura 153. Sitio web SNIS-VE

III.1.2.5.5.- Pruebas de comunicación

Las pruebas de comunicación consisten en verificar que la tecnología implantada funcione correctamente para lo cual se enviara archivos de un equipo de escritorio a otro de cada segmento de las redes conectadas

Figura 154. Equipo conectado en red

III.1.2.5.6.- Resultado de pruebas y problemas

Se llegó a la conclusión de que las pruebas resultaron satisfactorias ya que los equipos de computación se conectan de manera exitosa y la red de la institución funciona de manera fluida, así como también existe conexión entre los equipos de computación y las impresoras por último se comprobó que todos los programas funcionan y pueden ser accedidos correctamente siendo que cumplen con los requisitos propuestos.

III.1.2.5.6.1 Realizar pila de pruebas

Se realizará la prueba de velocidad de subida y de bajada de cada red de la institución en megabits por segundo dicha prueba se la hará en el tester del sitio web de Tigo

III.1.2.5.6.1.2 Pruebas de testeo de la red A de SEDES

Figura 155. Pruebas de testeo red A

La red A cuenta con un ping de 22 ms(milisegundos) la velocidad de descarga es de 9,5 Mbps (megabits por segundo) y la velocidad de subida es de 9,5 Mbps (megabits por segundo)

Figura 156. Pruebas de testeo red A

III.1.2.5.6.1.3.-Pruebas de testeo de la red B de SEDES

La red B cuenta con un ping de 22 ms(milisegundos) la velocidad de descarga es de 9,2 Mbps (megabits por segundo) y la velocidad de subida es de 9,5 Mbps (megabits por segundo)

Figura 157. Pruebas de testeo red B

III.1.2.5.6.1.4.-Pruebas de testeo de la red C de PAI

La red C cuenta con un ping de 22 ms(milisegundos) la velocidad de descarga es de 9,2 Mbps (megabits por segundo) y la velocidad de subida es de 9,5 Mbps (megabits por segundo)

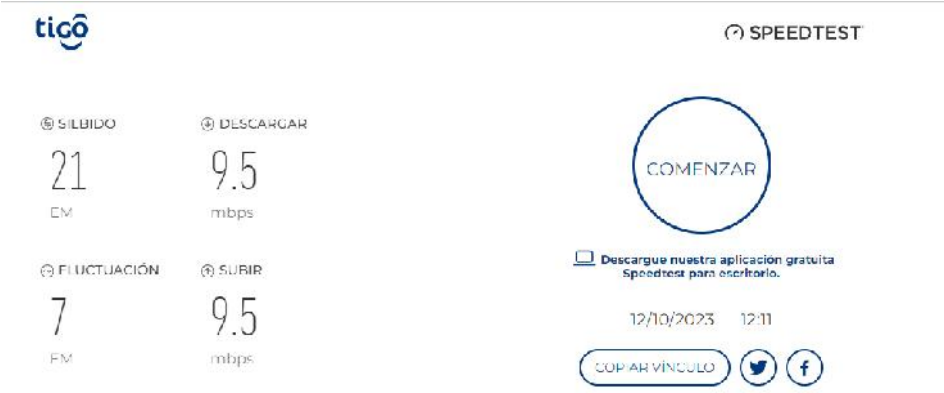


Figura 158. Pruebas de testeo red C

III.1.2.6. Fase 6.- Monitorear y optimizar la red

III.1.2.6.1. Monitoreo de la red

El monitoreo de la red se realizó con la herramienta de software Glasswire.

GlassWire es una plataforma de seguridad y supervisión de redes que proporciona diversas herramientas, como supervisión de redes en tiempo real, firewall integrado, funciones de seguridad de Internet, alertas, supervisión de la utilización del ancho de banda, supervisión de servidores, es una herramienta sencilla para monitorear la red con un firewall incorporado para permitir o negar el acceso a Internet a las aplicaciones.

En el caso de nuestra red utilizaremos 2 de las opciones que tiene este software lo que nos permitirá un monitoreo en tiempo real de la red

III.1.2.6.1.1. Monitoreo institucion SEDES red A

Monitoreo de la red en uso: En el siguiente cuadro se puede ver los datos de subida y de bajada junto con los programas que se estan usando en el equipo de computacion aqui se puede observar que se tiene un total de 371.2 mb usados en en el transcurso del dia en la red

