CAPÍTULO I

PRESENTACIÓN DEL PROYECTO

I.- CAPÍTULO I: PRESENTACIÓN DEL PROYECTO

I.1.- Presentación del Proyecto

Título del Proyecto: Rediseño y optimización de la infraestructura de red de la Clínica Santísima Trinidad

Nombre del Postulante: Cristian Nahuel Condori Condori

Celular: 69104131

Carrera/Unidad: Carrera Informática y Sistemas

Facultad: Ciencias y Tecnología

Correo Electrónico: crstnnhlcondori@gmail.com

Institución/Centro Cooperante: Clínica Santísima Trinidad de Tarija

Duración del Proyecto: 8 meses

Área/línea de investigación priorizada: Redes

I.2.- Perfil de Proyecto

I.2.1.- Introducción

La infraestructura de red es un componente fundamental para el funcionamiento eficiente de cualquier institución, ya sea pública o privada. En el caso de la Clínica Santísima Trinidad de Tarija, contar con una red moderna, segura y bien estructurada es clave para garantizar una atención médica ágil, confiable y de calidad.

Este proyecto propone el rediseño y optimización de la infraestructura de red corporativa de la clínica, utilizando tecnologías de redes avanzadas, reconocidas por su eficiencia, escalabilidad y bajo costo. A través de estas herramientas, se busca mejorar el rendimiento general de la red, gestionar mejor el ancho de banda, fortalecer la seguridad y facilitar el control tanto de redes alámbricas como inalámbricas.

La Clínica Santísima Trinidad es un centro médico privado de primer nivel, especializado en servicios de emergencia, internación, diagnóstico, cirugía y tratamiento integral de diversas patologías. Por lo tanto, requiere una red confiable que garantice la disponibilidad de servicios digitales críticos como historiales médicos, comunicación interna, telefonía IP y acceso a internet. Además, se destacará cómo los dispositivos de red permitirán aplicar políticas de seguridad robustas, configurar correctamente los protocolos, segmentar mediante VLANs y desplegar una red Wi-Fi eficiente, todo ello con el objetivo de mejorar la eficiencia operativa y la experiencia tanto del personal de salud como de los pacientes.

I.2.2.- Descripción del Proyecto

I.2.2.1.- Antecedentes de la Clínica

En lo que respecta a la institución, se ha planteado un rediseño integral de la red debido a que la infraestructura actual de la Clínica Santísima Trinidad de Tarija presenta interrupciones frecuentes, lo cual afecta negativamente la productividad del personal de salud y el acceso a recursos críticos. Estas interrupciones pueden deberse a problemas de conectividad, configuraciones deficientes o al uso de equipos obsoletos.

Además, se ha identificado que algunos usuarios han recurrido a la instalación de switches no configurados adecuadamente, lo que ha generado puntos de acceso no controlados dentro de la red. Este uso inadecuado compromete tanto la calidad como la seguridad de la red, afectando el funcionamiento fluido de los servicios clínicos.

La infraestructura actual no está ambientada ni estructurada de forma adecuada para responder a las necesidades actuales de la Clínica. Esto ha generado impactos significativos en términos de eficiencia, como pérdida de conectividad en puntos clave o una distribución deficiente del ancho de banda. En cuanto a la seguridad, se ha detectado acceso no controlado a la red, especialmente en la red inalámbrica, la cual es utilizada indistintamente por personal de salud y pacientes, generando riesgos de saturación y vulnerabilidad ante accesos no autorizados.

Para abordar estas problemáticas, se propone la implementación de un rediseño basado en tecnologías de red, que será más eficiente, segmentada y segura, facilitando el trabajo del personal médico y administrativo, y garantizando un mejor servicio a los pacientes.

I.2.2.2.- Antecedentes de Trabajos Similares

La infraestructura de red es un componente crítico para el funcionamiento eficiente de cualquier organización, ya que permite la conexión entre usuarios, dispositivos y servicios, facilitando la comunicación y el intercambio seguro de información. En el caso de la Clínica, una red moderna y bien estructurada es esencial para garantizar la continuidad de los servicios médicos, el acceso a registros clínicos y la coordinación entre el personal de salud.

Actualmente, la red de la clínica presenta múltiples desafíos relacionados con el rendimiento, la seguridad y la escalabilidad. Estos problemas afectan directamente la productividad del personal, la atención al paciente y la integridad de la información. Se han identificado deficiencias estructurales, uso de equipos mal configurados, y una red inalámbrica sin segmentación, lo que expone la infraestructura a riesgos de seguridad y dificulta su administración. Para resolver estos problemas, se propone un rediseño de la red utilizando sus diferentes tecnologías, reconocidas por su eficiencia, capacidad de gestión avanzada y relación costo-beneficio. La nueva red ofrece soluciones que permiten implementar políticas de seguridad, segmentación de tráfico, control de ancho de banda y

una administración centralizada, lo cual es ideal para entornos clínicos donde se requiere alta disponibilidad y protección de los datos sensibles.

En Bolivia, el uso de las tecnologías de red ha sido adoptado por diversos sectores, incluyendo proveedores de servicios de internet como Tigo, Entel y Viva, así como en instituciones educativas, municipios, hoteles y áreas rurales. Un caso destacable es el proyecto desarrollado por un estudiante de la Universidad Autónoma Juan Misael Saracho (UAJMS) en Tarija, titulado "Rediseño de la Red del Hospital Regional San Juan de Dios de Tarija para mejorar la eficiencia y seguridad", en el cual se aplicaron dispositivos para fortalecer la infraestructura de red de un hospital de referencia en la región, logrando una mejora significativa en la conectividad y el control de acceso.

De manera similar, el presente proyecto busca aplicar estas tecnologías en la Clínica Santísima Trinidad de Tarija, con el objetivo de solucionar las deficiencias en conectividad, seguridad y administración de red, garantizando así un entorno confiable, escalable y seguro para todos los servicios que ofrece la clínica.

I.2.3.- Justificación del Proyecto

I.2.3.1.- Tecnológica

Las tecnologías de redes avanzadas ofrecen gran escalabilidad, lo que significa que pueden adaptarse fácilmente al crecimiento de la Clínica Santísima Trinidad sin perder rendimiento. Gracias a esto, la red podrá manejar más tráfico de datos sin problemas.

Además, la implementación de VLANs permite dividir y organizar mejor la red, lo que mejora tanto la seguridad como el rendimiento. Por otro lado, integrar Asterisk como sistema de telefonía IP permitirá gestionar las llamadas internas de forma eficiente y con la posibilidad de expandirse según las necesidades.

I.2.3.2.- Económica

El uso de equipos de red es una opción económica y eficiente para mejorar la infraestructura de la clínica. Estos dispositivos son accesibles y fáciles de mantener, lo que ayuda a reducir gastos. Además, al mejorar la velocidad y la comunicación interna, se trabaja de forma más rápida y ordenada, evitando pérdidas de tiempo.

También ofrecen una buena seguridad, lo que ayuda a proteger la información importante y evita problemas que podrían generar costos extra.

I.2.3.3.- Social

La optimización de la infraestructura de red en la Clínica Santísima Trinidad de Tarija tendrá un impacto positivo en la calidad del servicio brindado tanto al personal de salud como a los pacientes. Una red más eficiente permitirá acceder de forma rápida y segura a historiales clínicos, resultados de laboratorio y sistemas de diagnóstico, mejorando significativamente la atención médica. Esto se

traduce en una atención más ágil, precisa y confiable, lo cual beneficia directamente a los pacientes y mejora su experiencia en la clínica. Además, la comunicación interna entre las distintas áreas será más fluida, lo que fortalece la coordinación y la respuesta ante emergencias.
Por otro lado, ofrecer conexión Wi-Fi a los pacientes mejora su comodidad durante la estadía y facilita la comunicación con sus familiares, brindando apoyo emocional en momentos delicados.

I.2.3.4.- Medio Ambiental

La mejora de la red en la Clínica hará que la comunicación y los procesos internos sean más rápidos y eficientes. Esto evitará traslados innecesarios dentro de la clínica y reducirá el uso de papel y otros materiales. Además, al usar tecnologías más sostenibles, la clínica ayudará a cuidar el medio ambiente sin afectar la calidad del servicio.

I.2.4.- Planteamiento del problema

La infraestructura de red actual presenta problemas de rendimiento y escalabilidad que afectan la eficiencia y productividad del personal médico y administrativo. Estos problemas se deben a la falta de una arquitectura de red adecuada, ya que no se ha realizado un rediseño de la red desde hace aproximadamente 10 años, para poder adaptarla a las necesidades actuales de la clínica. Además, la red no sigue las normas de cableado estructurado, lo que genera inconvenientes en la conexión y la transmisión de datos. También existen dificultades en el control de uso de aplicaciones, especialmente aquellas relacionadas con la gestión de pacientes y el acceso a la información médica. Asimismo, la red actual no es capaz de soportar la asignación de nuevos equipos, y los dispositivos de la clínica están expuestos a condiciones de riesgo debido a la falta de protección adecuada.

I.2.5.- Análisis del cuadro de involucrados

Grupo	Intereses	Problemas	Recursos/Mandatos
Administración	Gestionar el personal para coordinar las actividades generales de la clínica y controlar los proveedores.	Los procesos siguen siendo manuales porque no hay una comunicación en la red. Envió de Información lenta en el momento de compartir entre las distintas áreas.	M: Almacenamiento y copias de seguridad seguras y fiables de archivos importantes. Cumplimiento de las regulaciones de privacidad y seguridad de datos. M: Los proveedores deben cumplir con los plazos y condiciones acordadas.

Recepción	Brinda información sobre horarios, precios y disponibilidad de doctores. Registro de paciente que ingresa a la clínica.	La atención a los pacientes es lenta porque la red es muy amplia. El registro en el biométrico por la red es muy lento.	M: Priorizar la conectividad de recepción asegurando estabilidad en la red y evitando caídas del sistema.
Enfermería	Atender a los pacientes internados, suministrando medicamentos adecuados, utilizando manualmente los insumos de la clínica.	Genera demoras en la actualización de medicamentos por temas de la lentitud de la red (Stock). Problemas de conectividad afectan el monitoreo y suministro adecuado de medicamentos.	R: Plataforma que asegura la transmisión de datos entre el personal médico y de enfermería. M: Garantizar una red segura y estable para asegurar el acceso continuo a información clínica y comunicación eficiente.
Farmacia	Registrar los medicamentos en el sistema y distribuirlos en áreas internas de quirófano, emergencias, enfermería y terapia intensiva.	Llevar el control de medicamentos de forma manual Desabastecimiento en algunas áreas por falta de comunicación en la red. Fallas en la red o desconocimiento del personal en su uso.	R: Rediseñar la red con fibra para registrar y seguir distribuyendo medicamentos de manera rápida y eficiente.
Emergencias	Atender a pacientes que requieren atención inmediata.	No hay una comunicación por red para coordinación con las otras áreas. Falta de acceso rápido a historial clínico o pruebas médicas.	R: Notificación inmediata de emergencias. M: Garantizar conectividad rápida para atender emergencias usando el sistema de alerta y redes de comunicación.
Terapia Intensiva	Atender a pacientes en estado crítico, generalmente derivados de otros centros médicos ya sean públicos o privados del departamento.	Problemas de comunicación en la red para realizar insumos de equipos médicos específicos.	R: Conexión que garantiza la transferencia de datos médicos entre equipos médicos de forma eficiente. M: Asegurar la conectividad en terapia intensiva para un monitoreo continuo y atención rápida usando el sistema y redes seguras.

Pediatría	Brinda atención exclusiva a niños y bebés, contando con incubadoras y habitaciones especiales para internación pediátrica.	La información se gestiona manualmente, trasladando historiales clínicos a administración.	R: Red que garantiza la transferencia rápida de información sobre los pacientes pediátricos entre médicos y enfermeras.
Área Tercerizada	Gestionar servicios de Tomografía, Radiografía, Laboratorio y Ecografía	La comunicación y coordinación en la red no es óptima. Se registran errores en la facturación y cobro por temas de lentitud en la red.	M: Garantizar la conectividad de las áreas tercerizadas para una transferencia eficiente de resultados utilizando el sistema y redes seguras.
Contabilidad	La red se utiliza para poder ver los detalles de los historiales médicos del sistema para sacar información para la parte contable.	Cortes de conexión en la red, deficiente para poder realizar facturas por parte del contador.	R. Red de comunicación seguras y confiables
Internación	Comunicación de los pacientes internados con sus familiares.	Conexión inestable en la red por parte del rediseño de las ubicaciones de los Access Point	M. Ubicación de los Access Point (Wifi) que cubran todas las áreas de Internación.
Consultorio	Atiende a los pacientes enviados por administración, evalúa su estado de salud y brinda el tratamiento o seguimiento adecuado según sus necesidades.	Problemas de caídas de internet frecuentemente y lentitud en el momento de programar horarios.	R. La red de Internet de ENTEL no debe realizar ningún corte en específico.

Tabla 1. Análisis del cuadro de involucrados

I.2.6.- Árbol de Problemas

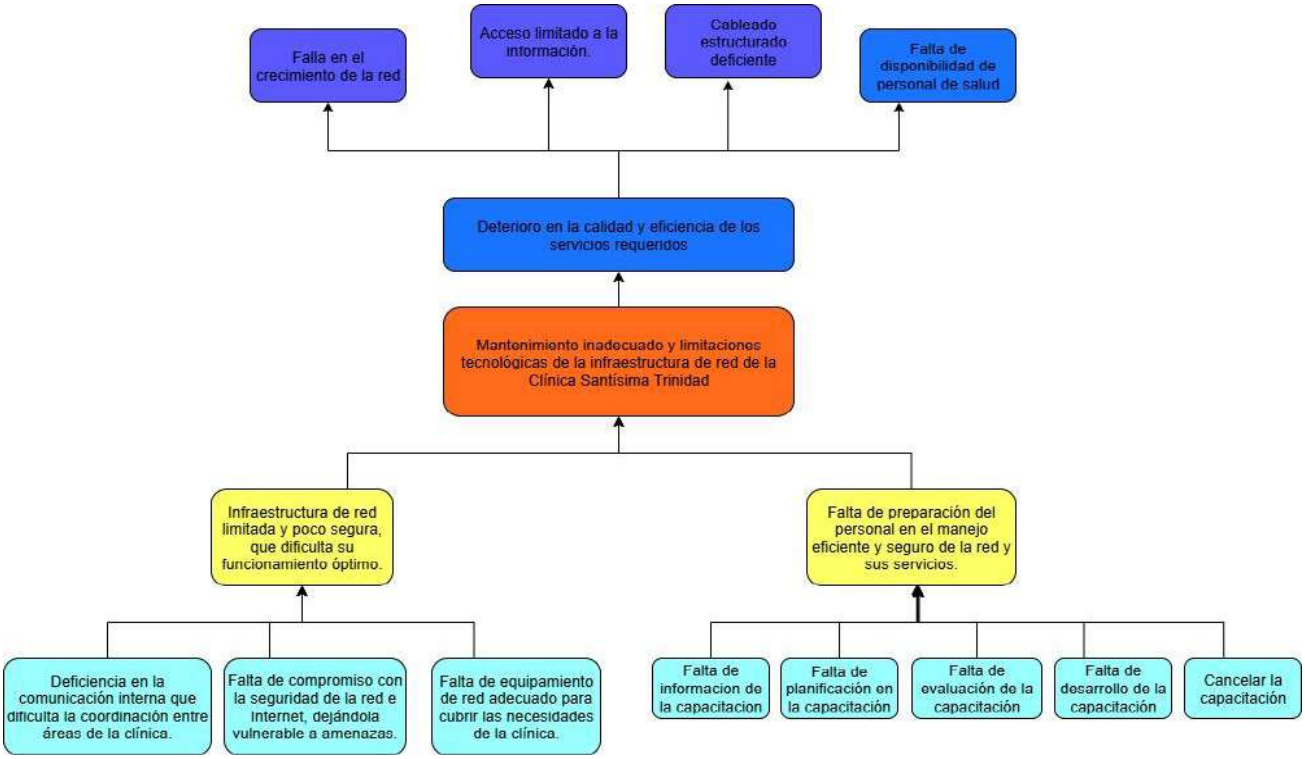

Figura 1. Árbol de Problemas

I.2.7.- Árbol de Objetivo

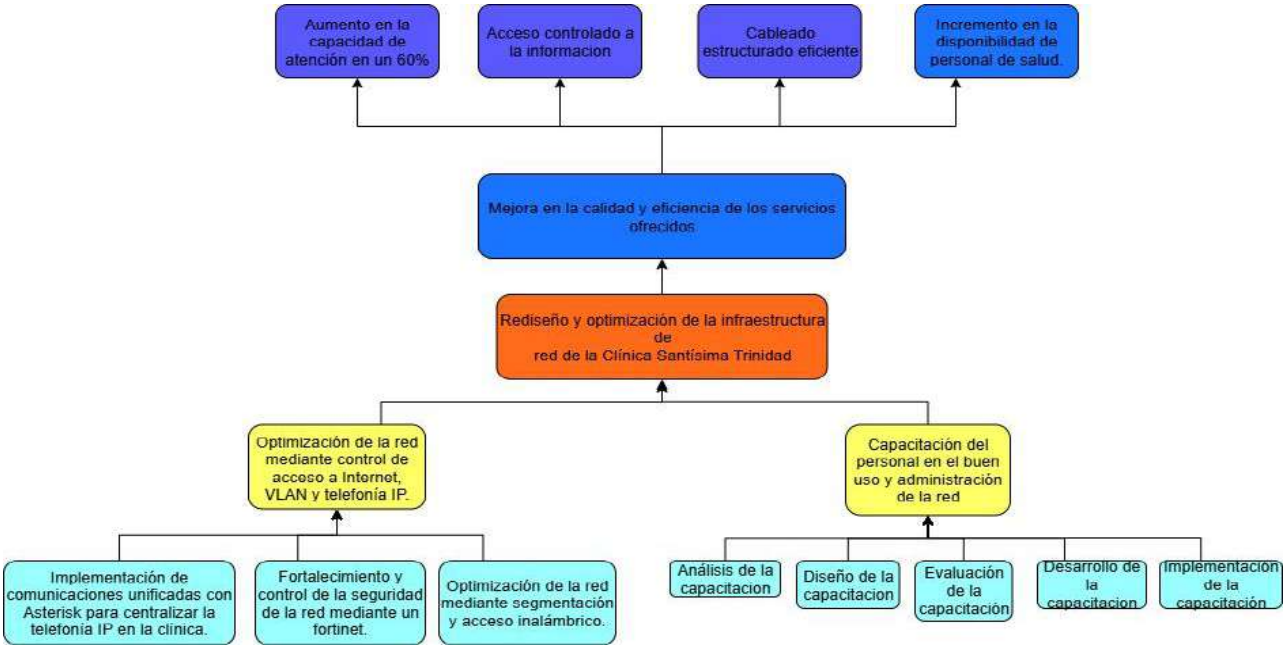

Figura 2. Árbol de Objetivos

I.2.8.- Objetivos

I.2.8.1.- Objetivo General

Rediseño y optimización de la infraestructura de red de la Clínica Santísima Trinidad

I.2.8.2.- Objetivos Específicos

- Implementación de servicios avanzados de red: monitoreo, segmentación mediante VLANs y telefonía IP.
- Capacitación del personal en el buen uso y administración de la red.

I.2.9.- Alcance

1. Análisis y diagnóstico de la situación actual

Comprende la evaluación del estado del cableado existente, los equipos activos, la conectividad y la distribución de los puntos de red en la clínica. También incluye la identificación de problemas críticos, como la falta de segmentación, caídas constantes, desorden en el direccionamiento IP y ausencia de políticas de seguridad, con el fin de definir las mejoras que serán implementadas durante el proyecto para optimizar la infraestructura de red.

2. Diseño lógico y físico de la nueva red

Se incluye el diseño lógico y físico de la nueva red de la clínica, contemplando la segmentación mediante VLANs para separar el tráfico de pacientes, personal de salud y administración. También comprende la definición de la topología general y del direccionamiento IP, así como la distribución del cableado estructurado (horizontal y vertical) siguiendo los estándares ANSI/TIA/EIA.

Se incluye la ubicación estratégica de los AP para garantizar cobertura total en cada piso y la selección y dimensionamiento de los equipos de red avanzados, tales como switches de capa 2 y 3, firewall, Access Points, servidor central, racks, UPS y patch panels, entre otros, asegurando un funcionamiento estable, seguro y eficiente de la infraestructura.

3. Implementación y configuración

Comprende la instalación de los equipos activos y pasivos aprobados en el diseño de la red, así como el reemplazo y etiquetado de cables y canaletas en mal estado. Incluye la implementación del firewall y las políticas de seguridad de la red, la configuración y prueba del sistema de telefonía IP, y la implementación de la red Wi-Fi segmentada para personal y pacientes.

Asimismo, se contempla el establecimiento de los enlaces principales entre pisos mediante fibra óptica, asegurando una comunicación rápida y estable.

4. Pruebas técnicas y verificación

Incluye la realización de pruebas de conectividad, rendimiento y comunicación entre VLANs, así como la verificación del funcionamiento del servidor central y de los módulos administrativos.

También comprende la evaluación de la cobertura Wi-Fi mediante herramientas profesionales y la validación del diseño de la red conforme a los requisitos funcionales y no funcionales establecidos en el estándar IEEE 830, garantizando que la infraestructura cumpla con los objetivos de desempeño y seguridad del proyecto.

5. Capacitación del personal

El alcance comprende la elaboración y ejecución del plan de capacitación definido en el proyecto, incluyendo el entrenamiento del personal en la administración de la red, buenas prácticas de seguridad y el uso de los nuevos sistemas implementados.

I.2.10.- Limitaciones

La realización del presente proyecto, se enfrenta a las siguientes limitaciones:

Dependencia del proveedor de Internet (ISP)

- La estabilidad y el ancho de banda dependen del proveedor TIGO, lo cual puede generar caídas eventuales o latencias.
- No es posible mejorar el rendimiento externo si el ISP no incrementa la capacidad o calidad del servicio.

Restricciones presupuestarias

- La clínica provee el hardware necesario, pero la compra de equipos avanzados podría retrasarse por presupuesto o tiempos de importación.

Exclusiones del proyecto

- No se incluye el reemplazo total del sistema informático central.
- No contempla el desarrollo de software o aplicaciones para la clínica.
- No abarca la modernización de la infraestructura eléctrica general solo se incluye UPS y soporte inmediato.
- No incluye la renovación, control de accesos y redirección del sistema de cámaras de seguridad.

Limitación por el hardware existente

- Algunos equipos existentes podrían no ser compatibles con tecnologías avanzadas, limitando la integración total del proyecto.

I.2.11.- Matriz del marco Lógico (MML)

RESUMEN NARRATIVO DEL PROYECTO	INDICADORES	MEDIOS DE VERIFICACION	SUPUESTOS
Fin Mejora en la calidad y eficiencia de los servicios ofrecidos	A un año finalizado el proyecto, la Clínica Santísima Trinidad de Tarija, contará con menos reclamos tecnológicos por parte del personal de salud en un 70%.	Carta de autorización a los funcionarios de la institución para proporcionar la información requerida para el desarrollo del proyecto.	Apoyo del personal Informático de la Clínica en el rediseño de la mejora de la red y la comunicación interna.
Propósito Rediseño y optimización de la infraestructura de red de la Clínica Santísima Trinidad	Una vez finalizado el proyecto se cumplirá con el 87% de los servicios requeridos y propuestos calculados por la siguiente formula: Cantidad de servicios Requeridos x 100 Cantidad de servicios Disponibles **Cantidad de servicios Disponibles:** 1. Conexión a la red de Internet 2. Control y seguridad al acceso a la web 3. Compartir todo tipo de archivos entre las diferentes áreas de la red. 4. Implementar un servidor SMTP (Protocolo simple de transferencia de correo). 5. Segmentación de la red mediante VLAN. 6. Implementar una central telefónica que gestiona llamadas internas usando protocolo IP. 7. Implementar un servidor DHCP 8. Despliegue de nuevos puntos de Acceso Wifi **Cantidad de servicios Requeridos:** 1. Conexión a la red de Internet 2. Control y seguridad al acceso a la web. 3. Compartir todo tipo de archivos entre las diferentes áreas de la red.	Carta de grado de satisfacción a cerca del cumplimiento del 87%.	Disponibilidad de recursos financieros propios para la implementación y mantenimiento del proyecto.

	4. Segmentación de la red mediante VLAN. 5. Implementar una central telefónica que gestiona llamadas internas usando protocolo IP. 6. Implementar un Servidor DHCP. 7. Despliegue de nuevo puntos de Acceso Wifi		
Componentes 1. Implementación de servicios avanzados de red: monitoreo, segmentación mediante VLANs y telefonía IP 2. Capacitación del personal en el buen uso y administración de la red	1. Al Finalizar el proyecto se cumplen las normas para las tecnologías de redes: Cableado estructurado • TIA/EIA-568 • TIA/EIA-569 ANSI-TIA/EIA (Asociación de la Industria de las Telecomunicaciones/ Alianza de las Industrias Electrónicas) • ANSI-TIA/EIA-568-B • ANSI-TIA/EIA-606-B • ANSI-TIA/EIA-569-B IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) • IEEE 802.3 • IEEE 802.11 • IEEE 802.11ax • IEEE 802.1Q IETF (Internet Engineering Task Force) • SIP • RTP • ISO/IEC 11801 • IETF 2. Al finalizar el proyecto se entregará el manual a los encargados administrativos de informática en la clínica.	1. Carta de la docente de Taller 3 Avalando que se han cumplido las normas establecidas. 2. Lista firmada de participantes de la capacitación	• Se reutilizarán algunos equipos que la Clínica ya posee y que actualmente están en funcionamiento dentro de la institución. • Disponibilidad de fondos de la clínica para la adquisición de nuevos dispositivos de red. • Se asume la estabilidad del tipo de cambio del dólar durante la adquisición de materiales electrónicos o equipos de red. • Se cuenta con los mismos encargados en la Clínica al finalizar el proyecto.
Actividades 1. • Analizar requerimientos	Resumen de Presupuesto:	Comprobantes de ingreso y egreso	• Apoyo del personal de la clínica con planos y datos de

- Desarrollar Diseño Lógico
- Desarrollar Diseño Físico
- Probar, optimizar y documentar diseño
- Implementar y probar la red
- Monitorear y Optimizar la Red

2.

- Análisis de la capacitación
- Diseño de la capacitación
- Desarrollo de la capacitación
- Implementación de la capacitación
- Evaluación de la capacitación

Componentes	**Aporte**
Análisis de la Infraestructura	24.000
Equipos y Dispositivos de la Infraestructura de Red	37.683,80
Rack Gabinetes	4.787
Materiales y Recursos Utilizados en la Implementación de la Red	6.917,50
Equipos de protección contra incendios	5.084
Servicio de Internet	6.348
Servicio de Telefonía IP por Asterisk	5.303,34
Servicio de Seguridad en la red	6.900
Costos Indirectos de Instalación, Certificación y Mantenimiento	13.400
Total	**110.423,64 Bs**

componentes actuales.

- Los desembolsos se realizan a tiempo

I.2.11.- Metodología de desarrollo del proyecto

I.2.11.1.- Metodología Top-Down

La metodología Top-Down se puede aplicar para el diseño de redes y consta de varias fases que permiten analizar los requerimientos y objetivos de negocio para desarrollar un diseño adecuado. Esta metodología se caracteriza por comenzar con una visión global y estratégica del proyecto, definiendo los objetivos generales y los requisitos antes de desglosarlos en componentes específicos. Esto proporciona una dirección clara desde el principio y permite una planificación detallada y estratégica del proyecto, garantizando así una alineación efectiva con los objetivos generales del mismo.

Figura 3. Metodologia Top-Down

Fase 1: Analizar Requerimientos

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

Fase 2: Desarrollar Diseño Lógico

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

Fase 3: Desarrollar Diseño Físico

- Seleccionar tecnologías y dispositivos para redes empresariales
- Seleccionar tipos de enlaces alámbricos o inalámbricos
- Considerar Distancias y tipos de conectores

Fase 4: Probar, optimizar y documentar diseño

- Probar el diseño de red
- Optimizar el diseño de red

Fase 5: Implementar y probar la red

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

Fase 6: Monitorear y Optimizar la Red

- Monitoreo de la red
- Optimización de la red

I.2.11.2.- Metodología ADDIE

La metodología ADDIE es un enfoque sistemático utilizado en el diseño instruccional para desarrollar programas efectivos de capacitación y aprendizaje en el proyecto como medio para elaborar la capacitación se tomarán en cuenta los puntos los que comprenden esta metodología los cuales son:
Fase de Análisis: En esta fase, se desarrolla una introducción al proyecto para ver para quien está dirigida la capacitación.
Fase de Diseño: En esta fase, se dispone de los métodos para el desarrollo de la capacitación ya sean medios o materiales necesarios para desarrollar la capacitación de la mejor manera.
Fase de Desarrollo: En esta fase, con los materiales dispuestos anteriormente se desarrolla o se gestiona el uso de los medios para la capacitación.
Fase de Implementación: En esta fase, se desarrolla un plan de contenidos de la capacitación para así brindarla a los capacitados.
Fase de Evaluación: En esta fase, se verifica según lo aprendido que tan beneficioso es el plan implementado con una comprobación de los resultados.

I.2.12.- Resultados esperados

Una vez implementado las nuevas tecnologías de redes avanzadas se espera obtener:

- Implementación de servicios avanzados de red: monitoreo, segmentación mediante VLANs y telefonía IP.
- Capacitación del personal en el buen uso y administración de la red.

Gracias a las herramientas avanzadas de seguridad, se espera contar con una red más segura, estable y menos expuesta a amenazas externas.

I.2.13.- Beneficiarios

I.2.13.1.- Beneficiarios Directos

Los principales beneficiarios del proyecto serán los colaboradores de la Clínica Santísima Trinidad, incluyendo al personal de las siguientes áreas: Administración, Recepción, Consultorios, Emergencias, Áreas Tercerizadas, Enfermería, Terapia Intensiva, Internación, Pediatría, Farmacia, Contabilidad y Esterilización.
El mejoramiento de la red permitirá que todos ellos trabajen de forma más rápida, segura y eficiente, lo

que se traduce en una mejor atención para los pacientes.

I.2.13.2.- Beneficiarios indirectos

Los beneficiarios indirectos son los pacientes, ya que una red más eficiente permite al personal brindar una atención más rápida, organizada y de mayor calidad.

Además, al contar con un sistema más seguro, los pacientes tendrán mayor confianza al realizar sus pagos, ya que se reducen los riesgos de errores o pérdidas de información en los procesos administrativos y financieros.

I.2.14.- Cronograma de Actividades

Actividad	Nº días	Fecha inicio	Fecha fin	M4	M5	M6	M7	M8	M9	M10	M11
Implementación de servicios avanzados de red: monitoreo, segmentación mediante VLANs y telefonía IP	**170**	**18/04/2025**	**30/09/2025**	**X**	**X**	**X**	**X**	**X**	**X**		
Analizar Requerimientos	16	18/04/2025	06/05/2025	X	X						
Desarrollar Diseño Lógico	20	07/05/2025	29/05/2025		X						
Desarrollar Diseño Físico	35	30/05/2025	09/07/2025		X	X	X				
Probar, optimizar y documentar diseño	25	10/07/2025	07/08/2025				X	X			
Implementar y probar la red	25	08/08/2025	05/09/2025					X	X		
Monitorear y Optimizar la Red	21	06/09/2025	30/09/2025						X		
Capacitación del personal en el buen uso y administración de la red	**28**	**01/10/2025**	**25/10/2025**							**X**	**X**
Análisis	2	01/10/2025	02/10/2025							X	
Diseño	5	03/10/2025	08/10/2025							X	
Desarrollo	5	09/10/2025	14/10/2025							X	
Implementación	5	15/10/2025	20/10/2025							X	
Evaluación	11	21/10/2025	01/11/2025							X	X

Tabla 2. Cronograma de Actividades

I.2.15.- Presupuesto general

Concepto	**Análisis de la Infraestructura**				
#	**RUBROS**	**Aporte Universidad**	**Aporte de la Clínica**	**Bimestral**	**TOTAL (Bs)**
1	Estipendio por el trabajo	0.00	6.000	4	24.000
Sub Total Componente					**24.000**

Concepto	**FINALIDAD**					
	Equipos y Dispositivos de la Infraestructura de Red					
#	**Tipo de equipo**	**Recurso**	**Aporte UAJMS**	**Aporte de la Clínica**	**Cantidad**	**TOTAL (Bs)**
1	Router	Cisco 2901 - CISCO2901/K9	0.00	828,95	1	828,95
2	Switch Capa 2	Cisco WS-C2960S-24PD-L Catalyst 2960S	0.00	1.260,90	4	5.043,60
3	Switch Capa 2	TL-SG2210P V3 10 puertos	0.00	969,94	4	3.879,76
3	Switch Capa 3	Cisco Catalyst 3750X-12S-S	0.00	6.873,90	1	6.873,90
4	Access Point	TP-Link Omada EAP225	0.00	560,90	8	4.487,20
5	Servidor Central del Sistema Clínico	HPE ProLiant MicroServer Gen11	0.00	8.079,60	1	8.079,60
6	Patch Pannel	Patch Pannel de 24 puertos	0.00	107,32	4	429,28
7	UPS	UPS Forza 1000VA	0.00	1.265	1	1.265
8	Consola	Consola de conmutador KVM VGA	0.00	6.796,51	1	6.796,51
Sub total componente						**37.683,80**

Concepto	FINALIDAD				
	Rack Gabinetes				
#	**Recurso**	**Aporte UAJMS**	**Aporte de la Clínica**	**Cantidad**	**TOTAL (Bs)**
1	Rack 10U	0.00	850,50	3	2.551,5
2	Rack 22U	0.00	987,29	1	987,29
3	Bandeja porta equipos	0.00	90,50	1	90,50
4	Organizador de cableado	0.00	21,47	8	171,76
5	Regleta de fuerza	0.00	160,00	5	800
6	Ventilador rack	0.00	46,51	4	186
Sub total componente					**4.787**

Concepto	FINALIDAD					
	Materiales y Recursos Utilizados en la Implementación de la Red					
#	**Tipo de Producto**	**Recurso**	**Aporte UAJMS**	**Aporte de la Clínica**	**Cantidad**	**TOTAL (Bs)**
1	Cable de red caja de 305 metros	UTP Categoría 5e	0.00	143,00	7	1000
2	Cable de red 35 metros con su conector SC	Fibra Óptica monomodo	0.00	1.225	1	1.225
3	Conector	RJ45	0.00	2,50	243	607,50
4	Roseta UTP de 4 puertos	Rosetas RJ45	0.00	60	30	1.800
5	Roseta UTP	Placa de pared	0.00	25	60	1.500

6	Canaleta	Canaletas de 40x20	0.00	8,50	70	595
7	Canaleta	Canaletas de 70x40	0.00	9,50	20	190
Subtotal componente						**6.917,50**

Concepto	**FINALIDAD**				
	Equipos de protección contra incendios				
#	**Recurso**	**Aporte UAJMS**	**Aporte institucional**	**Cantidad**	**TOTAL (Bs)**
1	Pulsador de Pánico	0.00	20	9	180
2	Central contra incendios	0.00	105	1	105
3	Sirena con luz estroboscópica	0.00	61	9	549
4	Sensor fototérmico	0.00	120	25	3.000
5	Extintores	0.00	250	5	1.250
Subtotal componente					**5.084**

Concepto	**FINALIDAD**				
	Servicio de Internet				
#	**Recurso**	**Aporte UAJMS**	**Aporte de la Clínica**	**Anual**	**TOTAL (Bs)**
1	Servicio de Internet TIGO completo	0.00	529	12	6.348
Sub total componente					**6.348**

Concepto	FINALIDAD				
	Servicios de Telefonía IP por Asterisk				
#	Recurso	Aporte UAJMS	Aporte de la Clínica	Cantidad	TOTAL (Bs)
1	Aplicación Zoiper (Licencia Premium)	0.00	453.97	1	453,97
2	Audífonos con micrófono para computadoras de Escritorio	0.00	90	30	2.700
3	Servidor DELL PowerEdge T40	0.00	2.149,37	1	2.149,37
Sub total componente					5.303,34

Concepto	FINALIDAD				
	Servicio de seguridad en la red				
#	Recurso	Aporte UAJMS	Aporte de la Clínica	Cantidad	TOTAL (Bs)
1	Fortinet 60E	0.00	4.830	1	4.830
2	Licencia	0.00	2.070	1	2.070
Sub total componente					6.900

Concepto	FINALIDAD					
	Costos Indirectos de Instalación, Certificación y Mantenimiento					
#	RUBROS	Aporte Universidad	Aporte de la Clínica	Detalle	Observación	TOTAL (Bs)
1	Instalación y cableado estructurado	0.00	3.000	Mano de obra, canalización, etiquetado y certificación de puntos de red.	Incluye pruebas de continuidad y etiquetado.	3.000
2	Instalación y configuración	0.00	1.000	Creación de extensiones,	Requiere credenciales	1.000

	Servidor de Telefonía IP Issabel			troncal SIP, buzones y pruebas de llamadas.	SIP activas, incluye puesta en marcha y validación operativa.	
3	Instalación y configuración de Fortinet	0.00	1.500	Políticas de seguridad en firewall Fortinet (interfaces, VLAN, NAT y filtrado web).	Incluye pruebas de conectividad y validación de reglas; requiere licencias activas y credenciales administrativas.	1.500
4	Configuración y puesta en marcha	0.00	2.500	Carga de configuraciones VLAN, ACL, IP, servidores y seguridad	Incluye validación técnica	2.500
5	Certificación de red	0.00	1.200	Certificación de cables y equipos activos (Fluke Test)	Según norma TIA/EIA-568	1.200
6	Capacitación técnica	0.00	800	Programa de habilitación técnica para el equipo de TI	Entre 1 y 2 horas, modalidad presencial	800
7	Mantenimiento preventivo anual	0.00	1.500	Limpieza, revisión de ventiladores, firmware, respaldo	Contrato anual	1.500
8	Mantenimiento correctivo	0.00	1.000	Fondo para reemplazo de cables/conectores o equipos	Estimado por incidencias	1.000
9	Seguridad y respaldo	0.00	900	Software antivirus, licencias y backups externos	Licencias anuales	900
Sub Total Componente						**13.400**

Análisis por Componente			
Componente	**Descripción**	**Subtotal (Bs)**	**Porcentaje del total**
Análisis de la Infraestructura	Diseño y evaluación técnica de la red.	24.000	21,7 %

Equipos y Dispositivos de la Infraestructura de Red	Insumos y equipos esenciales para la instalación de la red.	37.683,80	34,1 %
Rack Gabinetes	Soporte y organización del equipamiento de red.	4.787	4,3 %
Materiales y Recursos Utilizados en la Implementación de la Red	Componentes físicos y accesorios para el tendido y conexión de la red.	6.917,50	6,3 %
Equipos de protección contra incendios	Dispositivos de seguridad para detección y respuesta ante emergencias.	5.084	4,6 %
Servicio de Internet	Conectividad externa para acceso y operación de la red institucional.	6.348	5,8 %
Servicios de Telefonía IP por Asterisk	Comunicación interna mediante servidor VoIP centralizado.	5.303,34	4,8 %
Servicio de seguridad en la red	Protección perimetral y control del tráfico mediante firewall y licencias de seguridad.	6.900	6,3 %
Costos Indirectos de Instalación, Certificación y Mantenimiento	Servicios auxiliares para instalación.	13.400	12,1 %
Presupuesto Total en Bs		**110.423,64**	**100 %**

Tabla 3. Análisis por Componente

Condiciones

- El presupuesto tiene una duración de un año
- Sujeto a variación de precios por aumento en costos nivel nacional e internacional
- Tomando en cuenta el reutilizar los equipos de la anterior red en caso que sea necesario
- Equipos sujetos a cambio en caso de fallo ya que son pedidos que llegan de otro departamento sede
- Entrega de equipos en 170 días.

CAPÍTULO II
MARCO TEÓRICO

II.- CAPÍTULO II: MARCO TEÓRICO

II.1.- Marco Teórico

II.1.1.- Introducción

La Clínica Santísima Trinidad requiere una infraestructura de red confiable, segura y eficiente para garantizar la calidad en la atención médica y la operatividad de sus servicios. El rediseño e implementación de una red moderna permitirá mayor capacidad de transmisión de datos, estabilidad y velocidad en la comunicación interna, optimizando procesos administrativos y clínicos, y facilitando el acceso ágil a historiales y resultados. Asimismo, fortalecerá la seguridad informática mediante políticas avanzadas, segmentación por VLANs y control de accesos. La modernización con fibra óptica y soluciones de seguridad posiciona a la clínica como una institución preparada para enfrentar desafíos tecnológicos, asegurando un entorno digital eficiente y seguro para el personal y los pacientes.

II.1.2.- Modelos de protocolos y de referencias

En lo que se refiere a la interconexión de los equipos los principios para la comunicación de redes son necesarios para garantizar una transmisión de datos eficiente y fiable en un entorno de red. Los dos principios fundamentales son el modelo de capas OSI y TCP/IP.

II.1.2.1.- Modelo OSI

El modelo OSI (Interconexión de Sistemas Abiertos) es un modelo conceptual creado por la Organización Internacional para la Estandarización, el cual permite que diversos sistemas de comunicación se conecten usando protocolos estándar. En otras palabras, el OSI proporciona un estándar para que distintos sistemas de equipos puedan comunicarse entre sí.

El modelo OSI se puede ver como un lenguaje universal para la conexión de las redes de equipos. Se basa en el concepto de dividir un sistema de comunicación en siete capas abstractas, cada una apilada sobre la anterior.

Figura 4. Modelo OSI

I.1.2.1.1.- Importancia el modelo OSI

A pesar de que el Internet moderno no sigue estrictamente el modelo OSI (sigue más de cerca el paquete de protocolos de Internet más simple), este modelo sigue siendo muy útil para resolver problemas de red. Ya sea una persona que no puede lograr que su ordenador portátil se conecte a Internet o un sitio web que está caído para miles de usuarios, el modelo OSI puede ayudar a desintegrar el problema y aislar la fuente. Si el problema puede reducirse a una capa específica del modelo, se puede evitar mucho trabajo innecesario.

II.1.2.1.2.- Las 7 capas del Modelo OSI

Las siete capas de abstracción del modelo OSI pueden definirse de la siguiente manera, en orden descendente:

Capa – 7 Capa de Aplicación

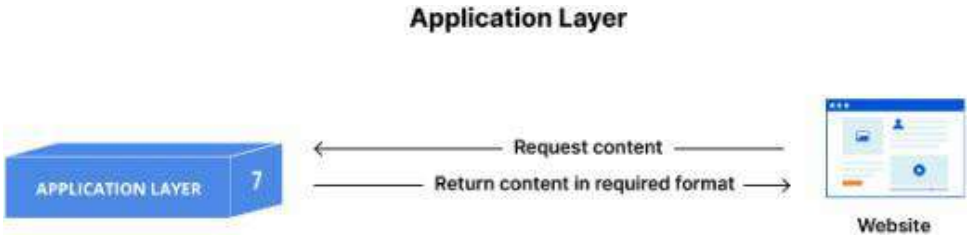

Figura 5. Capa de Aplicación

Esta es la única capa que interactúa directamente con los datos del usuario. Las aplicaciones de software, como navegadores web y clientes de correo electrónico, dependen de la capa de aplicación para iniciar comunicaciones. Sin embargo, debe quedar claro que las aplicaciones de software cliente no forman parte de la capa de aplicación; más bien, la capa de aplicación es responsable de los protocolos y la manipulación de datos de los que depende el software para presentar datos significativos al usuario.

Los protocolos de la capa de aplicación incluyen HTTP, así como también SMTP (el Protocolo simple de transferencia por correo electrónico, uno de los protocolos que permiten las comunicaciones por correo electrónico).

Capa – 6 Capa de presentación

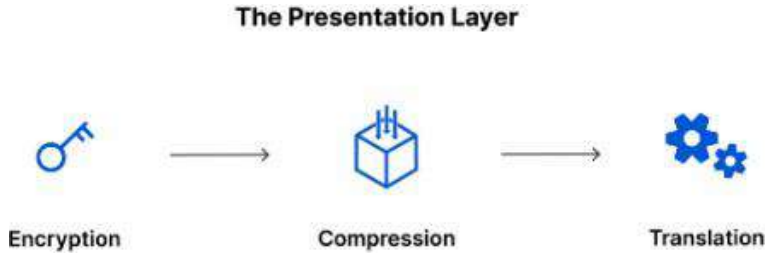

Figura 6. Capa de presentación

Esta capa es principalmente responsable de preparar los datos para que los pueda usar la capa de aplicación; en otras palabras, la capa 6 hace que los datos se preparen para su consumo por las aplicaciones. La capa de presentación es responsable de la traducción, el cifrado y la compresión de los datos.

Dos dispositivos de comunicación que se conectan entre sí podrían estar usando distintos métodos de codificación, por lo que la capa 6 es la responsable de traducir los datos entrantes en una sintaxis que la capa de aplicación del dispositivo receptor pueda comprender.

Si los dispositivos se comunican a través de una conexión cifrada, la capa 6 es responsable de añadir el cifrado en el extremo del emisor, así como de decodificar el cifrado en el extremo del receptor, para poder presentar a la capa de aplicación datos descifrados y legibles.

Después, la capa de presentación es también la encargada de comprimir los datos que recibe de la capa de aplicación antes de ser enviados a la capa 5. Esto ayuda a mejorar la velocidad y la eficiencia de la comunicación mediante la minimización de la cantidad de datos que serán transferidos.

Capa – 5 Capa de sesión

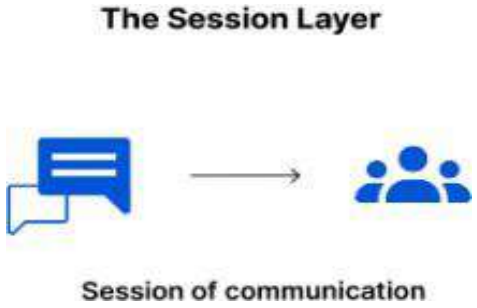

Figura 7. Capa de sesión

La capa de sesión es la responsable de la apertura y cierre de comunicaciones entre dos dispositivos. Ese tiempo que transcurre entre la apertura de la comunicación y el cierre de esta se conoce como sesión. La capa de sesión garantiza que la sesión permanezca abierta el tiempo suficiente como para transferir todos los datos que se están intercambiando; tras esto, cerrará sin demora la sesión para evitar desperdicio de recursos.

La capa de sesión también sincroniza la transferencia de datos utilizando puntos de control. Por ejemplo, si un archivo de 100 megabytes está transfiriéndose, la capa de sesión podría fijar un punto de control cada 5 megabytes. En caso de desconexión o caída tras haberse transferido, por ejemplo, 52 megabytes, la sesión podría reiniciarse a partir del último punto de control, con lo cual solo quedarían unos 50 megabytes pendientes de transmisión. Sin esos puntos de control, la transferencia en su totalidad tendría que reiniciarse desde cero.

Capa – 4 Capa de transporte

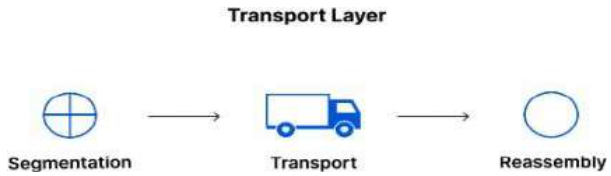

Figura 8. Capa de transporte

La capa 4 es la responsable de las comunicaciones de extremo a extremo entre dos dispositivos. Esto

implica, antes de proceder a ejecutar el envío a la capa 3, tomar datos de la capa de sesión y fragmentarlos seguidamente en trozos más pequeños llamados segmentos. La capa de transporte del dispositivo receptor es la responsable luego de rearmar tales segmentos y construir con ellos datos que la capa de sesión pueda consumir.