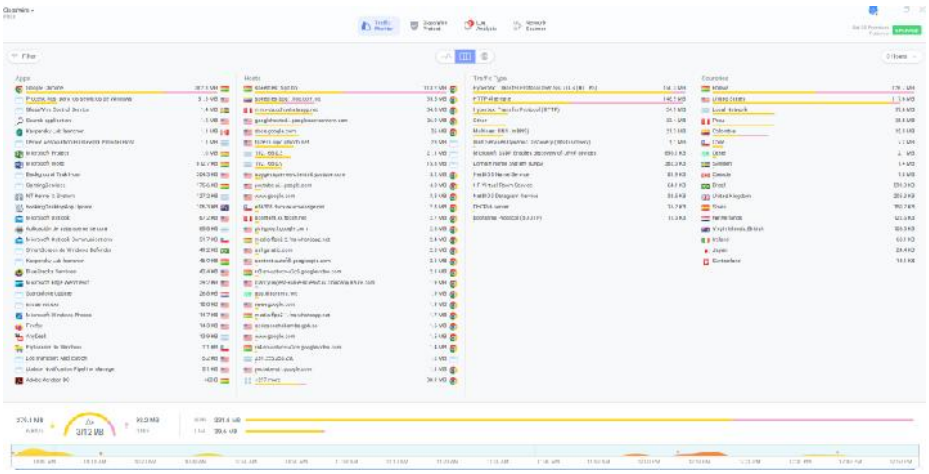


Figura 159. Monitoreo red A

Monitoreo de la red en modo grafico

En la imagen se podrá observar de forma gráfica el consumo de la red en subida que es lo que este color rnaranja, lo que se encuentra en color amarillo es el consumo de bajada de la red y lo que está de color naranja es la unión de las dos graficas.

Figura 160. Monitoreo grafico red A

III.1.2.6.1.2. Monitoreo institucion SEDES red B

Monitoreo de la red en uso: En el siguiente cuadro se puede ver los datos de subida y de bajada junto con los programas que se estan usando en el equipo de computacion aqui se puede observar que se tiene un total de 1.5 mb usados en en el transcurso del dia en la red

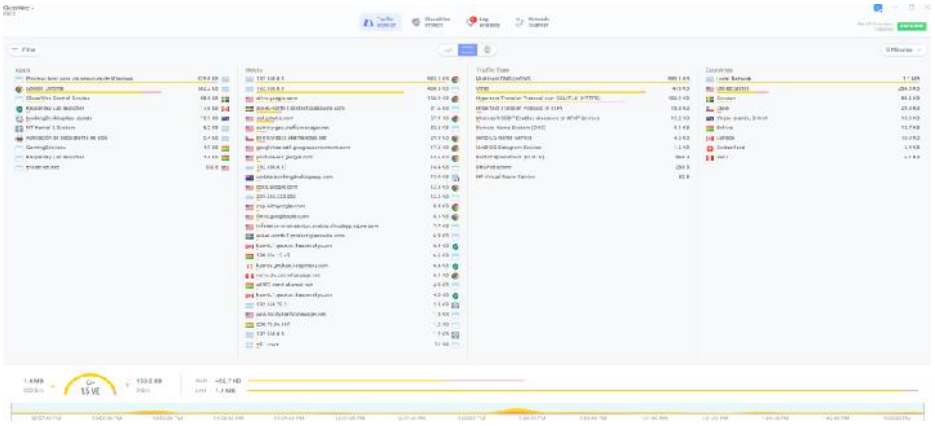


Figura 161. Monitoreo de red B

Monitoreo de la red en modo grafico

En la imagen se podrá observar de forma gráfica el consumo de la red en subida que es lo que este color naranja, lo que se encuentra en color amarillo es el consumo de bajada de la red y lo que está de color naranja es la unión de las dos graficas.

Figura 162. Monitoreo grafico red B

III.1.2.6.1.3. Monitoreo institución PAI red C

Monitoreo de la red en uso: En el siguiente cuadro se puede ver los datos de subida y de bajada junto con los programas que se estan usando en el equipo de computacion aqui se puede observar que se tiene un total de 297.2 mb usados en en el transcurso del dia en la red

Figura 163. Monitoreo de red C

Monitoreo de la red en modo grafico

En la imagen se podrá observar de forma gráfica el consumo de la red en subida que es lo que este color naranja, lo que se encuentra en color amarillo es el consumo de bajada de la red y lo que está de color naranja es la unión de las dos gráficas.