La capa de transporte también es responsable del control de flujo y el control de errores. El control de flujo determina una velocidad óptima de transmisión para garantizar que un emisor con una conexión rápida no abrume a un receptor con una conexión lenta. La capa de transporte realiza un control de errores en el extremo receptor al garantizar que los datos recibidos estén completos y solicitar una retransmisión si no lo están.

Los protocolos de la capa de transporte incluyen el Protocolo de control de transmisión (TCP) y el User Datagram Protocol (UDP).

Capa – 3 Capa de red

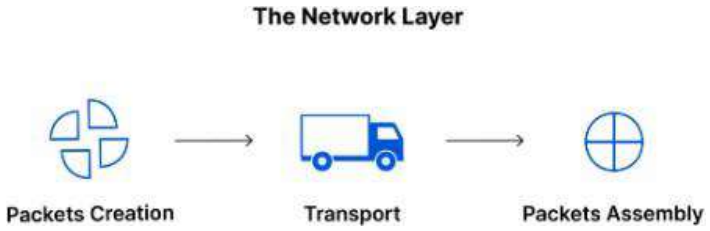

Figura 9. Capa de red

La capa de red es responsable de facilitar la transferencia de datos entre dos redes diferentes. Si los dispositivos que se comunican se encuentran en la misma red, entonces la capa de red no es necesaria. Esta capa divide los segmentos de la capa de transporte en unidades más pequeñas, llamadas paquetes, en el dispositivo del emisor, y vuelve a juntar estos paquetes en el dispositivo del receptor. La capa de red también busca la mejor ruta física para que los datos lleguen a su destino; esto se conoce como enrutamiento.

Los protocolos de la capa de red incluyen la dirección IP, el Protocolo de mensajes de control de Internet (ICMP), el Protocolo de mensajes de grupo de Internet (IGMP) y el paquete IPsec.

Capa – 2 Capa de enlace de datos

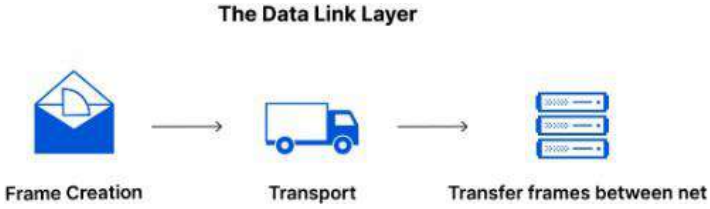

Figura 10. Capa de enlace de datos

La capa de enlace de datos es muy similar a la capa de red, excepto que la capa de enlace de datos facilita la transferencia de datos entre dos dispositivos dentro la misma red. La capa de enlace de datos toma los paquetes de la capa de red y los divide en partes más pequeñas que se denominan tramas. Al igual que la

capa de red, esta capa también es responsable del control de flujo y el control de errores en las comunicaciones dentro de la red (la capa de transporte solo realiza tareas de control de flujo y de control de errores para las comunicaciones dentro de la red).

Capa – 1 Capa física

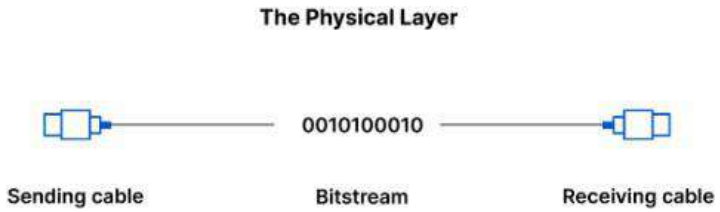

Figura 11. Capa física

Esta capa incluye el equipo físico implicado en la transferencia de datos, tal como los cables y los conmutadores de red. Esta también es la capa donde los datos se convierten en una secuencia de bits, es decir, una cadena de unos y ceros. La capa física de ambos dispositivos también debe estar de acuerdo en cuanto a una convención de señal para que los 1 puedan distinguirse de los 0 en ambos dispositivos.

Cómo transitan los datos a través del modelo OSI

Para que la información sea legible para los seres humanos se pueda transferir a través de una red de un dispositivo a otro, los datos deben atravesar las siete capas del modelo OSI en orden descendente en el dispositivo emisor y luego en orden ascendente en el extremo del receptor.

Por ejemplo, el señor Cooper quiere enviar a la señora Palmer un correo electrónico. El señor Cooper redacta dicho mensaje en una aplicación de correo y después le da a enviar. Su aplicación de correo pasa entonces su mensaje a la capa de aplicación, y esta elige un protocolo (SMTP) y pasa los datos a la capa de presentación. La capa de presentación comprime entonces los datos y los pasa a la capa de sesión, que será la que inicie la sesión de comunicación.

Los datos llegarán entonces a la capa de transporte del emisor y serán allí segmentados. Después, esos segmentos serán rotos en trozos más pequeños, paquetes, en la capa de red y en trozos aún más pequeños, tramas, en la capa de enlace de datos. Entonces la capa de enlace de datos enviará las tramas a la capa física para que puedan ser convertidas por esta en una secuencia de bits formada por unos y ceros que viaje a través de un medio físico, por ejemplo, un cable.

Cuando el ordenador de la señora Palmer reciba la secuencia de bits a través de un medio físico (por ejemplo, su wifi), los datos viajarán a través de la misma serie de capas, solo que ahora en su dispositivo y en orden inverso. Primero, la capa física convertirá la secuencia de bits en tramas que pasarán a la capa de enlace de datos. Segundo, esta capa ensamblará las tramas para formar paquetes que pueda utilizar la capa de red. Tercero la capa de red creará segmentos a partir de tales paquetes y los enviará a la capa de transporte. Por último, la capa de transporte convertirá tales segmentos en trozos de información.

Los ahora ya datos pasarán a la capa de sesión del receptor, y esta, a su vez, los hará llegar a la capa de presentación; después pondrá fin a la sesión de comunicación. La capa de presentación eliminará entonces

la compresión y pasará dos datos brutos a la capa de aplicación. Por último, la capa de aplicación suministrará datos legibles por humanos al software de correo de la señora Palmer a fin de que esta persona pueda leer en la pantalla de su portátil el correo del señor Cooper.

II.1.2.2.- Modelo TCP/IP

El modelo TCP/IP es un modelo teórico diseñado para que toda la comunicación entre computadoras y dispositivos se realice en el "mismo idioma" para que todos los dispositivos involucrados se entiendan entre sí y entreguen los mensajes correctamente.

TCP/IP (Transmission Control Protocol/Internet Protocol) es un conjunto de protocolos ampliamente utilizado para la comunicación en redes. TCP/IP se basa en el modelo de capas TCP/IP, que se asemeja al modelo de capas OSI, pero con una estructura más simplificada. El modelo TCP/IP consta de cuatro capas:

Capa – 4 Capa de aplicación

Contiene los protocolos utilizados por las aplicaciones para comunicarse a través de la red, como el Hypertext Transfer Protocol (HTTP) para la navegación web, el Simple Mail Transfer Protocol (SMTP) para el correo electrónico, el File Transfer Protocol (FTP) para la transferencia de archivos, entre otros.

Capa – 3 Capa de transporte

Proporciona servicios de transporte confiable de extremo a extremo. El protocolo más utilizado en esta capa es el Transmission Control Protocol (TCP), que garantiza la entrega y el orden de los datos.

Capa – 2 Capa de enlace de datos

Se ocupa de la transmisión de datos a nivel de bits a través del medio físico de la red. Incluye los protocolos Ethernet, Wi-Fi y otros protocolos de acceso a medios.

Capa – 1 Capa de red

Es responsable del direccionamiento y enrutamiento de los paquetes de datos en la red. El protocolo principal utilizado en esta capa es el Internet Protocol (IP).

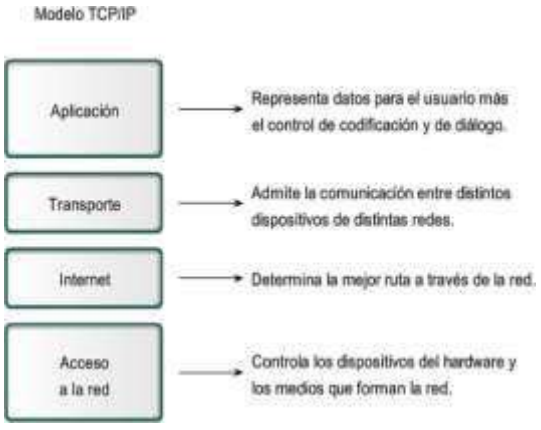

Figura 12. Modelo TCP/IP

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

La capa de aplicación del modelo TCP/IP representa 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.
El modelo OSI define un marco conceptual que divide el proceso de comunicación de la red en siete capas, cada una con funciones y responsabilidades específicas. El modelo de protocolos OSI permite que diferentes componentes de una red se comuniquen entre sí de forma estandarizada. El modelo OSI ayuda a diseñar, desarrollar y resolver problemas de redes al proporcionar una estructura modular que facilita la implementación de nuevas tecnologías y la interoperabilidad entre sistemas de diferentes proveedores.
Por otro lado, TCP/IP es un conjunto de protocolos más utilizado en la actualidad para la comunicación en Internet y en muchas redes locales. TCP/IP se basa en un modelo de cuatro capas, que se alinea de manera general con el modelo OSI. TCP/IP proporciona un conjunto de protocolos para la transmisión y el enrutamiento de datos en una red. El protocolo IP, que forma parte de TCP/IP, es responsable del direccionamiento y enrutamiento de paquetes de datos en la red, permitiendo que los datos se transmitan entre diferentes dispositivos y redes. TCP, otro protocolo clave en TCP/IP, garantiza una entrega confiable de datos mediante la segmentación, el control de flujo y la detección de errores.

Figura 13. Diferencia de Modelo TCP/IP y OSI

II.1.3.- Metodología Top-Down

En el enfoque de gestión Top-Down (descendente), promovido en la década de 1970 por los investigadores de IBM Harlan Mills y Niklaus Wirth, un equipo o gerente de proyectos toma decisiones, que luego se transmiten a través de una estructura jerárquica. Los gerentes reúnen información, la analizan y sacan conclusiones concretas. Luego, desarrollan procesos que comunican al resto del equipo para su implementación. Es posible que escuches que este estilo de gestión se conoce como “dominio y control” o “liderazgo autocrático”.

El diseño Top-Down es probablemente lo que se te pasa por la cabeza cuando piensas en el proceso de gestión. Las industrias tradicionales, como el comercio minorista, la salud o la fabricación, suelen aplicar el estilo de gestión top-down.

Cómo funciona el enfoque Top-Down

Cuando se aborda un proyecto mediante el enfoque Top-Down, los responsables de la toma de decisiones en el nivel superior comienzan con un objetivo general (ya sea a corto o largo plazo) y trabajan en retrospectiva para determinar qué acciones tendrán que realizar los diferentes grupos e individuos para alcanzar ese objetivo y lograr una posición competitiva.

El proceso de planificación de todo el proyecto se lleva a cabo a nivel de la gerencia. Luego, una vez que se crea un plan de acción, los responsables de la toma de decisiones lo comunican al resto del equipo para que lo implementen (generalmente sin mucho margen de ajuste).

El enfoque Top-Down puede ser eficaz porque se mantiene igual de un proyecto a otro. Esto permite que los equipos puedan establecer y llegar a dominar un proceso que se vuelve más eficiente con el tiempo. Dado que la naturaleza del estilo Top-Down es tan estable y confiable, muchas organizaciones (como IBM, The New York Times y otras organizaciones tradicionales) eligen dirigir todas sus empresas según este enfoque.

Diseño jerárquico de Cisco (Core – Distribution – Access)

El diseño jerárquico de Cisco se relaciona con el enfoque Top-Down porque organiza la red de forma estructurada y por niveles de responsabilidad. Se divide en tres capas:

- **Core (Núcleo):** Es la capa principal de la red. Se encarga del transporte rápido del tráfico entre los distintos pisos y áreas de la clínica mediante los enlaces troncales de fibra óptica.
- **Distribution (Distribución):** Esta capa controla la seguridad y el enrutamiento entre las VLAN y aplica políticas como las ACL. Aquí se ubican los switches principales por piso.
- **Access (Acceso):** Es donde se conectan directamente los dispositivos finales como PC, teléfonos IP, laptops y puntos de acceso WiFi. Proporciona acceso a la red interna según permisos de cada área.

Modelo Top-Down de Cisco

El Modelo Top-Down de Cisco es una metodología de diseño de redes que inicia desde las necesidades del usuario y de la organización hasta llegar a la implementación de los componentes tecnológicos. Primero se analiza qué servicios requiere la red, qué aplicaciones se utilizarán y qué niveles de seguridad y rendimiento se necesitan. Luego, se va definiendo la arquitectura lógica (protocolos, direccionamiento, segmentación) y finalmente la infraestructura física.

Principios de escalabilidad, redundancia y resiliencia

En el diseño de redes modernas es fundamental asegurar que la infraestructura pueda crecer, mantenerse disponible y recuperarse ante fallos. Para ello se aplican tres principios esenciales:

- ✓ **Escalabilidad:**

  La red debe poder crecer fácilmente conforme aumenten los dispositivos, usuarios y servicios de la clínica, sin necesidad de reemplazar toda la infraestructura. Esto incluye la posibilidad de añadir nuevos switches, access points o extensiones de red sin afectar el funcionamiento actual.

- ✓ **Redundancia:**

  Consiste en disponer de caminos o equipos alternos que permitan mantener la comunicación cuando ocurre un fallo. Por ejemplo, enlaces de respaldo entre switches o dispositivos que puedan reemplazar a otro en caso de avería, para evitar que un único punto dañe toda la red.

- ✓ **Resiliencia:**

  Es la capacidad de la red para recuperarse y continuar operativa ante interrupciones o fallos inesperados. Una red resiliente detecta el problema, se adapta automáticamente y vuelve a operar con el menor impacto posible en los servicios clínicos.

II.1.4.- Cableado Estructurado (Medios Físicos de Transmisión)

El cableado estructurado es un sistema de infraestructura de telecomunicaciones diseñado de forma estandarizada para integrar y soportar múltiples servicios como voz, datos, video y sistemas de control, dentro de un mismo entorno físico.

Este tipo de proporciona una solución flexible, organizada y escalable, que permite adaptarse fácilmente a los cambios tecnológicos y a las necesidades futuras de una organización, facilitando el mantenimiento y la expansión de la red sin necesidad de rediseñar todo el sistema.

El diseño del cableado estructurado se basa en normas internacionales, como la ANSI/TIA/EIA-568, que establecen los requerimientos técnicos para su instalación, rendimiento y compatibilidad. Estas normas garantizan una instalación eficiente y de alta calidad.

Está compuesto por diversos elementos, entre ellos:

- Cables de cobre (como par trenzado Cat 5e, Cat 6, Cat 6A) y/o fibra óptica
- Conectores (RJ45, entre otros)
- Paneles de parcheo (patch panels)
- Racks y gabinetes
- Rosetas, canaletas y dispositivos de terminación

Gracias a su diseño modular, el cableado estructurado mejora la gestión de redes, reduce el desorden de cables, y asegura un funcionamiento confiable de los sistemas de comunicación en edificios empresariales, centros de datos, instituciones educativas, hospitales, entre otros.

II.1.4.1.- Cableado Horizontal

El cableado horizontal es una parte fundamental del sistema de cableado estructurado, definido en normas como la TIA/EIA-568-B e ISO/IEC 11801. Se refiere al tramo que va desde el área de telecomunicaciones

hasta el área de trabajo del usuario, por ejemplo, una roseta o toma de red en la pared.
El cableado horizontal incluye:

- Cable de red UTP, STP o fibra óptica de baja distancia.
- Roseta o conector de red en el área de trabajo.
- Patch panel en el armario de telecomunicaciones.
- Patch cords en ambos extremos desde el patch panel al switch y desde la roseta al dispositivo.

La longitud máxima total debe ser de 90 metros, sin incluir los patch cords. Si se suman entonces la longitud total del canal puede ser de hasta 100 metros.

II.1.4.2.- Cableado Vertical o Backbone

El cableado vertical o Backbone en redes informáticas es la porción de cableado que conecta los equipos de telecomunicaciones en el cuarto(gabinete) de telecomunicaciones con los paneles de parcheo (patch panel) en los diferentes pisos de un edificio. Este tipo de cableado se utiliza en sistemas de cableado estructurado y es esencial para la transmisión de datos en una red informática. El cableado vertical se debe diseñar e instalar de acuerdo con los estándares técnicos, como el estándar ANSI/TIA/EIA-569-B, para garantizar un rendimiento óptimo de la red. El cableado del backbone incluye la conexión vertical entre pisos en edificios de varios pisos.

II.1.4.3.- Canalización del Cableado

La canalización del cableado es el sistema de conductos, rutas o estructuras diseñadas para organizar, proteger y facilitar la gestión de los cables en una red de telecomunicaciones o en un entorno de cableado estructurado. Esta es una parte fundamental para garantizar un entorno de trabajo ordenado, minimizar el desorden de cables y asegurar un acceso fácil y eficiente para el mantenimiento.
Tipos de Canalización del Cableado:

- Conductos físicos: Son tubos o canales que sirven para el paso de cables, proporcionando una ruta organizada y protegida. Los conductos pueden ser de materiales metálicos, PVC o bandejas porta cables. Además, los sistemas de piso elevado también se utilizan en instalaciones más grandes. Estos conductos protegen los cables de daños físicos y de interferencias externas, y mantienen una instalación ordenada.
- Canaletas y ductos de pared: Estos sistemas están diseñados para ocultar y proteger los cables que pasan a través de las paredes. Son ideales para instalaciones interiores, ya que ofrecen una solución estética y funcional al permitir una instalación limpia y discreta. Las canaletas y ductos también mejoran la seguridad al reducir los riesgos de daños accidentales a los cables.
- Etiquetado e identificación: El etiquetado adecuado de los cables y la canalización es esencial para facilitar la administración de la infraestructura de red. Al etiquetar correctamente los cables,

se facilita su identificación, lo que ayuda en la gestión de cambios, mantenimiento, y solución de problemas. El etiquetado puede incluir información sobre la función, origen y destino de los cables, reduciendo errores y aumentando la eficiencia durante las tareas de administración.

II.1.4.4.- Cables de red

Para seleccionar el cable de red más adecuado para una instalación, es fundamental tener en cuenta varios factores clave:

- Carga de tráfico en la red
- Nivel de seguridad requerido
- Distancia a cubrir por el cableado
- Opciones disponibles de cableado
- Presupuesto asignado

Cuanto mayor sea la protección del cable frente al ruido eléctrico, tanto interno como externo, mejor será la calidad de la señal transmitida. Un cable con mayor protección puede llevar una señal más clara, más lejos y a mayor velocidad.

II.1.4.4.1.- Cable de par trenzado

El cable de par trenzado está compuesto por varios pares de hilos de cobre entrelazados (trenzados) y protegidos por una cubierta exterior. Cada par de hilos trenzados ayuda a reducir las interferencias electromagnéticas y la diafonía entre los pares, lo que permite una transmisión de datos más estable y rápida. Usos comunes:

- ✓ Conexión de computadoras, impresoras y otros dispositivos
- ✓ Interconexión de switches, routers y puntos de acceso
- ✓ Sistemas de telefonía IP y transmisión de datos en oficinas, clínicas o centros educativos
- ✓ Cámaras de videovigilancia analógicas

II.1.4.4.2.- UTP

El cable UTP es una de las variedades más utilizadas en el ámbito de las conexiones a internet, por la gran cantidad de información que pueden transmitir, la precisión con la que realizan estos trabajos y la rapidez, que son aspectos muy importantes para el cumplimiento del cometido por el que se recurre a estos sistemas.

Así, el cable UTP es una solución muy presente en este sector, especialmente en las conexiones de redes LAN o de área local, aunque también puede verse en otras modalidades de redes.

Su nombre se debe a las siglas en inglés de Unshielded Twisted Pair, lo que en castellano se traduce como par trenzado no apantallado, para diferenciarse de las otras dos alternativas.

II.1.4.4.3.- Diferencia entre cable de red directo y cable de red cruzado

A pesar de los avances en las tecnologías inalámbricas, muchas redes de ordenadores aún dependen de

cables para la transferencia de datos de sus dispositivos. Existen varios tipos de estándares de cables de red, como, por ejemplo, el cable coaxial, el cable de par trenzado, el cable USB, el cable cruzado, el cable directo, el cable de fibra óptica, etc.

Entre estos, cable directo y cable cruzado son los tipos de cable más desconocidos. Curiosamente, ambos son dos tipos de cable Ethernet con las mismas características físicas.

II.1.4.4.4.- T-568A vs. T-568B

Antes de hablar sobre el cable directo y el cable cruzado, es necesario conocer los estándares T-568A y T-568B. Existen dos formas de conectividad diferentes, dependiendo de estos dos tipos de disposición de cableado de red.

La disposición de T-568B es sin duda la más común, aunque muchos dispositivos también son compatibles con la distribución T-568A. Si los dos extremos del cable directo están cableados conforme a un estándar, entonces estamos hablando de una conexión directa, siendo posible aplicar cualquiera de las disposiciones. Por el contrario, hablaríamos entonces de una conexión cruzada.

Algunas aplicaciones de red requieren un cable cruzado Ethernet, con un conector T-568A en un extremo y uno T-568B en el otro. Este tipo de cable se usa generalmente para conexiones directas de ordenador a ordenador. En la siguiente sección hablaremos más detalladamente sobre las características del cable directo y el cable cruzado.

II.1.4.4.4.1.- El cable de red directo

El cable de red directo no cambia su dirección. Ambos extremos utilizan el mismo estándar de cableado: T-568A o T-568B. Por lo tanto, ambos extremos (conector A y conector B) del cable directo tienen una disposición de cables del mismo color (como se muestra en la siguiente imagen). Así, el Pin 1 en el conector A se dirige al Pin 1 en el conector B, el Pin 2 al Pin 2, etc. Estos cables son ampliamente utilizados para conectar ordenadores a switches, concentradores o enrutadores.

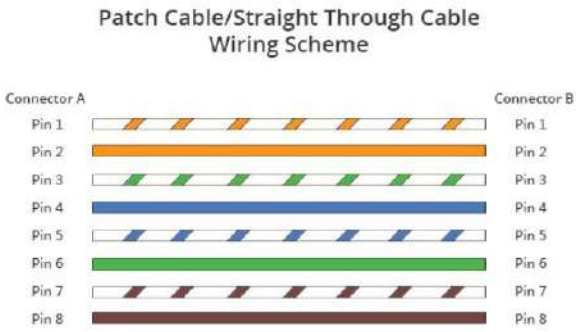

Figura 14. Cable de red directo

II.1.4.4.4.2.- El cable cruzado

El cable cruzado, como su nombre indica, se cruza o cambia de dirección de un extremo a otro. A diferencia del cable directo, el cable cruzado utiliza diferentes estándares de cableado en cada uno de sus extremos: uno el estándar T568A y el otro el estándar T568B.

Ambos lados (conector A y conector B) del cable cruzado tendrán una disposición de cables de diferente color; los cables que salen del conector A deben coincidir con sus pins correspondientes en el conector B, tal y como se muestra en el siguiente ejemplo. Los cables cruzados se usan principalmente para conectar dos enrutadores, ordenadores o concentradores (hub).

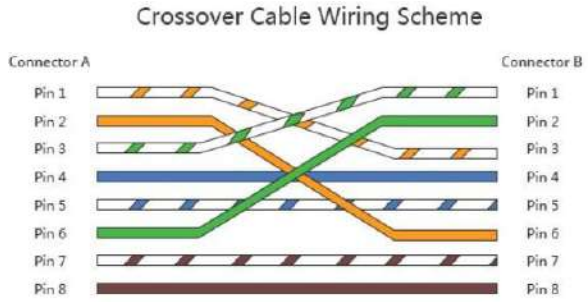

Figura 15. Cable cruzado

II.1.4.4.5.- Categorías de cables de red de par trenzado

Además de fijarnos en el tipo de cable en función del recubrimiento que incorpora, es muy importante fijarnos en el tipo de categoría de cable de red. Dependiendo de la categoría, el nivel de trenzado del cable será mayor o menor, además, en pruebas de laboratorio se puede ver la frecuencia que soporta para poder enviar datos a mayor o menor velocidad. Actualmente los cables Cat5 ya no se utilizan, sin embargo, los cables Cat5e (enhanced o mejorado) son los que vemos comúnmente en los routers domésticos cuando incorporan un cable de red.

Todos los cables de red soportan una distancia máxima de hasta 100 metros, esto es una limitación que impone el propio estándar Ethernet, no el cable en sí. En la siguiente tabla se pueden ver las diferentes categorías hasta Cat 7, la velocidad máxima que se permite y la frecuencia de funcionamiento del cable.

CATEGORÍA	VELOCIDAD	FRECUENCIA
CAT 5	100 Mbit/s	100 MHz
CAT 5E	1000 Mbit/s	100 MHz
CAT 6	1000 Mbit/s	250 MHz
CAT 6A	10000 Mbit/s	500 MHz
CAT 7	10000 Mbit/s	600 MHz

Figura 16. Categorías de cables de red de par trenzado

II.1.4.4.6.- Cable de fibra óptica

Es un tipo de cable utilizado para transmitir datos a través de pulsos de luz. A diferencia de los cables de cobre tradicionales, los cables de fibra óptica ofrecen una mayor capacidad de ancho de banda y una menor atenuación, lo que permite transmitir datos a largas distancias con menos pérdida de señal. Este tiene bastantes usos principalmente en el manejo de telecomunicaciones servicio de internet, también se puede aplicar a redes de área local o transmisión de señales de televisión, pero su alto costo con relación al

par trenzado de cobre no tan agradable para uso común.

- ✓ Servicios de Internet de alta velocidad
- ✓ Redes de área local (LAN) en empresas o centros de datos
- ✓ Transmisión de señales de televisión
- ✓ Interconexión de edificios o campus

II.1.4.4.7.- Longitud del cable

La longitud total del cablead en una red incluye todos los tramos desde el dispositivo final hasta el equipo de red (como un switch), abarcando el cable desde el dispositivo hasta la toma de red en la pared, el cable horizontal hasta el patch panel, y los patch cords que conectan el patch panel al switch. Según el estándar ANSI/TIA/EIA-568-B, la longitud máxima permitida para una instalación con cable UTP es de 100 metros por canal, compuesta por hasta 90 metros de cableado horizontal permanente y hasta 10 metros de cables de conexión (patch cords) distribuidos entre ambos extremos. Superar esta distancia puede afectar el rendimiento y la calidad de la señal de la red, por lo que es fundamental considerar todos los tramos, incluyendo interconexiones entre pisos o edificios, dentro del cálculo total.

II.1.4.4.8.- Certificación de cableado

Se probarán todos los cables de cobre y fibra óptica instalados en cada piso y área de la clínica, utilizando certificadores especializados que verifican continuidad, velocidad, diafonía y atenuación. Los resultados se registrarán en informes técnicos para identificar posibles fallas. En caso de detectar cables defectuosos, se corregirán o reemplazarán y se volverán a probar hasta obtener la certificación completa. Esto garantizará que la red funcione de manera confiable, segura y con el rendimiento necesario para los servicios clínicos y administrativos.

II.1.5.- Equipos Tecnológicos

En una red existen dos clasificaciones principales de dispositivos. La primera corresponde a los dispositivos de usuario final, que son aquellos que proporcionan servicios directamente al usuario, como computadoras, impresoras, escáneres, teléfonos IP, entre otros. La segunda clasificación incluye los dispositivos de red, cuya función principal es permitir y gestionar la comunicación entre los dispositivos de usuario final. En esta categoría se encuentran equipos como switches, routers, access points, firewalls.

II.1.5.1.- Dispositivo de red avanzadas

Para garantizar una red segura, eficiente y preparada para el crecimiento futuro, la Clínica Santísima Trinidad implementa dispositivos de red avanzados que permiten un control centralizado, segmentación eficiente del tráfico y conectividad confiable en todos sus pisos.

- **Firewall de seguridad:**

  Dispositivo esencial para proteger la red de accesos no autorizados y amenazas externas. Permite aplicar políticas de seguridad diferenciadas para personal médico, pacientes, y servicios críticos

como sistemas de historia clínica y administración.

- **Router de alto rendimiento:**
  Encargados de interconectar y enrutar el tráfico entre las distintas VLANs y hacia internet. Permiten establecer políticas de comunicación, direccionamiento IP, control de acceso y asegurar la conectividad estable entre todos los pisos de la clínica.
- **Switches gestionables de alto rendimiento:**
  Permiten segmentar la red mediante VLANs, garantizando el aislamiento y seguridad entre áreas. También permiten supervisar y priorizar el tráfico, especialmente en aplicaciones sensibles como videollamadas o telemedicina.
- **Access Points profesionales:**
  Puntos de acceso inalámbrico distribuidos estratégicamente por la clínica, que permiten a médicos, personal y pacientes conectarse a la red con buena cobertura, estabilidad y seguridad. Se configuran con SSID diferenciados para separar el tráfico según el tipo de usuario.
- **Patch panel y racks de comunicaciones:**
  Infraestructura física organizada que facilita la gestión del cableado, mantenimiento, escalabilidad y orden en cada piso de la clínica.

II.1.5.1.1.- Router de alto rendimiento

En primer lugar, un Router se utiliza para conectar varias redes. Por ejemplo, puede utilizar un Router para conectar Ordenadores en red a Internet, por lo tanto, compartir una conexión de Internet entre varios usuarios.

El Router actuará como distribuidor, como resultado, seleccionará la mejor ruta de desplazamiento de la información para que la reciba rápidamente.

Los Routers analizan los datos que se van a enviar a través de una red, como resultado, los empaquetan de forma diferente y los envían a otra red o a través de un tipo de red distinto. Conecta su negocio con el mundo exterior, además de proteger la información de amenazas a la seguridad e, incluso, pueden decidir qué computadoras tienen prioridad sobre las demás.

El funcionamiento de una red consiste en conectar ordenadores y periféricos mediante dos partes del equipo, por lo general: Switches y Routers. Estos dos elementos permiten a los dispositivos conectados a la red comunicarse con los demás y con otras redes.

Un Router es útil para dividir las LAN en dominios de difusión (broadcast) separados, sobre todo se debe utilizar al conectar estas LAN sobre una WAN.

Los Routers se comunican entre sí mediante conexiones WAN, y conectan redes dentro de sistemas locales, así como el backbone de Internet.

Operan en la capa 3, tomando decisiones basadas en direcciones de red.

Figura 17. Router

II.1.5.1.2.- Switches gestionables de alto rendimiento

Conmutador

Conmutador (switch) es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más host de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada esta.

Los conmutadores se utilizan cuando se desea conectar múltiples tramos de una red, fusionándolos en una sola red. Al igual que los puentes, dado que funcionan como un filtro en la red y solo retransmiten la información hacia los tramos en los que hay el destinatario de la trama de red, mejoran el rendimiento y la seguridad de las redes de área local (LAN).

Figura 18. Switch conmutador

Conmutadores de capa 2

Son los conmutadores tradicionales, que funcionan como puentes multi-puertos. Su principal finalidad es dividir una LAN en múltiples dominios de colisión, o en los casos de las redes en anillo, segmentar la LAN en diversos anillos. Basan su decisión de envío en la dirección MAC destino que contiene cada trama.

Los conmutadores de la capa 2 posibilitan múltiples transmisiones simultáneas sin interferir en otras sub-redes. Los switches de capa 2 no consiguen, sin embargo, filtrar difusiones o broadcasts, multicasts (en el caso en que más de una sub-red contenga las estaciones pertenecientes al grupo multicast de destino), ni tramas cuyo destino aún no haya sido incluido en la tabla de direccionamiento.

Conmutadores de capa 3

Son los conmutadores que, además de las funciones tradicionales de la capa 2, incorporan algunas funciones de enrutamiento o routing, como por ejemplo la determinación del camino basado en informaciones de capa de red (capa 3 del modelo OSI), validación de la integridad del cableado de la capa 3 por checksum y soporte a los protocolos de routing tradicionales (RIP, OSPF, etc.).

Los conmutadores de capa 3 soportan también la definición de redes virtuales (VLAN), y según modelos posibilitan la comunicación entre las diversas VLAN sin la necesidad de utilizar un router externo.

Por permitir la unión de segmentos de diferentes dominios de difusión o broadcast, los switches de capa 3 son particularmente recomendados para la segmentación de redes LAN muy grandes, donde la simple utilización de switches de capa 2 provocaría una pérdida de rendimiento y eficiencia de la ADSL, debido a la cantidad excesiva de broadcasts.

Se puede afirmar que la implementación típica de un switch de capa 3 es más escalable que un enrutador, pues este último utiliza las técnicas de enrutamiento a nivel 3 y enrutamiento a nivel 2 como complementos, mientras que los switches sobreponen la función de enrutamiento encima del encaminamiento, aplicando el primero donde sea necesario.

II.1.5.1.3.- Patch panel y racks de comunicaciones

Un patch panel, también conocido como panel de conexión o bahía de rutas, es una pieza de montaje de hardware con varios puertos para conectar y gestionar los cables LAN o los cables de fibra/cobre entrantes y salientes. Los paneles de conexión pueden ser bastante pequeños, con sólo unos pocos puertos, o muy grandes, con varios centenares de puertos. También pueden configurarse para cables de fibra óptica, cables RJ45 y muchos otros.

Patch panel Ethernet

Patch panel Ethernet Cat5e/Cat6: está diseñado para cables de cobre apantallados y sin apantallar, como los cables Ethernet Cat5e, Cat6 y Cat6a. Los paneles de conexión Ethernet Cat5e/Cat6 están disponibles con los diseños de paso (feed-through) y de punzonado (punch-down).

Patch panel Keystone en blanco: Este panel acepta tanto acopladores como conectores Keystone para configurar tu patch panel Ethernet de modo que se adapte a una variedad de esquemas. Puedes montarlo en cualquier rack de relés, armario o soporte de pared con las medidas estándar (19 pulgadas) para crear un patch panel de montaje en rack especializado que se adapte a tus necesidades de red particulares.

Figura 19. Patch panel ethernet

Gabinete de Telecomunicaciones

Un bastidor o rack un soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones. Las medidas para la anchura están normalizadas para que sean compatibles con equipamiento de distintos fabricantes. También son llamados cabinas, gabinetes o armarios.
Externamente, los racks para montaje de servidores tienen una anchura estándar de 600 milímetros (mm) y un fondo de 600, 800, 900, 1000 e incluso 1200 mm. La anchura de 600 mm para racks de servidores coincide con el tamaño estándar de las losetas en los centros de datos. De esta manera es muy sencillo hacer distribuciones de espacios en centros de datos (CPD). Para el cableado de datos se utilizan también racks de 800 mm de ancho, cuando es necesario disponer de suficiente espacio lateral para el guiado de cables.
Está diseñada para alojar y organizar equipos y dispositivos de telecomunicaciones en una red. Proporciona un entorno seguro y ordenado para montar los componentes de la infraestructura de red, facilitando la gestión de cables, la ventilación, la seguridad y la escalabilidad de la red.

Tipos de Gabinetes:

Gabinete de montaje en pared: Ideal para espacios reducidos, se monta en la pared y se utiliza para equipos más pequeños como switches, routers y patch panels.

Figura 20. Gabinete de pared

Gabinete de piso: Estructura independiente que se coloca en el suelo, adecuada para redes más grandes. Permite alojar servidores, switches, unidades de almacenamiento, entre otros.

Figura 21. Gabinete de piso

IDF

Un IDF (Marco de Distribución Intermedio) es un punto donde se organiza y distribuye el cableado de red dentro de un edificio. Su función es conectar los cables que vienen del MDF (Marco de Distribución

Principal) con los equipos que están en diferentes áreas o pisos. Gracias al IDF, el cableado no tiene que salir directamente del MDF hasta cada dispositivo, lo que hace que la red sea más ordenada, fácil de mantener y funcione mejor.

MDF

Una sala MDF (Main Distribution Frame) es el punto central de comunicaciones dentro de un edificio grande o un campus empresarial. Funciona como un hub principal, donde convergen todas las líneas de comunicación: telefonía, datos y acceso a Internet.

Su función es organizar, distribuir y gestionar esas conexiones para garantizar una transmisión de datos rápida, eficiente y segura entre todos los dispositivos de la red.

En otras palabras, la sala MDF concentra todas las conexiones entrantes y salientes de la infraestructura de red. Dentro de ella se encuentra el marco de distribución principal, que consiste en uno o varios paneles donde terminan y se conectan los cables procedentes de distintas áreas del edificio.

Desde el MDF, el cableado se distribuye hacia los distintos pisos o sectores a través de salas IDF (Intermediate Distribution Frame) o mediante conmutadores de red, que luego llevan la conexión hasta oficinas y dispositivos finales.

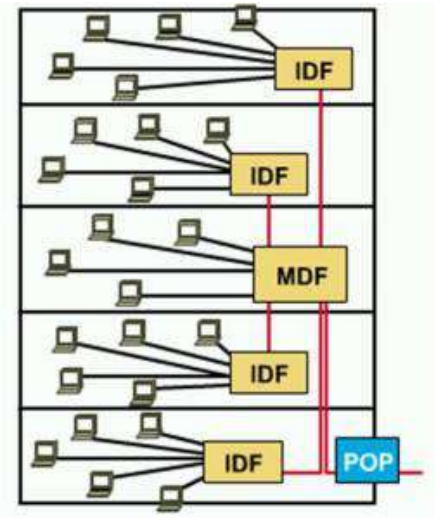

Figura 22. MDF e IDF

II.1.5.1.4.- Access Points profesionales

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 de los puntos de acceso

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 dispositivos 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.

Permite más usuarios conectados, al mismo tiempo.

Ubicación recomendable de tu punto de acceso

Para elegir una ubicación para estos puntos de acceso, se debe tener en cuenta estar lo más cerca posible del dispositivo, es recomendable instalar el punto de acceso en una posición elevada en la pared o en el techo, lo que facilita una mayor cobertura al evitar obstáculos directos. De esta forma se conseguirá la mejor señal posible. Sin embargo, También se tiene que tener en cuenta que las paredes, tuberías de agua, masas de agua, planchas metálicas y emisores de frecuencias similares como microondas interfieren en la conexión de estos dispositivos. Por lo que es importante tenerlas en cuenta a la hora de situarlos.

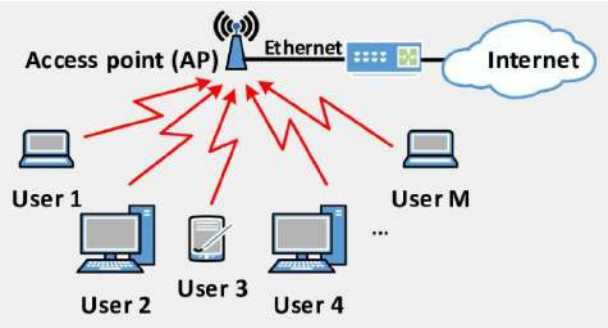

Figura 23. Ubicación recomendable de tu punto de acceso

II.1.5.1.4.1.- Wi-fi (Fidelidad inalámbrica)

Wifi, que es una contracción del término en inglés Wireless Fidelity (Wi-Fi o fidelidad inalámbrica), es una tecnología de redes inalámbricas que permite a los dispositivos electrónicos conectarse entre sí de manera fluida a una red mediante frecuencias de radio. La red, llamada una red inalámbrica de área local (o WLAN por su acrónimo en inglés) permite a ciertos dispositivos, como smartphones, tablets,

ordenadores portátiles o de sobremesa, conectarse a internet y comunicarse entre sí sin necesidad de cables físicos, como sí ocurre con los puertos Ethernet.

La mayoría de las redes inalámbricas se configuran mediante un Access Point, que actúa como un centro de transmisión de la señal inalámbrica o la frecuencia de wifi. Dada su simplicidad y facilidad de acceso, el uso de las redes wifi se ha generalizado en diversos lugares, como oficinas comerciales, aeropuertos, hoteles, cafeterías, bibliotecas y otros espacios públicos. Esto, sin embargo, es motivo de preocupaciones en el ámbito de la seguridad, porque diversas redes públicas carecen de los protocolos de seguridad adecuados, posibilitando así que los hackers accedan y roben información personal o confidencial.

El Wi-Fi opera principalmente en la Capa 1 (Física), encargada de la transmisión de datos mediante ondas de radio, y en la Capa 2 (Enlace de datos), que regula el acceso al medio inalámbrico, administra las direcciones MAC y organiza la transmisión de tramas entre los dispositivos.

Funcionamiento del wifi

Las redes wifi funcionan mediante la transmisión de ondas de radio en diversas frecuencias para brindar conectividad inalámbrica a redes y a internet a diversas velocidades. Típicamente se les agrupa en rangos de frecuencia de 2.4 GHz, 5 GHz y 6 GHz. En general, mientras mayor es la frecuencia, mayores son las velocidades. Sin embargo, dependiendo de sus necesidades, una frecuencia mayor no siempre es la mejor opción. Las frecuencias menores, como las de 2,4 GHz viajan más lejos y brindan un mayor rango a velocidades menores que los 6 GHz, lo que brinda unas mayores velocidades y rendimiento, pero menos rango de movimiento.

Para proporcionar una conexión eficiente y confiable, las redes wifi usan uno de los muchos protocolos IEEE 802.11, un conjunto de estándares desarrollados por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) para determinar las especificaciones de WLAN. Entre los protocolos más utilizados están 802.11a, 802.11b, 802.11g, 802.11n y 802.11ac, cada uno de los cuales brinda un conjunto único de parámetros, como rango de frecuencias de operación, tasa máxima de datos y técnicas de modulación.

Las redes wifi funcionan como un mecanismo de comunicación bidireccional entre un dispositivo y el Access Point. Cuando un dispositivo quiere conectarse a una red wifi, emite un mensaje conocido como una solicitud de sondeo que escanea las redes disponibles cercanas. El Access Point, más conocido como un punto de acceso de wifi, recibe la solicitud y responde con su propio mensaje, llamado baliza, que contiene el nombre de la red (SSID), el tipo de cifrado que se usa (si lo hay) y la fuerza de la señal (RSSI).

Una vez que un dispositivo recibe la baliza del punto de acceso, se conecta a la red enviando una “solicitud de autenticación”. A continuación, el punto de acceso verifica las credenciales del dispositivo (por ejemplo, la contraseña de wifi) y le asigna a una dirección IP. En ese momento, el dispositivo está oficialmente conectado a la red wifi. Puede acceder a internet si la red está conectada a esta, o puede comunicarse con otros dispositivos en la misma red.

Seguridad inalámbrica

La seguridad inalámbrica es un aspecto crucial para permanecer seguro en línea.

El uso de las medidas adecuadas de seguridad de Wi-Fi es fundamental; sin embargo, al hacerlo, es importante comprender las diferencias entre los diferentes estándares de cifrado inalámbrico, incluidos WEP, WPA, WPA2 y WPA3.

WEP (Wired Equivalent Privacy): Un protocolo de seguridad inalámbrica antiguo y vulnerable a ataques de hacking.

WPA (Wi-Fi Protected Access): Reemplazó a WEP con un cifrado más fuerte.

WPA2: Mejoró la seguridad más allá de WPA.

WPA3: El estándar más reciente con protocolos de autenticación y cifrado mejorados, ofreciendo una mejor protección contra amenazas cibernéticas.

WEP (Wired Equivalent Privacy)

Las redes Wi-Fi transmiten datos a través de ondas de radio, lo que hace que puedan ser fácilmente interceptadas si no se usan medidas de seguridad. WEP, introducido en 1997, fue el primer intento de proteger las redes inalámbricas mediante el cifrado de los datos.

Con WEP, la información enviada por la red se codifica con una clave única de 64 o 128 bits, lo que significa que todos los dispositivos de la red usan la misma contraseña para cifrar y descifrar la información. Esto permite que los dispositivos autorizados se comuniquen de forma segura, mientras que cualquier persona que intente interceptar los datos no pueda leerlos fácilmente.

WPA (Wi-Fi Protected Access)

WPA surgió en 2003 como reemplazo de WEP para mejorar la seguridad de las redes Wi-Fi. A diferencia de WEP, que usaba la misma clave para todos los dispositivos, WPA cambia dinámicamente la clave de cifrado mediante un sistema llamado TKIP (Protocolo de Integridad de Clave Temporal), lo que dificulta que los intrusos descifren la información.

WPA también incorporó comprobaciones de integridad para asegurarse de que los datos no hayan sido alterados durante la transmisión y utilizaba claves de 256 bits, mucho más seguras que las de WEP. Posteriormente, TKIP fue reemplazado por el cifrado AES, más robusto y confiable.

La “clave WPA” es simplemente la contraseña que un dispositivo necesita para conectarse a la red. Esta puede venir impresa en el router o ser asignada por el administrador de la red, y en caso de pérdida, se puede restablecer.

WPA2(Acceso Wi-Fi Protegido 2)

WPA2 se introdujo en 2004 como una mejora de WPA, ofreciendo mayor seguridad para redes Wi-Fi. Funciona en dos modos:

- **Modo personal o clave precompartida (WPA2-PSK)**: utiliza una contraseña compartida, generalmente para redes domésticas.

- **Modo empresarial (WPA2-EAP)**: pensado para empresas u organizaciones, usando un sistema de autenticación más avanzado.

Ambos modos usan CCMP (Protocolo de Código de Autenticación de Mensajes en Modo de Contador), basado en AES (Cifrado Estándar Avanzado), que garantiza que los datos transmitidos sean auténticos e íntegros. CCMP es mucho más seguro que TKIP, usado en WPA, dificultando que los atacantes descifren la información.

Sin embargo, WPA2 no es perfecto: es vulnerable a ataques como KRACK, que permiten a un atacante engañar a un dispositivo para conectarse a una red falsa y obtener parte de la información transmitida. Aun así, WPA2 sigue siendo más seguro que WEP o WPA y puede actualizarse para proteger la red.

WPA3 (Acceso Wi-Fi Protegido 3)

Es la versión más reciente del protocolo de seguridad para redes Wi-Fi, introducida en 2018 por Wi-Fi Alliance, y ofrece mejoras significativas para uso personal y empresarial.

- **Cifrado individualizado de datos:** cada dispositivo que se conecta a la red pública recibe su propio cifrado, lo que protege la información incluso si la red es compartida. WPA3 utiliza GCMP-256, un cifrado más fuerte que el usado en WPA2.
- **Autenticación segura mediante Wi-Fi DPP:** permite conectar dispositivos usando NFC o códigos QR, creando un enlace seguro entre el dispositivo y el punto de acceso, incluso si la contraseña es débil.
- **Protección contra ataques de fuerza bruta:** limita los intentos de adivinar contraseñas fuera de línea, obligando al atacante a interactuar físicamente con el dispositivo, aumentando significativamente la seguridad en redes públicas abiertas.

En resumen, WPA3 es más seguro y moderno que WPA2, ofreciendo protección avanzada frente a ataques y mayor privacidad para usuarios y dispositivos conectados a la red.

II.1.5.1.4.2.- 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.1.5.1.5.- Seguridad en la red

La seguridad en la red es esencial para proteger la infraestructura tecnológica de la clínica, garantizar la continuidad de los servicios médicos y evitar accesos no autorizados. Para ello, se implementa un firewall Fortinet que permite monitorear, filtrar y controlar todo el tráfico de datos que ingresa o sale de la red. Este dispositivo actúa como una barrera entre redes confiables y no confiables, aplicando reglas de seguridad basadas en direcciones IP, puertos, protocolos y tipos de contenido. Además, opera

principalmente en las capas 3 (Red) y 4 (Transporte) del modelo OSI, lo que le permite gestionar el tráfico en función de su origen, destino y naturaleza.

Segmentación por VLAN

La segmentación por VLAN se implementará creando redes lógicas separadas para cada área de la clínica (Administración, Internación, Consultorios, etc). Cada VLAN tendrá un ID independiente y se interconectará mediante el router o firewall Fortinet, que será el encargado de decidir qué VLANs pueden comunicarse entre sí.Lista de Control de Acceso (ACL)

Listas de Control de Acceso (ACL)

Se configurarán ACLs en el router para controlar y filtrar el tráfico que entra y sale de la red. Estas listas definirán qué dispositivos o direcciones IP pueden acceder a ciertos servicios y aplicaciones, asegurando que solo usuarios autorizados puedan utilizar los recursos de la clínica. Por ejemplo, se permitirá el acceso de la VLAN de administración a los servidores de gestión, mientras que se restringirá a los pacientes.

II.1.5.1.5.1.- Fortinet

Figura 25. Fortinet

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.

Políticas de acceso

Son reglas configuradas en el firewall Fortinet que permitirán decidir qué VLANs, equipos o áreas de la clínica pueden comunicarse entre sí y qué tipo de tráfico se autoriza. Estas políticas permiten controlar, limitar o bloquear accesos entre departamentos, mejorar la seguridad y evitar que usuarios no autorizados entren a recursos internos.

Filtrado por aplicación

Es una técnica de seguridad que permite permitir o bloquear el uso de aplicaciones específicas como Netflix, Zoom o juegos en línea dentro de la red, para controlar qué tipos de programas pueden conectarse a internet y proteger el uso adecuado de los recursos.

Control de trafico

El control de tráfico en Fortinet permite gestionar cómo circulan los datos dentro de la red de la clínica. A través de políticas y reglas, el firewall puede priorizar servicios importantes, limitar conexiones innecesarias, bloquear tráfico sospechoso y asegurar que cada VLAN utilice el ancho de banda adecuado.

Control de tráfico entrante

Permite el tráfico entrante mediante el protocolo HTTPS, a través del puerto 443, dirigido al servidor web de la clínica. Esta medida garantiza el acceso seguro desde redes externas, protegiendo la confidencialidad e integridad de los datos transmitidos mediante cifrado.

Control de tráfico saliente

Permiten al personal de salud y a los pacientes acceder solo a sitios web previamente autorizados, relacionados con funciones médicas, educativas o de interés general. Esta medida busca garantizar un uso adecuado de los recursos de red, evitando el acceso a contenidos no pertinentes o peligrosos.

Necesidad para la clínica

La necesidad de Fortinet en la Clínica Santísima Trinidad es garantizar la seguridad integral de la red, proteger la información sensible de los pacientes, controlar el acceso a aplicaciones críticas y prevenir amenazas de forma automatizada, asegurando que los servicios clínicos y administrativos funcionen sin interrupciones por problemas de seguridad.

II.1.5.1.5.2.- Glaswire

Figura 26. GlassWire

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.

Como funciona Glaswire

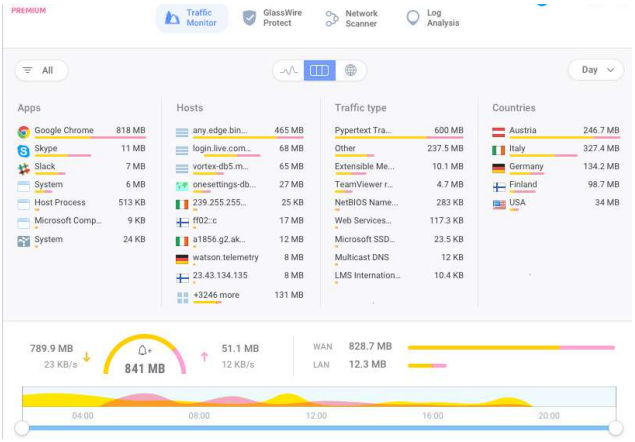

Figura 27. Como funciona Glaswire

En la imagen se muestra cómo GlassWire monitorea el tráfico de red del equipo en tiempo real. La herramienta presenta de forma clara qué aplicaciones están usando Internet, a qué servidores se están conectando, qué tipos de tráfico se generan y desde qué países provienen las conexiones. También incluye un gráfico que permite ver la actividad de la red a lo largo del día. En general, la imagen refleja que

GlassWire ofrece una visión completa del consumo de datos y del comportamiento de la red del dispositivo.

Cortafuegos

Figura 28. Cortafuegos

El objetivo del cortafuegos GlassWire 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.

II.1.6.- Direccionamiento y Segmentación de Redes

Una dirección IP es una dirección única que identifica a un dispositivo en Internet o en una red local. IP significa “protocolo de Internet”, que es el conjunto de reglas que rigen el formato de los datos enviados a través de Internet o la red local.

En esencia, las direcciones IP son el identificador que permite el envío de información entre dispositivos en una red. Contienen información de la ubicación y brindan a los dispositivos acceso de comunicación. Internet necesita una forma de diferenciar entre distintas computadoras, enrutadores y sitios web. Las direcciones IP proporcionan una forma de hacerlo y forman una parte esencial de cómo funciona Internet.

Una dirección IP es una cadena de números separados por puntos. Las direcciones IP se expresan como un conjunto de cuatro números, por ejemplo, 192.158.1.38. Cada número del conjunto puede variar de 0 a 255. Por lo tanto, el rango completo de direcciones IP va desde 0.0.0.0 hasta 255.255.255.255.

Las direcciones IP no son aleatorias. La Autoridad de números asignados de Internet (Internet Assigned Numbers Authority, IANA), una división de Internet Corporation para números y nombres asignados (Internet Corporation for Assigned Names and Numbers, ICANN), genera y asigna matemáticamente las direcciones IP.

ICANN es una organización sin fines de lucro que se estableció en los Estados Unidos en 1998 para ayudar a mantener la seguridad de Internet y permitir que todos puedan utilizarla. Cada vez que alguien registra un dominio en Internet, debe dirigirse a un registrador del nombre de dominio, quien paga una pequeña tarifa a ICANN para registrarlo.

Máscara de red

Combinación de bits para delimitar una red de computadoras. Se trata de 32 bits separados en 4 octetos (como las direcciones IP) su función es indicar a los dispositivos qué parte de la dirección IP corresponde a la red/subred y cual al host.

Un router generalmente tiene dos direcciones IP, cada una en un rango distinto. Por ejemplo, una en el rango de una subred pequeña y otra en otra subred más grande cuya puerta de enlace da acceso a Internet. Solo se ven entre sí los equipos de cada subred o aquellos que tengan los router y puertas de enlace bien definidas para enviar paquetes y recibir respuestas. De este modo se forman y definen las rutas de comunicación entre computadoras de distintas subredes.

Mediante la máscara de red, un dispositivo sabrá si debe enviar un paquete dentro o fuera de la red en la que está conectado. Por ejemplo, si el router tiene una dirección IP 192.168.1.1 y máscara de red 255.255.255.0, todo lo que se envía a una dirección IP con formato 192.168.1.x deberá ir hacia la red local, mientras que las direcciones con un formato distinto se enviarán hacia afuera (Internet, otra red local, etc). Es decir, 192.168.1 indica la red en cuestión y .x corresponderá a cada host.

La máscara de red se representa colocando en 1 los bits de red y en cero los bits de host. Para el ejemplo anterior, sería de esta forma:

11111111.11111111.11111111.00000000 y la representación decimal es 255.255.255.0

Considerando los bits de red, 8 bit x 3 octetos = 24 bit y al escribir una dirección con máscara de red, esta se indica así: 192.168.1.1/24

El /24 corresponde a los bits en 1 que tiene la máscara.

En cada subred, el número de hosts se determina como el número de direcciones IP posibles menos dos: una con todos los bits a ceros en la parte del host que se reserva para nombrar la subred y otra con todos los bits a uno para la dirección de difusión, la cual se utiliza para enviar una señal a todos los equipos de una subred.

Decimal	CIDR	Número de host	Clase
/255.0.0.0	/8	16,777,214	A
/255.255.0.0	/16	65,534	B
/255.255.128.0	/17	32,766	
/255.255.192.0	/18	16,382	
/255.255.224.0	/19	8,190	
/255.255.240.0	/20	4,094	
/255.255.248.0	/21	2,046	
/255.255.252.0	/22	1,022	
/255.255.254.0	/23	510	
/255.255.255.0	/24	254	C
/255.255.255.128	/25	126	
/255.255.255.192	/26	62	
/255.255.255.224	/27	30	
/255.255.255.240	/28	14	
/255.255.255.248	/29	6	
/255.255.255.252	/30	2	

Figura 29. Máscaras de red

Puerta de enlace

La pasarela (en inglés gateway) o puerta de enlace es el dispositivo que actúa de interfaz de conexión entre aparatos o dispositivos, y también posibilita compartir recursos entre dos o más ordenadores. Su propósito es traducir la información del protocolo utilizado en una red inicial, al protocolo usado en la red de destino.

La pasarela es normalmente un equipo informático configurado para dotar a las máquinas de una red de área local (Local Area Network, LAN) conectadas a él de un acceso hacia una red exterior, generalmente realizando para ello operaciones de traducción de direcciones de red (Network Address Translation, NAT). Esta capacidad de traducción de direcciones permite aplicar una técnica llamada enmascaramiento de IP, usada muy a menudo para dar acceso a Internet a los equipos de una LAN compartiendo una única conexión a Internet, y por tanto, una única dirección IP externa.

La dirección IP de una pasarela a menudo es 192.168.1.1 o 192.168.0.1 y utiliza algunos rangos predefinidos, como por ejemplo 127.x.x.x, 10.x.x.x, 172.x.x.x, 192.x.x.x. La puerta de enlace de un enrutador se puede averiguar ejecutando el comando ipconfig desde el símbolo del sistema de Windows, o con el comando ip route desde una terminal en macOS y GNU/Linux. Un equipo que haga de puerta de enlace en una red debe tener necesariamente dos tarjetas de red (Network Interface Card, NIC).

La puerta de enlace predeterminada (default gateway) es la ruta predeterminada o ruta por defecto que se le asigna a un equipo y tiene como función enviar cualquier paquete del que no conozca por cuál interfaz enviarlo y no esté definido en las rutas del equipo, enviando el paquete por la ruta predeterminada.

En entornos domésticos, se usan los routers ADSL como puertas de enlace para conectar la red local doméstica con Internet; aunque esta puerta de enlace no conecta dos redes con protocolos diferentes, sí

que hace posible conectar dos redes independientes haciendo uso de NAT.

II.1.6.1.- VLSM

VLSM, del inglés Variable Length Subnet Mask o Máscara de Subred de Longitud Variable, es una técnica que se utiliza para aprovechar de manera más eficiente el espacio de direccionamiento IP en una red. A diferencia del método tradicional de subdivisión de redes, donde todas las subredes reciben la misma máscara, VLSM asigna diferentes máscaras según la cantidad de hosts que cada subred requiere. La principal ventaja de VLSM es que permite adaptar cada subred a su tamaño real, evitando desperdiciar direcciones IP. Por ejemplo, una red que conecta cientos de dispositivos puede recibir una máscara más amplia, mientras que una red que solo conecta unos pocos equipos puede recibir una máscara más pequeña.

Un aspecto importante de la implementación de VLSM es que la configuración de las subredes debe realizarse en forma descendente, es decir, se comienza asignando primero las subredes de mayor tamaño (las que requieren más hosts) y luego se procede con las de menor tamaño. Este enfoque evita el solapamiento de direcciones y asegura que las redes grandes tengan suficiente espacio de direccionamiento disponible antes de asignar los bloques más pequeños.

En resumen, VLSM no solo mejora la eficiencia en el uso de direcciones IP, sino que también aporta flexibilidad en el diseño de redes jerárquicas, facilita el enrutamiento sin desperdicio de recursos y es ampliamente utilizado en entornos empresariales donde se manejan múltiples VLANs, routers y segmentos de red con diferentes necesidades de tamaño.

Cabe resaltar que el VLSM pertenece a la Capa 3 del modelo OSI (Capa de Red), ya que trabaja directamente con direcciones IP y enrutamiento.

II.1.6.2.- VLAN (Red de Área Local Virtual)

A grandes rasgos, una VLAN es una subdivisión lógica de una red física. En lugar de estar limitados por la infraestructura física, los dispositivos conectados a una VLAN pueden comunicarse entre sí como si estuvieran en la misma red local, aunque estén en ubicaciones geográficas distintas. Esto brinda una gran flexibilidad y permite un mejor control del tráfico de red.

En términos del modelo OSI, las VLAN pertenecen principalmente a la Capa 2 (Enlace de datos), ya que funcionan mediante la manipulación de tramas Ethernet y el uso de etiquetas definidas en el estándar IEEE 802.1Q. Sin embargo, cuando se requiere comunicación entre diferentes VLANs (enrutamiento inter-VLAN), se hace uso también de la Capa 3 (Red), puesto que se trabaja con direcciones IP y tablas de enrutamiento.

Aquí hay algunas razones clave:

Seguridad

Las VLANs ayudan a mejorar la seguridad al aislar diferentes segmentos de red. Por ejemplo, una empresa puede tener VLANs separadas para sus departamentos de finanzas, recursos humanos y

desarrollo. Esto evita que usuarios no autorizados accedan a información confidencial de otros departamentos.

Optimización del tráfico de red

Las VLANs permiten agrupar dispositivos con necesidades de tráfico similares, lo que mejora la eficiencia de la red al reducir la cantidad de tráfico innecesario. Por ejemplo, si una empresa tiene cámaras de seguridad IP y terminales VoIP en la misma red física, crear una VLAN específica para cada tipo de dispositivo puede mejorar la calidad de las llamadas telefónicas y reducir la latencia en la transmisión de video.

Escalabilidad

Las VLANs facilitan la expansión de la red al eliminar la necesidad de agregar switches físicos. Si un departamento necesita agregar nuevos dispositivos, simplemente se pueden asignar a la VLAN existente, evitando costos adicionales en hardware.

VLANs y seguridad de red: Cómo proteger tu infraestructura

En el mundo actual de las redes, las VLANs (Virtual Local Area Networks) juegan un papel esencial en la seguridad de la red. Por ejemplo, una de las ventajas clave de las VLANs es la posibilidad de segmentar diferentes partes de la red, mejorando así la protección de la información sensible.

Además, la implementación de VLANs adecuadas puede ayudar a prevenir la propagación de ataques y amenazas. En consecuencia, es crucial comprender cómo proteger tu infraestructura de red utilizando VLANs.

VLANs y segmentación de redes

Las VLAN proporcionan una manera de agrupar dispositivos dentro de una LAN. Un grupo de dispositivos dentro de una VLAN se comunica como si estuvieran conectados al mismo cable. Las VLAN se basan en conexiones lógicas, en lugar de conexiones físicas.

Una red de área local virtual (VLAN) permiten que el administrador divida las redes en segmentos según factores como la función, el equipo del proyecto o la aplicación, sin tener en cuenta la ubicación física del usuario o del dispositivo. Los dispositivos dentro de una VLAN funcionan como si estuvieran en su propia red independiente, aunque compartan una misma infraestructura con otras VLAN.

II.1.6.2.1.- Razones para la Implementación de VLANs

La red de la clínica requiere ser segmentada debido a la existencia de múltiples áreas y funciones distribuidas a lo largo de los cuatro pisos del edificio. Algunas dependencias se repiten en distintos niveles por lo que se necesita separar el tráfico de cada grupo de usuarios para evitar interferencias, mejorar el rendimiento y aumentar la seguridad.

La implementación de VLANs permite organizar la red de forma lógica, asignando un esquema de direccionamiento IP específico para cada segmento, independientemente de la ubicación física de los dispositivos. Con esto se logrará una red más ordenada, segura y eficiente, facilitando la gestión y el

control del tráfico entre áreas críticas, personal de salud, administración y pacientes.

II.1.7.- Sistemas de Telefonía IP y Comunicaciones Unificadas

II.1.7.1.- Asterisk

Asterisk es una solución de VoIP (Voz sobre IP), telefonía VoIP de código abierto (bajo licencia GPL) que proporciona funciones de una centralita telefónica PBX o call center.

Desarrollada por Digium hace más de 20 años le permite instalar una interfaz web FreePBX con la que gestionar todas las funciones de telefonía de forma amigable.

Con Asterisk la centralita deja de ser una caja negra inaccesible y nos abre las puertas a gestionar las funciones telefónicas de manera muy sencilla.

La escalabilidad de Asterisk, su principal ventaja.

Una de las principales ventajas de Asterisk es su escalabilidad, el sistema responde a las necesidades de cada compañía, desde una pequeña empresa con dos usuarios hasta una gran empresa con 5.000 usuarios repartidos por varias sedes alrededor del mundo. Además, permite gestionar la centralita a través de una configuración web o interfaz gráfica.

Asterisk pertenece a la Capa 7 (Aplicación) del modelo OSI, ya que actúa como software de comunicación que gestiona llamadas, conferencias, buzón de voz y otras funciones de telefonía IP directamente a nivel de aplicación.

Destaca en el mercado por su competitividad en costes, gracias a su arquitectura de hardware que utiliza un servidor estándar de propósito no específico. Es decir, puede ser instalado en un servidor IBM x86 sin ningún problema que complique su configuración.

Figura 30. Asterisk

II.1.7.2.- Issabel

Issabel es un software con nombre de mujer que nació en 2016 de la mano de la comunidad de Asterisk para evitar la pérdida de los avances realizados durante años con Elastix, su predecesor.

Se trata de un software de código abierto de telefonía IP y comunicaciones unificadas basado en Asterisk, y que se utiliza para montar servidores incluyendo correo electrónico, fax, PBX IP, mensajería

instantánea, video conferencia, centro de llamadas y funciones colaborativas.

El objetivo que se buscaba al crear esta alternativa era poder ofrecer una herramienta global que pudiera unificar de forma integral todas las comunicaciones de la empresa.

Funcionalidades de Issabel

Las numerosas aplicaciones de Issabel hacen de este software una de las más completas herramientas de comunicaciones. No solamente provee de telefonía a la compañía, sino que, además, integra de un modo rápido y eficaz otros canales de comunicación. Algo imprescindible hoy en día para el correcto desarrollo de la actividad empresarial. Sus funciones más destacadas son las siguientes:

VoIP PBX: la central telefónica de Issabel cuenta con un amplio número de utilidades entre las que podemos destacar:

- Grabación de llamadas
- Identificación de llamadas
- Configuración de callback
- Llamada en espera
- Soporte para videoconferencias
- Sintetización de voz
- Colas de llamadas
- Herramientas para crear lotes de extensiones.
- IVR flexible y configurable
- Soporte para configuración de la central de llamadas dependiendo del horario.

II.1.7.3.- Los servidores VoIP

Un servidor VoIP es tanto un dispositivo como un software que administra las llamadas de voz por la red IP. Esto significa que convierte las señales de audio en datos digitales para su transmisión por internet y realiza el proceso inverso. Gracias a esto, es posible comunicarse con cualquier persona que cuente con acceso a internet y un dispositivo compatible, como teléfonos, computadoras o smartphones.

La tecnología revolucionaria de los servidores VoIP te permite realizar y recibir llamadas de voz por medio de la red IP, ofreciendo una solución eficaz y económica para tus necesidades de comunicación.

SIP

SIP (Session Initiation Protocol o Protocolo de Inicio de Sesión) es un protocolo utilizado en las llamadas VoIP para realizar y recibir llamadas de voz y vídeo, utilizado frecuentemente en la telefonía IP. Permite mantener sesiones multimedia con más de un participante de una manera muy sencilla y consistente.

Funcionamiento del SIP

Para poder hacer estas llamadas, el usuario debe tener una dirección SIP, obtener un cliente SIP en el dispositivo en el que lo vaya a utilizar y configurarlo. Una vez hecho esto, se podrá registrar, invitar a un usuario a una sesión, establecer una comunicación con uno o varios usuarios, y finalizar una sesión.

La tecnología SIP aprovecha las ventajas de la VoIP para mejorar las comunicaciones por voz y vídeo mediante Internet.

Necesidades del SIP

Para comunicarse mediante SIP, es necesario disponer de:

- Una dirección o cuenta SIP, que se contrata a través de un proveedor de servicios de telefonía. A menudo es gratuita y puede hacerse mediante un registro en línea. 24
- Instalación de un softphone o interfaz en el ordenador para establecer las comunicaciones, también llamada "cliente SIP". Consiste en una aplicación o programa que se instala en el dispositivo donde se quiere utilizar el SIP. Lo más habitual es que lo proporcionen los servicios de VoIP.
- Conexión a Internet con una calidad alta de la banda ancha, preferiblemente por cable. Para una buena conexión SIP es necesario suficiente ancho de banda y una conexión estable, especialmente para las llamadas de vídeo, ya que requieren un mayor ancho de banda.
- Uno o varios dispositivos para hacer y recibir llamadas: smartphone, ordenador, teléfono fijo, etc. Deberá tener altavoz y micrófono y, si se hacen llamadas de vídeo, cámara web.
- Compartir la dirección SIP con el usuario con el que se quiera comunicar. Igual que se da el teléfono o la dirección de correo electrónico, se dispondrá de una dirección SIP que el otro usuario necesita conocer para comunicarse. Este es el funcionamiento de los teléfonos SIP.

Beneficios de utilizar el protocolo SIP

Como hemos visto, el SIP permite iniciar y terminar sesiones con los usuarios que se desee, en las que se utilizan tantos datos de voz, vídeo u otra clase de datos. Esto tiene las siguientes ventajas:

- Se ahorran costes en los equipos tradicionales como primarios o redes RDSI ya que, para utilizar SIP, solo es necesario tener una conexión a Internet.
- Las llamadas son más económicas: el SIP permite a los proveedores de telefonía reducir costes de llamadas nacionales e internacionales, tanto internas como externas de la empresa.
- Permite llamadas múltiples. Al no depender del cableado, soporta mayor volumen de llamadas sin perder calidad.
- Permite la misma utilización de las direcciones SIP, independientemente desde dónde se estén utilizando. Para este protocolo, no existen prefijos ni áreas como ocurre con la telefonía tradicional.
- Es un sistema con escalabilidad, es decir, se puede aumentar el número de usuarios, sin que ello ponga en compromiso la velocidad de respuesta. Esto también permite un número mayor de extensiones o de numeraciones de forma muy sencilla.

Extensión de teléfono

Las extensiones son números cortos que puedes asignar a un empleado individual, un equipo o un

departamento de tu empresa. Es un código interno que permite a los usuarios comunicarse con sus compañeros de forma rápida y sencilla. Tus clientes también pueden omitir la operadora automática normal marcando el número de extensión de la persona con la que quieres hablar. La función también se denomina marcación de extensión por este motivo.

Los interlocutores internos y externos utilizan los mismos números de extensión de diferentes formas. Supón que tienes a Alex y Juan trabajando en la misma oficina. La extensión de Alex es 103 y el número de Juan es 104. Si Alex quiere hablar con Juan, puede levantar su teléfono y marcar 104. No es necesario marcar el número completo de la empresa.

Para las personas que llaman externas, como clientes o proveedores, los números de extensión deben añadirse al número comercial principal. Entonces, si el número de teléfono de tu empresa es 987-6543, el cliente debe marcar 987-6543-103 para hablar con Alex o 987-6543-104 para hablar con Juan.

Servidor PBX

El Servidor PBX (Private Branch Exchange) es la central telefónica digital que controla todas las llamadas internas y externas de una organización. En sistemas VoIP modernos, este PBX suele estar integrado en plataformas como Issabel o Asterisk, por lo que sí, Issabel incluye un PBX basado en Asterisk.

En la Clínica el PBX funcionará como el sistema encargado de gestionar extensiones, enrutar llamadas, habilitar buzón de voz, conferencias, desvíos y otras funciones avanzadas de comunicación.

II.1.7.4.- Diferencias entre VoIP y telefonía tradicional.

La telefonía tradicional (PSTN o Red Telefónica Conmutada) transmite la voz mediante circuitos analógicos dedicados, requiere infraestructura física de cables de cobre y líneas telefónicas, y cada llamada utiliza un canal exclusivo. Esto limita la flexibilidad y suele generar costos más altos por llamadas, especialmente internacionales.

Por otro lado, la VoIP (Voice over IP) convierte la voz en datos digitales que se transmiten a través de redes IP (como la red de internet o la LAN de la clínica). Esto permite que múltiples llamadas compartan el mismo canal de datos, ofrece integración con computadoras y aplicaciones, reduce costos, facilita funciones avanzadas como videollamadas, buzón de voz y conferencias, y brinda mayor escalabilidad y flexibilidad que la telefonía tradicional.

II.1.7.5.- Zoiper

Zoiper es un softphone que permite hacer y recibir llamadas telefónicas a través de internet. Se trata de una aplicación de comunicaciones unificadas que se ha convertido en una alternativa popular para empresas y usuarios individuales que buscan una solución flexible y eficiente para sus necesidades de comunicación.

Entre sus características más destacadas, podemos avanzar que Zoiper se encuentra su compatibilidad con diferentes sistemas operativos, la posibilidad de integrar diferentes cuentas SIP y la capacidad de realizar videoconferencias. Además, Zoiper ofrece una gran cantidad de opciones de personalización y

configuración que permiten adaptar la aplicación a las necesidades específicas de cada usuario.

Funcionalidades principales

Zoiper es una herramienta de comunicación muy versátil y eficiente que puede resultar muy útil tanto para empresas como para usuarios individuales que buscan una solución de softphone fácil de usar y personalizable. A continuación, podrás ver algunas de las funcionalidades principales que ofrece:

Integración de cuentas SIP: Zoiper permite integrar diferentes cuentas SIP, lo que significa que puedes utilizar diferentes proveedores de telefonía IP para realizar y recibir llamadas. Esto te da una gran flexibilidad y te permite elegir la opción que mejor se adapte a tus necesidades.

Calidad de las llamadas: También ofrece una excelente calidad de sonido en sus llamadas. Esto se debe a que utiliza una tecnología de compresión de audio de alta calidad que garantiza una transmisión de voz nítida y sin interferencias. Además, Zoiper soporta el códec de audio G.711 que ofrece una calidad de sonido aún mayor.

Capacidad de videoconferencia: Zoiper también ofrece la capacidad de realizar videoconferencias, lo que te permite mantener reuniones en línea con tus colegas o clientes de una manera fácil y eficiente. La calidad de vídeo de Zoiper es excelente y se adapta automáticamente a la calidad de tu conexión a Internet.

Registro de llamadas: Zoiper ofrece una función de registro de llamadas que te permite tener un registro detallado de todas las llamadas que has realizado y recibido. Esto te permite tener un control total sobre tu actividad de llamadas y realizar un seguimiento de tus comunicaciones.

Personalización y configuración: Zoiper ofrece una gran cantidad de opciones de personalización y configuración que te permiten adaptar la aplicación a tus necesidades específicas. Puedes personalizar el aspecto de la interfaz, configurar diferentes atajos de teclado, ajustar la calidad de audio y vídeo, y mucho más.

Integración con otros servicios: Zoiper también ofrece integración con otros servicios como Google Voice, Microsoft Teams y SIP URI. Esto te permite utilizar Zoiper en conjunto con otras herramientas de comunicación y aumentar la eficiencia de tus comunicaciones.

II.1.8.- Topologías de una red

Existen 5 topologías más utilizadas:

- **Topología de bus:** En esta topología, todos los dispositivos están conectados a un único medio de transmisión, conocido como "bus". Los datos se transmiten a lo largo del bus y son recibidos por todos los dispositivos conectados. Cualquier dispositivo puede enviar o recibir datos, pero solo el dispositivo destinatario procesa la información.
- **Topología de estrella:** En esta topología, todos los dispositivos están conectados a un nodo central, como un switch o un concentrador. Cada dispositivo tiene una conexión dedicada con el nodo central. Cuando un dispositivo envía datos, estos se transmiten directamente al nodo central,

que luego los envía al dispositivo de destino. La falla de un dispositivo no afecta la comunicación de los demás.

- **Topología de anillo:** En esta topología, los dispositivos están conectados en forma de anillo cerrado, donde cada dispositivo está conectado directamente a los dos dispositivos adyacentes. Los datos se transmiten en una dirección alrededor del anillo. Cada dispositivo recibe los datos y los pasa al siguiente dispositivo en el anillo hasta que llegan al destino. La falla de un dispositivo puede interrumpir la comunicación en el anillo.
- **Topología de malla:** En esta topología, todos los dispositivos están conectados directamente entre sí, creando múltiples rutas de comunicación. Cada dispositivo tiene una conexión dedicada con todos los demás dispositivos. Esto proporciona redundancia y mayor confiabilidad, ya que, si una ruta falla, los datos pueden seguir una ruta alternativa.
- **Topología en árbol:** Esta topología utiliza una estructura jerárquica en forma de árbol, donde los dispositivos están conectados en niveles, comenzando desde un nodo raíz hasta los nodos hoja. El nodo raíz es el punto central de la red y los nodos hoja son los dispositivos finales. La comunicación se realiza a través del nodo raíz, y los datos se transmiten hacia abajo a través de los niveles del árbol.

II.1.8.1.- Topología seleccionada

Para la infraestructura de la clínica se utilizará la topología en árbol, debido a que es la más adecuada para una red distribuida en varios pisos y áreas diferenciadas. Su estructura jerárquica permite:

- Organizar los switches por niveles (principal, distribución y acceso).
- Facilitar la segmentación mediante VLANs en cada piso.
- Garantizar un flujo de datos eficiente y controlado desde el nodo raíz.
- Permitir equipos futuros sin reestructurar toda la red.
- Asegurar orden, estabilidad y facilidad de administración dentro de una red clínica compleja.

Esta topología es la más apropiada para entornos donde existen múltiples áreas, diferentes niveles de dispositivos y enlaces principales entre pisos.

II.1.9.- Tipos de Redes de Comunicación

Red LAN (Red de Área Local)

Una red LAN (Local Area Network), o Red de Área Local, es un sistema de interconexión que permite que varios dispositivos, como computadoras, impresoras, teléfonos, servidores y otros equipos, se comuniquen y compartan recursos dentro de un espacio físico reducido, como una casa, una oficina, un colegio o una empresa.

Este tipo de red se caracteriza por su alta velocidad de transmisión de datos y por estar limitada a un área geográfica pequeña. Gracias a una LAN, los usuarios pueden compartir archivos, utilizar impresoras en

red, acceder a internet y trabajar de forma colaborativa sin importar en qué parte del edificio se encuentren.

Red WAN (Red de Área Amplia)

Una WAN es una red de telecomunicaciones que abarca grandes extensiones geográficas y que permite la conexión de varias redes locales (LAN) ubicadas en diferentes lugares. Su objetivo es facilitar la comunicación y el intercambio de información entre computadoras, servidores y dispositivos que se encuentran en distintas ciudades, países o incluso continentes.

El ejemplo más grande de una WAN es Internet, que conecta redes de todo el mundo. Las WAN suelen implementarse mediante enlaces de fibra óptica, satélite o proveedores de servicios especializados, garantizando que la información viaje de forma rápida y confiable a pesar de las largas distancias.

Red WLAN (Red de Área Local Inalámbrica)

Una WLAN es una red de área local que utiliza tecnología inalámbrica (WiFi) para conectar dispositivos dentro de un espacio físico limitado, como una vivienda, oficina, clínica o campus. A diferencia de una LAN tradicional que depende de cables Ethernet, una WLAN ofrece movilidad y flexibilidad, permitiendo que equipos como laptops, smartphones y tablets se conecten sin necesidad de estar cableados.

Las WLAN son muy comunes en la vida diaria porque brindan acceso rápido a Internet y a los recursos internos de una red sin depender de conexiones físicas, aunque dependen de la calidad de la señal y de factores como la distancia al punto de acceso o la cantidad de usuarios conectados.

Red de Punto a Punto

La topología más sencilla es un enlace permanente entre dos puntos finales conocida como punto a punto (PtP). La topología punto a punto conmutada es la pasarela básica de la telefonía convencional. El valor de una red permanente de PtP es la comunicación sin obstáculos entre los dos puntos finales. El valor de una conexión PtP a demanda es proporcional al número de pares posibles de abonados y se ha expresado como la ley de Metcalfe.

II.1.10.- Servicio de DHCP

El DHCP (Dynamic Host Configuration Protocol) es un protocolo que permite asignar de forma automática direcciones IP y otros parámetros de red a los dispositivos que se conectan a una red, como computadoras, teléfonos, impresoras y más. Opera en la capa 7(Aplicación), su principal objetivo es agilizar y simplificar la configuración de red, evitando la necesidad de hacerlo manualmente en cada equipo.

DHCP opera de la siguiente manera:

- *Solicitud del dispositivo:* Cuando un dispositivo se conecta a la red, envía una petición para obtener una dirección IP y configuración de red.
- *Respuesta del servidor DHCP:* Un servidor DHCP recibe la solicitud y asigna automáticamente una dirección IP libre, además de otros datos como la máscara de subred, la puerta de enlace

(gateway) y servidores DNS.

- *Asignación temporal:* Estos datos se entregan al dispositivo por un tiempo determinado, tras el cual pueden renovarse.

Ventajas del uso de DHCP:

- ✓ *Evita conflictos de IP:* Al asignar IP automáticamente y de forma centralizada, se evita que dos dispositivos tengan la misma dirección.
- ✓ *Facilita la administración:* Permite a los administradores o personal de TI gestionar grandes redes sin tener que configurar cada equipo uno por uno.
- ✓ *Ahorra tiempo y reduce errores:* Al eliminar la configuración manual, se reduce el riesgo de errores humanos.

II.1.11.- Organismos de Normalización y Estándares

Organismos

- IEC: (Comisión Electrotécnica Internacional)
- EIA: (Alianza de Industrias Electrónicas).
- TIA: (Asociación de la Industria de las Telecomunicaciones)
- ISO: (Organización Internacional de Normalización)
- IEEE: (Instituto de Ingenieros Eléctricos y Electrónicos)
- IETF: (Grupo de Trabajo de Ingeniería de Internet)
- ANSI (American National Standards Institute)

Normas

ANSI-TIA/EIA (Telecommunications Industry Association / Electronic Industries Alliance)

- **ANSI-TIA/EIA-568-B:** Estándar para cableado estructurado (categorías de cable, topología, longitudes máximas). Define los requisitos para la instalación de cableado de telecomunicaciones en edificios comerciales. El objetivo de esta norma es asegurar la integridad, eficiencia y confiabilidad en las redes de datos y telecomunicaciones.
- **ANSI-TIA/EIA-606-B**: Administración del cableado (etiquetado, identificación). Se enfoca en la identificación de los cables, paneles de conexiones, puntos de acceso y demás componentes del sistema de telecomunicaciones, asegurando que cualquier persona que trabaje en la red.
- **ANSI-TIA/EIA-569-B**: Canalizaciones y espacios para telecomunicaciones. Proporcionar directrices para la planificación y organización del espacio físico dentro de los edificios donde se instalarán los sistemas de telecomunicaciones. Esto incluye el diseño de los conductos, cables, paneles de conexión, tomas de usuario, y componentes de red en función del espacio disponible y las necesidades futuras.

IEEE (Institute of Electrical and Electronics Engineers)

- **IEEE 802.3**: Estándar de Ethernet (comunicación por cable). Define las especificaciones para las redes de Ethernet en cableado de par trenzado como cables Cat5e, Cat6,Cat7 y fibra óptica. Cubre todas las tecnologías de redes de área local (LAN) y especifica las reglas para la transmisión de datos en Ethernet, que es el protocolo más común utilizado en redes locales. Este estándar define los aspectos físicos y de enlace de datos de la red Ethernet, incluyendo el medio físico como cables y conectores, el protocolo de control de acceso al medio (MAC) y los métodos de transmisión de los datos.
- **IEEE 802.11**: Estándar para redes inalámbricas, también conocidas como Wi-Fi. Este estándar define las reglas y tecnologías necesarias para la comunicación de dispositivos de manera inalámbrica en redes locales, permitiendo que los dispositivos como computadoras, teléfonos móviles, impresoras y otros, se conecten a una red sin necesidad de cables físicos.
- **802.11ax:** El IEEE 802.11ax, conocido como Wi-Fi 6 (y Wi-Fi 6E en 6 GHz), es el sucesor de 802.11ac. Su principal ventaja no es solo la velocidad, sino la alta eficiencia en entornos densos, ofreciendo hasta 4 veces más rendimiento por área. Esto se logra gracias a la tecnología OFDMA, que permite manejar mejor múltiples usuarios al mismo tiempo.
- **IEEE 802.1Q:** El IEEE 802.1Q (Dot1q) es el estándar que permite implementar VLANs en redes Ethernet, añadiendo etiquetas a las tramas para identificar a qué VLAN pertenecen. Esto posibilita segmentar la red en subredes lógicas, mejorar la seguridad y optimizar el rendimiento. Además, incorpora mecanismos de priorización de tráfico (802.1p) y sigue evolucionando con revisiones que amplían sus capacidades.

IETF (Internet Engineering Task Force)

- **SIP (Session Initiation Protocol – RFC 3261):** Protocolo estándar para llamadas VoIP usando por Asterisk, Issabel y Zoiper.
- **RTP (Real-time Transport Protocol – RFC 3550):** Transporte de audio/video en tiempo real.
- **ISO/IEC 27001**: Gestión de seguridad de la información.
- **IETF:** Define el estándar de protocolo de seguridad como:

  Firewall Policies (RFCs relacionados)

  RFC 791 define el protocolo de IPv4.

II.1.12.- Protocolos de Comunicación

Protocolo IAX usado en voz ip

IAX (Inter-Asterisk eXchange protocol) es uno de los protocolos utilizado por Asterisk. Es utilizado para manejar conexiones VoIP entre servidores Asterisk, y entre servidores y clientes que también utilizan protocolo IAX. El protocolo IAX ahora se refiere generalmente al IAX2, la segunda versión del protocolo

IAX. El protocolo original ha quedado obsoleto en favor de IAX2.

IAX2 es robusto, lleno de novedades y muy simple en comparación con otros protocolos. Permite manejar una gran cantidad de códecs y un gran número de streams, lo que significa que puede ser utilizado para transportar virtualmente cualquier tipo de dato. Esta capacidad lo hace muy útil para realizar videoconferencias o realizar presentaciones remotas.

Protocolo de transporte en tiempo real (RTP)

El Protocolo de transporte en tiempo real conocido por las siglas RTP , es un protocolo de red utilizado en aplicaciones en tiempo real como, por ejemplo, la entrega de datos de audio punto a punto , como la Voz sobre IP . Funciona como una subcapa de la capa de transporte, capa 4 del Modelo OSI , y define cómo se debe fragmentar el flujo de datos de audio, añadiendo a cada fragmento información de secuencia y tiempo de entrega, siendo el control realizado por RTCP - Tiempo Real.

RTP utiliza UDP como protocolo de transporte, ya que este permite enviar los paquetes de manera rápida y continua sin esperar confirmaciones de entrega, lo que es fundamental para aplicaciones en tiempo real donde la velocidad y la continuidad de la transmisión son más importantes que la corrección de errores.

Protocolo HTTP

HTTP, de sus siglas en inglés: "Hypertext Transfer Protocol", es el nombre de un protocolo el cual nos permite realizar una petición de datos y recursos, como pueden ser documentos HTML. Es la base de cualquier intercambio de datos en la Web, y un protocolo de estructura cliente-servidor, esto quiere decir que una petición de datos es iniciada por el elemento que recibirá los datos (el cliente), normalmente un navegador Web.

Protocolo HTTPS

El protocolo de transferencia de hipertexto seguro (HTTPS) es la versión segura de HTTP, que es el principal protocolo utilizado para enviar datos entre un navegador web y un sitio web. El HTTPS está encriptado para aumentar la seguridad de las transferencias de datos. Esto es especialmente importante cuando los usuarios transmiten datos confidenciales, como al iniciar sesión en una cuenta bancaria, un servicio de correo electrónico o un proveedor de seguros médicos.

Cualquier sitio web, especialmente los que requieren credenciales de inicio de sesión, debe utilizar HTTPS. En los navegadores modernos, como Chrome, los sitios web que no utilizan HTTPS se señalan de forma diferente a los que sí lo hacen. Identifica un candado en la barra de URL que te indicará que la página web es segura. Los navegadores web se toman en serio el protocolo HTTPS. Google Chrome y otros navegadores marcan todas las páginas web que no utilizan HTTPS como no seguras.

La importancia de los protocolos TLS y SRTP en telefonía VoIP

Los protocolos TLS y SRTP se utilizan principalmente con el objetivo de asegurar las comunicaciones empresariales. El creciente riesgo de sufrir ataques y hackeos a las infraestructuras tecnológicas de empresas e instituciones hace que sea necesario utilizar protocolos como estos.

Tanto TLS y SRTP proporcionan características avanzadas de seguridad para proteger el envió de datos multimedia en comunicaciones. Asimismo, también garantiza una transmisión antiescucha de datos telefónicos entre varios interlocutores. De esta forma, las empresas que utilizan sistemas de telefonía VoIP pueden tener la tranquilidad de que los datos de sus llamadas y videollamadas están siempre a salvo.

II.1.13.- Pruebas en la red

Es un proceso crítico para garantizar que la red funcione de manera eficiente, segura y confiable antes de su implementación en un entorno de producción, estas son unas características a tomar en cuenta al implementar una nueva red.

- Pruebas de Conectividad: Se prueba la conectividad de red para garantizar que los dispositivos puedan comunicarse a través de la red sin problemas. Se verifica que no haya pérdida de paquetes y que la latencia sea aceptable.
- Pruebas de Rendimiento: Se evalúa el rendimiento de la red, incluyendo la velocidad de transferencia de datos, la capacidad de ancho de banda y la escalabilidad. Esto asegura que la red pueda manejar la carga prevista.
- Pruebas de Seguridad: Se realizan pruebas de seguridad para identificar y solucionar vulnerabilidades de red. Se verifica la efectividad de las medidas de seguridad, como cortafuegos y sistemas de detección de intrusiones.
- Pruebas de Tolerancia a Fallos: Se simulan fallos en la red para evaluar su capacidad de recuperación. Se verifica que la red pueda mantener la disponibilidad en caso de problemas.
- Pruebas de Calidad de Servicio (QoS): Si es necesario, se prueban las políticas de QoS para garantizar que se cumplan los requisitos de calidad de servicio para aplicaciones críticas.
- Pruebas de Interoperabilidad: Si la red se integra con sistemas de terceros, se realizan pruebas de interoperabilidad para garantizar que todos los sistemas funcionen juntos de manera eficiente.
- Pruebas de Documentación: Se revisa y actualiza la documentación de la red, incluyendo diagramas de red, políticas y procedimientos.

II.1.14.- Protección contra incendios

La protección contra incendios es fundamental para salvaguardar tanto la vida humana como los bienes materiales. Un sistema eficaz de prevención y control de incendios debe ser capaz de prevenir, detectar y extinguir el fuego en su etapa inicial, minimizando así el riesgo de daños mayores.

Para lograr este objetivo, es indispensable un enfoque integral que abarque diversas disciplinas del diseño, incluyendo la hidráulica, eléctrica, mecánica y estructural. Cada una de estas áreas contribuye al funcionamiento coordinado y eficiente del sistema.

Las características y especificaciones de estos sistemas deben basarse en normativas internacionales reconocidas, como las de la NFPA (National Fire Protection Association). Esta organización es referente

mundial gracias a que sus códigos y normas son desarrollados mediante un proceso abierto, participativo y basado en el consenso, lo cual garantiza su confiabilidad y aplicabilidad en distintos contextos.

Extintores

Los extintores son equipos portátiles que se usan para apagar fuegos pequeños antes de que se conviertan en incendios grandes. Son una herramienta muy importante en la seguridad contra incendios y deben estar siempre disponibles y en buen estado.

No todos los fuegos son iguales, y por eso existen diferentes tipos de extintores, según el tipo de material que esté ardiendo. A continuación, te explicamos los tipos de fuego más comunes:

- **Fuego Clase A:** Son los que queman materiales sólidos como papel, madera, cartón o tela.
- **Fuego Clase B:** Se producen con líquidos inflamables como gasolina, aceite, pintura o alcohol.
- **Fuego Clase C:** Involucran gases inflamables, como butano, propano o gas natural.
- **Fuego Clase D:** Se dan cuando se queman metales especiales como magnesio, sodio o aluminio en polvo. Estos suelen ocurrir en industrias.

Cada tipo de fuego necesita un extintor específico, por eso es importante elegir el extintor adecuado para cada área o lugar. Además, todos los extintores deben estar bien señalizados, ubicados en lugares accesibles y recibir mantenimiento regular para asegurar que funcionen correctamente en caso de emergencia.

II.1.15.- Tecnologías utilizadas

Objetivo de la simulación en diseño de redes

El uso de simuladores en el diseño de redes tiene como objetivo principal probar, validar y optimizar la infraestructura antes de su implementación real. A través de estas herramientas, es posible recrear la topología de la red, configurar dispositivos y verificar el correcto funcionamiento del tráfico entre los diferentes equipos y áreas de la clínica.

Gracias a la simulación, se pueden identificar errores, evaluar el rendimiento, realizar ajustes y tomar decisiones técnicas sin generar costos adicionales ni afectar los servicios reales.

Diferencia entre simulación, emulación y virtualización.

- *Simulación:* Es una representación aproximada del funcionamiento de una red o dispositivo. No se usan los equipos reales, sino modelos que imitan su comportamiento. Por ejemplo, en Packet Tracer se simula cómo funcionan routers y switches sin que exista el hardware físico. La simulación permite probar configuraciones y flujos de datos de manera segura y rápida.
- *Emulación:* Es una reproducción más exacta del comportamiento de un dispositivo real, utilizando software que ejecuta el mismo sistema operativo del hardware real. Por ejemplo, GNS3 emula routers y switches Cisco, permitiendo que se comporten casi igual que los equipos físicos.
- *Virtualización:* Consiste en crear versiones virtuales de recursos físicos, como servidores, redes o

dispositivos de almacenamiento, usando software especializado. VMware permite instalar sistemas operativos y servicios en máquinas virtuales, compartiendo los recursos de un mismo equipo físico, pero funcionando como si fueran independientes.

II.1.15.1.- Packet tracer

Figura 31. 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 32. 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 33. Software VMWare

VMware es una empresa de software líder en el campo de la virtualización y la computación en la nube. La virtualización consiste en crear mediante software una representación virtual de recursos físicos, como servidores, redes o dispositivos de almacenamiento, permitiendo que varios sistemas operativos o aplicaciones se ejecuten de forma independiente en un mismo equipo físico.

II.1.15.4.- Ventajas y limitaciones de cada herramienta

Packet Tracer

- ✓ *Ventajas:* Fácil de usar, ideal para pruebas rápidas de topologías Cisco; permite simular configuraciones y protocolos básicos.
- ✓ *Limitaciones:* No emula dispositivos reales ni permite simular redes muy complejas o fallos avanzados.

GNS3

- ✓ *Ventajas:* Emula dispositivos reales de Cisco y otros fabricantes; permite pruebas avanzadas de protocolos, servicios y fallos; ideal para escenarios complejos.
- ✓ *Limitaciones:* Requiere más recursos de hardware y conocimientos avanzados; puede ser más lento en simulaciones grandes.

VMware

- ✓ *Ventajas:* Permite crear servidores y redes virtuales completas; soporta múltiples sistemas operativos; útil para pruebas de virtualización y servicios de red.
- ✓ *Limitaciones:* No es específico de Cisco, requiere hardware potente y experiencia en virtualización; no simula dispositivos físicos de red de forma exacta.

CAPÍTULO III

COMPONENTES

III.- CAPÍTULO III: COMPONENTES

III. Componente 1: Optimización de la red

Objetivo específico del componente

- Segmentación de la red por VLAN para separar el tráfico de distintas áreas clínicas y administrativas.
- Implementación de enlaces de fibra óptica para interconexión de pisos y alta velocidad de transmisión de datos.
- Instalación y configuración de un firewall Fortinet para controlar el acceso y proteger la red contra amenazas externas.
- Configuración de telefonía IP (VoIP), integrando extensiones internas y conexión con redes externas.
- Implementación de Wi-Fi segura, con control de acceso y cifrado moderno (WPA3).
- Configuración de servidores DHCP, para la asignación automática y ordenada de direcciones IP a los dispositivos de la red.
- Implementación de NAT (Network Address Translation), para permitir que los equipos internos accedan a Internet mediante una única dirección pública, manteniendo seguridad y ahorro de direcciones IP.
- Aplicación de QoS (Quality of Service) para priorizar tráfico crítico como voz y datos médicos.
- Reorganización del cableado estructurado y racks, asegurando orden, eficiencia y facilidad de mantenimiento.
- Optimización del diseño físico y lógico de la red, garantizando comunicación estable, rápida y segura en todas las áreas.