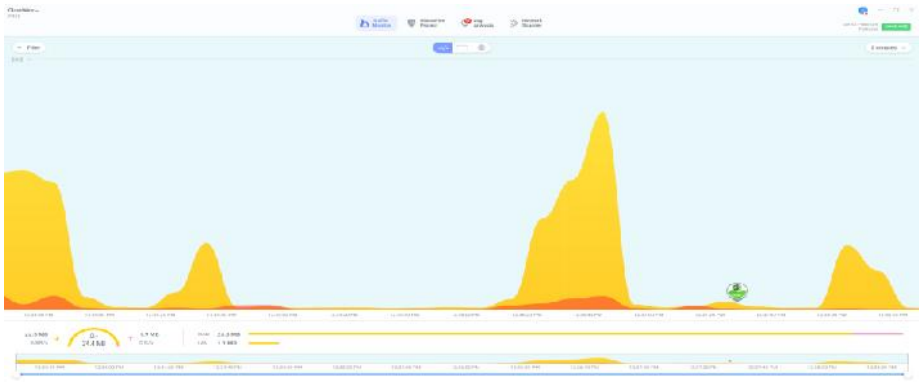


Figura 164. Monitoreo grafico red C

III.1.2.6.2. Optimización de la red

La optimización de la red es una tecnología utilizada para mejorar el rendimiento de la red para un entorno determinado. Se considera un componente importante de la gestión eficaz de los sistemas de información. La optimización de la red desempeña un papel importante ya que la tecnología de la información está creciendo a tasas exponenciales con usuarios comerciales que producen grandes

volúmenes de datos y, por lo tanto, consumen anchos de banda de red más grandes. Si no se cuenta con la optimización de red adecuada, el crecimiento continuo puede agregar tensión a la arquitectura de red del entorno u organización en cuestión.

El monitoreo de indicadores clave de rendimiento ayuda a optimizar los parámetros de la red. Es imposible monitorear manualmente estos para los cientos y miles de dispositivos en una red. Para monitorear estas métricas críticas y optimizarlas para obtener la máxima eficiencia, necesita herramientas de optimización de red como la que estamos usando que es Glaswire

En el diseño de la red para ambas instituciones aparte de las redes físicas se dividió la red en redes lógicas con el objetivo de optimizarlas, así como también para que cada una tuviera su propio ancho de banda

El diseño de la red tiene los siguientes métodos de optimización:

- Cableado de red categoría 5e que mejora el desempeño de la transmisión de datos.
- La velocidad de la red por conexión Ethernet y LAN es correcta por el ancho de banda que se dio a cada red.
- Uso del cableado utp es únicamente para la conexión de dispositivos hacia la red.
- Mantener actualizados todos los equipos para que se tenga un buen rendimiento de CPU, para que así la red pueda ser más veloz.
- La red por conexión Ethernet trae muchas ventajas, entre ellas bajo costo para la migración ya que el cableado puede compartirse.
- La red por conexión inalámbrica es accesible para los equipos que requieren está en constante movimiento personal.

III.2.- Componente II: Capacitación para el personal responsable de la red

III.2.1.- Introducción

Una vez concluido el diseño y hecho las pruebas necesarias a la red se procede a la capacitación al personal responsable de la administración y el centro de datos el cual obtendrá conocimientos sobre el uso de las tecnologías y servicios implementados en la nueva re-estructuración para que de esta manera sea capaz de administrarlos correctamente y para futuros mantenimientos si lo necesitara

III.2.2.-Propósito

Se tiene como propósito concluir el componente con la capacitación del personal de manera que este sea capaz de administrar el centro de datos de SEDES y PAI de manera idónea

III.2.3.-Objetivos

III.2.3.1.- Objetivo general

Elaborar un programa de capacitación al personal responsable del manejo y administración de la red de SEDES

III.2.3.2.- Objetivos específicos

- Planificar material y estrategias para la capacitación
- Realizar la capacitación sobre la nueva estructura, tecnologías y servicios del nuevo diseño de red

III.2.4.- Contexto

Se realizó la guía para la capacitación teniendo en cuenta las tecnologías y servicios que se utilizó. El personal que será capacitado es el encargado de la administración del centro de datos

de SEDES solo se capacitara al personal técnico debido a que este el único que tiene acceso y autorización de su uso y administración

III.2.5.-Propuesta pedagógica

Se utilizó métodos de enseñanza haciendo énfasis principalmente en tres formas de aprendizajes como:

Aprendizaje significativo: El aprendizaje significativo es conocido como uno de los tipos de aprendizaje más efectivos, y consiste en establecer relaciones entre los conocimientos nuevos y los que ya se tenían

Aprendizaje cognitivo: Consta de varias operaciones mentales que se basan en la experiencia y en el procesamiento de la información que hace el individuo a partir de esta, con el fin de asimilar un conocimiento y dar una respuesta. De esta manera, en la mente, se conectan las ideas ya existentes, es decir, lo que ya uno conoce, con la nueva información para profundizar en la memoria y la capacidad de retención.