III.1.- Metodología para diseño de red top-Down

La metodología Top-Down, usada en este proyecto, parte de una visión general de la red y se divide en fases como análisis de requerimientos, diseño lógico y selección de tecnologías. Se eligió porque se adapta a las necesidades de la Clínica Santísima Trinidad de Tarija.

La metodología está compuesta por estas fases:

- ✓ 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

En lo que respecta a esta metodología cubre todos los puntos para poner en funcionamiento la red desarrollada debido a eso para la propuesta de este proyecto se cubrirán completamente los puntos hasta la fase 4 y las otras fases se tomarán en cuenta los puntos que se puedan analizar tomando en cuenta la escala de desarrollo actual.

III.1.1.-Fase 1: Análisis de Requerimientos

III.1.1.2.- Análisis de Metas del Negocio

Misión

La Clínica Santísima Trinidad de Tarija es una institución de salud de referencia departamental que atiende las necesidades sanitarias de la población con calidad, equidad y solidaridad. Ofrece servicios médicos y quirúrgicos especializados, de mediana y alta complejidad, garantizando atención eficiente, oportuna, cálida y sin ningún tipo de discriminación social.

Visión

La Clínica Santísima Trinidad de Tarija es un modelo de gestión moderna en el ámbito hospitalario, con administración eficiente y responsable de sus recursos materiales, financieros y humanos. Cuenta con personal altamente capacitado que trabaja de forma coordinada y en equipo, estando integrada a la red de servicios de salud y ofreciendo atención con calidad y calidez a la población del departamento de Tarija, cumple con diversas funciones importantes para la comunidad:

Atención médica integral: Proporciona servicios de atención médica integral que incluyen consultas médicas, exámenes físicos, diagnóstico y tratamiento de enfermedades, atención de urgencias y emergencias, así como seguimiento de enfermedades crónicas.

Servicios especializados: La clínica cuenta con especialistas en diversas áreas médicas, como cardiología, gastroenterología, ginecología, pediatría, oftalmología, reumatología, dermatología entre otras, para ofrecer atención especializada a pacientes con necesidades específicas.

Tecnología médica avanzada: La clínica está equipada con tecnología médica avanzada para el diagnóstico y tratamiento de diversas condiciones médicas, entre estas se encuentran: máquinas de Tomografía, Rayos x, Ecografía, Quirófanos lo que permite ofrecer un nivel de atención de alta calidad.

Atención de emergencias: Tiene un área dedicada a la atención de emergencias médicas, equipada para brindar atención inmediata a pacientes con situaciones médicas urgentes. También este cuenta con convenios hacia otras clínicas ya sea para el uso de sus máquinas, como ser tomografías, ecografías y más.

III.1.1.3.- Análisis de Metas Técnicas

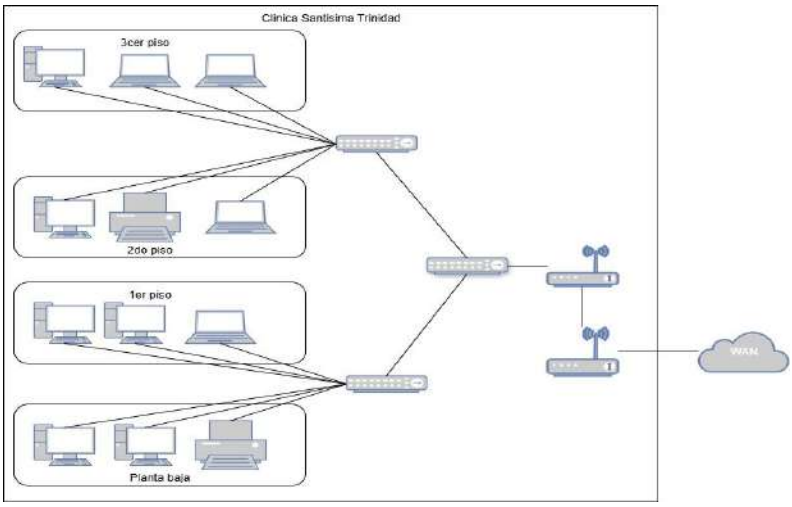

Figura 34. Diagrama de red actual

Para un mejor análisis de los datos se optó para analizar cada piso de la del edificio lo cual cuenta con un total de 4 pisos:

La **planta baja** cuenta con el personal aproximado de al menos de 17 personas los cuales se distribuyen de la siguiente la siguiente manera:

- 1 en recepción
- 2 en administración
- 5 médicos en consultorios
- 2 emergencias
- 7 áreas tercerizadas

Planta Baja	Cantidad de host
recepción	1
administración	2
consultoría	5
emergencias	1
áreas tercerizadas	4
Impresoras	7
Total	20

Tabla 4. Host de la planta baja

Planta baja equipos de tipo terminal se encontraron 20.

El **primer piso** cuenta con un aproximado de al menos de 7 personas de salud los cuales se distribuyen de la siguiente manera:

- 2 internación
- 2 enfermería
- 3 terapia intensiva

Primer Piso	Cantidad de host
internación	7
enfermería	2
Terapia intensiva	1
Impresoras	2
Total	12

Tabla 5. Host del Primer Piso

Primer piso equipos de tipo terminal se encontraron 12.

El **segundo piso** cuenta con un aproximado de al menos de 5 personas los cuales se distribuyen de la siguiente manera:

- 2 internación
- 1 enfermería
- 2 terapia intensiva

Segundo Piso	Cantidad de host
internación	7
enfermería	1
Terapia intensiva	1
Impresoras	1
Total	10

Tabla 6. Host del Segundo Piso

Segundo piso equipos de tipo terminal se encontrarían 10.

El **tercer piso** cuenta con un aproximado de al menos de 12 personas los cuales se distribuyen de la siguiente manera:

- 4 pediatría
- 1 áreas tercerizadas
- 3 internación
- 1 enfermería
- 3 terapia intensiva

Tercer Piso	Cantidad de host
Pediatría	3
áreas tercerizadas	1
internación	5
enfermería	1
Terapia intensiva	1
Impresoras	2
Total	13

Tabla 7. Host del Tercer Piso

Tercer piso equipos de tipo terminal se encontrarían 13

Extensión tercer piso cuenta con un aproximado de al menos de 6 personas los cuales se distribuyen de la siguiente manera:

- 2 farmacia
- 3 esterilización
- 1 contabilidad

Extensión Tercer Piso	Cantidad de host
Farmacia	1
esterilización	3
contabilidad	2
Impresoras	3
Total	9

Tabla 8. Host del Extensión Tercer Piso

Equipos de tipo terminal se encontrarían 9.

III.1.1.4.- Analizar red existente

Actualmente, la Clínica Santísima Trinidad no cuenta con una topología de red definida ni un cuarto de telecomunicaciones adecuado. El cableado carece de organización: no está etiquetado, existe cableado viejo mezclado con el actual, y hay canaletas en mal estado o en desuso que generan desorden y confusión.

En la Planta Baja, un AP se conecta directamente al proveedor de internet y un segundo AP amplía la señal. Este segundo AP también enlaza un DVR, varias máquinas y PCs, y un switch que concentra gran parte del tráfico de la planta baja y del primer piso.

En el Segundo Piso hay un switch conectado a un AP exclusivo para quirófano. Este switch también distribuye conexión al tercer piso y su extensión, donde no hay switch propio. Sin embargo, en el Tercer Piso existe además una red independiente con otro proveedor de internet y un AP para pediatría.

Por último, el primer switch mencionado se encuentra conectado al Access Point de Administración, así permitiendo la comunicación entre pisos, aunque actualmente no hay una estructura de red organizada ni un diseño que garantice eficiencia, seguridad o escalabilidad.

ID	**Dispositivo**	**Marca**	**Localización**	**Justificación**
1	Access Point	Arris	Administration	De la empresa telecomunicaciones Tigo
2	Access Point	Tenda AC1200	Quirófano	De la Clínica
3	Switch	TP-Link TL-SF1016DS	Enfermería	De la Clínica
4	Access Point	TL-WR941ND	Administración	De la Clínica

5	Access Point	Arris	Pediatría	De la empresa telecomunicaciones Tigo
6	DVR	Dahua	Administración	De la Clínica
7	Switch	TP LINK-SG1024D	Administración	De la Clínica

Tabla 9. Dispositivos de red existentes

III.1.1.4.1.- Direccionamiento actual de las IP

Nro.	Equipo	Dirección IP	Máscara de red	Puerta de enlace
1	PC-1	192.168.10.9	255.255.255.0	192.168.10.1

Tabla 10. Área de Recepción

Nro.	Equipo	Dirección IP	Máscara de red	Puerta de enlace
2	PC-2	192.168.10.10	255.255.255.0	192.168.10.1
3	PC-3	192.168.10.11	255.255.255.0	192.168.10.1

Tabla 11. Área de Administración

Nro.	Equipo	Dirección IP	Máscara de red	Puerta de enlace
4	LP-4	192.168.10.12	255.255.255.0	192.168.10.1
5	LP-5	192.168.10.13	255.255.255.0	192.168.10.1
6	LP-6	192.168.10.14	255.255.255.0	192.168.10.1
7	LP-7	192.168.10.15	255.255.255.0	192.168.10.1
8	LP-8	192.168.10.16	255.255.255.0	192.168.10.1

Tabla 12.Área de Consultorio

Nro.	Equipo	Dirección IP	Máscara de red	Puerta de enlace
9	PC-9	192.168.10.17	255.255.255.0	192.168.10.1
10	PC-10	192.168.10.18	255.255.255.0	192.168.10.1
11	PC-11	192.168.10.19	255.255.255.0	192.168.10.1
12	PC-12	192.168.10.20	255.255.255.0	192.168.10.1
13	PC-13	192.168.10.21	255.255.255.0	192.168.10.1

Tabla 13. Área Tercerizada

Nro.	Equipo	Dirección IP	Máscara de red	Puerta de enlace
13	PC-14	192.168.10.22	255.255.255.0	192.168.10.1

Tabla 14. Área de Emergencias

Nro.	Equipo	Dirección IP	Máscara de red	Puerta de enlace
14	PC-14	192.168.10.30	255.255.255.0	192.168.10.1
15	PC-15	192.168.10.31	255.255.255.0	192.168.10.1
16	PC-16	192.168.10.32	255.255.255.0	192.168.10.1
17	PC-17	192.168.10.33	255.255.255.0	192.168.10.1
18	PC-18	192.168.10.34	255.255.255.0	192.168.10.1

19	PC-19	192.168.10.35	255.255.255.0	192.168.10.1
20	PC-20	192.168.10.36	255.255.255.0	192.168.10.1
21	PC-21	192.168.10.37	255.255.255.0	192.168.10.1
22	PC-22	192.168.10.38	255.255.255.0	192.168.10.1
23	PC-23	192.168.10.39	255.255.255.0	192.168.10.1
24	PC-24	192.168.10.40	255.255.255.0	192.168.10.1
25	PC-25	192.168.10.41	255.255.255.0	192.168.10.1
26	PC-26	192.168.10.42	255.255.255.0	192.168.10.1
27	PC-27	192.168.10.43	255.255.255.0	192.168.10.1
28	PC-28	192.168.10.44	255.255.255.0	192.168.10.1
29	PC-29	192.168.10.45	255.255.255.0	192.168.10.1
30	PC-30	192.168.10.46	255.255.255.0	192.168.10.1
31	PC-31	192.168.10.47	255.255.255.0	192.168.10.1
32	PC-32	192.168.10.48	255.255.255.0	192.168.10.1

Tabla 15. Área de Internación

Nro.	Equipo	Dirección IP	Máscara de red	Puerta de enlace
33	PC-33	192.168.10.50	255.255.255.0	192.168.10.1
34	PC-34	192.168.10.51	255.255.255.0	192.168.10.1
35	PC-35	192.168.10.52	255.255.255.0	192.168.10.1
36	PC-36	192.168.10.53	255.255.255.0	192.168.10.1

Tabla 16. Área de Enfermería

Nro.	Equipo	Dirección IP	Máscara de red	Puerta de enlace
37	PC-37	192.168.10.54	255.255.255.0	192.168.10.1
38	PC-38	192.168.10.55	255.255.255.0	192.168.10.1
39	PC-39	192.168.10.56	255.255.255.0	192.168.10.1

Tabla 17. Área de Terapia Intensiva

Nro.	Equipo	Dirección IP	Máscara de red	Puerta de enlace
40	PC-40	192.168.10.60	255.255.255.0	192.168.10.1
41	PC-41	192.168.10.61	255.255.255.0	192.168.10.1
42	PC-42	192.168.10.62	255.255.255.0	192.168.10.1
43	PC-43	192.168.10.63	255.255.255.0	192.168.10.1

Tabla 18. Área de Pediatría

Nro.	Equipo	Dirección IP	Máscara de red	Puerta de enlace
44	PC-44	192.168.10.70	255.255.255.0	192.168.10.1
45	PC-45	192.168.10.71	255.255.255.0	192.168.10.1

Tabla 19. Área de Contabilidad

Nro.	Equipo	Dirección IP	Máscara de red	Puerta de enlace
46	PC-46	192.168.10.80	255.255.255.0	192.168.10.1

Tabla 20. Área de Farmacia

Nro.	Equipo	Dirección IP	Máscara de red	Puerta de enlace
47	PC-47	192.168.10.81	255.255.255.0	192.168.10.1
48	PC-48	192.168.10.82	255.255.255.0	192.168.10.1
49	PC-49	192.168.10.83	255.255.255.0	192.168.10.1

Tabla 21. Área de Esterilización

Nro.	Equipo	Dirección IP	Máscara de red	Puerta de enlace
50	Print-50	192.168.10.100	255.255.255.0	192.168.10.1
51	Print-51	192.168.10.101	255.255.255.0	192.168.10.1
52	Print-52	192.168.10.102	255.255.255.0	192.168.10.1
53	Print-53	192.168.10.103	255.255.255.0	192.168.10.1
54	Print-54	192.168.10.104	255.255.255.0	192.168.10.1
55	Print-55	192.168.10.105	255.255.255.0	192.168.10.1
56	Print-56	192.168.10.106	255.255.255.0	192.168.10.1
57	Print-57	192.168.10.110	255.255.255.0	192.168.10.1
58	Print-58	192.168.10.111	255.255.255.0	192.168.10.1
59	Print-59	192.168.10.112	255.255.255.0	192.168.10.1
60	Print-60	192.168.10.113	255.255.255.0	192.168.10.1
61	Print-61	192.168.10.114	255.255.255.0	192.168.10.1
62	Print-62	192.168.10.115	255.255.255.0	192.168.10.1
63	Print-63	192.168.10.116	255.255.255.0	192.168.10.1
64	Print-64	192.168.10.117	255.255.255.0	192.168.10.1

Tabla 22. Impresoras

III.1.1.4.2.- Planos de la Clínica Santísima Trinidad de Tarija

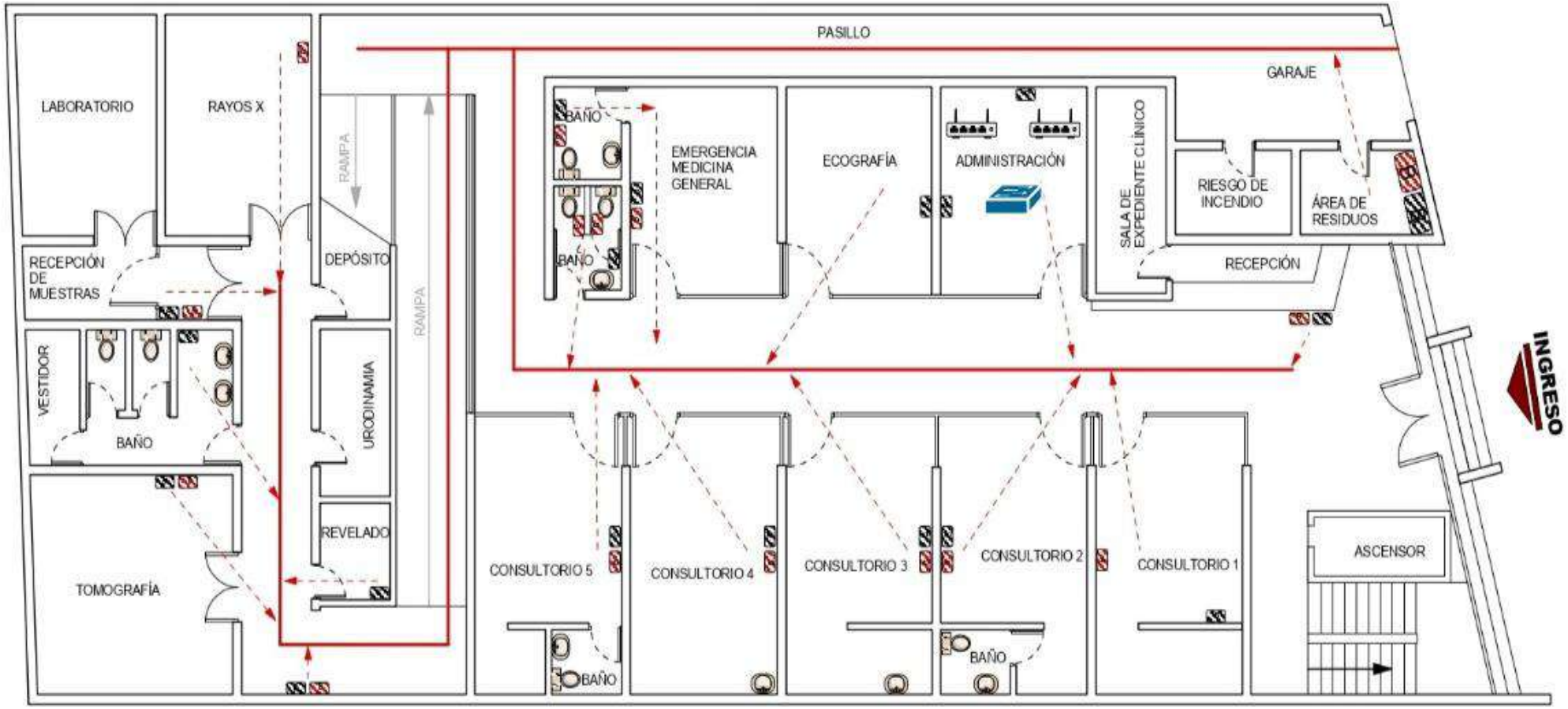

Figura 26. Plano Planta Baja

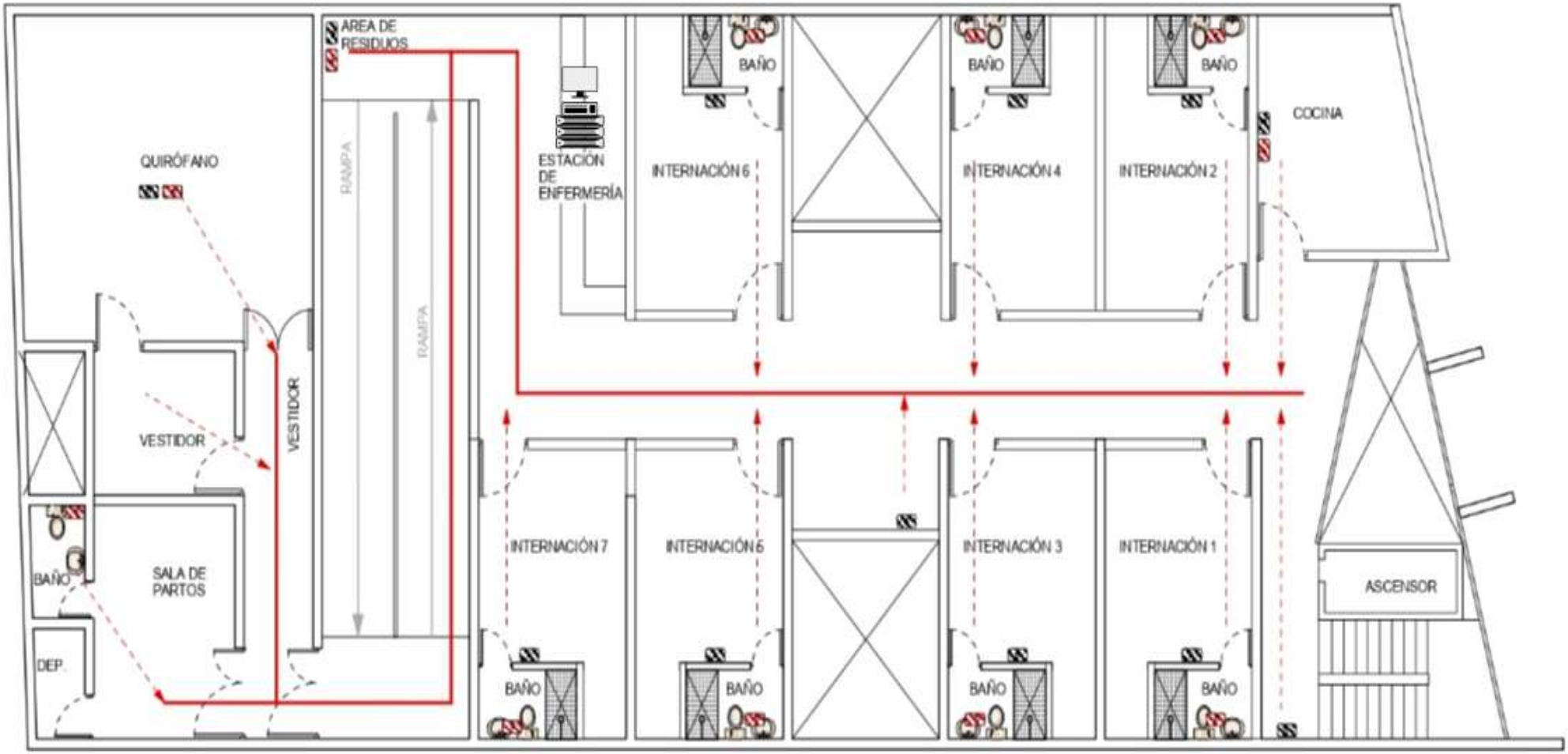

Figura 35. Plano Primer Piso

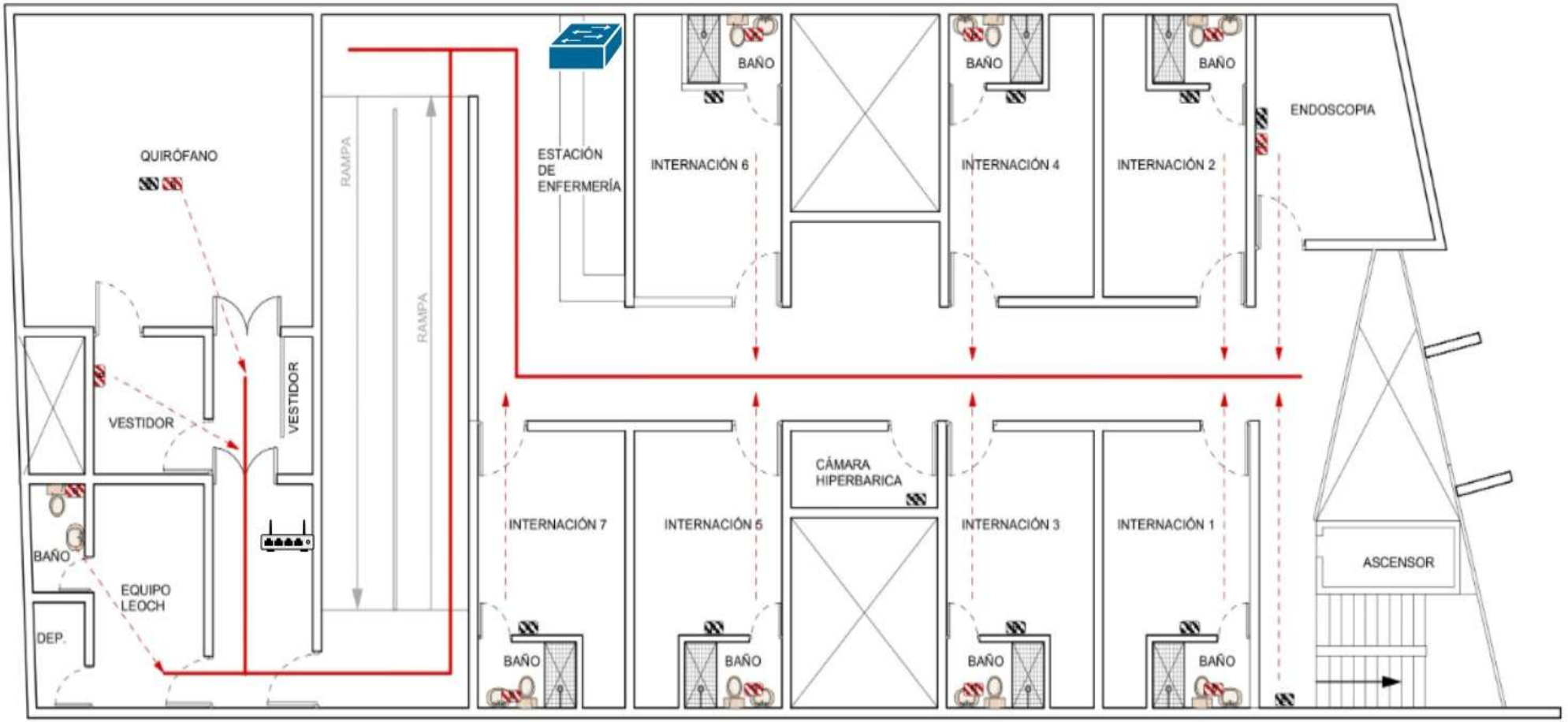

Figura 36. Plano Segundo Piso

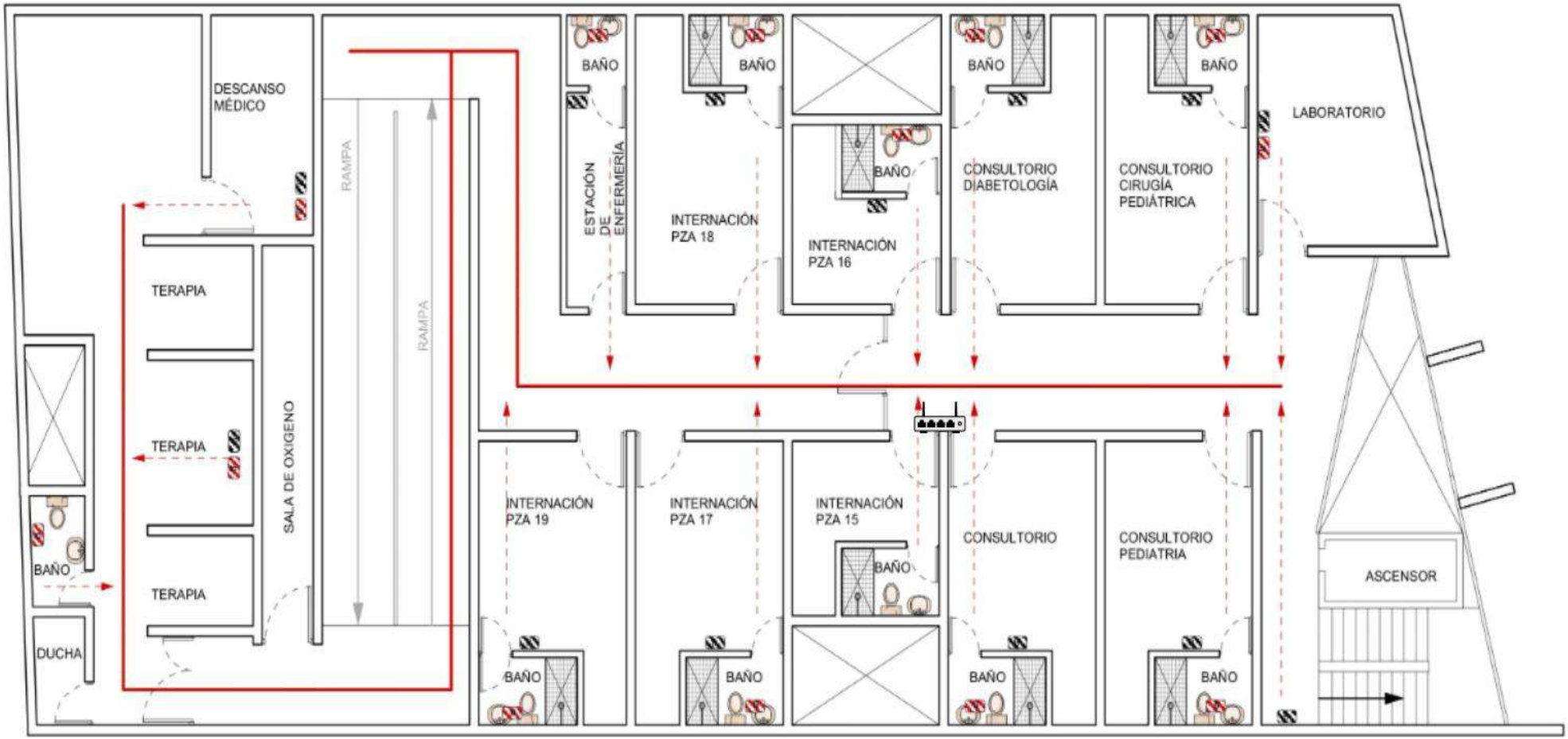

Figura 37. Plano Tercer Piso

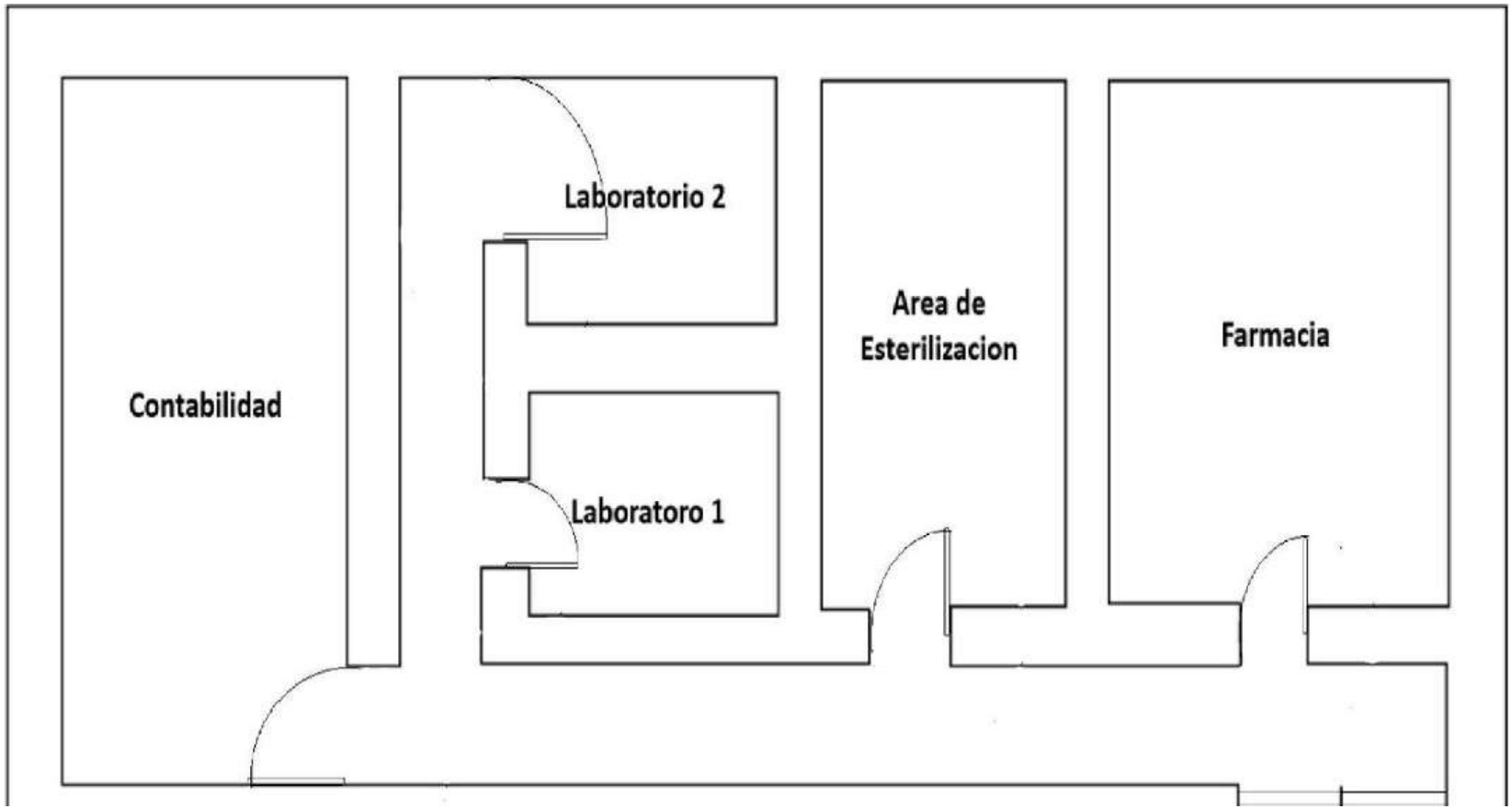

Figura 38. Plano Extensión Tercer Piso

III.1.1.4.3.- Explicación de los planos

La Clínica cuenta con 4 pisos en lo que se presenta.

- En la planta baja se encuentran recepción, consultorios, administración, emergencias y la Área tercerizada. Alberga los equipos de red (Switch, AP, Router) que interconectan con las demás plantas y desde donde se recibe el servicio de internet del proveedor.
- En el primer piso se encuentran internaciones, enfermería, terapia intensiva y el sistema de su base de datos de la clínica. Planta donde se encuentra ubicado el servidor de la base de datos de la clínica, el cual gestiona los módulos de Ingresos, Contabilidad e Inventarios.
- En el segundo piso continua con internaciones, enfermería y terapia intensiva. Planta donde se encuentran el switch y el punto de acceso que interconectan con la tercera planta.
- En la tercera planta se encuentran pediatría, internaciones, áreas tercerizadas y terapia intensiva. Planta donde se encuentra el Access Point del personal de pediatría, conectado a un proveedor de servicio de internet independiente de la clínica y que no forma parte de su red interna.
- En la extensión tercer planta se encuentran farmacia, esterilización y contabilidad.

III.1.1.4.4.- Explicación de la antigua red

- En la planta baja en la parte de Administración se encuentran dos Access point lo cual uno recibe Internet y el otro sirve como un repetidor, este se encuentra conectado al Switch la cual están también están varias PCs el DVR de cámaras de seguridad.
- En el primer piso hay PCs de Internación, Terapia intensiva y el sistema que maneja su base de datos que tienen un cableado conectado hacia el Switch de la planta baja.
- En el segundo piso hay PCs de Internación y un Access point en la entrada de quirófano, más una laptop para poder realizar grabaciones de operaciones en directo lo cual todo el cableado de red está conectado a otro Switch que se encuentra en este mismo piso y que este está conectado hacia el Access point de la planta baja.
- En el tercer piso igualmente hay PCs de Internación, Terapia intensiva, Área de Esterilización y Enfermería que se encuentran conectados al switch de la segunda planta. También existe otra red que son para el área de Pediatría, y cuentan con su propio servicio de internet y sus Laptops están conectados a su Access point de forma inalámbrica.
- En la extensión del tercer piso hay puro equipos PCs tanto en Farmacia, Esterilización y Contabilidad, lo cual se encuentran conectados hacia el Switch de la segunda planta.

En la antigua infraestructura de red de la Clínica, se utilizaba la red IP 192.168.10.0 siguiendo inicialmente un orden y jerarquía definidos. Sin embargo, el análisis reveló que las direcciones IP estaban desorganizadas y mezcladas en todos los switches, sin segmentación lógica.

Esta situación se debía al deterioro o mala organización de las etiquetas de red, lo que dificultaba

identificar correctamente los puntos de conexión. Además, por la necesidad de mantener los servicios operativos y conectar rápidamente nuevos dispositivos, se asignaban manualmente IPs disponibles sin seguir una estructura planificada.

Esta práctica afectaba la administración y control de la red, incrementaba el riesgo de conflictos de IP y complicaba el mantenimiento técnico.

III.1.1.5.- Análisis de tráfico existente

Figura 39. Aplicaciones en uso

Comportamiento	Solicitud	Breed	Paquetes totales	Bytes totales	Bytes enviados	Bytes recibidos	Porcentaje
	HTTP	Acceptable	28,282 Pkts	28.02 MB	131.11 KB	27.89 MB	83 %
	MDNS	Acceptable	9,329 Pkts	2.75 MB	7.00 KB	2.74 MB	9 %
	YouTube	Fun	622 Pkts	646.38 KB	625.00 B	645.77 KB	2 %
	SSDP	Acceptable	1,537 Pkts	581.77 KB	9.67 KB	572.10 KB	2 %
	GoogleServices	Acceptable	728 Pkts	560.26 KB	0.00 B	560.26 KB	2 %
	Microsoft	Safe	466 Pkts	344.66 KB	2.38 KB	342.27 KB	1 %
	TLS	Safe	1,417 Pkts	327.54 KB	13.96 KB	313.57 KB	1 %
	Microsoft365	Acceptable	785 Pkts	324.85 KB	7.66 KB	317.19 KB	1 %
	Google	Acceptable	522 Pkts	246.82 KB	110.00 B	246.71 KB	1 %
	Unknown	Unrated	127 Pkts	108.05 KB	13.61 KB	94.44 KB	1 %

Comportamiento	Solicitud	Breed	Paquetes totales	Bytes totales	Bytes enviados	Bytes recibidos	Porcentaje
	QUIC	Acceptable	90 Pkts	65.68 KB	38.32 KB	27.36 KB	1 %
	ICMPV6	Acceptable	395 Pkts	38.91 KB	1.44 KB	37.47 KB	1 %
	DNS	Acceptable	220 Pkts	28.04 KB	8.95 KB	19.09 KB	1 %
	MS_OneDrive	Acceptable	61 Pkts	19.25 KB	704.00 B	18.56 KB	1 %
	WindowsUpdate	Safe	41 Pkts	14.19 KB	780.00 B	13.43 KB	1 %
	PlayStore	Safe	22 Pkts	10.19 KB	0.00 B	10.19 KB	1 %
	DHCP	Acceptable	22 Pkts	8.92 KB	2.79 KB	6.13 KB	1 %
	LLMNR	Acceptable	65 Pkts	7.10 KB	4.43 KB	2.67 KB	1 %
	IGMP	Acceptable	101 Pkts	4.86 KB	2.55 KB	2.31 KB	1 %
	NetBIOS	Acceptable	27 Pkts	2.76 KB	514.00 B	2.26 KB	1 %

Comportamiento	Solicitud	Breed	Paquetes totales	Bytes totales	Bytes enviados	Bytes recibidos	Porcentaje
	ICMP	Acceptable	19 Pkts	2.63 KB	1.55 KB	1.08 KB	1 %
	DHCPV6	Acceptable	11 Pkts	1.41 KB	482.00 B	960.00 B	1 %
	CNP-IP	Acceptable	18 Pkts	1.11 KB	516.00 B	620.00 B	1 %
	WSD	Acceptable	1 Pkts	718.00 B	718.00 B	0.00 B	1 %
	SMBv1	Dangerous	2 Pkts	486.00 B	486.00 B	0.00 B	1 %
	SSH	Acceptable	2 Pkts	132.00 B	132.00 B	0.00 B	1 %

Figura 40. Detalle de consumo de aplicaciones

Solicitud	Porcentaje (%)	Bytes Totales	Descripción
HTTP	83	28.02 MB	Tráfico web no cifrado (páginas sin HTTPS, no seguras)
MDNS	9	2.75 MB	Comunicación en red local para detectar dispositivos (impresoras, TV)
YouTube	2	646.38 KB	Consumo de YouTube (video en línea)
SSDP	2	581.77 KB	Protocolo de búsqueda de dispositivos (Smart TV, impresoras)
GoogleServices	2	560.26 KB	Servicios de Google (correo, sincronización, cuentas)
Microsoft	1	344.66 KB	Servicios de Microsoft (cuentas, apps, actualizaciones)
Microsoft365	1	324.85 KB	Servicios de Microsoft 365 (correo, apps)
TLS	1	327.54 KB	Cifrado de tráfico TLS (conexiones seguras)
Unknown	1	108.05 KB	Tráfico no identificado (aplicaciones desconocidas)

Tabla 23. Consumo de aplicaciones de la red

III.1.1.5.1.- Ancho de banda actual de la red

Mediante un testeo se pudo analizar el ancho de banda lo cual pertenece al proveedor de servicios Tigo. El plan de internet que llega a la clínica es de 93Mbps, de tipo plan hogar Tigo.

Figura 41. Ancho de banda actual

III.1.1.5.2.- Estado de la red Actual

El estado actual de la red de la clínica presenta múltiples limitaciones tanto en términos de rendimiento como de seguridad. La falta de segmentación, la obsolescencia de los equipos representa los principales desafíos.

Infraestructura de red Equipos de red

La infraestructura actual es una simple red LAN sin una topología, compuesta principalmente por access points y switches de generación pasada, sin soporte para tecnologías avanzadas como VLAN. Además, no se ha implementado una segmentación de red efectiva. Esta configuración, aunque simple, presenta importantes desventajas: al depender de dos únicos cables troncales, existe un punto de falla, lo que significa que, si uno de los dos cables principales se daña, diferentes pisos podrían verse afectados. Además, la falta de segmentación limita la eficiencia y la seguridad de la red, y la obsolescencia de los equipos impide un rendimiento adecuado

Rendimiento de la red

Velocidad y latencia: Se han detectado velocidades inestables en la red interna, lo que afecta a los sistemas de gestión, como la actualización de historiales médicos y la comunicación entre dispositivos médicos. Las latencias registradas son altas durante las horas pico, afectando los sistemas que requieren alta disponibilidad.

Seguridad de la red

La red no tiene una segmentación, lo que representa un riesgo para la seguridad, ya que no se distingue entre las diferentes áreas operativas, como administración, áreas médicas y servicios críticos.

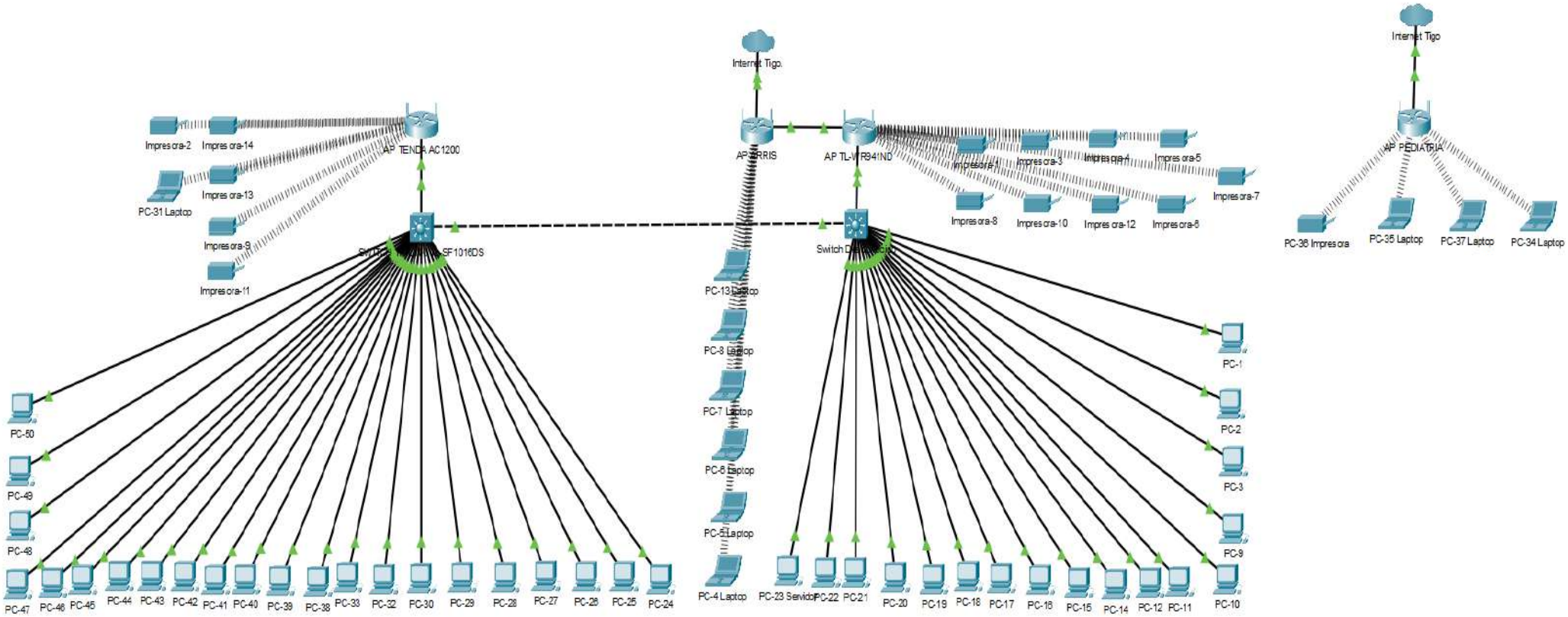

Figura 42. Diagrama de estado actual de la red

Problemas detectados -Componentes desactualizados y sin soporte

- Falta de segmentación en la red, tanto en la infraestructura cableada como en la red WiFi.
- No cuenta con una Topología de red.
- No cuenta con algún tipo de seguridad en la red.
- Caídas constantes en la red.
- No cumple con los estándares de diseño y configuración recomendados para una infraestructura de red.
- La parte del cableado no se encuentra etiquetado para poder saber su función y a que área pertenece.
- Direccionamiento IP desordenado y sin control centralizado, lo que genera vulnerabilidades y fallos operativos.

III.1.1.5.3.- Análisis de Riesgos para la Clínica Santísima Trinidad de Tarija

III.1.1.5.3.1.- Identificación de Riesgos

Riesgos Tecnológicos

Fallo de la infraestructura tecnológica

- Descripción: La infraestructura de red de la clínica es crucial para mantener la operatividad de todos los sistemas médicos y administrativos. Un fallo podría paralizar la comunicación interna, el acceso a historiales médicos, o la administración de recursos.
- Impacto: Alta
- Probabilidad: Moderada (dependiendo del mantenimiento y la antigüedad de los equipos)

Riesgos Operativos

Interrupción en el suministro eléctrico

- Descripción: Los cortes de energía pueden afectar tanto el funcionamiento de equipos médicos como de la infraestructura crítica, incluida la iluminación y los sistemas de soporte vital.
- Impacto: Alta
- Probabilidad: Baja (dependiendo de la infraestructura de energía de respaldo)

Accidentes o desastres naturales

- Descripción: Terremotos, inundaciones o incendios pueden causar daños significativos a las instalaciones físicas del hospital, interrumpiendo los servicios médicos y poniendo en riesgo a pacientes y personal.
- Impacto: Alta
- Probabilidad: Baja (dependiendo de la ubicación geográfica)

Riesgo	Probabilidad	Impacto	Puntaje de Riesgo
Fallo de la Infraestructura Tecnológica	Moderada	Alta	6(alto)
Interrupción en el Suministro eléctrico	Baja	Alta	4(moderado)
Accidentes o desastres naturales	Baja	Alta	4(moderado)

Tabla 24. Análisis de Riesgos

III.1.1.5.4.- Plan de Mitigación de Riesgos para la Clínica Santísima Trinidad de Tarija

Riesgos Tecnológicos

Fallo de Infraestructura Tecnológica

Estrategias de Mitigación:

- Redundancia de Infraestructura: Implementar redes y dispositivos de red redundantes para evitar puntos únicos de fallo. Esto incluye Switch, AP, Servidores adicionales y conexiones de red alternativas para garantizar que, en caso de fallo, los servicios sigan operando.
- Mantenimiento Preventivo: Establecer un plan de mantenimiento preventivo para todos los equipos tecnológicos, con revisiones periódicas y actualizaciones.

Riesgos Operativos

Interrupción en el Suministro Eléctrico

Estrategias de Mitigación:

- Generadores de Respaldo: Instalar generadores eléctricos de respaldo de alta capacidad para garantizar el funcionamiento de los sistemas críticos de la clínica (iluminación, equipos médicos, sistemas de comunicación) durante un corte de energía.
- Mantenimiento de Generadores: Realizar un mantenimiento preventivo regular a los generadores y sistemas de energía de respaldo para asegurar su funcionamiento adecuado.
- Pruebas Periódicas: Realizar pruebas de corte de energía simuladas para garantizar que el sistema de respaldo funcione correctamente en situaciones reales.

Accidentes o desastres naturales

Estrategias de Mitigación:

- Infraestructura Resistente: Asegurar que las instalaciones físicas de la clínica estén diseñadas para resistir desastres naturales, con refuerzos sísmicos, sistemas de drenaje para inundaciones y medidas contra incendios.
- Planes de Evacuación: Desarrollar y practicar planes de evacuación detallados, asegurando que todo el personal esté capacitado para manejar situaciones de emergencia.
- Simulacros de Emergencia: Realizar simulacros regulares de evacuación y respuesta ante

desastres naturales para evaluar la efectividad de los planes y mejorar la preparación.

III.1.2.-Fase 2: Desarrollar Diseño Lógico

III.1.2.1.-Diseño de Topología de red

El diseño de la red de la Clínica busca garantizar conectividad eficiente, segura y confiable para sus áreas médicas y administrativas. Tras evaluar la distribución física, el número de dispositivos y la necesidad de segmentación por VLANs, se optó por una topología en árbol. Esta estructura jerárquica conecta los switches de cada piso a un switch central en planta baja, lo que mejora el rendimiento, la seguridad y el mantenimiento.

III.1.2.1.1.-Topología en árbol

Se ha optado por implementar una topología en árbol, ya que combina las ventajas de la topología en estrella con una estructura jerárquica que facilita la administración y el crecimiento de la red. En este modelo, cada piso cuenta con un switch secundario que concentra la conexión de los dispositivos locales, y estos switches se enlazan con un router central que actúa como núcleo de la red. Esta elección se basa en los siguientes beneficios:

- **Escalabilidad:** Permite añadir nuevos segmentos o dispositivos sin modificar la infraestructura existente.
- **Organización jerárquica:** Facilita la identificación de fallas y la segmentación.
- **Facilidad de mantenimiento:** Es posible aislar una sección de la red para realizar tareas sin afectar al resto.
- **Optimización del cableado:** Reduce la longitud de los cables y mejora la organización física en racks y canalizaciones.
- **Gestión eficiente del tráfico:** La jerarquía permite controlar, priorizar y segmentar el flujo de datos según las necesidades de la clínica.

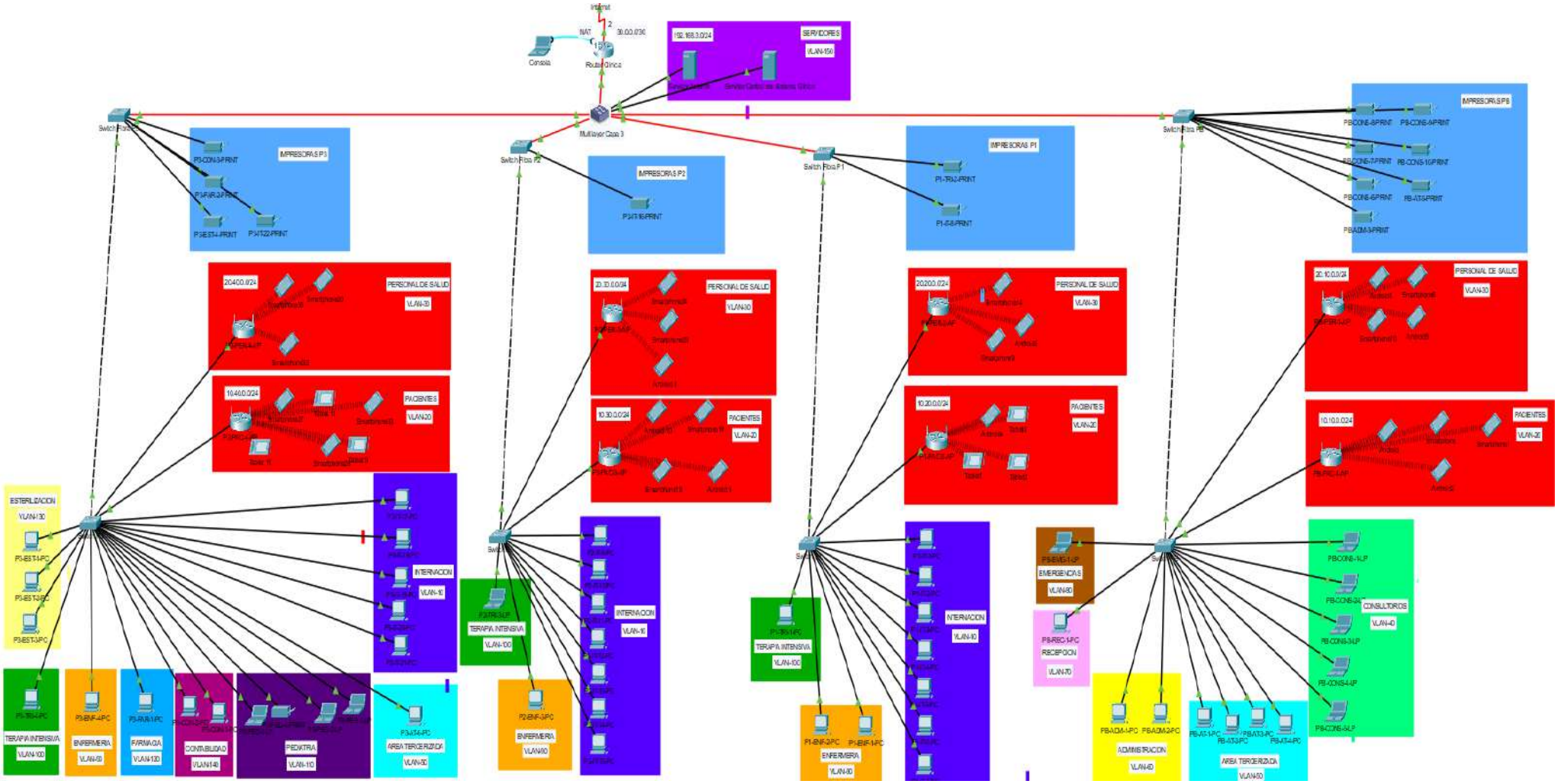

Figura 43. Diseño lógico de la red

III.1.2.1.2.- Cableado

El cableado estructurado es esencial para el transporte de información en la red. Se utilizará cable UTP de cobre de categoría 5e por su bajo costo, facilidad de instalación y capacidad para transmitir voz y datos en distancias de hasta 100 metros. Su tamaño reducido facilita la instalación en espacios limitados, aunque, al no contar con blindaje, no es apto para zonas con alta interferencia electromagnética. Esta elección garantiza una comunicación confiable y eficiente en la clínica.

Figura 44. Cable UTP categoría 5e

En este diseño se utilizará cable UTP categoría 5e, cumpliendo con los estándares ANSI/TIA/EIA-568-B, 606-B y 569-B, que establecen el orden y colores en los conectores RJ45. Se emplearán dos tipos de conexión: cable directo (T568A o T568B) y cable cruzado, cada uno con funciones específicas.
Los cables directos, utilizados en la mayoría de las instalaciones, permiten la conexión estándar entre dispositivos. Los cables cruzados, en cambio, se emplean para la transmisión y recepción simultánea de datos entre ciertos equipos.

III.1.2.1.3.- Racks

Se implementarán diferentes Racks, es una estructura metálica diseñada para alojar y organizar de manera ordenada los equipos de red y servidores, como switches, routers, firewalls y otros dispositivos informáticos. Permite una instalación segura, facilita la ventilación y el mantenimiento de los equipos, optimiza el uso del espacio y contribuye a una gestión más eficiente del cableado y de la infraestructura tecnológica.

Distribución

La Clínica, compuesta por cuatro pisos, contará con la instalación de un rack de piso y gabinetes de pared en cada planta, con el objetivo de organizar el cableado horizontal y vertical de los equipos de red.
En la planta baja se ubicará el rack de piso principal o cuarto de telecomunicaciones, que funcionará como el núcleo central de la red. En este se instalarán los equipos más importantes: switches troncales, firewall, router, servidor de telefonía IP y la central del sistema, enlaces de fibra óptica que conectarán los diferentes pisos.
En las demás plantas se dispondrá de gabinetes de pared, dentro de los cuales se instalarán switches para la extensión y distribución de la red en cada nivel. Esta disposición permitirá una administración más ordenada y eficiente de la infraestructura.
El cableado horizontal cumplirá con los requisitos de la norma ANSI/TIA/EIA-568-B, utilizando cable de

pares trenzados no blindado (UTP), con especificaciones claras para cableado, conectores y dispositivos. El cableado vertical conectará los paneles de distribución horizontal de cada cuarto de telecomunicaciones con la red troncal, utilizando fibra óptica para garantizar alta capacidad, estabilidad y escalabilidad.

- Se instalará un armazón de cableado vertical en el cuarto de telecomunicaciones de la planta baja, el cual funcionará como MDF (Marco de Distribución Principal) de toda la red.
- Desde este punto, se tenderá cable de fibra óptica hacia los gabinetes de pared ubicados en los cuartos de telecomunicaciones de cada piso superior, los cuales actuarán como IDF (Marco de Distribución Intermedio).
- El cableado de fibra óptica se terminará en cada IDF utilizando conectores SC, asegurando una conexión confiable entre el MDF y los diferentes niveles de la clínica.

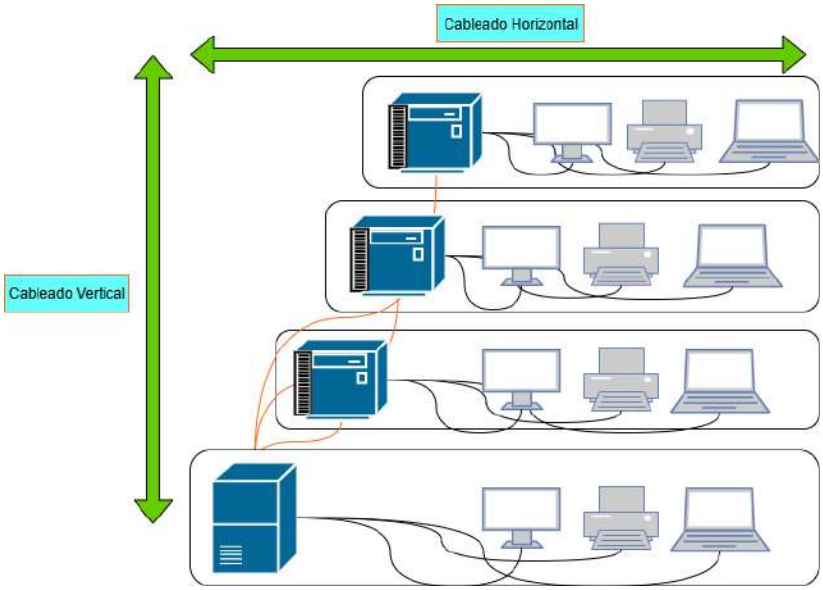

Figura 45. Diseño cableado horizontal y vertical

III.1.2.1.4.- Switches

Los switches son dispositivos de red que conecta múltiples equipos dentro de una red de área local (LAN), permitiendo el intercambio eficiente de datos entre ellos. Opera bajo el estándar Ethernet y es fundamental para la comunicación interna de la red, gestionando el tráfico de información de manera organizada y asegurando que los datos lleguen correctamente a su destino.

- **Un switch capa 3 de 12 puertos con conectividad por fibra óptica**, que funcionará como servidor DHCP y permitirá la interconexión eficiente de las distintas VLANs de la clínica, facilitando el tráfico de datos de manera segura y optimizada.
- **Cuatro switches capa 2 de 10 puertos**, uno en cada piso, encargados de distribuir y conmutar el tráfico local. Cada uno recibirá la conexión principal mediante fibra óptica desde el switch central (MDF). En ellos se conectarán las impresoras asignadas a cada VLAN, garantizando una

segmentación eficiente y un rendimiento estable para cada área o departamento.

- **Cuatro switches capa 2 de 24 puertos**, destinados a la conexión de equipos finales como computadoras, laptops, dispositivos médicos y puntos de acceso inalámbrico (AP). Esta capacidad garantiza la atención a la demanda actual de la clínica y permite un margen suficiente para futuras ampliaciones.

Características de los switchs:

- Número de puertos de Fibra óptica: 12 puertos SFP
- Número de puertos: 4 RJ45 Ethernet.
- Velocidad de transferencia de datos: 1 Gbps (Gigabit por segundo)
- Protocolo de interconexión de datos: Ethernet, Giga Ethernet.
- Fuente de alimentación interna

Figura 46. Cisco Catalyst 3750X-12S-S

- Número de puertos: 8 puertos 10/100/1000 Mbps
- Número de puertos de Fibra óptica: 2 ranuras SFP Gigabit para módulos de fibra óptica
- Velocidad de transferencia de datos: 1 Gbps (Gigabit por segundo)
- Protocolo de interconexión de datos: IEEE 802.3i (Ethernet), IEEE 802.3u (Fast Ethernet), IEEE 802.3ab (Gigabit Ethernet), IEEE 802.3z (Gigabit sobre fibra), IEEE 802.3x (control de flujo), IEEE 802.1Q (VLAN)
- Fuente de alimentación interna, AC 100–240 V, 50/60 Hz
- Montaje: En rack o sobremesa

Figura 47. TL-SG2210P V3 10 puertos

- 24 puertos Gigabit Ethernet
- Ranuras conectables de factor de forma pequeño (SFP) de 1G o ranuras SFP+ de 1G/10G
- Apilamiento Cisco FlexStack con 20 Gbps de rendimiento de pila (opcional)
- PoE+ compatible con IEEE 802.3at para hasta 30 W de potencia por puerto

- Hasta 740 W de presupuesto combinado PoE/PoE+
- Interfaces USB para gestión y transferencia de archivos

Figura 48. Cisco WS-C2960S-24PD-L Catalyst 2960S

Esta configuración ha sido diseñada considerando una posible ampliación de la red y el ingreso de nuevos usuarios que se integren a las actividades diarias de la clínica. Así, se asegura que no habrá limitaciones en la capacidad de acceso a la red ni en la calidad del servicio, manteniendo siempre la seguridad y el control necesarios para la operación.

III.1.2.1.5.- Router

Los routers son dispositivos de red encargado de conectar dos o más redes diferentes, analizando las direcciones de destino de los paquetes de datos y determinando la ruta más eficiente para su envío. Además, puede asignar direcciones IP a los dispositivos, permitir el acceso simultáneo a internet, aplicar políticas de seguridad y enlazar redes que utilicen distintos tipos de conexión, como cableado, fibra óptica o inalámbrica. De esta manera, garantiza que la información llegue de forma rápida, eficiente y segura a su destino.

Características de router

Se eligió un router empresarial modular de la serie ISR G2(Router de Servicios Integrados de Segunda Generación de Cisco), diseñado para ofrecer servicios integrados como Enrutamiento, Políticas de seguridad, VLANs y VoIP en redes pequeñas o medianas.

- Código de producto: CISCO2901/k9
- Interfaces: 2 puertos Ethernet 10/100/1000Mbps integrados
- Ranuras de expansión Interfaces Fibra Óptica: 2 Puertos SPF
- 4 ranuras para tarjetas de interfaz WAN de alta velocidad mejoradas
- RAM: 512 MB (instalada) / 2 GB (máximo)
- Memoria Flash: 256 MB (instalada) / 8 GB (máximo)
- Fuente de alimentación interna

Figura 49. Cisco 2901 - CISCO2901/K9

III.1.2.1.6.- Access point

Se implementarán diferentes puntos de acceso de red que permitan la conexión inalámbrica de múltiples dispositivos a través de tecnología Wi-Fi, ofreciendo cobertura, velocidad y estabilidad en la comunicación. Está diseñado para entornos con alta demanda de conexión, como oficinas, empresas o instituciones, garantizando un acceso eficiente a la red. En este proyecto, se instalarán 8 puntos de acceso, los cuales estarán conectados directamente mediante cable Ethernet para asegurar un rendimiento óptimo y una transmisión de datos estable.

- **Velocidad:** Soporta velocidades combinadas de hasta 1350 Mbps (450 Mbps en 2.4 GHz o 867 Mbps en 5 GHz), ideal para streaming, videoconferencias y múltiples dispositivos conectados al mismo tiempo.
- **Dual Band:** Funciona en dos frecuencias (2.4 GHz y 5 GHz), lo que ayuda a reducir interferencias y mejorar el rendimiento.

  La Banda 2.4 GHz cubre hasta 100 metros en interiores y alrededor de 300 metros en exteriores.

  Banda 5 GHz cubre menor cobertura, típicamente 30-50 metros en interiores y hasta 100 metros en exteriores.
- **Montaje:** Puede instalarse en pared o techo, adaptándose a diferentes espacios.
- **Tecnología MU-MIMO:** Permite comunicarse con varios dispositivos simultáneamente, mejorando la eficiencia.
- **PoE (Power over Ethernet):** Se alimenta y conecta por un solo cable Ethernet, facilitando la

instalación sin necesidad de un enchufe cercano.

Figura 50. TP-Link EAP225

III.1.2.1.7.- Fortinet

Se implementará un firewall Fortinet de seguridad de red diseñado para proteger la infraestructura informática frente a accesos no autorizados y amenazas cibernéticas. Ofrece una protección integral mediante el control del tráfico que entra y sale de la red, aplicando políticas de filtrado, detección y prevención de intrusiones, así como funciones avanzadas de análisis y gestión. Gracias a su tecnología integrada y automatizada, permite crear redes seguras, optimizar el rendimiento y responder eficazmente ante amenazas emergentes y sofisticadas. Cabe destacar que el Fortinet es bien conocido tanto por su rendimiento como por su eficacia de seguridad, se puede ver 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.

Características del Fortinet

- USB Port
- Console Port
- 2x GE RJ45 WAN Ports
- 1x GE RJ45 DMZ Ports
- 7x GE RJ45 Internal Ports

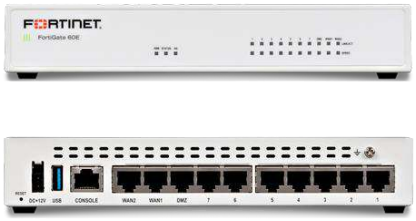

Figura 51. Fortinet 60E

III.1.2.1.8.- Servidores

Un servidor es un sistema informático diseñado para proporcionar servicios, recursos o información a otros dispositivos dentro de una red. Su función principal es recibir, procesar y responder solicitudes, facilitando la comunicación y el intercambio de datos entre los equipos conectados. Están construidos para operar de manera continua, con alta capacidad de procesamiento, memoria suficiente, almacenamiento adecuado y medidas de seguridad que garanticen un acceso rápido, confiable y protegido. De esta manera, permiten centralizar y administrar eficientemente los servicios que optimizan el funcionamiento de la red.

Figura 52. HPE ProLiant MicroServer Gen11

Caracteristicas:

- Factor de forma: Torre ultra-compacta (Ultra Micro Tower).
- Procesador: Socket único compatible con Intel Xeon 6300-series, Xeon E-2400 o Pentium Gold.
- Memoria: 4 ranuras UDIMM DDR5 hasta 4400 MT/s, con un máximo de 128 GB (4×32 GB).
- Almacenamiento interno: Hasta 4 bahías para unidades de 3.5″ LFF sin hot-plug o 4 unidades de 2.5″ SFF con kit adaptador.
- Controladora de almacenamiento: Intel VROC SATA (RAID por software integrado).
- Expansión: 2 ranuras PCIe (una compatible con PCIe 5.0).
- Conectividad de red: 4 puertos Gigabit Ethernet integrados.
- Gestión remota: HPE iLO 6 incorporado con soporte TPM 2.0 para mayor seguridad.
- Fuente de alimentación: Adaptador externo de 180 W (no redundante).
- Dimensiones aproximadas: 15.4 cm (H) × 26.1 cm (W) × 24.9 cm (D).

Figura 53. Servidor DELL PowerEdge T40

Caracteristicas:

- Procesador: Intel Xeon E-2224G de 4 núcleos, 3.5 GHz (hasta 4.7 GHz turbo).
- Memoria: 4 ranuras DDR4 UDIMM hasta 2666 MT/s, máximo 64 GB.
- Almacenamiento: Hasta 3 bahías para discos de 3.5″ SATA, capacidad total aproximada de 12 TB.
- Fuente de alimentación: 300 W, certificación Bronze.
- Factor de forma: Torre compacta (Mini Tower).
- Dimensiones: 33.5 cm (alto) × 17.6 cm (ancho) × 35.9 cm (profundidad); peso aproximado de 8kg.
- Seguridad y gestión: Arranque seguro, TPM 2.0, Intel SGX y gestión integrada Intel AMT.
- Conectividad de red: 1 puerto Gigabit Ethernet integrado.
- Puertos: Varios USB 2.0 y 3.1 en panel frontal y posterior.
- Ranuras de expansión: 1 PCIe Gen3 x16, 2 PCIe Gen3 x4 y 1 PCI.

Se menciona los servidores que utilizara la clínica:

Servidor DHCP

El servidor DHCP se integrará con el switch multicapa (Capa 3) de la red y se configurará mediante un pool de direcciones IP. Este servidor asignará automáticamente las direcciones IP a los dispositivos conectados dentro de la red local (LAN), definiendo el rango de direcciones, la puerta de enlace (Gateway) y los servidores DNS. Los Access Points (AP) se conectarán a la LAN y recibirán direcciones IP privadas desde el servidor DHCP, permitiendo distribuir conectividad inalámbrica a los clientes. Para este proyecto, los servicios DNS estarán dirigidos a la IP 192.168.3.100, correspondiente al servidor de telefonía, exceptuando el área de pacientes, que seguirá una configuración independiente.

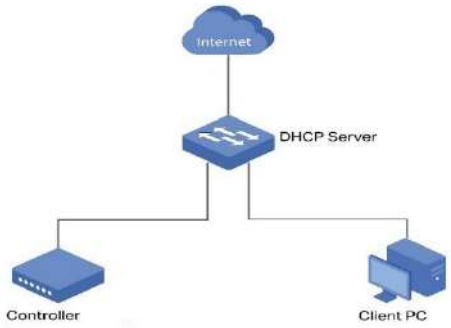

Figura 54. Servidor DHCP

Servidor Asterisk

Asterisk es un software central de telefonía PBX (Central Telefónica Privada). Ofrece flexibilidad para integrar líneas telefónicas tradicionales, teléfonos IP y aplicaciones móviles.

Escalabilidad en Comunicaciones:

- El servidor Asterisk estará configurado para soportar un mayor número de extensiones y funcionalidades, integración con aplicaciones móviles.
- Capacidad de expansión para manejar mayor tráfico de llamadas o agregar funcionalidades como grabación de llamadas o respuesta automática.

Facilidad de Gestión:

- La arquitectura basada en software permite añadir nuevos usuarios, áreas o servicios sin necesidad de hardware adicional, solo ampliando recursos del servidor.

Ejemplo de Expansión: Si la clínica desea incluir extensiones para un nuevo departamento, se pueden añadir fácilmente con configuraciones en el software.

Issabel

Es una distribución completa basada en Linux que incluye Asterisk en su interior, puede funcionar junto con Issabel, una plataforma de software que proporciona una interfaz gráfica para administrar y configurar la centralita telefónica. Issabel permitirá gestionar a la clínica extensiones, colas de llamadas, buzones de voz, horarios de atención, video llamadas y grabaciones de llamadas, todo sin necesidad de manipular directamente la configuración compleja de Asterisk. De esta forma, el servidor se convierte en una solución completa de telefonía IP, facilitando la comunicación interna y externa dentro de la organización, mejorando la eficiencia y la administración de los servicios de voz. se explica cada función:

- **Extensiones:** Números internos asignados a teléfonos o usuarios dentro de la centralita, que permiten la comunicación directa entre diferentes dispositivos de la red sin usar la línea externa. Cada extensión funciona como un identificador único dentro del sistema de telefonía IP.
- **Colas de llamadas:** Sistemas que gestionan múltiples llamadas entrantes, organizándolas en un orden de atención y distribuyéndolas automáticamente a los agentes disponibles según reglas

predefinidas, garantizando un manejo eficiente del tráfico de llamadas.

- **Buzones de voz:** Espacios donde se almacenan los mensajes de voz de las llamadas no atendidas, permitiendo que los usuarios puedan escuchar los mensajes posteriormente desde sus teléfonos o mediante correo electrónico.
- **Grabaciones de llamadas:** Función que permite registrar las conversaciones telefónicas para fines de control, capacitación o respaldo, garantizando trazabilidad y calidad en la atención.
- **Videollamadas:** Función que permite la comunicación en tiempo real mediante audio y video entre usuarios dentro de la red, mejorando la interacción y la colaboración al combinar voz e imagen en la misma sesión.

III.1.2.2.-Diseño modelos de direccionamiento y host-name

III.1.2.2.1.- Dispositivos con necesidad de dirección IP

Para definir este punto lo que se necesita conocer es principalmente cuantos hosts y/o equipos necesitan direccionamiento IP en la red.

Los equipos que necesitan dirección IP son:

- Computadoras
- Laptops
- Impresoras
- Access Points
- Dispositivos Móviles

III.1.2.2.2.- VLSM

El VLSM (Máscara de Subred de Longitud Variable) es una técnica de direccionamiento IP que permite dividir una red en subredes de distintos tamaños, asignando a cada una máscara de subred específica según la cantidad de hosts que necesite.

Esto optimiza el uso de direcciones IP, evitando desperdicio y permitiendo una planificación más eficiente de la red.

Una vez definido los equipos que utilizaran IP en la red se procede a ejecutar VLSM que satisfagan lo que requiere la clínica, como la clínica requiere un control determinado dependiendo de cada área de trabajo, necesitan un total de 14 subredes a partir de la red 192.168.2.0.

Área de Internación – VLAN 10

Se ha asignado una subred exclusiva para el área de Internación, la cual pertenece a la VLAN 10. Aunque actualmente se requieren solo 22 equipos, se ha considerado un posible crecimiento, por lo que se aplicó VLSM para asignar una subred que permita al menos 30 hosts.

Parámetro	Valor
Fórmula para hosts	$2^n - 2 \geq$ Hosts
Cálculo para 30 hosts	$2^5 - 2 = 30 \rightarrow$ **n = 5**
Nueva máscara de red	**/27** → 11111111.11111111.11111111.11100000
Nueva máscara en decimal	**255.255.255.224**
Salto de red	256 - 224 = **32**

Tabla 25. Área de Internación – VLAN 10

Área de Pacientes – VLAN 20

Se ha asignado una subred exclusiva para el área de Pacientes, la cual pertenece a la VLAN 20. La capacidad de pacientes que ingresan a la clínica es aproximadamente 30 por día, en este caso se asignará 8 host lo cual uno pertenecerá al Access Point ya que con esa IP podrá crearse otra subred con la IP: 10.0.0.0/24

Parámetro	Valor
Fórmula para hosts	$2^n - 2 \geq$ Hosts
Cálculo para 8 hosts	$2^4 - 2 = 14 \rightarrow$ **n = 4**
Nueva máscara de red	**/28** → 11111111.11111111.11111111.11110000
Nueva máscara en decimal	**255.255.255.240**
Salto de red	256 - 240 = **16**

Tabla 26. Área de Pacientes – VLAN 20

Área del Personal de Salud – VLAN 30

Se ha asignado una subred exclusiva para el área de Personal de Salud, la cual pertenece a la VLAN 30. La capacidad del Personal varia lo cual se puede sacar una aproximación de 30 por día, en este caso se asignará 8 host lo cual uno pertenecerá al AccessPoint ya que con esa IP podrá crearse otra subred con la IP: 10.0.0.0/24

Parámetro	Valor
Fórmula para calcular hosts	$2^n - 2 \geq$ Hosts
Cálculo para 8 hosts	$2^4 - 2 =$ **14** $\rightarrow$ **n = 4**
Nueva máscara de red	**/28** → 11111111.11111111.11111111.11110000
Máscara de subred en decimal	**255.255.255.240**
Salto de red	256 - 240 = **16**

Tabla 27. Área del Personal de Salud – VLAN 30

Área de Consultorio – VLAN 40

Se ha asignado una subred exclusiva para el área de Consultoría, la cual pertenece a la VLAN 40. Actualmente se requieren solo 10 equipos, se ha considerado un posible crecimiento, por lo que se aplicó

VLSM para asignar una subred que permita al menos 14 hosts.

Parámetro	Valor
Fórmula para calcular hosts	$2^n - 2 \geq$ Hosts
Cálculo para 14 hosts	$2^4 - 2 =$ **14 → n = 4**
Nueva máscara de red	**/28** → 11111111.11111111.11111111.11110000
Máscara de subred en decimal	**255.255.255.240**
Salto de red	256 - 240 = **16**

Tabla 28. Área de Consultorio – VLAN 40

Área Tercerizada – VLAN 50

Se ha asignado una subred exclusiva para el Área Tercerizada, la cual pertenece a la VLAN 50. Aunque actualmente se requieren solo 6 equipos, se ha considerado un posible crecimiento, por lo que se aplicó VLSM para asignar una subred que permita al menos 10 hosts.

Parámetro	Valor
Fórmula para calcular hosts	$2^n - 2 \geq$ Hosts
Cálculo para 10 hosts	$2^4 - 2 =$ **14 → n = 4**
Máscara de red	**/28** = 11111111.11111111.11111111.11110000
Máscara en decimal	**255.255.255.240**
Salto de red	256 - 240 = **16**

Tabla 29. Área Tercerizada – VLAN 50

Área de Administración – VLAN 60

Se ha asignado una subred exclusiva para el área de Administración, la cual pertenece a la VLAN 60. Aunque actualmente se requieren solo 3 equipos, se ha considerado un posible crecimiento, por lo que se aplicó VLSM para asignar una subred que permita al menos 6 hosts.

Parámetro	Valor
Fórmula para calcular hosts	$2^n - 2 \geq$ Hosts
Cálculo para 6 hosts	$2^3 - 2 =$ **6 → n = 3**
Máscara de red	**/29** = 11111111.11111111.11111111.11111000
Máscara en decimal	**255.255.255.248**
Salto de red	256 - 248 = **8**

Tabla 30. Área de Administración – VLAN 60

Área de Recepción – VLAN 70

Se ha asignado una subred exclusiva para el área de Recepción, la cual pertenece a la VLAN 70. Aunque actualmente se requieren solo 1 equipo, se ha considerado un posible crecimiento, por lo que se aplicó VLSM para asignar una subred que permita al menos 3 hosts.

Parámetro	Valor
Fórmula para calcular hosts	$2^n - 2 \geq$ Hosts
Cálculo para 3 hosts	$2^3 - 2 =$ **6 → n = 3**
Máscara de red	**/29** = 11111111.11111111.11111111.11111000
Máscara en decimal	**255.255.255.248**
Salto de red	256 - 248 = **8**

Tabla 31. Área de Recepción – VLAN 70

Área de Emergencias – VLAN 80

Se ha asignado una subred exclusiva para el área de Emergencias, la cual pertenece a la VLAN 80. Aunque actualmente se requieren solo 1 equipo, se ha considerado un posible crecimiento, por lo que se aplicó VLSM para asignar una subred que permita al menos 4 hosts.

Parámetro	Valor
Fórmula para calcular hosts	$2^n - 2 \geq$ Hosts
Cálculo para 4 hosts	$2^3 - 2 =$ **6 → n = 3**
Máscara de red	**/29** = 11111111.11111111.11111111.11111000
Máscara en decimal	**255.255.255.248**
Salto de red	256 - 248 = **8**

Tabla 32. Área de Emergencias – VLAN 80

Área de Enfermería – VLAN 90

Se ha asignado una subred exclusiva para el área de Enfermería, la cual pertenece a la VLAN 90. Aunque actualmente se requieren solo 4 equipos, se ha considerado un posible crecimiento, por lo que se aplicó VLSM para asignar una subred que permita al menos 6 hosts.

Parámetro	Valor
Fórmula para calcular hosts	$2^n - 2 \geq$ Hosts
Cálculo para 6 hosts	$2^3 - 2 =$ **6 → n = 3**
Máscara de red	**/29** = 11111111.11111111.11111111.11111000
Máscara en decimal	**255.255.255.248**
Salto de red	256 - 248 = **8**

Tabla 33. Área de Enfermería – VLAN 90

Área de Terapia Intensiva – VLAN 100

Se ha asignado una subred exclusiva para el área de Terapia Intensiva, la cual pertenece a la VLAN 100. Aunque actualmente se requieren solo 4 equipos, se ha considerado un posible crecimiento, por lo que se aplicó VLSM para asignar una subred que permita al menos 6 hosts.

Parámetro	Valor
Fórmula para calcular hosts	$2^n - 2 \geq$ Hosts
Cálculo para 6 hosts	$2^3 - 2 =$ **6 → n = 3**

Máscara de red	**/29** = 11111111.11111111.11111111.11111000
Máscara en decimal	**255.255.255.248**
Salto de red	256 - 248 = **8**

Tabla 34. Área de Terapia Intensiva – VLAN 100

Área de Pediatría – VLAN 110

Se ha asignado una subred exclusiva para el área de Pediatría, la cual pertenece a la VLAN 110. Aunque actualmente se requieren solo 4 equipos, se ha considerado un posible crecimiento, por lo que se aplicó VLSM para asignar una subred que permita al menos 6 hosts.

Parámetro	Valor
Fórmula para calcular hosts	$2^n - 2 \geq$ Hosts
Cálculo para 6 hosts	$2^3 - 2 =$ **6 → n = 3**
Máscara de red	**/29** = 11111111.11111111.11111111.11111000
Máscara en decimal	**255.255.255.248**
Salto de red	256 - 248 = **8**

Tabla 35. Área de Pediatría – VLAN 110

Área de Farmacia – VLAN 120

Se ha asignado una subred exclusiva para el área de Farmacia, la cual pertenece a la VLAN 120. Aunque actualmente se requieren solo 2 equipos, se ha considerado un posible crecimiento, por lo que se aplicó VLSM para asignar una subred que permita al menos 5 hosts.

Parámetro	Valor
Fórmula para calcular hosts	$2^n - 2 \geq$ Hosts
Cálculo para 5 hosts	$2^3 - 2 =$ **6 → n = 3**
Máscara de red	**/29** = 11111111.11111111.11111111.11111000
Máscara en decimal	**255.255.255.248**
Salto de red	256 - 248 = **8**

Tabla 36. Área de Farmacia – VLAN 120

Área de Esterilización – VLAN 130

Se ha asignado una subred exclusiva para el área de Esterilización, la cual pertenece a la VLAN 130. Aunque actualmente se requieren solo 4 equipos, se ha considerado un posible crecimiento, por lo que se aplicó VLSM para asignar una subred que permita al menos 6 hosts.

Parámetro	Valor
Fórmula para calcular hosts	$2^n - 2 \geq$ Hosts
Cálculo para 6 hosts	$2^3 - 2 =$ **6 → n = 3**

Máscara de red	**/29** = 11111111.11111111.11111111.11111000
Máscara en decimal	**255.255.255.248**
Salto de red	256 - 248 = **8**

Tabla 37. Área de Esterilización – VLAN 130

Área de Contabilidad – VLAN 140

Se ha asignado una subred exclusiva para el área de Contabilidad, la cual pertenece a la VLAN 140. Aunque actualmente se requieren solo 3 equipos, se ha considerado un posible crecimiento, por lo que se aplicó VLSM para asignar una subred que permita al menos 4 hosts.

Parámetro	Valor
Fórmula para calcular hosts	$2^n - 2 \geq$ Hosts
Cálculo para 4 hosts	$2^3 - 2 =$ **6** → **n = 3**
Máscara de red	**/29** = 11111111.11111111.11111111.11111000
Máscara en decimal	**255.255.255.248**
Salto de red	256 - 248 = **8**

Tabla 38. Área de Contabilidad – VLAN 140

Nombre de Subred	Dirección	Mascara de la Subred	Primera IP Utilizable	Ultima IP Utilizable	Broadcast
Internación	192.168.2.0	255.255.255.224	192.168.2.1	192.168.2.30	192.168.2.31
Pacientes	192.168.2.32	255.255.255.240	192.168.2.33	192.168.2.46	192.168.2.47
Personal de Salud	192.168.2.48	255.255.255.240	192.168.2.49	192.168.2.62	192.168.2.63
Consultoría	192.168.2.64	255.255.255.240	192.168.2.65	192.168.2.78	192.168.2.79
Área Tercerizada	192.168.2.80	255.255.255.240	192.168.2.81	192.168.2.94	192.168.2.95
Administración	192.168.2.96	255.255.255.248	192.168.2.97	192.168.2.102	192.168.2.103
Recepción	192.168.2.104	255.255.255.248	192.168.2.105	192.168.2.110	192.168.2.111
Emergencias	192.168.2.112	255.255.255.248	192.168.2.113	192.168.2.118	192.168.2.119
Enfermería	192.168.2.120	255.255.255.248	192.168.2.121	192.168.2.126	192.168.2.127
Terapia Intensiva	192.168.2.128	255.255.255.248	192.168.2.129	192.168.2.134	192.168.2.135
Pediatría	192.168.2.136	255.255.255.248	192.168.2.137	192.168.2.142	192.168.2.143
Farmacia	192.168.2.144	255.255.255.248	192.168.2.145	192.168.2.150	192.168.2.151
Esterilización	192.168.2.152	255.255.255.248	192.168.2.153	192.168.2.158	192.168.2.159

Contabilidad	192.168.2.160	255.255.255.248	192.168.2.161	192.168.2.166	192.168.2.167

Tabla 39. Tabla de Direccionamiento VLSM

Area de Servidores – VLAN 150

En esta área se implementará una subred independiente con el direccionamiento 192.168.3.0/24, distinta de la red de usuarios (192.168.2.0/24). Esta separación tiene como objetivo reforzar la seguridad, evitando que los equipos de usuarios tengan acceso directo a los servidores de manera no controlada.

Nombre del Servidor	Dirección	Mascara de la Subred	Vlan	Broatcast
Asterisk	192.168.3.100	255.255.255.0	150	192.168.3.255
Sistema Central	192.168.3.101	255.255.255.0	150	192.168.3.255

Tabla 40. Tabla de Servidores

III.1.2.2.3.- Equipos Inalámbricos

Tomando en cuenta lo que comprende a los equipos inalámbricos se dispondrá de los siguientes segmentos de red:

	IP de red VLAN	Red LAN	Mascara
Pacientes PB	192.168.2.34	10.10.0.1/24	255.255.255.0
Pacientes P1	192.168.2.35	10.20.0.1/24	255.255.255.0
Pacientes P2	192.168.2.36	10.30.0.1/24	255.255.255.0
Pacientes P3	192.168.2.37	10.40.0.1/24	255.255.255.0
Persona Salud PB	192.168.2.50	20.10.0.1/24	255.255.255.0
Persona Salud P1	192.168.2.51	20.20.0.1/24	255.255.255.0
Persona Salud P2	192.168.2.52	20.30.0.1/24	255.255.255.0
Persona Salud P3	192.168.2.53	20.40.0.1/24	255.255.255.0

Tabla 41. Equipos Inalámbricos

- ✓ La primera columna indica la IP asignada a la interfaz de la VLAN.
- ✓ La segunda columna corresponde a la red LAN que se usará para los dispositivos conectados en cada segmento (pacientes o personal de salud, según el piso).
- ✓ La tercera columna presenta la máscara de subred que define el rango disponible de direcciones IP para cada grupo.

En el caso de los dispositivos inalámbricos se tomará en cuenta la ubicación de los equipos en un área

donde pueda cubrir en su totalidad el radio de alcance del área de trabajo.

III.1.2.2.4.-Host-name

Con respecto al host-name esta será una característica que nos permitirá identificar los equipos conectados a la red se tomará en cuenta a que piso pertenece y a que segmento de red este asignado.

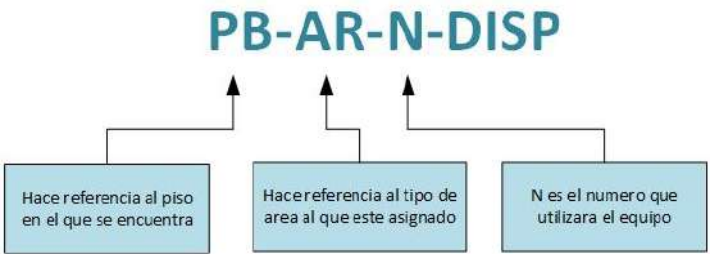

Figura 55. Nombre de host

Con respecto a la identificación de los equipos al que se refiere que está conectado estos tomando en cuenta si se trata de una PC de escritorio **(PC),** laptop **(LP),** Impresora **(PRINT),** Access Point **(AP),** Servidor **(SERV).**

III.1.2.2.5.- Diseño del Direccionamiento

Planificación de las IP para la VLAN10 Internación

NOMBRES	DIRECCIONES
SERVIDOR DHCP	192.168.2.0
MASCARA DE RED	255.255.255.224
AMBITO DE DHCP	192.168.2.1-192.168.2.30
PUERTA DE ENLACE	192.168.2.1
DNS	192.168.3.100
IP INTERFACE DHCP	192.168.2.30

Tabla 42. Direccionamiento VLAN10

Planificación de las IP para la VLAN20 Pacientes

NOMBRES	DIRECCIONES
SERVIDOR DHCP	192.168.2.32
MASCARA DE RED	255.255.255.240
AMBITO DE DHCP	192.168.2.33-192.168.2.46
PUERTA DE ENLACE	192.168.2.33
DNS	8.8.8.8
IP INTERFACE DHCP	192.168.2.46

Tabla 43. Direccionamiento VLAN20

Planificación de las IP para la VLAN30 Personal de Salud

NOMBRES	DIRECCIONES
SERVIDOR DHCP	192.168.2.48
MASCARA DE RED	255.255.255.240
AMBITO DE DHCP	192.168.2.49-192.168.2.62

PUERTA DE ENLACE	192.168.2.49
DNS	192.168.3.100
IP INTERFACE DHCP	192.168.2.62

Tabla 44. Direccionamiento VLAN30

Planificación de las IP para la VLAN40 Consultorio

NOMBRES	DIRECCIONES
SERVIDOR DHCP	192.168.2.64
MASCARA DE RED	255.255.255.240
AMBITO DE DHCP	192.168.2.65-192.168.2.78
PUERTA DE ENLACE	192.168.2.65
DNS	192.168.3.100
IP INTERFACE DHCP	192.168.2.78

Tabla 45. Direccionamiento VLAN40

Planificación de las IP para la VLAN50 Área Tercerizada

NOMBRES	DIRECCIONES
SERVIDOR DHCP	192.168.2.80
MASCARA DE RED	255.255.255.240
AMBITO DE DHCP	192.168.2.81-192.168.2.94
PUERTA DE ENLACE	192.168.2.81
DNS	192.168.3.100
IP INTERFACE DHCP	192.168.2.94

Tabla 46. Direccionamiento VLAN50

Planificación de las IP para la VLAN60 Administración

NOMBRES	DIRECCIONES
SERVIDOR DHCP	192.168.2.96
MASCARA DE RED	255.255.255.248
AMBITO DE DHCP	192.168.2.97-192.168.2.102
PUERTA DE ENLACE	192.168.2.97
DNS	192.168.3.100
IP INTERFACE DHCP	192.168.2.102

Tabla 47. Direccionamiento VLAN60

Planificación de las IP para la VLAN70 Recepción

NOMBRES	DIRECCIONES
SERVIDOR DHCP	192.168.2.104
MASCARA DE RED	255.255.255.248
AMBITO DE DHCP	192.168.2.105-192.168.2.110
PUERTA DE ENLACE	192.168.2.105
DNS	192.168.3.100
IP INTERFACE DHCP	192.168.2.110

Tabla 48. Direccionamiento VLAN70

Planificación de las IP para la VLAN80 Emergencias

NOMBRES	DIRECCIONES
SERVIDOR DHCP	192.168.2.112
MASCARA DE RED	255.255.255.248
AMBITO DE DHCP	192.168.2.113-192.168.2.118
PUERTA DE ENLACE	192.168.2.113
DNS	192.168.3.100
IP INTERFACE DHCP	192.168.2.118

Tabla 49. Direccionamiento VLAN80

Planificación de las IP para la VLAN90 Enfermería

NOMBRES	DIRECCIONES
SERVIDOR DHCP	192.168.2.120
MASCARA DE RED	255.255.255.248
AMBITO DE DHCP	192.168.2.121-192.168.2.126
PUERTA DE ENLACE	192.168.2.121
DNS	192.168.3.100
IP INTERFACE DHCP	192.168.2.126

Tabla 50. Direccionamiento VLAN90

Planificación de las IP para la VLAN100 Terapia Intensiva

NOMBRES	DIRECCIONES
SERVIDOR DHCP	192.168.2.128
MASCARA DE RED	255.255.255.248
AMBITO DE DHCP	192.168.2.129-192.168.2.134
PUERTA DE ENLACE	192.168.2.129
DNS	192.168.3.100
IP INTERFACE DHCP	192.168.2.134

Tabla 51. Direccionamiento VLAN100

Planificación de las IP para la VLAN110 Pediatría

NOMBRES	DIRECCIONES
SERVIDOR DHCP	192.168.2.136
MASCARA DE RED	255.255.255.248
AMBITO DE DHCP	192.168.2.137-192.168.2.142
PUERTA DE ENLACE	192.168.2.137
DNS	192.168.3.100
IP INTERFACE DHCP	192.168.2.142

Tabla 52. Direccionamiento VLAN110

Planificación de las IP para la VLAN120 Farmacia

NOMBRES	DIRECCIONES
SERVIDOR DHCP	192.168.2.144
MASCARA DE RED	255.255.255.248
AMBITO DE DHCP	192.168.2.145-192.168.2.150

PUERTA DE ENLACE	192.168.2.145
DNS	192.168.3.100
IP INTERFACE DHCP	192.168.2.150

Tabla 53. Direccionamiento VLAN120

Planificación de las IP para la VLAN130 Esterilización

NOMBRES	DIRECCIONES
SERVIDOR DHCP	192.168.2.152
MASCARA DE RED	255.255.255.248
AMBITO DE DHCP	192.168.2.153-192.168.2.158
PUERTA DE ENLACE	192.168.2.153
DNS	192.168.3.100
IP INTERFACE DHCP	192.168.2.158

Tabla 54. Direccionamiento VLAN130

Planificación de las IP para la VLAN140 Contabilidad

NOMBRES	DIRECCIONES
SERVIDOR DHCP	192.168.2.160
MASCARA DE RED	255.255.255.248
AMBITO DE DHCP	192.168.2.161-192.168.2.166
PUERTA DE ENLACE	192.168.2.161
DNS	192.168.3.100
IP INTERFACE DHCP	192.168.2.166

Tabla 55. Direccionamiento VLAN140

Planificación de las IP Access Points Pacientes

NOMBRES	DIRECCIONES
SERVIDOR DHCP	10.10.0.0
MASCARA DE RED	255.255.255.0
AMBITO DE DHCP	10.10.0.1-10.0.0.50
PUERTA DE ENLACE	192.168.2.33
DNS	8.8.8.8

Tabla 56. Direccionamiento Interno Pacientes Planta Baja

NOMBRES	DIRECCIONES
SERVIDOR DHCP	10.20.0.0
MASCARA DE RED	255.255.255.0
AMBITO DE DHCP	10.20.0.1-10.20.0.50
PUERTA DE ENLACE	192.168.2.33
DNS	8.8.8.8

Tabla 57. Direccionamiento Interno Pacientes Primer piso

NOMBRES	DIRECCIONES
SERVIDOR DHCP	10.30.0.0
MASCARA DE RED	255.255.255.0
AMBITO DE DHCP	10.30.0.1-10.30.0.50

PUERTA DE ENLACE	192.168.2.33
DNS	8.8.8.8

Tabla 58. Direccionamiento Interno Pacientes Segundo piso

NOMBRES	DIRECCIONES
SERVIDOR DHCP	10.40.0.0
MASCARA DE RED	255.255.255.0
AMBITO DE DHCP	10.40.0.1-10.40.0.50
PUERTA DE ENLACE	192.168.2.33
DNS	8.8.8.8

Tabla 59. Direccionamiento Interno Pacientes Tercer piso

Planificación de las IP Access Points Personal de Salud

NOMBRES	DIRECCIONES
SERVIDOR DHCP	20.10.0.0
MASCARA DE RED	255.255.255.0
AMBITO DE DHCP	20.40.0.1-20.40.0.50
PUERTA DE ENLACE	192.168.2.49
DNS	192.168.3.100

Tabla 60. Direccionamiento Interno Personal Planta Baja

NOMBRES	DIRECCIONES
SERVIDOR DHCP	20.20.0.0
MASCARA DE RED	255.255.255.0
AMBITO DE DHCP	20.20.0.1-20.20.0.50
PUERTA DE ENLACE	192.168.2.49
DNS	192.168.3.100

Tabla 61. Direccionamiento Interno Personal Primer piso

NOMBRES	DIRECCIONES
SERVIDOR DHCP	20.30.0.0
MASCARA DE RED	255.255.255.0
AMBITO DE DHCP	20.30.0.1-20.30.0.50
PUERTA DE ENLACE	192.168.2.49
DNS	192.168.3.100

Tabla 62. Direccionamiento Interno Personal Segundo piso

NOMBRES	DIRECCIONES
SERVIDOR DHCP	20.40.0.0
MASCARA DE RED	255.255.255.0
AMBITO DE DHCP	20.40.0.1-20.40.0.50
PUERTA DE ENLACE	192.168.2.49
DNS	192.168.3.100

Tabla 63. Direccionamiento Interno Personal Tercer piso

III.1.2.2.6.- Tabla de Direccionamiento IP de Subinterfaz del Router, Servidor y Access Point

Equipo	Interfaz	Dirección IP	Mascara	Gateway
RouterClínica	Gi 0/3/0.10	192.168.2.1	255.255.255.224	No aplica
	Gi 0/3/0.20	192.168.2.33	255.255.255.240	No aplica
	Gi 0/3/0.30	192.168.2.49	255.255.255.240	No aplica
	Gi 0/3/0.40	192.168.2.65	255.255.255.240	No aplica
	Gi 0/3/0.50	192.168.2.81	255.255.255.240	No aplica
	Gi 0/3/0.60	192.168.2.97	255.255.255.248	No aplica
	Gi 0/3/0.70	192.168.2.105	255.255.255.248	No aplica
	Gi 0/3/0.80	192.168.2.113	255.255.255.248	No aplica
	Gi 0/3/0.90	192.168.2.121	255.255.255.248	No aplica
	Gi 0/3/0.100	192.168.2.129	255.255.255.248	No aplica
	Gi 0/3/0.110	192.168.2.137	255.255.255.248	No aplica
	Gi 0/3/0.120	192.168.2.145	255.255.255.248	No aplica
	Gi 0/3/0.130	192.168.2.153	255.255.255.248	No aplica
	Gi 0/3/0.140	192.168.2.161	255.255.255.248	No aplica
	Gi 0/3/0.150	192.168.3.1	255.255.255.0	No aplica
Servidor Asterisk	Fa 0	192.168.3.100	255.255.255.0	192.168.3.1
Servidor Central del Sistema Clínico	Fa 0	192.168.3.101	255.255.255.0	192.168.3.1

Tabla 64. Tabla de Direccionamiento IP de Subinterfaz del Router y Servidor

Equipo	Interfaz	WAN (DHCP)	LAN	Mascara
PB-PAC-1-AP	Internet	192.168.2.33-192.168.2.46	10.10.0.1	255.255.255.0
P1-PAC-2-AP	Internet		10.20.0.1	
P2-PAC-3-AP	Internet		10.30.0.1	
P3-PAC-4-AP	Internet		10.40.0.1	
PB-PER-1-AP	Internet	192.168.2.49-192.168.2.62	20.10.0.1	
P1-PER-2-AP	Internet		20.20.0.1	
P2-PER-3-AP	Internet		20.30.0.1	
P3-PER-4-AP	Internet		20.40.0.1	

Tabla 65. Tabla de Direccionamiento IP Access Point

III.1.2.2.7.- Segmentación IPV4 con VLAN de direccionamiento dinámico

Se aborda la asignación de direcciones IP a dispositivos dentro de cada subred, considerando la dirección IPv4 y la implementación de DHCP.