III.2.5.1.- Contenido de la capacitación

Lección 1: Configuración del router

Lección 2: Configuración del servidor DHCP

Lección 3: Configuración de las VLANs

Lección 4: Configuración de los Access point

Lección 5: Configuración de los equipos de computación para los usuarios

Lección 6: Instalación de programas para los equipos

Lección 7: Configuración de la telefonía VoIP

Lección 8: Administración del centro de datos

Lección 9: Monitoreo de control al rack del centro de datos

III.2.5.2.- Plan de capacitación

Nro	Contenido	Objetivo	Fecha	Duración	Material didáctico	Medios de enseñanza y aprendizaje	Destinatario
1	Configuración del router	Que el administrador tenga conocimiento de las nuevas configuraciones y sea capaz de administrarlo	08/01/24	2 horas	Demostración real	Equipo de computación	Encargado de cuarto de telecomunicación
2	Configuración del servidor DHCP	Que el administrador aprenda el manejo del servidor y pueda asignar direcciones a los usuarios de manera dinámica	15/01/24	3 horas	Demostración real	Equipo de computación	Encargado de cuarto de telecomunicación
3	Configuración de las VLANs	Que se tenga conocimiento de cómo segmentar y manejar las redes lógicas	22/01/24	2 horas	Guía esquematizada	Pizarra y dispositivo de red	Encargado de cuarto de telecomunicación
4	Configuración de los Access point	Que el administrador aprenda a configurar los AP correctamente	29/01/24	1 hora	Diapositivas	Access Point	Encargado de cuarto de telecomunicación

		y con las nuevas configuraciones					
5	Configuración de los equipos de computación para los usuarios	Que el administrador domine la administración y configuración de los equipos	05/02/24	1 hora	Demostración real	Equipo de computación	Encargado de cuarto de telecomunicación
6	Instalación de programas para los equipos	Que el administrador pueda instalar los programas de manera correcta	12/02/24	1 hora	Demostración real	Equipo de computación	Encargado de cuarto de telecomunicación
7	Configuración de la telefonía VoIP	Que el administrador aprenda la configuración de telefonía IP y pueda administrarla correctamente	19/02/24	2 horas	Guía esquematizada	Pizarra y teléfonos IP	Encargado de cuarto de telecomunicación
8	Administración del centro de datos	Que el administrador domine el manejo de	26/02/24	2 horas	Diapositivas	Equipo de computación	Encargado de cuarto de

		la red y del centro de datos					telecomunicación
9	Monitoreo de control al rack del centro de datos	Que el administrador aprenda a monitorear y supervisar el tráfico de datos de forma correcta	04/03/24	1 hora	Demostración real	Equipo de computación	Encargado de cuarto de telecomunicación

Tabla 29. Plan de capacitación

III.2.6.-Resultados

El personal del servicio departamental de salud SEDES fue capacitado cumpliendo con las expectativas del componente y con los medios de enseñanza mostrando de manera real las configuraciones propuestas en el diseño

III.2.7.-Conclusiones

Una vez finalizada la capacitación se llegó a la conclusión de que el personal del SEDES se encuentra preparado para administrar y supervisar el centro de datos

III.2.8.-Medios de verificación

- Carta de conformidad sobre la capacitación realizada emitida por el responsable de SEDES
- Lista de asistentes a la capacitación

CAPITULO IV

CONCLUSIONES Y RECOMENDACIONES

IV.1.-Conclusiones

Una vez finalizado el proyecto **"Mejoramiento de la gestión de tráfico de datos de la red LAN de comunicación del Servicio Departamental de Salud SEDES-Tarija en el área de trabajo PAI utilizando VLANS y servicios de administración de redes"** se llegó a las siguientes conclusiones:

- Diseño lógico y físico del proyecto hecho con la metodología Top – Down permite realizar las estructuraciones de la red tales como el análisis, la implementación y el monitoreo de la red
- Diseño y normas del cableado estructurado permiten que la institución tenga una conexión de red más optima
- Segmentación de la red en redes lógicas utilizando VLANs evita que el tráfico de red se congestione y ayuda en la administración y manejo de la misma
- Seguridad y protección de la red mejorada utilizando el firewall Fortigate en el nuevo diseño de la red de SEDES
- Sistema operativo Linux Debian de servidor es adecuado para realizar las configuraciones por la facilidad de manejo en los comandos
- La implementación del DHCP mejora la administración y manejo de la red
- El congestionamiento en el tráfico de red se ve reducido debido a las implementaciones de los servicios

IV.2.- Recomendaciones

- Se debe mejorar la infraestructura en la que se encuentra el centro de datos debido a que no cuenta con las medidas de seguridad necesarias para evitar algún problema
- Se recomienda hacer mantenimientos preventivos en periodos de tiempos cortos debido a que la infraestructura física no es actual
- Se deberá tener un plan de contingencia en caso de que haya fallos en el servidor o en algún punto de la red, así como también en caso de fallos en el hardware
- Se recomienda realizar un plan de migración de equipos de computación, con el fin de no esperar daños irreparables en un futuro, por fallas en la parte electrónica de los componentes de los mismos
- Se recomienda mejorar el Sistema de refrigeración del centro de datos debido a que este es de uso básico
- Se recomienda renovar equipos de computación ya que los equipos actuales a futuro dejaran de soportar futuras actualizaciones de Sistema operativo