Nombre	Equipos	Rango de IP (DHCP)	Mascara de Subred	Puerta de enlace
VLAN10 Internación 22 hosts	P1-IT-1-PC	192.168.2.1-192.168.2.30	255.255.255.224	192.168.2.1
	P1-IT-2-PC			
	P1-IT-3-PC			
	P1-IT-4-PC			
	P1-IT-5-PC			

	P1-IT-6-PC			
	P1-IT-7-PC			
	P1-IT-8-PRINT			
	P2-IT-9-PC			
	P2-IT-10-PC			
	P2-IT-11-PC			
	P2-IT-12-PC			
	P2-IT-13-PC			
	P2-IT-14-PC			
	P2-IT-15-PC			
	P2-IT-16-PRINT			
	P3-IT-17-PC			
	P3-IT-18-PC			
	P3-IT-19-PC			
	P3-IT-20-PC			
	P3-IT-21-PC			
	P3-IT-22-PRINT			
VLAN 20 Pacientes 4 hosts	PB-PAC-1-AP	192.168.2.33- 192.168.2.46	255.255.255.240	192.168.2.33
	P1-PAC-2-AP			
	P2-PAC-3-AP			
	P3-PAC-4-AP			
VLAN 30 Personal de Salud 4 hosts	PB-PER-1-AP	192.168.2.49- 192.168.2.62	255.255.255.240	192.168.2.49
	P1-PER-2-AP			
	P2-PER-3-AP			
	P3-PER-4-AP			
VLAN 40 Consultorio 10 hosts	PB-CONS-1-LP	192.168.2.65- 192.168.2.78	255.255.255.240	192.168.2.65
	PB-CONS-2-LP			
	PB-CONS-3-LP			
	PB-CONS-4-LP			
	PB-CONS-5-LP			
	PB-CONS-6-PRINT			
	PB-CONS-7-PRINT			
	PB-CONS-8-PRINT			
	PB-CONS-9-PRINT			
	PB-CONS-10-PRINT			
VLAN 50 Área Tercerizada 6 hosts	PB-AT-1-PC	192.168.2.81- 192.168.2.94	255.255.255.240	192.168.2.81
	PB-AT-2-PC			
	PB-AT-3-PC			
	PB-AT-4-PC			
	PB-AT-5-			

	PRINT			
	PB-AT-6-PC			
VLAN 60 Administración 3 hosts	PB-ADM-1-PC	192.168.2.97- 192.168.2.102	255.255.255.248	192.168.2.97
	PB-ADM-2-PC			
	PB-ADM-3-PRINT			
VLAN 70 Recepción 1 host	PB-REC-1-PC	192.168.2.105- 192.168.2.110	255.255.255.248	192.168.2.105
VLAN 80 Emergencias 1 host	PB-EMG-1-LP	192.168.2.113- 192.168.2.118	255.255.255.248	192.168.2.113
VLAN 90 Enfermería 4 hosts	P1-ENF-1-PC	192.168.2.121- 192.168.2.126	255.255.255.248	192.168.2.121
	P1-ENF-2-PC			
	P2-ENF-3-PC			
	P3-ENF-4-PC			
VLAN 100 Terapia Intensiva 4 hosts	P1-TRI-1-PC	192.168.2.129- 192.168.2.134	255.255.255.248	192.168.2.129
	P1-TRI-2-PRINT			
	P2-TRI-3-LP			
	P3-TRI-4-PC			
VLAN 110 Pediatría 4 hosts	P3-PED-1-LP	192.168.2.137- 192.168.2.142	255.255.255.248	192.168.2.137
	P3-PED-2-LP			
	P3-PED-3-LP			
	P3-PED-4-PRINT			
VLAN 120 Farmacia 2 hosts	P3-FAR-1-PC	192.168.2.145- 192.168.2.150	255.255.255.248	192.168.2.145
	P3-FAR-2-PRINT			
VLAN 130 Esterilización 4 hosts	P3-EST-1-PC	192.168.2.153- 192.168.2.158	255.255.255.248	192.168.2.153
	P3-EST-2-PC			
	P3-EST-3-PC			
	P3-EST-4-PRINT			
VLAN 140	P3-CON-1-PC	192.168.2.161- 192.168.2.166	255.255.255.248	192.168.2.161
	P3-CON-2-PC			
	P3-CON-3-PRINT			
VLAN 150	PB-SERV-1-SERVA	192.168.3.100, 192.168.3.101	255.255.255.0	192.168.3.1
	PB-SERV-2-SERVC			

Tabla 66. Segmentación IPV4 con VLAN de direccionamiento dinámico

III.1.2.2.8.- Direccionamiento de la VLAN a puertos del switch

Rack	Switch	VLAN	Puertos	N.º de componentes
Rack_de_Suelo	Switch PB	VLAN60	Fa 0/1-3	2PC
		VLAN40	Fa 0/4-8	5LP
		VLAN50	Fa 0/9-12	4PC
		VLAN80	Fa 0/13	1PC
		VLAN70	Fa 0/14	1PC
		VLAN30	Fa 0/22	1AP
		VLAN20	Fa 0/23	1AP
		TRUNK	Fa 0/24	---
	Switch Fibra PB	VLAN50	Fa 2/1	1PRINT
		VLAN40	Fa 3/1, Fa 5-8/1	5PRINT
		VLAN60	Fa 9/1	1PRINT
		TRUNK	Fa 0/1, Gi 4/1	---
	Switch Principal	VLAN150	Fa 0/1	2SERV
			Fa 1/1	
		TRUNK	Gi 4-9/1	---
Rack Gabinete-1	Switch P1	VLAN10	Fa 0/1-7	7PC
		VLAN90	Fa 0/8-9	2PC
		VLAN100	Fa 0/10	1PC
		VLAN20	Fa 0/11	1AP
		VLAN30	Fa 0/12	1AP
		TRUNK	Fa 0/24	---
	Switch Fibra P1	VLAN10	Fa 8/1	1PRINT
		VLAN100	Fa 9/1	1PRINT
		TRUNK	Fa 0/1, Gi 6/1	---
Rack Gabinete-2	Switch P2	VLAN10	Fa 0/1-7	7PC
		VLAN100	Fa 0/8	1PC
		VLAN90	Fa 0/9	1PC
		VLAN30	Fa 0/22	1AP
		VLAN20	Fa 0/23	1AP
		TRUNK	Fa 0/24	---
	Switch Fibra P2	VLAN10	Fa 9/1	1PRINT
Rack Gabinete-3	Switch P3	VLAN50	Fa 0/1	1PC
		VLAN110	Fa 0/2-5	3LP,1PRINT
		VLAN10	Fa 0/6-10	5PC
		VLAN100	Fa 0/11	1PC
		VLAN90	Fa 0/12	1PC
		VLAN120	Fa 0/13	1PC
		VLAN130	Fa 0/14-16	3PC
		VLAN140	Fa 0/17-18	2PC
		VLAN30	Fa 0/22	1AP
		VLAN20	Fa 0/23	1AP

		TRUNK	Fa 0/24	---
	Switch Fibra P3	VLAN10	Fa 6/1	1PRINT
		VLAN130	Fa 7/1	1PRINT
		VLAN120	Fa 8/1	1PRINT
		VLAN140	Fa 9/1	1PRINT

Tabla 67. Direccionamiento de la VLAN a puertos del switch

III.1.2.2.9.- Direccionamiento de componente a puertos del switch

RACK DE SUELO							
	CONECTOR DE PARED			PATCH PANEL			
COMPONENTE	JACK	ROSETA	PUNCHDOWN	PUNCHDOWN	JACK	SWITCH	VLAN
PB-ADM-1-PC	J2	R-3	PD2	PD2	J2	Fa 0/2	60
PB-ADM-2-PC	J3	R-3	PD3	PD3	J3	Fa 0/3	60
PB-CONS-5-LP	J1	R-8	PD1	PD4	J4	Fa 0/4	40
PB-CONS-4-LP	J1	R-7	PD1	PD5	J5	Fa 0/5	40
PB-CONS-3-LP	J1	R-6	PD1	PD6	J6	Fa 0/6	40
PB-CONS-2-LP	J1	R-5	PD1	PD7	J7	Fa 0/7	40
PB-CONS-1-LP	J1	R-4	PD1	PD8	J8	Fa 0/8	40
PB-AT-4-PC	J1	R-2	PD1	PD9	J9	Fa 0/9	50
PB-AT-3-PC	J2	R-1	PD2	PD10	J10	Fa 0/10	50
PB-AT-2-PC	J1	R-1	PD1	PD11	J11	Fa 0/11	50
PB-AT-1-PC	J1	R-9	PD1	PD12	J12	Fa 0/12	50
PB-EMG-1-LP	J2	R-9	PD2	PD13	J13	Fa 0/13	80
PB-REC-1-PC	J2	R-4	PD2	PD14	J14	Fa 0/14	70
PB-ADM-3-PRINT	J1	R-3	PD1	PD15	J15	Fa 9/1	60
PB-CONS-6-PRINT	J3	R-4	PD3	PD16	J16	Fa 8/1	40
PB-CONS-7-PRINT	J2	R-5	PD2	PD17	J17	Fa 7/1	40
PB-CONS-8-PRINT	J2	R-6	PD2	PD18	J18	Fa 6/1	40
PB-CONS-9-PRINT	J2	R-7	PD2	PD19	J19	Fa 5/1	40
PB-CONS-10-PRINT	J3	R-8	PD3	PD20	J20	Fa 3/1	40
PB-AT-5-PRINT	J3	R-1	PD3	PD21	J21	Fa 2/1	50
PB-PER-1-AP	J2	R-8	PD2	PD23	J23	Fa 0/22	30
PB-PAC-1-AP	J4	R-3	PD4	PD24	J24	Fa 0/23	20

Tabla 68. Direccionamiento de componente a puertos del switch Rack de Suelo

RACK GABINETE-1							
	CONECTOR DE PARED			PATCH PANEL			
COMPONENTE	JACK	ROSETA	PUNCHDOWN	PUNCHDOWN	JACK	SWITCH	VLAN
P1-IT-7-PC	J2	R-15	PD2	PD1	J1	Fa 0/1	10
P1-IT-6-PC	J1	R-13	PD1	PD2	J2	Fa 0/2	10
P1-IT-5-PC	J1	R-15	PD1	PD3	J3	Fa 0/3	10
P1-IT-4-PC	J2	R-11	PD2	PD4	J4	Fa 0/4	10
P1-IT-3-PC	J2	R-12	PD2	PD5	J5	Fa 0/5	10
P1-IT-2-PC	J1	R-11	PD1	PD6	J6	Fa 0/6	10
P1-IT-1-PC	J1	R-12	PD1	PD7	J7	Fa 0/7	10

P1-ENF-2-PC	J3	R-14	PD3	PD8	J8	Fa 0/8	90
P1-ENF-1-PC	J1	R-14	PD1	PD9	J9	Fa 0/9	90
P1-TRI-1-PC	J1	R-10	PD1	PD10	J10	Fa 0/10	100
P1-TRI-2-PRINT	J2	R-10	PD2	PD11	J11	Fa 9/1	100
P1-IT-8-PRINT	J4	R-14	PD4	PD12	J12	Fa 8/1	10
P1-PER-2-AP	J2	R14	PD2	PD23	J23	Fa 0/21	30
P1-PAC-2-AP	J2	R13	PD2	PD24	J24	Fa 0/23	20

Tabla 69. Direccionamiento de componente a puertos del switch Rack Gabinete

RACK GABINETE-2							
	CONECTOR DE PARED			**PATCH PANEL**			
COMPONENTE	JACK	ROSETA	PUNCHDOWN	PUNCHDOWN	JACK	SWITCH	VLAN
P2-IT-9-PC	J1	R-21	PD1	PD1	J1	Fa 0/1	10
P2-IT-10-PC	J1	R-20	PD1	PD2	J2	Fa 0/2	10
P2-IT-11-PC	J2	R-21	PD2	PD3	J3	Fa 0/3	10
P2-IT-12-PC	J2	R-20	PD2	PD4	J4	Fa 0/4	10
P2-IT-13-PC	J1	R-17	PD1	PD5	J5	Fa 0/5	10
P2-IT-14-PC	J1	R-18	PD1	PD6	J6	Fa 0/6	10
P2-IT-15-PC	J2	R-17	PD2	PD7	J7	Fa 0/7	10
P2-TRI-3-LP	J1	R-16	PD1	PD8	J8	Fa 0/8	100
P2-ENF-3-PC	J1	R-19	PD1	PD9	J9	Fa 0/9	90
P2-IT-16-PRINT	J3	R-19	PD3	PD10	J10	Fa 9/1	10
P2-PER-3-AP	J2	R-19	PD2	PD23	J23	Fa 0/22	30
P2-PAC-3-AP	J2	R-18	PD2	PD24	J24	Fa 0/23	20

Tabla 70. Direccionamiento de componente a puertos del switch Rack Gabinete-2

RACK GABINETE-3							
	CONECTOR DE PARED			**PATCH PANEL**			
COMPONENTE	JACK	ROSETA	PUNCHDOWN	PUNCHDOWN	JACK	SWITCH	VLAN
P3-AT-6-PC	J1	R-22	PD1	PD1	J1	Fa 0/1	50
P3-PED-1-PC	J1	R-23	PD1	PD2	J2	Fa 0/2	110
P3-PED-2-PC	J2	R-22	PD2	PD3	J3	Fa 0/3	110
P3-PED-3-PC	J3	R-22	PD3	PD4	J4	Fa 0/4	110
P3-PED-4-PRINT	J2	R-23	PD2	PD5	J5	Fa 0/5	110
P3-IT-17-PC	J1	R-24	PD1	PD6	J6	Fa 0/6	10
P3-IT-18-PC	J1	R-25	PD1	PD7	J7	Fa 0/7	10
P3-IT-19-PC	J2	R-24	PD2	PD8	J8	Fa 0/8	10
P3-IT-20-PC	J2	R-25	PD2	PD9	J9	Fa 0/9	10
P3-IT-21-PC	J1	R-26	PD1	PD10	J10	Fa 0/10	10
P3-TRI-4-PC	J1	R-27	PD1	PD11	J11	Fa 0/11	100
P3-ENF-4-PC	J3	R-25	PD3	PD12	J12	Fa 0/12	90
P3-FAR-1-PC	J1	R-30	PD1	PD13	J13	Fa 0/13	120
P3-EST-1-PC	J2	R-30	PD2	PD14	J14	Fa 0/14	130
P3-EST-2-PC	J1	R-29	PD1	PD15	J15	Fa 0/15	130
P3-EST-3-PC	J2	R-29	PD2	PD16	J16	Fa 0/16	130

P3-CON-1-PC	J1	R-28	PD1	PD17	J17	Fa 0/17	140
P3-CON-2-PC	J2	R-28	PD2	PD18	J18	Fa 0/18	140
P3-CON-3-PRINT	J3	R-28	PD3	PD19	J19	Fa 9/1	140
P3-FAR-2-PRINT	J3	R-30	PD3	PD20	J20	Fa 8/1	120
P3-EST-4-PRINT	J3	R-29	PD3	PD21	J21	Fa 7/1	130
P3-IT-22-PRINT	J3	R-25	PD3	PD22	J22	Fa 6/1	10
P3-PER-4-AP	J2	R-26	PD2	PD23	J23	Fa 0/22	30
P3-PAC-4-AP	J3	R-24	PD3	PD24	J24	Fa 0/23	20

Tabla 71. Direccionamiento de componente a puertos del switch Rack Gabinete-3

III.1.2.3.- Seleccionar protocolos para Switching y Routing

Por qué se eligieron ciertas VLAN.

Se decidió implementar VLANs con el protocolo IEEE 802.1Q para segmentar la red y optimizar el tráfico, especialmente en Administración, Contabilidad y Recepción, donde se detecta mayor congestión en horas pico (10:00–12:00 y 15:00–18:00).

Por qué se eligieron ciertos equipos

Se seleccionaron switches con soporte para VLAN y enlaces troncales porque permiten segmentar la red y mejorar el rendimiento entre las diferentes áreas de la clínica. Se eligió un switch principal que cumple la función de servidor DHCP y varios que ayuden a interconectar la red para asignar direcciones IP automáticamente a cada VLAN y facilitar la administración. También se implementó un firewall perimetral para proteger la red y controlar los diferentes accesos. Además, los puntos de acceso inalámbricos fueron elegidos porque permiten separar la red WiFi del personal y la del personal, evitando congestión e inseguridad. Finalmente, se utilizó fibra óptica para la conexión entre pisos debido a su alta velocidad y estabilidad.

Cómo cada problema inicial será resuelto

La creación de VLANs reduce la congestión separando el tráfico por áreas, evitando que una afecte el rendimiento de las demás. El switch principal con DHCP organiza la asignación de IP y evita conflictos. Los enlaces de fibra óptica entre pisos eliminan cuellos de botella y mejoran la velocidad. El firewall protege la red controlando accesos y filtrando el tráfico. Finalmente, los puntos de acceso WiFi permiten separar la red interna y la de visitantes, evitando saturación y aumentando la seguridad.

III.1.2.3.1.- Red de Área Local Virtual (VLAN)

Las VLAN (Redes de Área Local Virtual) permiten crear redes lógicas independientes dentro de la misma red física, segmentando el tráfico y facilitando su administración. Sus beneficios principales son:

- **Seguridad:** Permiten aislar redes, controlar el tráfico entre VLANs y decidir qué comunicación es posible, usando enrutamiento entre VLANs (inter-VLAN routing) cuando sea necesario.
- **Segmentación:** Cada subred se asigna a una VLAN diferente, como administración, personal o pacientes, permitiendo un uso independiente de las comunicaciones y un mejor control del

dominio de broadcast.

- **Flexibilidad:** Facilitan mover equipos entre subredes y definir políticas de acceso a otras VLANs o Internet, por ejemplo, restringiendo ciertos servicios a invitados.
- **Optimización de la red:** Al reducir los dominios de broadcast, se mejora el rendimiento, evitando congestión y sobrecarga, especialmente en redes con mucho tráfico.

Subinterfaces

Las subinterfaces son divisiones lógicas de una interfaz física que se utilizará en el router de la clínica y permitirá manejar múltiples VLANs a través de un solo enlace físico. Cada subinterface se asigna a una VLAN específica y recibe una dirección IP que actúa como puerta de enlace para esa VLAN.

En la red de la clínica:

- Se configurarán 15 subinterfaces en el router principal, una para cada VLAN utilizada en los diferentes pisos y áreas de la institución.
- Cada subinterface permitirá que el enrutamiento entre VLANs (inter-VLAN routing) se realice de manera ordenada y segura, asegurando que solo el tráfico permitido entre subredes se comunique.
- Gracias a estas subinterfaces, se podrá gestionar eficientemente el tráfico entre las distintas áreas de la clínica sin necesidad de múltiples interfaces físicas, optimizando recursos y manteniendo la segmentación y seguridad de la red.

Modo Truncamiento

El modo troncal permitirá que un switch transporte el tráfico de múltiples VLANs a través de un mismo enlace, identificando a qué VLAN pertenece cada trama mediante el protocolo IEEE 802.1Q.

En la red de la institución se implementará de la siguiente manera:

- Los 5 switches de fibra estarán configurados en modo troncal, lo que permitirá que el tráfico de todas las VLANs pueda circular entre ellos sin perder la segmentación de cada subred.
- El switch principal tendrá sus puertos de entrada y salida en modo trunk, de modo que reciba y envíe tráfico de todas las VLANs hacia los switches secundarios y hacia otros dispositivos de la red.
- Los switches secundarios también tendrán los enlaces hacia el switch principal en modo trunk, para garantizar que el tráfico de cada VLAN llegue correctamente y se mantenga la segmentación.

De esta forma, se está asegurando que todas las VLANs puedan comunicarse de manera ordenada entre switches, mientras que el tráfico queda segmentado y controlado según la configuración de cada VLAN.

Modo Acceso

El modo acceso se utiliza en los puertos de los switches para conectar dispositivos finales a una VLAN específica. A diferencia del modo troncal, un puerto en modo acceso solo pertenece a una VLAN, por lo que todo el tráfico que pase por él se considera de esa VLAN.

En la red de la clínica:

- Los puertos de los switches secundarios que conectan a PCs del personal, dispositivos de pacientes o impresoras estarán configurados en modo acceso, asignándolos a la VLAN correspondiente según su área.
- Esto garantiza que cada dispositivo se comunique solo dentro de su VLAN y que el tráfico entre VLANs pase únicamente por el router a través del inter-VLAN routing, asegurando seguridad y control del tráfico.
- El uso del modo acceso junto con el modo troncal en los enlaces entre switches permite mantener la segmentación de la red sin complicar el cableado físico.

III.1.2.3.2.- Protocolo de Enrutamiento Estático

El enrutamiento estático consiste en configurar rutas fijas manualmente en el router, indicando de forma precisa cómo enviar el tráfico hacia Internet. Esto asegura que los datos salgan por la puerta de enlace correcta, manteniendo la comunicación externa eficiente y segura. En la clínica, el enrutamiento estático permite controlar el acceso a Internet desde la red interna, evitando rutas incorrectas o pérdidas de tráfico y reduciendo la carga de procesamiento en el router.

Enrutamiento por defecto

En esta simulación se configuró la comunicación entre el router de la clínica y Internet de la siguiente manera:

- Se asignó la dirección 10.0.0.1/30 al router de la clínica y 10.0.0.2/30 al router de Internet, representando el enlace entre ambos.
- Se configuró un enrutamiento por defecto en el router de la clínica, para que todo el tráfico destinado a redes externas salga a través del router de Internet.
- Se agregó una ruta de regreso en el router de Internet hacia la red de la clínica, garantizando que las respuestas puedan retornar correctamente.

Esta configuración permite simular de manera controlada la comunicación entre la red interna de la clínica y el acceso a Internet.

Traducción de direcciones de red (NAT)

La Traducción de Direcciones de Red (NAT) permitirá que varias PC dentro de la red accedan a Internet usando una sola dirección IP pública. En el router de la clínica se aplicó la modalidad NAT con sobrecarga (PAT), donde cada dispositivo interno comparte la misma IP pública, pero se diferencia por el número de puerto asignado.

III.1.2.3.3.- Calidad de Servicio (QoS)

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.

En la configuración de la red, usamos una política llamada QoS (Calidad de Servicio) que permite reservar un porcentaje del ancho de banda disponible para tipos específicos de tráfico, como el tráfico web (HTTP), mensajes de control de red (ICMP), Transferencia de archivos de redes (TFTP), protocolos de telefonía IP como (Skinny, RTP**),** configurados con prioridad estricta para que las llamadas siempre pasen primero en caso de congestión**,** tráfico de (RTP, UDP) asignan ancho de banda garantizado, de modo que las videollamadas médicas se mantengan estables. Esto significa que cuando la red está muy ocupada, el sistema asegura que estos servicios críticos tengan la capacidad mínima necesaria para funcionar correctamente.

No es que dividamos la red en partes fijas, sino que priorizamos y reservamos recursos para evitar que el tráfico importante se vea afectado, garantizando así un buen rendimiento y estabilidad para la clínica, especialmente en el acceso a internet y la comunicación de red

Al utilizar QoS en redes, las organizaciones tienen la capacidad de optimizar el rendimiento de múltiples aplicaciones en su red y obtener visibilidad de la velocidad de bits, el retraso, la fluctuación y la velocidad de paquetes de su red. Esto garantiza que puedan diseñar el tráfico en su red y cambiar la forma en que los paquetes se enrutan a Internet u otras redes para evitar demoras en la transmisión. Esto también garantiza que la organización logre la calidad de servicio esperada para las aplicaciones y brinde las experiencias de usuario esperadas.

Según el significado de QoS, el objetivo clave es permitir que las redes y las organizaciones prioricen el tráfico, lo que incluye ofrecer ancho de banda dedicado, fluctuación controlada y menor latencia. Las tecnologías utilizadas para garantizar esto son vitales para mejorar el rendimiento de las aplicaciones empresariales, las redes de área ancha (WAN) y las redes de proveedores de servicios.

III.1.2.4.- Desarrollo de estrategias de seguridad

Se analizarán los riesgos de la red y se propondrá un plan para proteger los datos de los pacientes, ya que actualmente no cuenta con medidas de seguridad y es vulnerable a robos o pérdidas de información.

III.1.2.4.1.- Desarrollar un plan de seguridad

Se propone: **Firewall**

Implementar un firewall Fortinet 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 por medio de filtrado web y detectar malware.

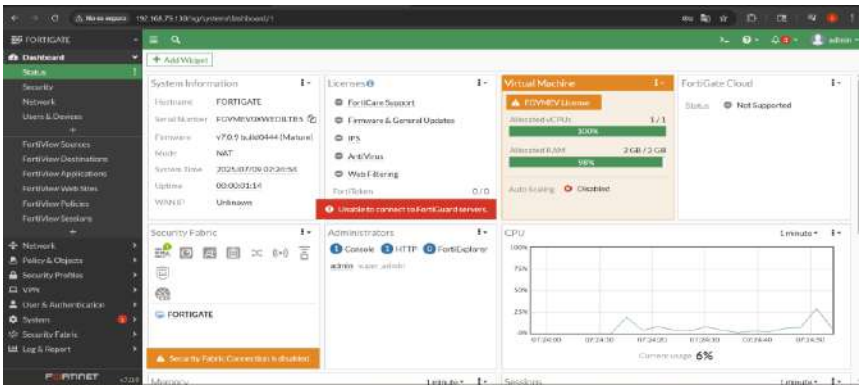

Figura 56. Pantalla de inicio Fortinet

Bloqueo de Aplicaciones

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

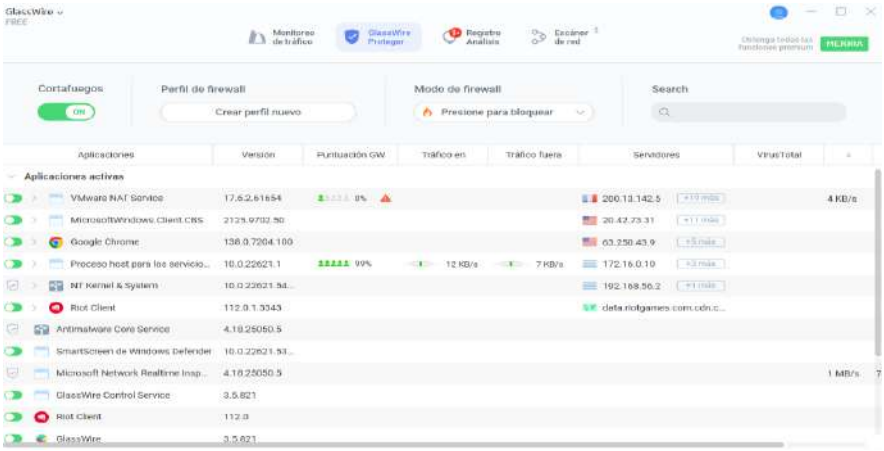

Figura 57. Bloqueo de aplicaciones

Segmentación de red VLANs

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.

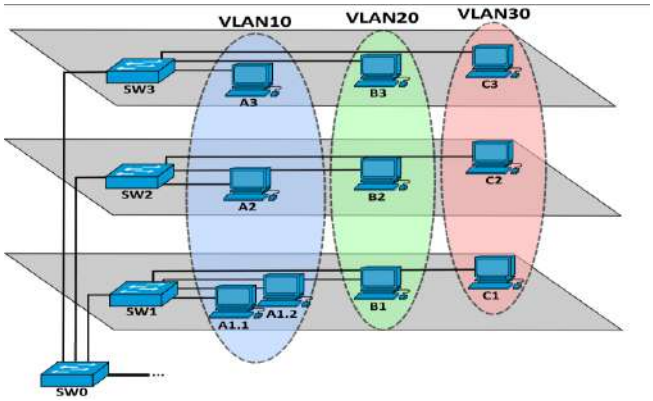

Figura 58. Diagrama de Vlans

Políticas de Seguridad del Router

En el router Cisco 2901 de la clínica se implementarán políticas de seguridad para controlar el tráfico entre VLANs y proteger la red interna. Se definirán reglas específicas que determinen qué direcciones IP pueden comunicarse entre sí. Por ejemplo, los dispositivos pertenecientes a la VLAN 20 (Pacientes) estarán restringidos para que únicamente tengan acceso al Access Point y a Internet. Se bloqueará cualquier intento de conexión hacia otras VLANs y también hacia el servidor de telefonía IP, garantizando una segmentación segura y evitando el acceso no autorizado a recursos internos.

Seguridad Inalámbrica

Se utilizará*:* WPA3 y Cambio de SSID (Nombre de la red), esto se realizará para evitar un ataque, necesita productos específicamente diseñados para proteger la red inalámbrica.

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

Autenticación: Se utilizará el Cifrado WPA3 todas las oficinas de las plantas estarán conectadas de este modo con este tipo de seguridad tanto para Pacientes y Personal de Salud tendrán diferentes contraseñas.

Análisis del Tráfico de Red

Wireshark se utilizará en este análisis como herramienta principal para la captura, inspección y diagnóstico del tráfico de red. Su función permitirá observar en tiempo real los paquetes que circulan a través de la infraestructura, identificando protocolos, direcciones IP, puertos de origen y destino, así como posibles retransmisiones o pérdidas de datos.

El uso de Wireshark es fundamental porque:

- Permite un análisis detallado del comportamiento de la red, detectando cuellos de botella, latencias y anomalías en la comunicación.
- Facilita la detección de problemas de configuración, como direcciones IP duplicadas, VLANs mal asignadas o tráfico no autorizado.
- Ayuda en la seguridad, ya que permite identificar intentos de acceso indebido o patrones de tráfico sospechosos.
- Es una herramienta estándar en la industria, ampliamente utilizada por administradores de redes e ingenieros para monitoreo y auditoría.

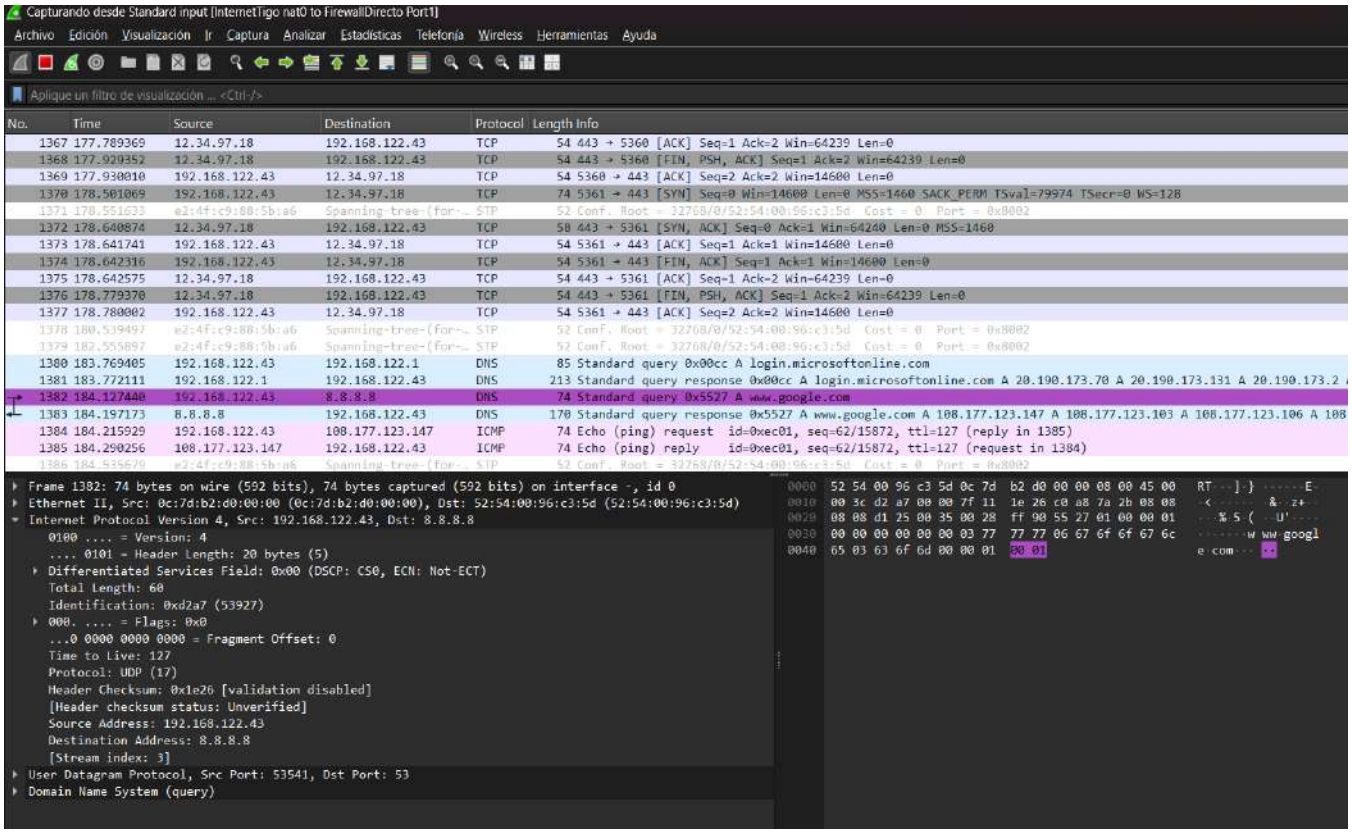

Figura 59. Control de trafico de diferentes conexiones

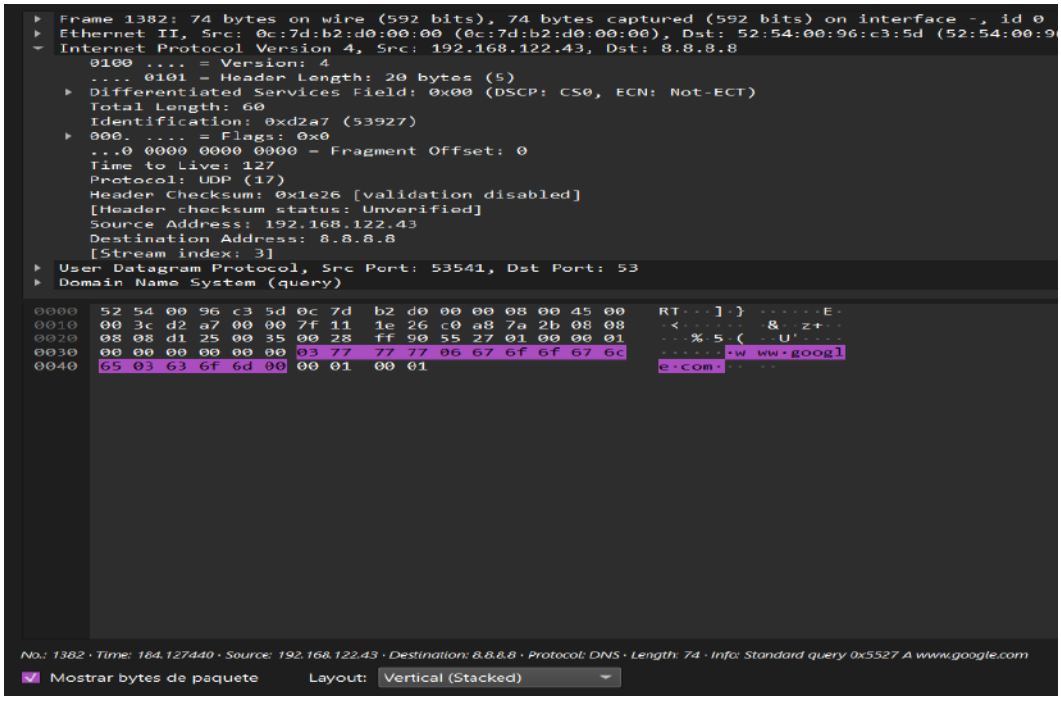

Figura 60. Control de trafico en especifico

III.1.3.- Fase 3: Desarrollar Diseño Físico

III.1.3.1.- Seleccionar tecnologías y dispositivos para redes de campus

III.1.3.1.1.-Descripción del edificio

El proyecto estará diseñado para la Clínica Santísima Trinidad de Tarija privada esta institución cuenta con 4 plantas en todas las plantas deben estar conectadas a los dispositivos de tecnologías de redes avanzadas.

Planta Baja: En la planta baja se encuentra recepción tanto como administración, consultorios, ecografías, emergencias, tomografías, rayos x y laboratorio. También se toma en cuenta que en la planta baja se encontrara el rack de piso principal lo cual estará ubicado en el cuarto de depósito y este actuara como puesto de telecomunicaciones.

Primer Piso: En el primer piso se encuentra las internaciones, cocina, estación de enfermería, la sala de partos y quirófano en esta planta se encontrará igualmente con un rack de pared que distribuirá el servicio en todo el piso.

Segundo Piso: En el segundo piso se encuentran lo que son endoscopia, internación, estación de enfermería, lugar del quirófano conformado por el equipo leoch. Esta igualmente contará con un rack de pared que distribuirá el servicio en todo el piso.

Tercer Piso: En el tercer piso se encuentra el laboratorio que pertenece al área tercerizada, consultorio de pediatría, consultorio cirugía pediátrica, consultorio diabetología, internaciones y los cuartos de terapias lo cual toda esta planta tendrá un rack de pared para que en toda la planta incluyendo la expansión del tercer piso puedan estar en servicio.

Expansión Tercer Piso: Esta planta se encuentra en la misma zona que el tercer piso y cuenta con farmacia, desinfección y esterilización de equipos de instrumentos lo cual estos contarán con dos laboratorios y por último y más importante contabilidad.

III.1.3.1.2.- Diseño de la conexión de la red

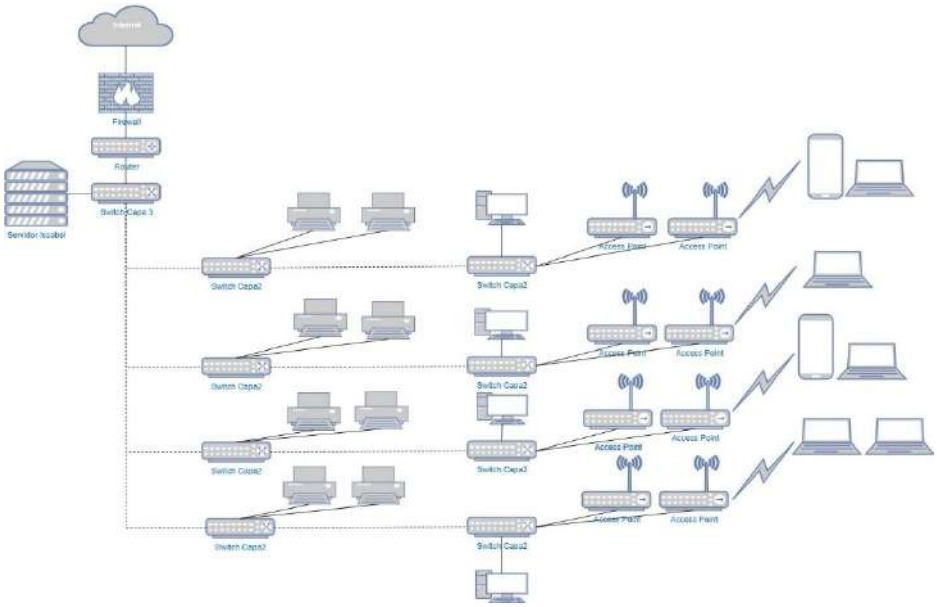

Figura 61. Diseño de la conexión de la red

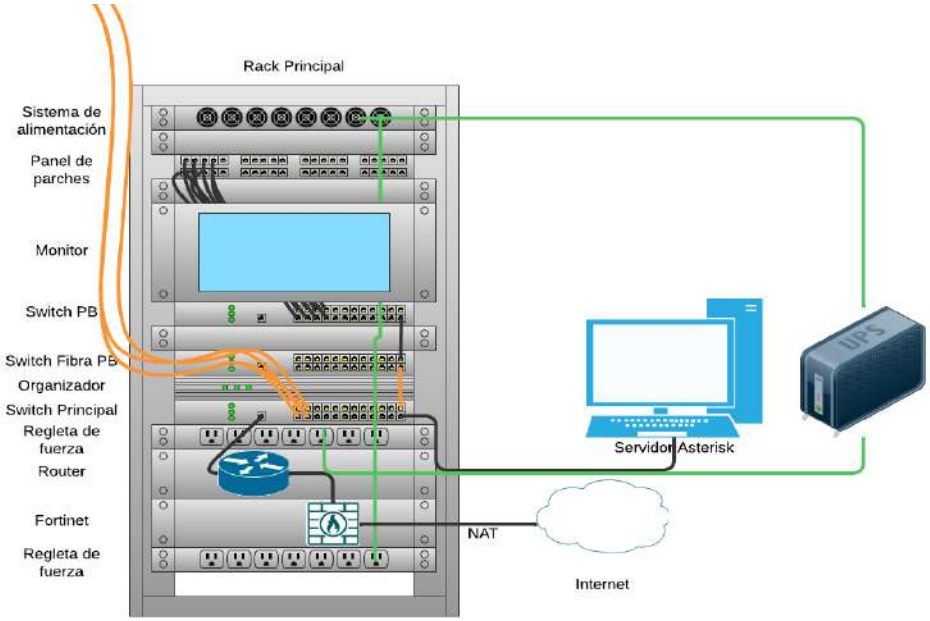

Figura 62. Diagrama del cuarto principal de telecomunicaciones

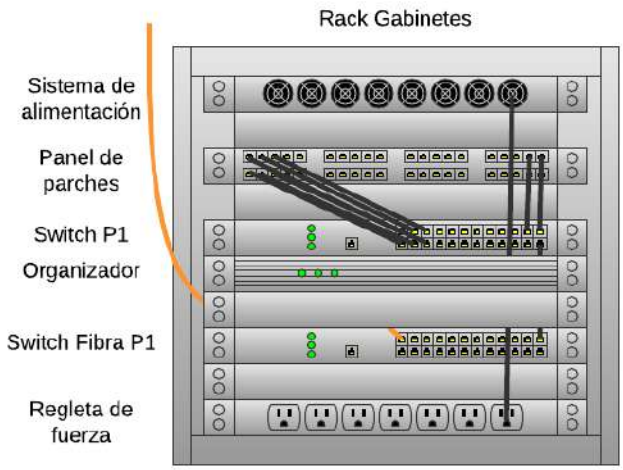

Figura 63. Diagrama de gabinetes

III.1.3.1.3.- Descripción detallada de la canalización

Este es un punto realmente importante porque por este medio se hará distribución para la llegada de los equipos terminales en el presente proyecto se realizó un cableado con canaletas de PVC de 2 tipos esto en el caso del cableado horizontal, en el cableado vertical se utilizará los canales de paso de piso dejados en anteriores instalaciones en el edificio este canal es necesario el paso del cable ya que es una disposición de topología de tipo árbol y se contara con cuatro cables de fibra troncales de datos.

En lo que se refiere a la canalización por pisos se dispondrá del uso de ellas en las oficinas, se dispondrá de un tendido principalmente por el techo de los pasillos de la institución por temas estéticos se buscará hacerlo por techo en las oficinas, se dispondrá a hacer la conexión por las paredes en la cual es fácil el paso de los cables atreves de ella y llegara de manera más fácil al punto del usuario.

III.1.3.1.3.1.- Distribución de canaletas

En esta sección se presenta la distribución física de las canaletas, indicando únicamente los recorridos que seguirán los cables desde el gabinete principal hacia cada ambiente o dispositivo.

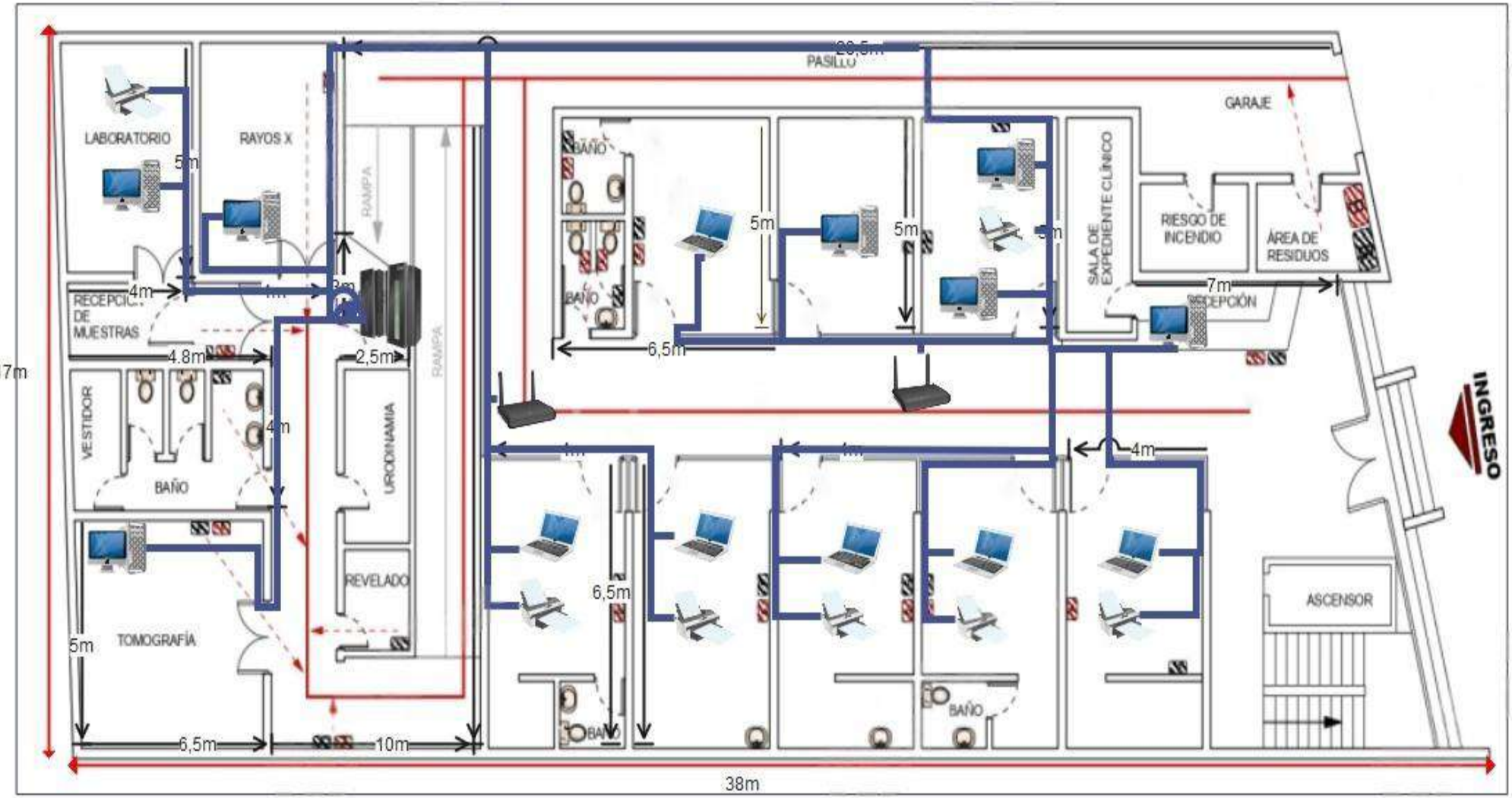

Figura 64. Canaletas Planta Baja

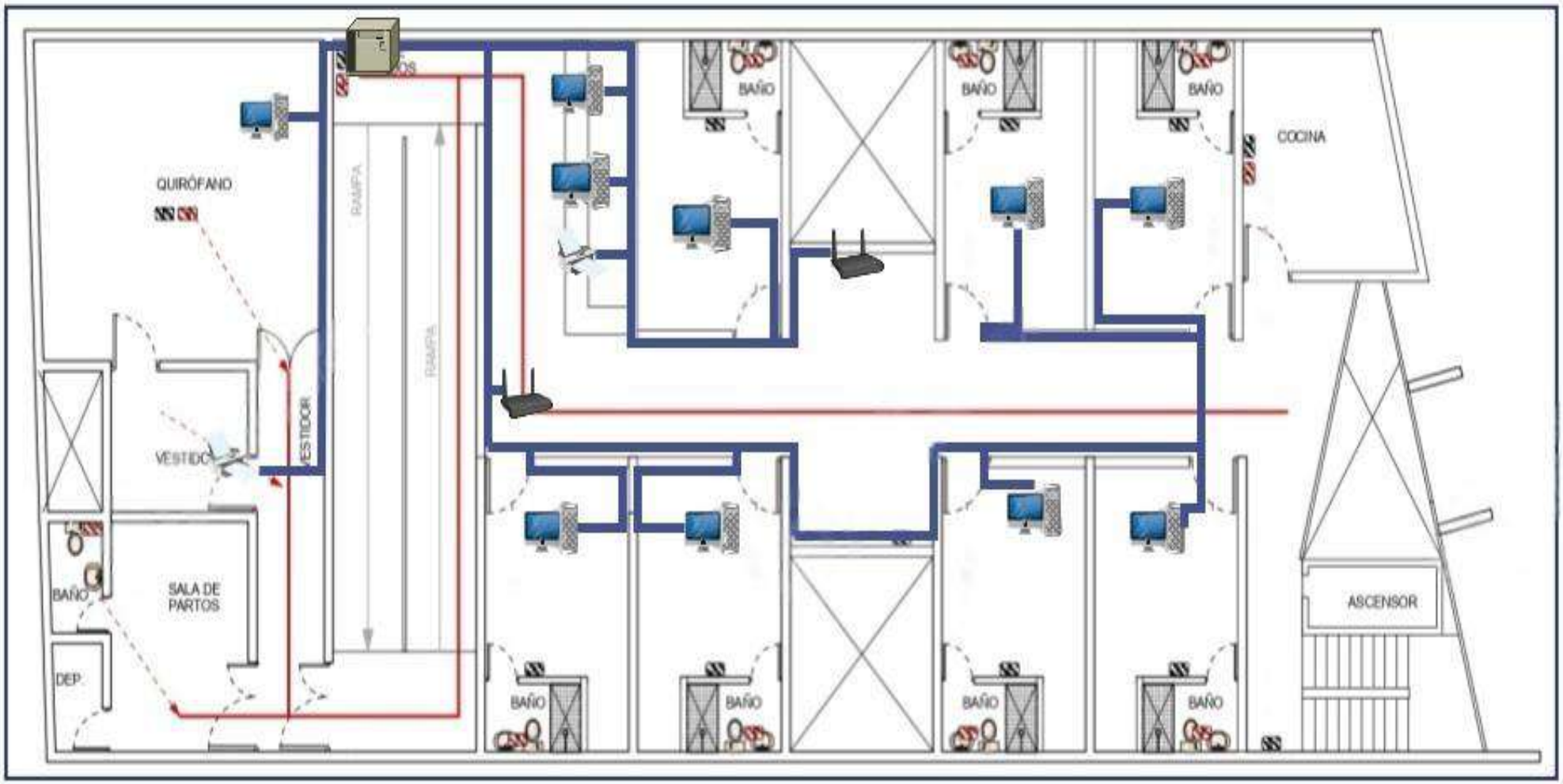

Figura 65. Canaletas Primer Piso

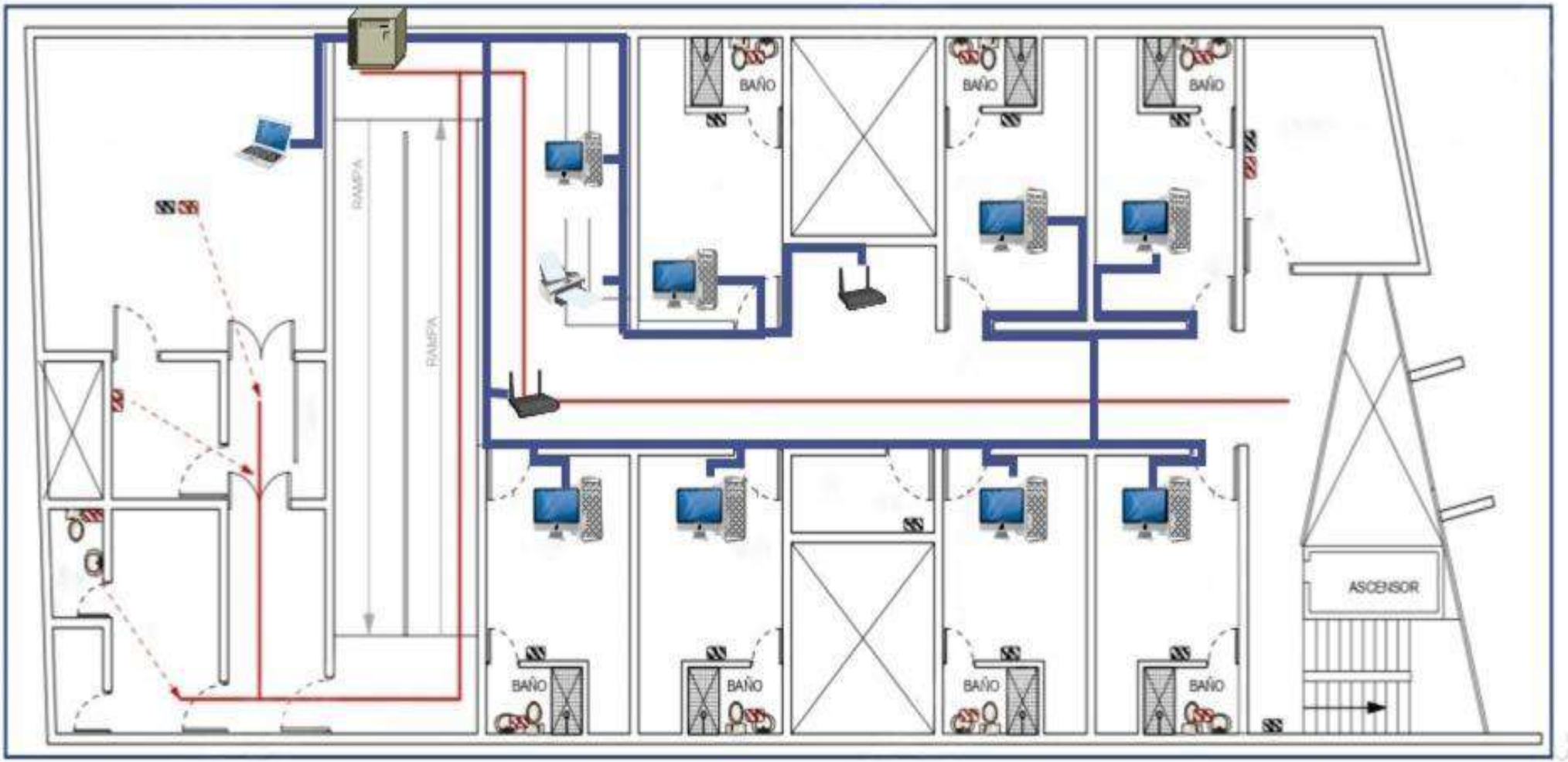

Figura 66. Canaletas Segundo Piso

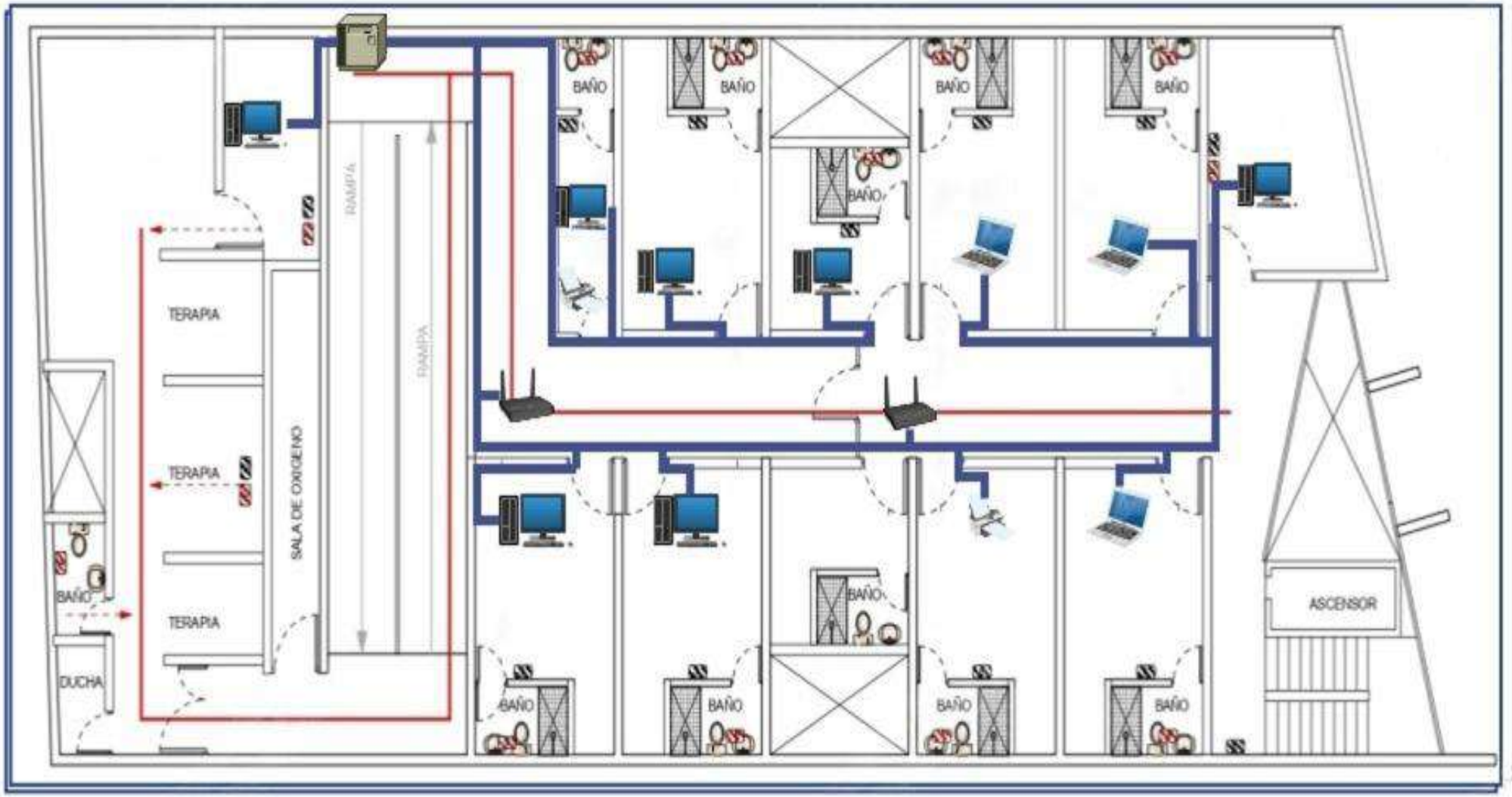

Figura 67. Canaletas Tercer Piso

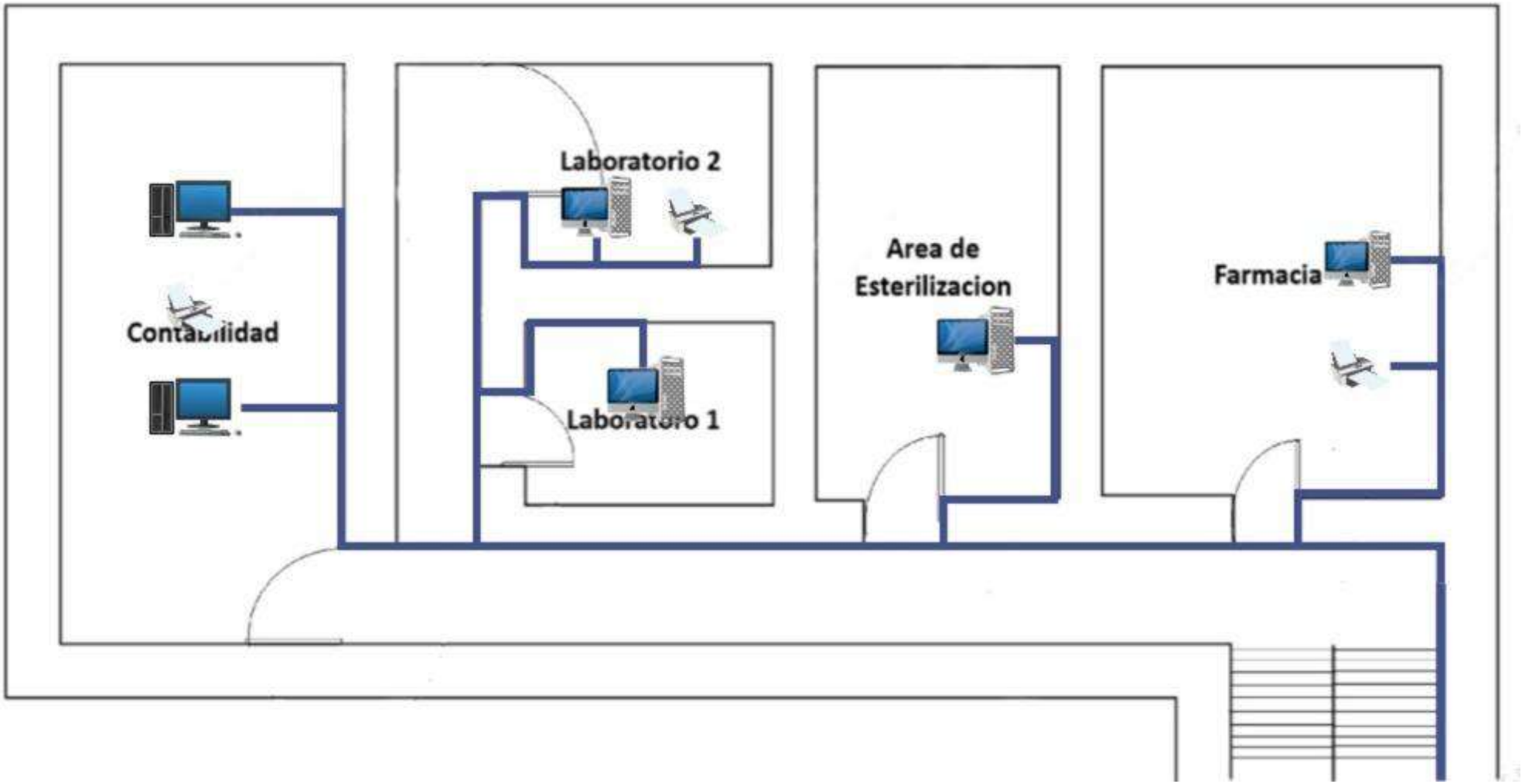

Figura 68. Canaletas Extensión Tercer Piso

En la siguiente imagen de elaboración propia se logra apreciar por donde se realizará la distribución de los equipos cada planta por donde pasará el cableado horizontal y en qué parte se ubicarán los equipos exactamente.

III.1.3.1.3.2.- Material de canalización

Canaleta Plástica

Canaleta 70x40 mm:

Para la canalización se hará material canaletas de 70x40 mm estas se utilizarán como principal salida desde los gabinetes de comunicación ya que llega el máximo grupo de cableado para la distribución a los equipos de salida.

Figura 69. Canaleta de PVC 70x40mm ranurada

Canaleta 40x20 mm:

Este tipo de canaleta se utilizará para la llegada a los equipos al ser más pequeñas con una capacidad de 10 cables se usarán para la distribución dentro de las habitaciones para los dispositivos finales.

Figura 70. Canaleta de PVC 40x20mm

III.1.3.1.3.3.- Material de Cableado

Para el presente proyecto se optó por utilizar el tipo de cableado UTP para esta instalación, ya que el costo no supone una inversión muy descomunal. El modelo elegido fue:

Modelo de cable UTP Cat.5e

- Velocidad de transmisión de hasta 1 Gbps
- Frecuencia de funcionamiento de 100 a 350 MHz
- Cuatro pares de hilos de cobre trenzados
- Cubierta exterior de plástico

Figura 71. Cableado UTP 4 pares Cat.5e

III.1.3.1.3.4.- Placa de pared categoría 5e

Está diseñada para entornos profesionales como clínicas y centros médicos, esta placa de pared RJ45 categoría 5e proporciona una solución limpia, organizada y funcional para la instalación de puntos de red. Ideal para áreas clínicas y administrativas donde se requiere una conectividad confiable para equipos médicos, sistemas informáticos y comunicaciones internas.

Se utilizarán este tipo de placas para que los usuarios puedan conectarse directamente a sus equipos, como PCs o laptops, estando lo más cerca posible de sus dispositivos. Cada placa estará conectada mediante un cable de red que llevará la conexión hasta las rosetas ubicadas fuera de sus oficinas, garantizando así una instalación ordenada, funcional y escalable.

Características Técnicas y Funcionales

Diseño profesional y discreto

Con un acabado blanco neutro y moderno, esta placa se integra perfectamente con el estilo arquitectónico y decorativo de clínicas, consultorios, laboratorios y oficinas. Su diseño permite mantener una imagen ordenada y profesional en todos los ambientes.

Instalación sencilla

No requiere herramientas especializadas. Solo se necesita un destornillador estándar para fijar la placa. El cable de red se conecta a la parte posterior del conector RJ45, y los dispositivos se conectan fácilmente al puerto frontal.

Compatible con Cat 5e – hasta 1000 Mbps

Soporta velocidades de hasta 1 Gbps, incluyendo acceso a sistemas de historia clínica electrónica, software de gestión hospitalaria, impresoras de red y navegación web.

Conector Keystone desmontable

El módulo RJ45 tipo Keystone es desmontable, lo que permite reemplazos sin necesidad de cambiar la placa completa. Esto representa una solución económica y escalable para el mantenimiento de la red.

Material resistente y duradero

Construida en plástico ABS de alta calidad, resistente a impactos y desgaste, ideal para entornos con tráfico constante de personal médico y administrativo.

Figura 72. Placa de pared cat 5e

III.1.3.1.3.5.- 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.

- Alta protección contra las interferencias electromagnéticas.
- Baja propagación de retardo.
- Altos valores ACR y error mínimo de velocidad.

Figura 73. Latiguillo de parcheo

III.1.3.1.3.6.- Rosetas y conectores

En lo que respecta a las rosetas, se instalarán justo afuera de cada cuarto, en una posición conveniente sobre la pared alta. Estas podrán ser de 2 o 4 slots (espacios), lo que permite conectar varios dispositivos desde una misma roseta y aprovechar al máximo cada punto de acceso. La instalación de rosetas facilita la conexión ordenada y segura de equipos como computadoras o dispositivos médicos, evitando el uso de cables expuestos y garantizando una mejor organización del cableado estructurado. Además, su ubicación estratégica permite flexibilidad para ampliar la red en caso de ser necesario.

Figura 74. Rosetas

El conector RJ45 es un tipo de conector modular utilizado para conectar cables de par trenzado a dispositivos de red. Tiene ocho pines o conexiones eléctricas, que se utilizan para conectar los pares de hilos del cable a los terminales del dispositivo.

- Ocho pines o conexiones eléctricas
- Dos tipos principales: macho y hembra
- Se utiliza para conectar cables de par trenzado a dispositivos de red
- Se puede conectar utilizando un crimpador de cables

Figura 75. Conector RJ45

III.1.3.1.4.- Descripción de los armarios de telecomunicaciones

No se cuenta con un cuarto de entrada de servicios por ende se realizará la distribución desde el gabinete de piso ubicado en la planta baja para la distribución en los demás pisos en sus gabinetes de pared que distribuirán servicio a los puntos de trabajo.

El **gabinete de piso** que se utilizará será de 23U, es una caja grande y rectangular que se usa para almacenar y proteger dispositivos de red. Los gabinetes de piso para redes suelen estar hechos de acero o aluminio y tienen puertas que se pueden cerrar con llave para evitar el acceso no autorizado. También pueden tener ruedas o patas para facilitar el movimiento.

Luego se dispondrá de un **gabinete de pared** de 10U más pequeño en los demás pisos este alojará dispositivos conmutadores como son los switchs principalmente para proveer el servicio a los dispositivos.

Rack de distribución planta baja

Gabinete de piso es un gabinete principal en este proyecto este será el gabinete más fundamental para su desarrollo por lo que se procuró que este en un lugar bien ambientado y espacioso. Sus dimensiones normalizadas según la especificación EIA- 310 permiten que sea compatible con equipos de cualquier

marca o fabricante.

- Altura: La altura de un gabinete de piso se mide en unidades de rack (U). Un gabinete de 23 unidades tiene una altura de 23U
- Ancho: El ancho de un gabinete de piso se mide en pulgadas este es de un ancho de 19 pulgadas.
- Material: Los gabinetes de piso suelen estar fabricados con acero o aluminio.
- Refrigeración: Los gabinetes de piso para servidores suelen tener un sistema de refrigeración incorporado para mantener los equipos a una temperatura adecuada.
- Accesibilidad: Los gabinetes de piso para servidores suelen tener puertas y paneles laterales que se pueden abrir para acceder a los equipos.
- Organización: Los gabinetes de piso para servidores suelen tener bandejas y soportes para organizar los equipos.

Figura 76. Rack de Piso 23U

Equipo	**Tamaño**	**Unidades**	**Total**
Ventilador	2U	1	2U
Patch panel 24 puertos	1U	1	1U
Router	1U	1	1U
Switch 12 puertos	1U	1	1U
Switch 10 puertos	1U	1	1U
Switch 24 puertos	1U	1	1U
Regleta de fuerza	1U	2	2U
Organizador de cable	3U	2	6U
Bandeja porta equipos	1U	1	1U
Servidor	2U	2	4U
Consola	1U	1	1U
Total	**15U**	**14**	**21U**

Tabla 72. Rack de suelo distribución

Rack de distribución primero, segundo y tercer piso

El gabinete del primer piso se optó por el uso de gabinete de pared ya que estos dispositivos solo reciben el puerto troncal configurado en un dispositivo switch este gabinete debe regirse según la especificación EIA-310 permiten que sea compatible con equipos de cualquier marca o fabricante.

- Altura: La altura de un gabinete de pared se mide en unidades de rack (U). Un gabinete de 10 unidades tiene una altura de 10 U
- Ancho: El ancho de un gabinete de piso se mide en pulgadas este es de un ancho de 19 pulgadas.
- Material: Los gabinetes de pared suelen estar fabricados con acero o aluminio.
- Accesibilidad: Los gabinetes de pared para servidores suelen tener puertas y paneles laterales que se pueden abrir para acceder a los equipos.
- Organización: Los gabinetes de pared para servidores suelen tener bandejas y soportes para organizar los equipos.

Figura 77. Rack de pared 10U

Equipo	Tamaño	Unidades	Total
Ventilador	2U	1	2U
Patch panel 24 puertos	1U	1	1U
Switch 10 puertos	1U	1	1U
Switch 24 puertos	1U	1	1U
Regleta de fuerza	1U	1	1U
Organizador de cable	2U	1	2U
Total	8U	11	8U

Tabla 73. Rack de pared distribución

III.1.3.1.4.1.- Descripción de dispositivos para el cuarto de telecomunicaciones

Se implementará un servidor DHCP configurado en un switch de capa 3, lo que permitirá asignar direcciones IP de manera dinámica a los dispositivos conectados a la red. Además, se utilizarán switches para la configuración de VLANs, con el fin de segmentar la red y reducir la congestión, mejorando así el rendimiento general.

Para reforzar la seguridad de la red, se incorporará un firewall que permitirá proteger la información crítica que maneja la clínica, controlando el acceso y regulando el tráfico de red.

En cuanto a la administración, se aplicará VLSM (Variable Length Subnet Masking) para optimizar el uso de direcciones IP según las necesidades específicas de cada subred, permitiendo una asignación más

eficiente y escalable de recursos.

También se adoptarán medidas de seguridad física en los ambientes donde se encuentren los equipos, tales como la instalación de sensores de humo, extintores y controles de acceso, para proteger los dispositivos ante posibles riesgos como incendios, acumulación de polvo o ingreso no autorizado. Todo esto contribuirá a garantizar la seguridad, disponibilidad y administración eficiente de la red.

Regleta de fuerza

Están fabricadas con un perfil de aluminio de alta calidad preparado para soportar temperaturas elevadas estos componentes normalmente llegan con la compra de un dispositivo como rack o gabinete.

El electroblock suministra alimentación al switch, repetidores y router dentro del distribuidor.

Referencia F2109.

- 1U.
- 8 tomas.
- Interruptor bipolar de 16 amperios.

Figura 78. Regleta de fuerza

Organizador de cableado

La función principal de un organizador de cables en un gabinete es mantener los cables ordenados, organizados y debidamente gestionados. Esto es esencial para garantizar un entorno limpio, seguro y eficiente en un gabinete o rack de equipos. Algunas de las ventajas del uso del organizador de cable son: mejora de la ventilación y refrigeración, prevención de enredos y confusión de cables.

Figura 79. Organizador de cables

Ventilador rack

En lo que comprende el ventilador es un dispositivo primordial su función es la de mantener una temperatura adecuada y constante dentro del gabinete. Los gabinetes informáticos albergan componentes electrónicos sensibles, como servidores, equipos de red y sistemas de almacenamiento, que generan calor durante su funcionamiento.

Figura 80. Ventilador rack

Patch panel

El uso de un patch pannel puede beneficiar mucho a mejorar la durabilidad de los dispositivos como switchs para reducir las conexiones y desconexiones constantes y evitar el desgasto.

Para este proyecto, se instalarán patch panels de 24 puertos en cada uno de los racks, en función de la cantidad de dispositivos conectados a los switches. Desde estos patch panels se distribuirán los cables de datos hacia los diferentes puestos de trabajo, permitiendo su conexión directa al switch mediante latiguillos de parcheo.

Figura 81. Patch Pannel 24 puertos

Consola

Un dispositivo compacto diseñado para montarse en un gabinete o rack de telecomunicaciones y que integra un monitor, teclado y touchpad en una sola unidad. Su principal función es permitir el acceso local a servidores o equipos de red directamente desde el rack, facilitando tareas de administración, configuración o mantenimiento sin necesidad de conectar dispositivos externos.

Consola de conmutador KVM VGA de 1U y 19 pulgadas con pantalla LCD, teclado y ratón integrados. Controla hasta 4 computadoras mediante una sola plataforma, soporta resolución de 1920x1080, compatibilidad USB PS/2 y encendido/apagado automático. Certificado por CE y RoHS para cumplir con los estándares de seguridad de la UE, asegurando el acceso al mercado.

Figura 82. Consola de conmutador KVM VGA

Bandeja porta equipos

Una bandeja porta equipos 1U es un accesorio metálico diseñado para instalarse en un gabinete o rack estándar de 19 pulgadas, ocupando 1 unidad de altura (1U). Su función principal es soportar equipos no rackeables, como firewalls, módems, o UPS de escritorio, permitiendo su integración ordenada dentro del rack.

Figura 83. Bandeja porta equipos

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 lo que nos indica implementar un 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 84. UPS Forza 1000VA

Servidor

Se utilizará un equipo compacto y flexible diseñado para ofrecer rendimiento, seguridad y fiabilidad de nivel empresarial en entornos pequeños o de crecimiento progresivo. Su diseño en minitorre permite colocarlo horizontal, vertical o incluso en pared, adaptándose al espacio disponible. Es compatible con procesadores Intel® Xeon® de la serie 6300, Intel® Xeon® E e Intel® Pentium®, ofreciendo buena capacidad de cómputo y memoria, así como administración remota segura mediante HPE iLO.

Figura 85. Servidor DELL PowerEdge T40

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 86. Aire acondicionado

III.1.3.1.4.2.- Diseño de la conexión del rack Planta Baja

Figura 87. Diseño de la conexión del Rack de Suelo PB

III.1.3.1.4.3.- Diseño de la conexión del rack Primer Piso

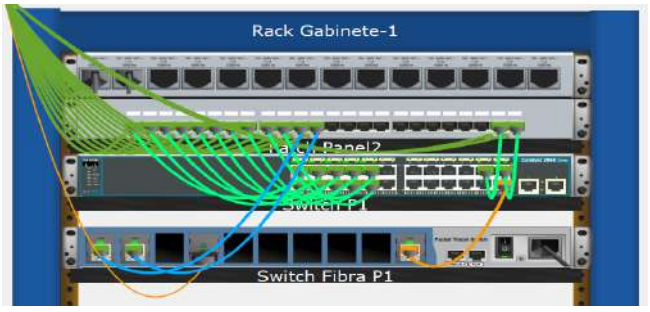

Figura 88. Diseño de la conexión del Rack de pared P1

III.1.3.1.4.4.- Diseño de la conexión del rack Segundo Piso

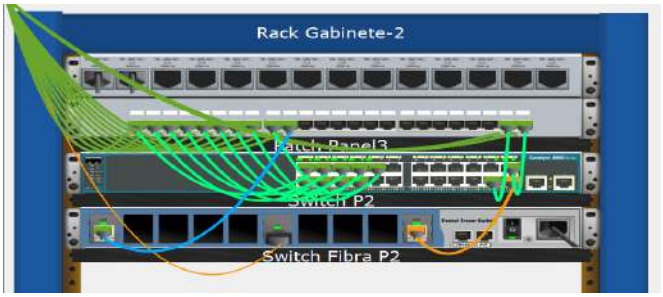

Figura 89. Diseño de la conexión del Rack de pared P2

III.1.3.1.4.5.- Diseño de la conexión del rack Tercer Piso

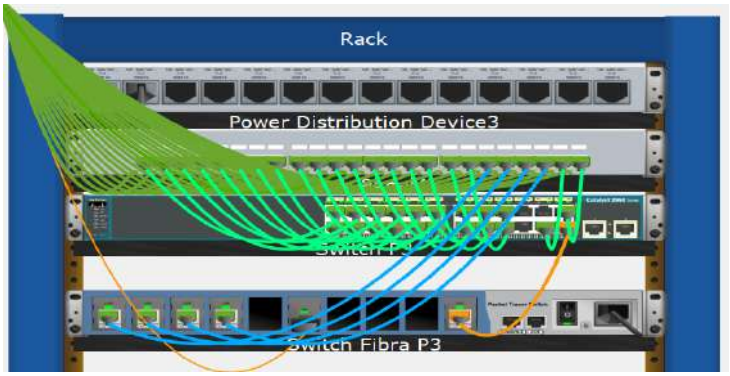

Figura 90. Diseño de la conexión del Rack de pared P3

III.1.3.1.5.- Etiquetado de la infraestructura de red

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.
- Repetidores y switch.
- Rosetas o tomas de usuario.
- Espacios donde se localicen terminales.
- Asegurarse que las etiquetas no sean visibles para los usuarios

III.1.3.1.5.1.- Abreviaturas para las Areas

- **REC:** Recepción
- **CONS:** Consultorios

- **ADM**: Administración
- **EMG:** Emergencias
- **IT:** Internación
- **TRI:** Terapia Intensiva
- **ENF:** Enfermería
- **PED:** Pediatría
- **FAR:** Farmacia
- **EST:** Esterilización
- **CON:** Contaduría
- **AT:** Áreas tercerizadas

Dispositivos de la red:

- **SP:** Switch Principal
- **SPB:** Switch PB
- **SP1:** Switch P1
- **SP2:** Switch P2
- **SP2:** Switch P3
- **RO:** Router
- **SFPB:** Switch Fibra PB
- **SFP1:** Switch Fibra P1
- **SFP2:** Switch Fibra P2
- **SFP3:** Switch Fibra P3
- **SERVA:** Servidor Asteriskl
- **SERVC:** Servidor Central
- **PER:** Personal de salud
- **PAC:** Pacientes

Puerto	Fibra	Puerto	Fibra
Gi 9/1	**RO**	**7**	**LIBRE**
Gi 8/1	**LIBRE**	**8**	**LIBRE**
Gi 7/1	**SFP3**	**9**	**LIBRE**
Gi 6/1	**SFP1**	**10**	**LIBRE**
Gi 5/1	**SFP2**	**Fa 1/1**	**SERVC**
Gi 4/1	**SFPB**	**Fa 0/1**	**SERVA**

Tabla 74. Etiquetado Switch Principal

Puerto	Fibra	Puerto	Fibra
Fa 9/1	PB-ADM-3-PRINT	Gi 4/1	SP
Fa 8/1	PB-CONS-6-PRINT	Fa 3/1	PB-CONS-10-PRINT
Fa 7/1	PB-CONS-7-PRINT	Fa 2/1	PB-AT-5-PRINT
Fa 6/1	PB-CONS-8-PRINT	9	LIBRE
Fa 5/1	PB-CONS-9-PRINT	Fa 0/1	SPB

Tabla 75. Etiquetado Switch Fibra PB

Puerto	RJ45	Puerto	RJ45	Puerto	RJ45
1	LIBRE	Fa 0/9	PB-AT-4-PC	17	LIBRE
Fa 0/2	PB-ADM-1-PC	Fa 0/10	PB-AT-3-PC	18	LIBRE
Fa 0/3	PB-ADM-2-PC	Fa 0/11	PB-AT-2-PC	19	LIBRE
Fa 0/4	PB-CONS-5-LP	Fa 0/12	PB-AT-1-PC	20	LIBRE
Fa 0/5	PB-CONS-4-LP	Fa 0/13	PB-EMG-1-LP	21	LIBRE
Fa 0/6	PB-CONS-3-LP	Fa 0/14	PB-REC-1-PC	Fa 0/22	PB-PER-1-AP
Fa 0/7	PB-CONS-2-LP	15	LIBRE	Fa 0/23	PB-PAC-1-AP
Fa 0/8	PB-CONS-1-LP	16	LIBRE	Fa 0/24	SFPB

Tabla 76. Etiquetado Switch PB

Puerto	Fibra	Puerto	Fibra
Fa 9/1	P1-TRI-2-PRINT	5	LIBRE
Fa 8/1	P1-IT-8-PC	6	LIBRE
3	LIBRE	7	LIBRE
Gi 6/1	SP	8	LIBRE
4	LIBRE	Fa 0/1	SP1

Tabla 77. Etiquetado Switch Fibra P1

Puerto	RJ45	Puerto	RJ45	Puerto	RJ45
Fa 0/1	P1-IT-7-PC	Fa 0/9	P1-ENF-1-PC	17	LIBRE
Fa 0/2	P1-IT-6-PC	Fa 0/10	P1-TRI-1-PC	18	LIBRE

Fa 0/3	**P1-IT-5-PC**	**11**	**LIBRE**	**19**	**LIBRE**
Fa 0/4	**P1-IT-4-PC**	**12**	**LIBRE**	**20**	**LIBRE**
Fa 0/5	**P1-IT-3-PC**	**13**	**LIBRE**	**Fa 0/21**	**P1-PER-2-AP**
Fa 0/6	**P1-IT-2-PC**	**14**	**LIBRE**	**22**	**LIBRE**
Fa 0/7	**P1-IT-1-PC**	**15**	**LIBRE**	**Fa 0/23**	**P1-PAC-2-AP**
Fa 0/8	**P1-ENF-2-PC**	**16**	**LIBRE**	**Fa 0/24**	**SFP1**

Tabla 78. Etiquetado Switch P1

Puerto	Fibra	Puerto	Fibra
Fa 9/1	**P2-IT-16-PRINT**	**Gi 4/1**	**SP**
2	**LIBRE**	**7**	**LIBRE**
3	**LIBRE**	**8**	**LIBRE**
4	**LIBRE**	**9**	**LIBRE**
5	**LIBRE**	**Fa 0/1**	**SP2**

Tabla 79. Etiquetado Switch Fibra P2

Puerto	RJ45	Puerto	RJ45	Puerto	RJ45
Fa 0/1	**P2-IT-9-PC**	**Fa 0/9**	**P2-ENF-3-PC**	**17**	**LIBRE**
Fa 0/2	**P2-IT-10-PC**	**10**	**LIBRE**	**18**	**LIBRE**
Fa 0/3	**P2-IT-11-PC**	**11**	**LIBRE**	**19**	**LIBRE**
Fa 0/4	**P2-IT-12-PC**	**12**	**LIBRE**	**20**	**LIBRE**
Fa 0/5	**P2-IT-13-PC**	**13**	**LIBRE**	**21**	**LIBRE**
Fa 0/6	**P2-IT-14-PC**	**14**	**LIBRE**	**Fa 0/22**	**P2-PER-3-AP**
Fa 0/7	**P2-IT-15-PC**	**15**	**LIBRE**	**Fa 0/23**	**P2-PAC-3-AP**
Fa 0/8	**P2-TRI-3-LP**	**16**	**LIBRE**	**Fa 0/24**	**SFP2**

Tabla 80. Etiquetado Switch P2

Puerto	Fibra	Puerto	Fibra
Fa 9/1	**P3-CON-3-PRINT**	**Gi 4/1**	**SP**
Fa 8/1	**P3-FAR-2-PRINT**	**7**	**LIBRE**

Fa 7/1	**P3-EST-4-PRINT**	**8**	**LIBRE**
Fa 6/1	**P3-IT-22-PRINT**	**9**	**LIBRE**
5	**LIBRE**	**Fa 0/1**	**SP3**

Tabla 81. Etiquetado Switch Fibra P3

Puerto	RJ45	Puerto	RJ45	Puerto	RJ45
Fa 0/1	**P3-AT-6-PC**	**Fa 0/9**	**P3-IT-20-PC**	**Fa 0/17**	**P3-CON-1-PC**
Fa 0/2	**P3-PED-1-PC**	**Fa 0/10**	**P3-IT-21-PC**	**Fa 0/18**	**P3-CON-2-PC**
Fa 0/3	**P3-PED-2-PC**	**Fa 0/11**	**P3-TRI-4-PC**	**19**	**LIBRE**
Fa 0/4	**P3-PED-3-PC**	**Fa 0/12**	**P3-ENF-4-PC**	**20**	**LIBRE**
Fa 0/5	**P3-PED-4-PRINT**	**Fa 0/13**	**P3-FAR-1-PC**	**21**	**LIBRE**
Fa 0/6	**P3-IT-17-PC**	**Fa 0/14**	**P3-EST-1-PC**	**Fa 0/22**	**P3-PER-4-AP**
Fa 0/7	**P3-IT-18-PC**	**Fa 0/15**	**P3-EST-2-PC**	**Fa 0/23**	**P3-PAC-4-AP**
Fa 0/8	**P3-IT-19-PC**	**Fa 0/16**	**P3-EST-3-PC**	**Fa 0/24**	**SFP3**

Tabla 82. Etiquetado Switch P3

III.1.3.2.- Seleccionar tipos de enlaces alámbricos o inalámbricos

III.1.3.2.1.- Enlaces alámbricos

III.1.3.2.1.1.- Cobre UTP Categoría 5e

En este proyecto se plantea utilizar cableado de cobre UTP Categoría 5e, ya que cada enlace permitirá transmitir datos a una velocidad de 1 Gbps, lo cual será empleado para la conexión de PCs, laptops en estaciones fijas e impresoras de red dentro de cada planta. Este tipo de cable es una solución práctica porque soporta velocidades de hasta 1 Gbps en distancias máximas de 100 metros, lo que resulta suficiente para cubrir las necesidades de conectividad del trabajo diario administrativo y médico de la clínica.

- Económico: se utilizará porque es más barato que cables de categorías superiores.
- Fácil instalación: la utilizará ya que es flexible, liviano y sencillo de instalar en canaletas y rosetas.
- Compatibilidad: se utilizará porque es compatible con la mayoría de switches, routers y equipos actuales.
- Velocidad suficiente: permite conexiones Gigabit.

Figura 91. Cobre UTP Categoría 5e

III.1.3.2.1.2.- Fibra óptica monomodo

Se utilizará fibra óptica monomodo para la interconexión entre los switches de cada piso y el switch central de la Planta Baja. Este tipo de enlace permite alta velocidad, baja latencia y largas distancias, además de estar apto para transmitir hasta 10 Gbps, garantizando un buen rendimiento y preparación para futuras ampliaciones de la red. esta puede propagar la luz de una sola forma, es decir, no pasa rebotando por las paredes de la fibra. Cuenta con un núcleo pequeño de 9 µm y trabaja entre los 1310 nm y 1550 nm. Las conexiones contarán con una entrada de tipo SC (Subscriber Connector), un conector cuadrado de inserción sencilla y segura que asegura una conexión firme y de baja pérdida.

Figura 92. Fibra óptica monomodo

III.1.3.2.2.- Enlaces inalámbricos

III.1.3.2.2.1.- Wifi

Se implementa wifi ya que permite que el personal de salud de la clínica conecte laptops, tablets y smartphones de manera inalámbrica, garantizando movilidad dentro de las distintas áreas y acceso rápido a los sistemas clínicos y administrativos. Esta tecnología facilita la instalación al reducir la necesidad de cableado, mantiene la red más organizada y permite escalar o agregar dispositivos de forma sencilla, adaptándose a las necesidades de conectividad de la clínica.

Wi-Fi segmentado en VLANs

Se configurará la red para controlar el acceso de manera segura. La VLAN 30, correspondiente al personal de salud, permitirá conectarse a todas las áreas de la clínica y a los servidores internos, asegurando acceso completo a los sistemas necesarios para su trabajo. En cambio, la VLAN 20, destinada a pacientes y visitantes, solo tendrá acceso a Internet, bloqueando cualquier comunicación con otras áreas o sistemas internos.

III.1.3.2.2.2.- Tecnología PoE (Alimentación a través de Ethernet)

En este proyecto se implementará PoE (Power over Ethernet) para los Access Points de la clínica. Esta tecnología permite que un solo cable de red transmita datos y energía eléctrica al mismo tiempo, eliminando la necesidad de enchufes adicionales y simplificando la instalación, lo que garantiza una

conexión confiable y un cableado más ordenado.

Tal como se muestra en la imagen el cable que viene del transformador (POE) (salida indicada LAN) debe conectarse al puerto AZUL (también rotulado como Internet o WAN) de su router. Se recomienda conectar PC's, Smart TV's y cualquier dispositivo que requiera buena velocidad de conexión con un cable de red directamente a los puertos amarillos del router numerados como LAN, dejando la conexión WiFi solo para dispositivos móviles (Celulares, Tablets, Notebook).

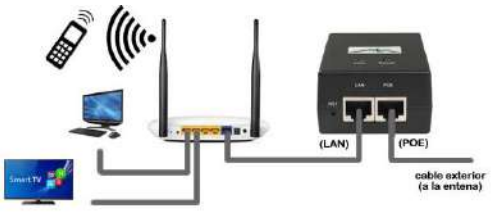

Figura 93. Tecnología PoE

III.1.3.2.3.- Descripción de dispositivos finales que se conectarán

La red de la clínica incluirá diferentes dispositivos finales distribuidos en cada planta según su función. Se conectarán PCs y laptops, impresoras de red, y dispositivos móviles como android, tablets y smartphones. Cada dispositivo estará asignado a la VLAN correspondiente para garantizar que el personal de salud pueda acceder a los sistemas internos, mientras que los pacientes y visitantes tendrán acceso limitado a Internet, manteniendo la seguridad y el control de la red.

Se describen que tipos de dispositivos finales actualmente tiene la clínica:

Lenovo ThinkCentre M93p SFF

Figura 94. PC Lenovo

Características:

- Procesador: Core i5-4570 3.2 GHz (Cuarta Generación)
- Memoria RAM: 6GB DDR3
- Almacenamiento: 500GB HDD (Disco duro)
- Lector CD, DVD: Sí
- Ranuras de Expansión Disponibles:
  1 ranura PCI Express para tarjeta de video
  Otros
- Puertos de E/S: VGA, DisplayPort x2, USB 3.0, 2.0, Ethernet, Audio, Micrófono
- Sistema Operativo: Windows 10 Profesional, con licencia digital

- Programas Básicos: Sí

Lenovo IdeaPad 3 Intel Core i5-1135G7 12GB 256GB SSD 15.6 FHD pantalla táctil portátil

Figura 95. Portatil Lenovo

Características:

- Procesador: Intel Core i5-1135G7 12GB 256GB SSD
- Gráficos: gráficos Intel UHD integrados
- Sistema operativo: Windows 10
- Memoria: hasta 12 GB DDR4 RAM
- Disco duro: SSD PCIe de hasta 256 GB
- Unidad óptica: No.
- Pantalla: 15.6 pulgadas FHD (1920x1080) TN 220nits antirreflejos
- Conectividad: Wi-Fi 2 x 2 802.11AC con Bluetooth 5.0
- Chip de audio: Audio de alta definición (HD)
- Teclado: sin retroiluminación, inglés

Delux Armada

Figura 96. PC Delux

Características:

- Equipo de Computación: Monitor LG, Mouse Delux, Teclado Tech
- CPU: Procesador Pentium Dual Core
- Memoria RAM: 3 GB

- Placa: DG4RQ
- Disco Duro: 1 Tera

Todo en Uno HP Pavilion

Figura 97. PC Todo en uno HP

Características:

- Sistema Operativo Windows 11 Home Single Language
- Procesador Intel Core i5
- Memoria RAM 8 GB
- Disco Duro Unidad de estado sólido de 512 GB
- Cámara web integrada
- Color del Equipo Blanco
- Periféricos:
    - ✓ Teclado de computadora marca Genius, color negro
    - ✓ Mouse a juego, marca Genius, color negro

Portátil HP 17-cp2003ns

Figura 98. Portatil HP

Características:

- Sistema operativo Windows 11 Home
- Procesador AMD Ryzen 5 7520U
- Memoria RAM16 GB RAM
- Disco duro512 GB SSD
- Pantalla43,9 cm (17,3 pulg.), FHD (1920 x 1080)
- Tarjeta GráficaGráficos AMD Radeon

Laptop Asus X541UA

Figura 99. Laptop Asus

Características:

- Computadora portátil Concha Gris
- Intel® Core™ i5 i5-7200U 2.5 GHz
- 39.6 cm (15.6") HD 1366 x 768 Pixeles Retroiluminación LED Brillo 16:9
- 8 GB DDR4-SDRAM 2133 MHz
- 1 TB Unidad de disco duro DVD Super Multi
- Intel® HD Graphics 620
- Wi-Fi 4 (802.11n) Ethernet 10,100 Mbit/s Bluetooth 4.0
- 36 Wh 45 W
- Windows 10 64-bit

Impresora Multifuncional Epson EcoTank L3150

Impresora Epson

- Sistema de tanque de tinta de super alta capacidad y economía
- Costo de impresión ultra bajo
- Inalámbrica

III.1.3.3.- Considerar Distancias y tipos de conectores

III.1.3.3.1.- Estimación total de la infraestructura física

La estimación de la distancia de la infraestructura se realizó tanto de manera física con un dispositivo de medida como con la ayuda de los planos dispuestos para este trabajo.

Para la estimación que se utilizara la herramienta metro se midió distancia por distancia tomando en

cuenta por donde pasara el cableado detallado en el plano de la clínica.

La altura desde la Planta baja es de 4 metros, a partir de aquí las demás plantas son de 3.50 metros, se está respetando la escala que nos da el plano lo cual es 1:47.

Origen	Destino	Tipo de cable	Metros	Tipo
Planta Baja Cable cat 5e: 754mts y rj45 73, Fibra Óptica: 35mts y SC 7				
Router Clinica Gi0/3/0	Switch Principal Gi9/1	Fibra Óptica SC	1	Monomodo
Router Clinica Console	Consola RS 323	Cable consola	1	---
Switch Principal Fa0/1	Serv Central Tel F0	Categoría 5e	1	Normal
Switch Principal Gi4/1	Switch Fibra PB Gi4/1	Fibra Óptica SC	1	Monomodo
Switch Principal Gi5/1	Switch Fibra P2 Gi4/1	Fibra Óptica SC	10	Monomodo
Switch Principal Gi6/1	Switch Fibra P1 Gi6/1	Fibra Óptica SC	7	Monomodo
Switch Principal Gi7/1	Switch Fibra P3 Gi4/1	Fibra Óptica SC	14	Monomodo
Switch Principal Gi9/1	RouterClinica Gi0/3/0	Fibra Óptica SC	1	Monomodo
Switch Fibra PB Fa0/1	Switch PB Fa0/24	Categoría 5e	1	Cruzado
Switch Fibra PB Fa2/1	Patch Panel1 J21	Categoría 5e	1	Normal
Switch Fibra PB Fa3/1	Patch Panel1 J20	Categoría 5e	1	Normal
Switch Fibra PB Gi4/1	Switch Principal Gi4/1	Fibra Óptica SC	1	Monomodo
Switch Fibra PB Fa5/1	Patch Panel1 J19	Categoría 5e	1	Normal
Switch Fibra PB Fa6/1	Patch Panel1 J18	Categoría 5e	1	Normal
Switch Fibra PB Fa7/1	Patch Panel1 J17	Categoría 5e	1	Normal
Switch Fibra PB Fa8/1	Patch Panel1 J16	Categoría 5e	1	Normal
Switch Fibra PB Fa9/1	Patch Panel1 J15	Categoría 5e	1	Normal
Switch PB Fa0/2	Patch Panel1 J2	Categoría 5e	1	Normal
Switch PB Fa0/3	Patch Panel1 J3	Categoría 5e	1	Normal
Switch PB Fa0/4	Patch Panel1 J4	Categoría 5e	1	Normal
Switch PB Fa0/5	Patch Panel1 J5	Categoría 5e	1	Normal
Switch PB Fa0/6	Patch Panel1 J6	Categoría 5e	1	Normal
Switch PB Fa0/7	Patch Panel1 J7	Categoría 5e	1	Normal
Switch PB Fa0/8	Patch Panel1 J8	Categoría 5e	1	Normal
Switch PB Fa0/9	Patch Panel1 J9	Categoría 5e	1	Normal
Switch PB Fa0/10	Patch Panel1 J10	Categoría 5e	1	Normal
Switch PB Fa0/11	Patch Panel1 J11	Categoría 5e	1	Normal
Switch PB Fa0/12	Patch Panel1 J12	Categoría 5e	1	Normal
Switch PB Fa0/13	Patch Panel1 J13	Categoría 5e	1	Normal
Switch PB Fa0/14	Patch Panel1 J14	Categoría 5e	1	Normal
Switch PB Fa0/22	Patch Panel1 J23	Categoría 5e	1	Normal
Switch PB Fa0/23	Patch Panel1 J24	Categoría 5e	1	Normal
Patch Pane1 PD2	R-3 PD2	Categoría 5e	26	Normal
Patch Pane1 PD3	R-3 PD3	Categoría 5e	26	Normal
Patch Pane1 PD4	R-8 PD1	Categoría 5e	18	Normal
Patch Pane1 PD5	R-7 PD1	Categoría 5e	21	Normal
Patch Pane1 PD6	R-6 PD1	Categoría 5e	35	Normal
Patch Pane1 PD7	R-5 PD1	Categoría 5e	31	Normal

Patch Pane1 PD8	R-4 PD1	Categoría 5e	31	Normal
Patch Pane1 PD9	R-2 PD1	Categoría 5e	8	Normal
Patch Pane1 PD10	R-1 PD2	Categoría 5e	5	Normal
Patch Pane1 PD11	R-1 PD1	Categoría 5e	5	Normal
Patch Pane1 PD12	R-9 PD1	Categoría 5e	34	Normal
Patch Pane1 PD13	R-9 PD2	Categoría 5e	34	Normal
Patch Pane1 PD14	R-4 PD2	Categoría 5e	31	Normal
Patch Pane1 PD15	R-3 PD1	Categoría 5e	26	Normal
Patch Pane1 PD16	R-4 PD3	Categoría 5e	31	Normal
Patch Pane1 PD17	R-5 PD2	Categoría 5e	31	Normal
Patch Pane1 PD18	R-6 PD2	Categoría 5e	35	Normal
Patch Pane1 PD19	R-7 PD2	Categoría 5e	21	Normal
Patch Pane1 PD20	R-8 PD3	Categoría 5e	18	Normal
Patch Pane1 PD21	R-1 PD3	Categoría 5e	5	Normal
Patch Pane1 PD23	R-8 PD2	Categoría 5e	18	Normal
Patch Pane1 PD24	R-3 PD4	Categoría 5e	26	Normal
Altura Techo 4 x 20 = 80mts				
R-4 J2-PD2	PB-REC-1-PC	Categoría 5e	4	Normal
R-3 J2-PD2	PB-ADM-1-PC	Categoría 5e	5	Normal
R-3 J3-PD3	PB-ADM-2-PC	Categoría 5e	3	Normal
R-4 J1-PD1	PB-CONS-1-LP	Categoría 5e	5	Normal
R-5 J1-PD1	PB-CONS-2-LP	Categoría 5e	4	Normal
R-6 J1-PD1	PB-CONS-3-LP	Categoría 5e	5	Normal
R-7 J1-PD1	PB-CONS-4-LP	Categoría 5e	5	Normal
R-8 J1-PD1	PB-CONS-5-LP	Categoría 5e	5	Normal
R-9 J1-PD1	PB-AT-1-PC	Categoría 5e	4	Normal
R-1 J1-PD1	PB-AT-2-PC	Categoría 5e	4	Normal
R-1 J2-PD2	PB-AT-3-PC	Categoría 5e	3	Normal
R-2 J1-PD1	PB-AT-4-PC	Categoría 5e	6	Normal
R-9 J2-PD2	PB-EMG-1-LP	Categoría 5e	4	Normal
R-8 J2-PD2	PB-PER-1-AP	Categoría 5e	3	Normal
R-3 J4-PD4	PB-PAC-1-AP	Categoría 5e	5	Normal
R-3 J1-PD1	PB-ADM-3-PRINT	Categoría 5e	2	Normal
R-4 J3-PD3	PB-CONS-6-PRINT	Categoría 5e	5	Normal
R-5 J2-PD2	PB-CONS-7-PRINT	Categoría 5e	5	Normal
R-6 J2-PD2	PB-CONS-8-PRINT	Categoría 5e	5	Normal
R-7 J2-PD2	PB-CONS-9-PRINT	Categoría 5e	5	Normal
R-8 J3-PD3	PB-CONS-10-PRINT	Categoría 5e	5	Normal
R-1 J3-PD3	PB-AT-5-PRINT	Categoría 5e	5	Normal

Tabla 83. Estimación total planta baja

Origen	Destino	Tipo de cable	Metros	Tipo
Primer Piso 277mts, rj45 53, SC 1				
Switch Fibra P1 Fa0/1	Switch P1 Fa0/24	Categoría 5e	1	Cruzado
Switch Fibra P1 Gi 6/1	Switch Principal Gi6/1	Fibra Óptica SC	7	Monomodo

Switch Fibra P1 Fa 8/1	Patch Panel2 J12	Categoría 5e	1	Normal
Switch Fibra P1 Fa 9/1	Patch Panel2 J11	Categoría 5e	1	Normal
Switch P1 Fa 0/1	Patch Panel2 J1	Categoría 5e	1	Normal
Switch P1 Fa 0/2	Patch Panel2 J2	Categoría 5e	1	Normal
Switch P1 Fa 0/3	Patch Panel2 J3	Categoría 5e	1	Normal
Switch P1 Fa 0/4	Patch Panel2 J4	Categoría 5e	1	Normal
Switch P1 Fa 0/5	Patch Panel2 J5	Categoría 5e	1	Normal
Switch P1 Fa 0/6	Patch Panel2 J6	Categoría 5e	1	Normal
Switch P1 Fa 0/7	Patch Panel2 J7	Categoría 5e	1	Normal
Switch P1 Fa 0/8	Patch Panel2 J8	Categoría 5e	1	Normal
Switch P1 Fa 0/9	Patch Panel2 J9	Categoría 5e	1	Normal
Switch P1 Fa 0/10	Patch Panel2 J10	Categoría 5e	1	Normal
Switch P1 Fa0/21	Patch Panel2 J23	Categoría 5e	1	Normal
Switch P1 Fa0/23	Patch Panel2 J24	Categoría 5e	1	Normal
Patch Panel2 PD1	R-15 PD2	Categoría 5e	14	Normal
Patch Panel2 PD2	R-13 PD1	Categoría 5e	13	Normal
Patch Panel2 PD3	R-15 PD1	Categoría 5e	14	Normal
Patch Panel2 PD4	R-11 PD2	Categoría 5e	29	Normal
Patch Panel2 PD5	R-12 PD2	Categoría 5e	27	Normal
Patch Panel2 PD6	R-11 PD1	Categoría 5e	29	Normal
Patch Panel2 PD7	R-12 PD1	Categoría 5e	27	Normal
Patch Panel2 PD8	R-14 PD1	Categoría 5e	5	Normal
Patch Panel2 PD9	R-14 PD3	Categoría 5e	5	Normal
Patch Panel2 PD10	R-10 PD1	Categoría 5e	3	Normal
Patch Panel2 PD11	R-10 PD2	Categoría 5e	1	Normal
Patch Panel2 PD12	R-14 PD4	Categoría 5e	1	Normal
Patch Panel2 PD23	R-14 PD2	Categoría 5e	5	Normal
Patch Panel2 PD24	R-13 PD2	Categoría 5e	13	Normal
Altura Techo 3,50 x 12= 42mts				
R-15 J2-PD2	P1-IT-7-PC	Categoría 5e	2	Normal
R-13 J1-PD1	P1-IT-6-PC	Categoría 5e	5	Normal
R-15 J1-PD1	P1-IT-5-PC	Categoría 5e	2	Normal
R-11 J2-PD2	P1-IT-4-PC	Categoría 5e	8	Normal
R-12 J2-PD2	P1-IT-3-PC	Categoría 5e	3	Normal
R-11 J1-PD1	P1-IT-2-PC	Categoría 5e	8	Normal
R-12 J1-PD1	P1-IT-1-PC	Categoría 5e	3	Normal
R-14 J1-PD1	P1-ENF-1-PC	Categoría 5e	5	Normal
R-14 J3-PD3	P1-ENF-2-PC	Categoría 5e	5	Normal
R-10 J1-PD1	P1-TRI-1-PC	Categoría 5e	2	Normal
R-10 J2-PD2	P1-TRI-2-PRINT	Categoría 5e	8	Normal
R-14 J4-PD4	P1-IT-8-PRINT	Categoría 5e	6	Normal
R-14 J2-PD2	P1-PER-2-AP	Categoría 5e	10	Normal
R-13 J2-PD2	P1-PAC-2-AP	Categoría 5e	5	Normal

Tabla 84. Estimación total primer piso

Origen	Destino	Tipo de cable	Metros	Tipo
Segundo Piso 292mts, rj45 43, SC 1				
Switch Fibra P2 Fa0/1	Switch P2	Categoría 5e	1	Cruzado
Switch Fibra P2 Gi4/1	Switch Principal	Fibra Óptica SC	10	Monomodo
Switch Fibra P2 Fa9/1	Patch Panel3 J10	Categoría 5e	1	Normal
Switch P2 Fa0/1	Patch Panel3 J1	Categoría 5e	1	Normal
Switch P2 Fa0/2	Patch Panel3 J2	Categoría 5e	1	Normal
Switch P2 Fa0/3	Patch Panel3 J3	Categoría 5e	1	Normal
Switch P2 Fa0/4	Patch Panel3 J4	Categoría 5e	1	Normal
Switch P2 Fa0/5	Patch Panel3 J5	Categoría 5e	1	Normal
Switch P2 Fa0/6	Patch Panel3 J6	Categoría 5e	1	Normal
Switch P2 Fa0/7	Patch Panel3 J7	Categoría 5e	1	Normal
Switch P2 Fa0/8	Patch Panel3 J8	Categoría 5e	1	Normal
Switch P2 Fa0/9	Patch Panel3 J9	Categoría 5e	1	Normal
Switch P2 Fa0/22	Patch Panel3 J23	Categoría 5e	1	Normal
Switch P2 Fa0/23	Patch Panel3 J24	Categoría 5e	1	Normal
Switch P2 Fa0/24	Switch Fibra P2 Fa0/1	Categoría 5e	1	Cruzado
Patch Panel3 PD1	R-21 PD1	Categoría 5e	22	Normal
Patch Panel3 PD2	R-20 PD1	Categoría 5e	26	Normal
Patch Panel3 PD3	R-21 PD2	Categoría 5e	22	Normal
Patch Panel3 PD4	R-20 PD2	Categoría 5e	26	Normal
Patch Panel3 PD5	R-17 PD1	Categoría 5e	14	Normal
Patch Panel3 PD6	R-18 PD1	Categoría 5e	13	Normal
Patch Panel3 PD7	R-17 PD2	Categoría 5e	14	Normal
Patch Panel3 PD8	R-16 PD1	Categoría 5e	4	Normal
Patch Panel3 PD9	R-19 PD1	Categoría 5e	5	Normal
Patch Panel3 PD10	R-19 PD3	Categoría 5e	5	Normal
Patch Panel3 PD23	R-19 PD2	Categoría 5e	5	Normal
Patch Panel3 PD24	R-18 PD2	Categoría 5e	13	Normal
Altura Techo 3,50 x 10= 35mts				
R-21 J1-PD1	P2-IT-9-PC	Categoría 5e	5	Normal
R-20 J1-PD1	P2-IT-10-PC	Categoría 5e	7	Normal
R-21 J2-PD2	P2-IT-11-PC	Categoría 5e	4	Normal
R-20 J2-PD2	P2-IT-12-PC	Categoría 5e	7	Normal
R-17 J1-PD1	P2-IT-13-PC	Categoría 5e	4	Normal
R-18 J1-PD1	P2-IT-14-PC	Categoría 5e	5	Normal
R-17 J2-PD2	P2-IT-15-PC	Categoría 5e	4	Normal
R-16 J1-PD1	P2-TRI-3-LP	Categoría 5e	3	Normal
R-19 J1-PD1	P2-ENF-3-PC	Categoría 5e	4	Normal
R-19 J3-PD3	P2-IT-16-PRINT	Categoría 5e	8	Normal
R-19 J2-PD2	P2-PER-3-AP	Categoría 5e	10	Normal
R-18 J2-PD2	P2-PAC-3-AP	Categoría 5e	6	Normal

Tabla 85. Estimación total segundo piso

Origen	Destino	Tipo de cable	Metros	Tipo

Tercer Piso 773mts, rj45 74, SC 1				
Switch Fibra P3 Fa0/1	Switch P3 Fa0/24	Categoría 5e	1	Cruzado
Switch Fibra P3 Gi4/1	Switch Principal Gi7/1	Fibra Óptica SC	14	Monomodo
Switch Fibra P3 Fa6/1	Patch Panel4 J22	Categoría 5e	1	Normal
Switch Fibra P3 Fa7/1	Patch Panel4 J21	Categoría 5e	1	Normal
Switch Fibra P3 Fa8/1	Patch Panel4 J20	Categoría 5e	1	Normal
Switch Fibra P3 Fa9/1	Patch Panel4 J19	Categoría 5e	1	Normal
Switch P3 Fa0/1	Patch Panel4 J1	Categoría 5e	1	Normal
Switch P3 Fa0/2	Patch Panel4 J2	Categoría 5e	1	Normal
Switch P3 Fa0/3	Patch Panel4 J3	Categoría 5e	1	Normal
Switch P3 Fa0/4	Patch Panel4 J4	Categoría 5e	1	Normal
Switch P3 Fa0/5	Patch Panel4 J5	Categoría 5e	1	Normal
Switch P3 Fa0/6	Patch Panel4 J6	Categoría 5e	1	Normal
Switch P3 Fa0/7	Patch Panel4 J7	Categoría 5e	1	Normal
Switch P3 Fa0/8	Patch Panel4 J8	Categoría 5e	1	Normal
Switch P3 Fa0/9	Patch Panel4 J9	Categoría 5e	1	Normal
Switch P3 Fa0/10	Patch Panel4 J10	Categoría 5e	1	Normal
Switch P3 Fa0/11	Patch Panel4 J11	Categoría 5e	1	Normal
Switch P3 Fa0/12	Patch Panel4 J12	Categoría 5e	1	Normal
Switch P3 Fa0/13	Patch Panel4 J13	Categoría 5e	1	Normal
Switch P3 Fa0/14	Patch Panel4 J14	Categoría 5e	1	Normal
Switch P3 Fa0/15	Patch Panel4 J15	Categoría 5e	1	Normal
Switch P3 Fa0/16	Patch Panel4 J16	Categoría 5e	1	Normal
Switch P3 Fa0/17	Patch Panel4 J17	Categoría 5e	1	Normal
Switch P3 Fa0/18	Patch Panel4 J18	Categoría 5e	1	Normal
Switch P3 Fa0/22	Patch Panel4 J23	Categoría 5e	1	Normal
Switch P3 Fa0/23	Patch Panel4 J24	Categoría 5e	1	Normal
Switch P3 Fa0/24	Switch Fibra P3 Fa0/1	Categoría 5e	1	Cruzado
Patch Panel4 PD1	R-22 PD1	Categoría 5e	29	Normal
Patch Panel4 PD2	R-23 PD1	Categoría 5e	23	Normal
Patch Panel4 PD3	R-22 PD2	Categoría 5e	29	Normal
Patch Panel4 PD4	R-22 PD3	Categoría 5e	29	Normal
Patch Panel4 PD5	R-23 PD2	Categoría 5e	23	Normal
Patch Panel4 PD6	R-24 PD1	Categoría 5e	17	Normal
Patch Panel4 PD7	R-25 PD1	Categoría 5e	13	Normal
Patch Panel4 PD8	R-24 PD2	Categoría 5e	17	Normal
Patch Panel4 PD9	R-25 PD2	Categoría 5e	13	Normal
Patch Panel4 PD10	R-26 PD1	Categoría 5e	14	Normal
Patch Panel4 PD11	R-27 PD1	Categoría 5e	3	Normal
Patch Panel4 PD12	R-25 PD3	Categoría 5e	13	Normal
Patch Panel4 PD13	R-30 PD1	Categoría 5e	10	Normal
Patch Panel4 PD14	R-30 PD2	Categoría 5e	10	Normal
Patch Panel4 PD15	R-29 PD1	Categoría 5e	20	Normal
Patch Panel4 PD16	R-29 PD2	Categoría 5e	20	Normal
Patch Panel4 PD17	R-28 PD1	Categoría 5e	25	Normal

Patch Panel4 PD18	R-28 PD2	Categoría 5e	25	Normal
Patch Panel4 PD19	R-28 PD3	Categoría 5e	23	Normal
Patch Panel4 PD20	R-30 PD3	Categoría 5e	10	Normal
Patch Panel4 PD21	R-29 PD3	Categoría 5e	20	Normal
Patch Panel4 PD22	R-25 PD4	Categoría 5e	13	Normal
Patch Panel4 PD23	R-26 PD2	Categoría 5e	12	Normal
Patch Panel4 PD24	R-24 PD3	Categoría 5e	17	Normal
Altura Techo 3,50 x 22= 77mts				
R-22 J1-PD1	P3-AT-6-PC	Categoría 5e	6	Normal
R-23 J1-PD1	P3-PED-1-PC	Categoría 5e	5	Normal
R-22 J2-PD2	P3-PED-2-PC	Categoría 5e	4	Normal
R-22 J3-PD3	P3-PED-3-PC	Categoría 5e	8	Normal
R-23 J2-PD2	P3-PED-4-PRINT	Categoría 5e	3	Normal
R-24 J1-PD1	P3-IT-17-PC	Categoría 5e	4	Normal
R-25 J1-PD1	P3-IT-18-PC	Categoría 5e	6	Normal
R-24 J2-PD2	P3-IT-19-PC	Categoría 5e	5	Normal
R-25 J2-PD2	P3-IT-20-PC	Categoría 5e	3	Normal
R-26 J1-PD1	P3-IT-21-PC	Categoría 5e	5	Normal
R-27 J1-PD1	P3-TRI-4-PC	Categoría 5e	3	Normal
R-25 J3-PD3	P3-ENF-4-PC	Categoría 5e	5	Normal
R-30 J1-PD1	P3-FAR-1-PC	Categoría 5e	10	Normal
R-30 J2-PD2	P3-EST-1-PC	Categoría 5e	9	Normal
R-29 J1-PD1	P3-EST-2-PC	Categoría 5e	6	Normal
R-29 J2-PD2	P3-EST-3-PC	Categoría 5e	4	Normal
R-28 J1-PD1	P3-CON-1-PC	Categoría 5e	5	Normal
R-28 J2-PD2	P3-CON-2-PC	Categoría 5e	8	Normal
R-28 J3-PD3	P3-CON-3-PRINT	Categoría 5e	6	Normal
R-30 J3-PD3	P3-FAR-2-PRINT	Categoría 5e	10	Normal
R-29 J3-PD3	P3-EST-4-PRINT	Categoría 5e	4	Normal
R-25 J4-PD4	P3-IT-22-PRINT	Categoría 5e	4	Normal
R-26 J4-PD2	P3-PER-4-AP	Categoría 5e	3	Normal
R-24 J4-PD3	P3-PAC-4-AP	Categoría 5e	5	Normal

Tabla 86. Estimación total tercer piso

Dado que se está utilizando una topología de red en árbol, el Rack de piso ubicado en la planta baja actuará como nodo central de la red. Desde este punto, se establecerán conexiones de fibra óptica hacia las tres plantas superiores. Debido a la distribución vertical del edificio, cada tramo de cableado de fibra óptica será progresivamente más largo conforme se ascienda de piso, lo cual responde a la distancia física entre el rack principal y los gabinetes de cada nivel.

III.1.3.4.- Diseño de seguridad física

III.1.3.4.1.- 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.1.3.4.1.1.- Dispositivos de prevención de incendios

Sensor

Bosch D-273TH

Figura 100. 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 101. 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 102. 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 103. 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 104. Extintor

Planta	Pulsadores	Sirenas	Sensores
Importaciones planta baja	2	2	7
Importaciones primer piso	2	2	5
Importaciones segundo piso	2	2	5
Importaciones tercer piso	2	2	5
Importaciones extensión tercer piso	1	1	3

Tabla 87. Distribución de elementos de sistema de prevención de incendios

III.1.3.4.1.2.- Planos sistema de prevención de incendios

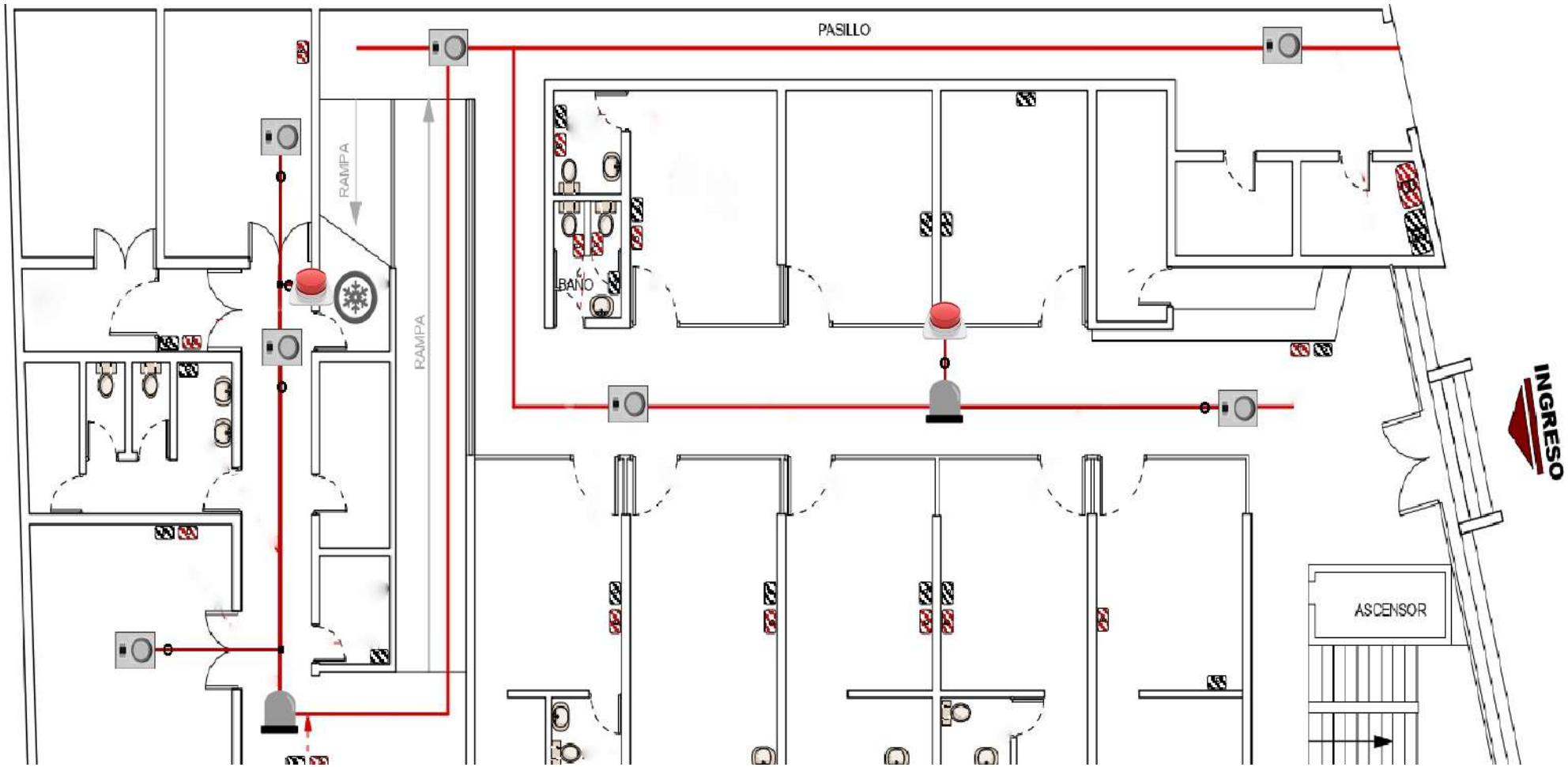

Figura 105. Sistema de prevencion Planta Baja

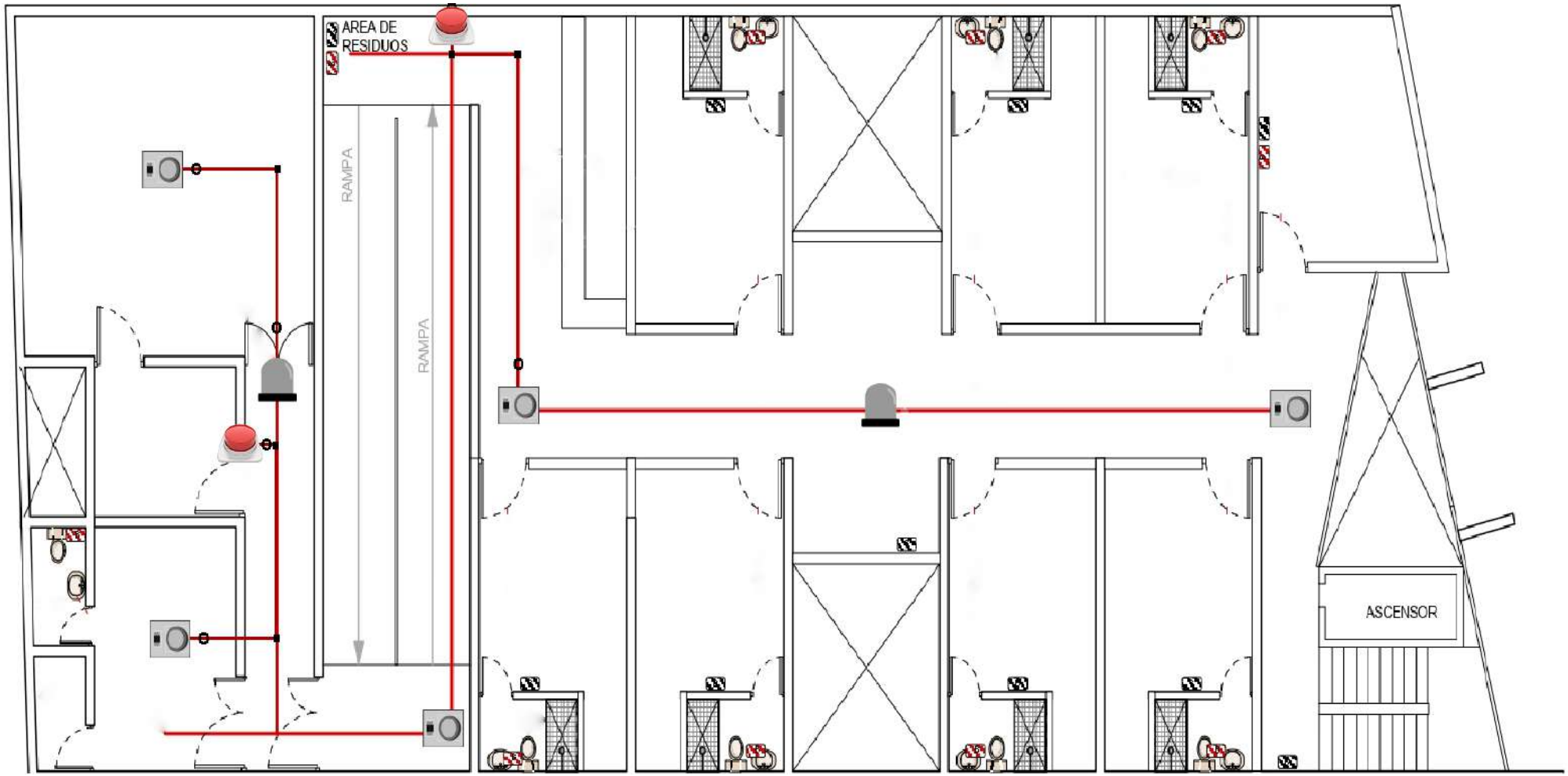

Figura 106. Sistema de prevención Primer Piso

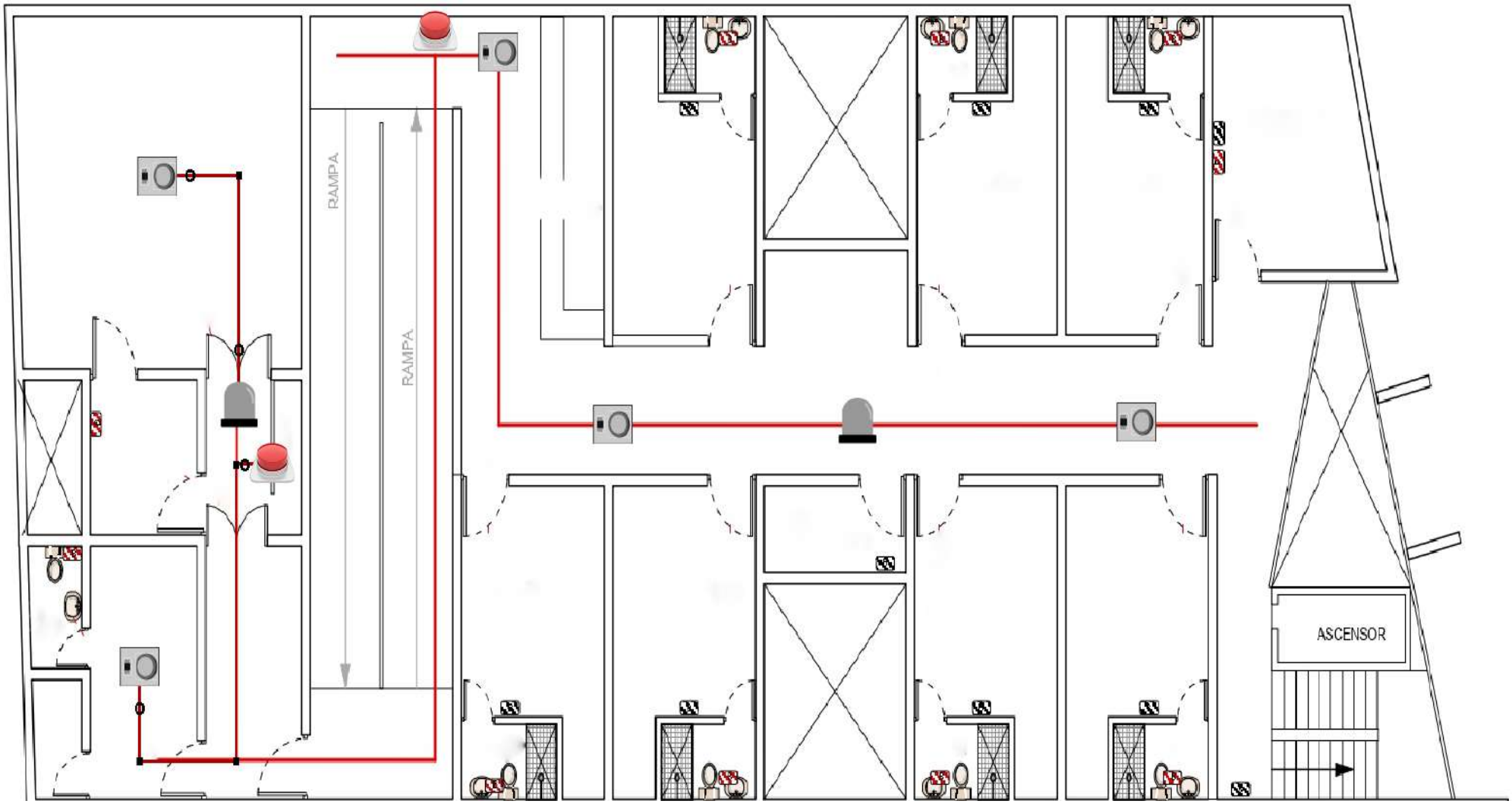

Figura 107. Sistema de prevención Segundo Piso

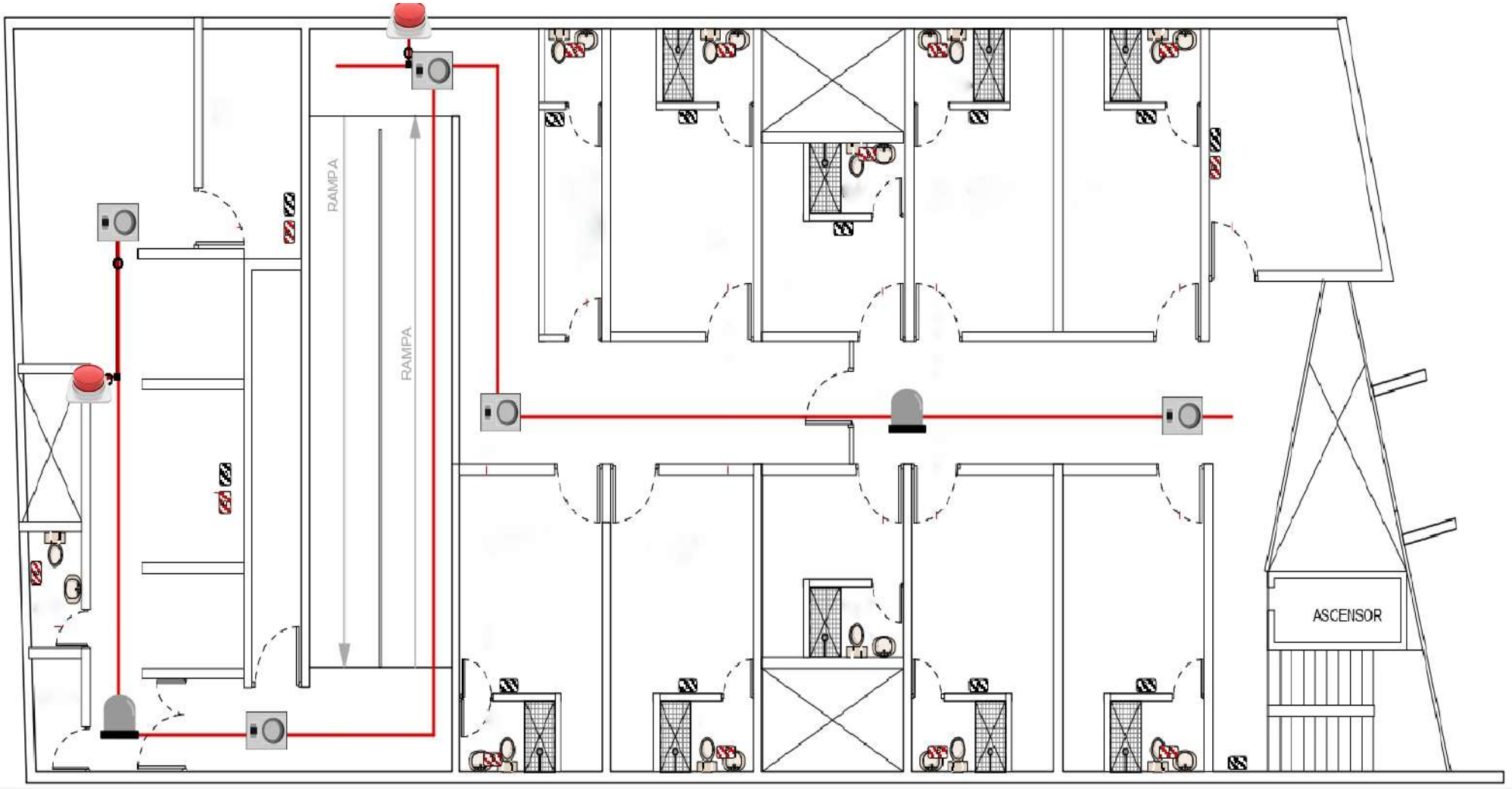

Figura 108. Sistema de prevención Tercer Piso

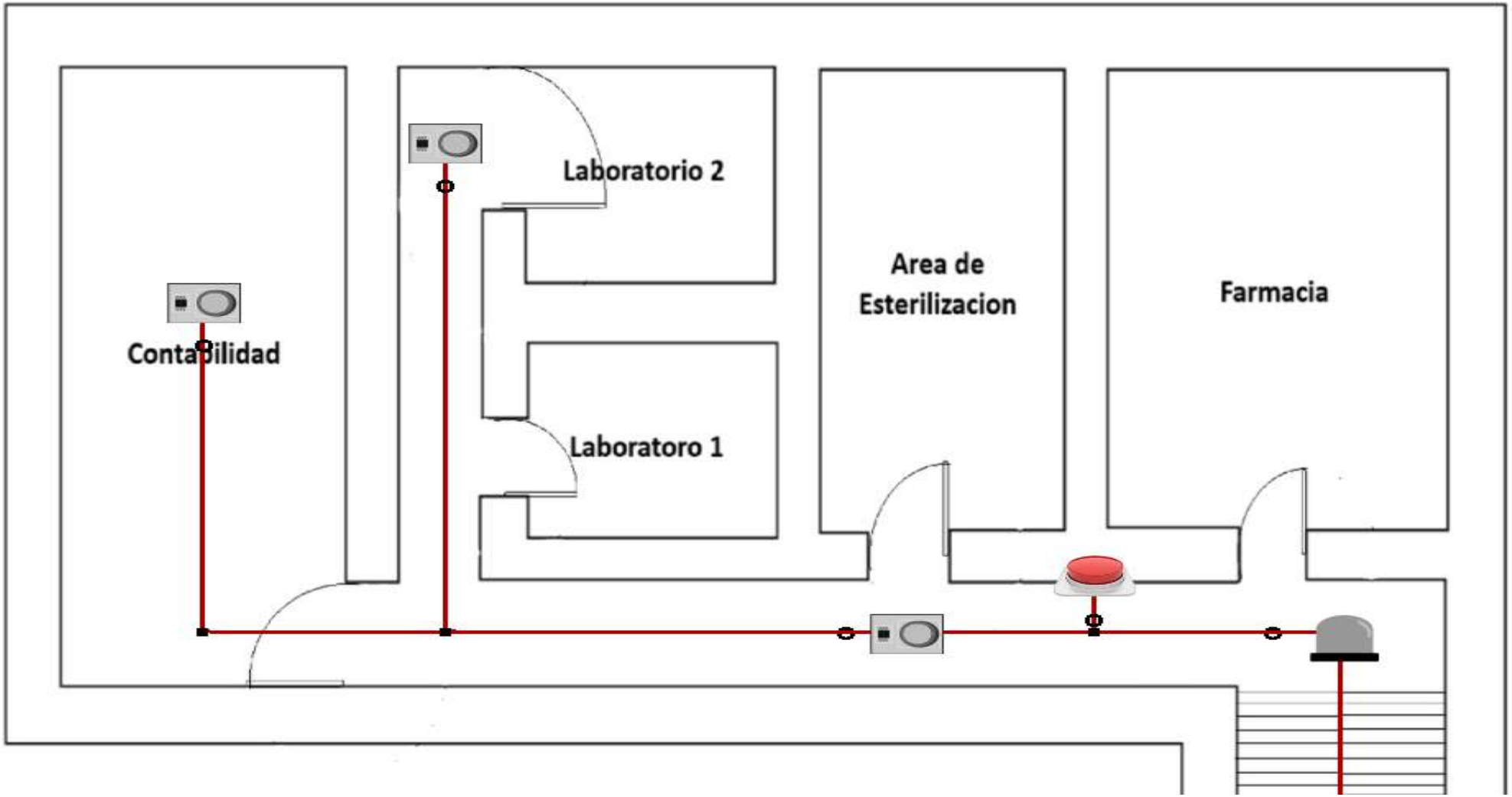

Figura 109. Sistema de prevención Extensión Tercer Piso

III.1.4.- Fase 4: Probar, optimizar y documentar diseño

III.1.4.1.- Simulación del diseño en Packet tracer

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.

Separación de la red por Áreas y Vlans:

Internación	(VLAN10)
Pacientes	(VLAN20)
Personal de salud	(VLAN30)
Consultorios	(VLAN40)
Administración	(VLAN50)
Enfermería	(VLAN60)
Recepción	(VLAN70)
Emergencias	(VLAN80)
Área Tercerizada	(VLAN90)
Terapia Intensiva	(VLAN100)
Pediatría	(VLAN110)
Farmacia	(VLAN120)
Esterilización	(VLAN130)
Contabilidad	(VLAN140)
Servidores	(VLAN150)

Se presenta el diagrama final en Cisco Packet Tracer, donde se configura la segmentación por áreas y VLAN. Cada color representa una VLAN diferente, correspondiente a secciones como administración, emergencias, internación, consultorios, entre otras. En la red se integran PCs, impresoras, servidores, routers, switches, puntos de acceso y dispositivos móviles, conectados mediante fibra óptica y cableado Ethernet.

A partir de este diseño se realizarán las configuraciones de las VLANs, así como pruebas de conectividad (ping) y comunicación entre redes, utilizando el DNS público de Google. También se aplicarán reglas de denegación de acceso entre determinadas VLANs, diferenciando las redes privadas y públicas, con el fin de mantener la seguridad y el control del tráfico dentro de la infraestructura.

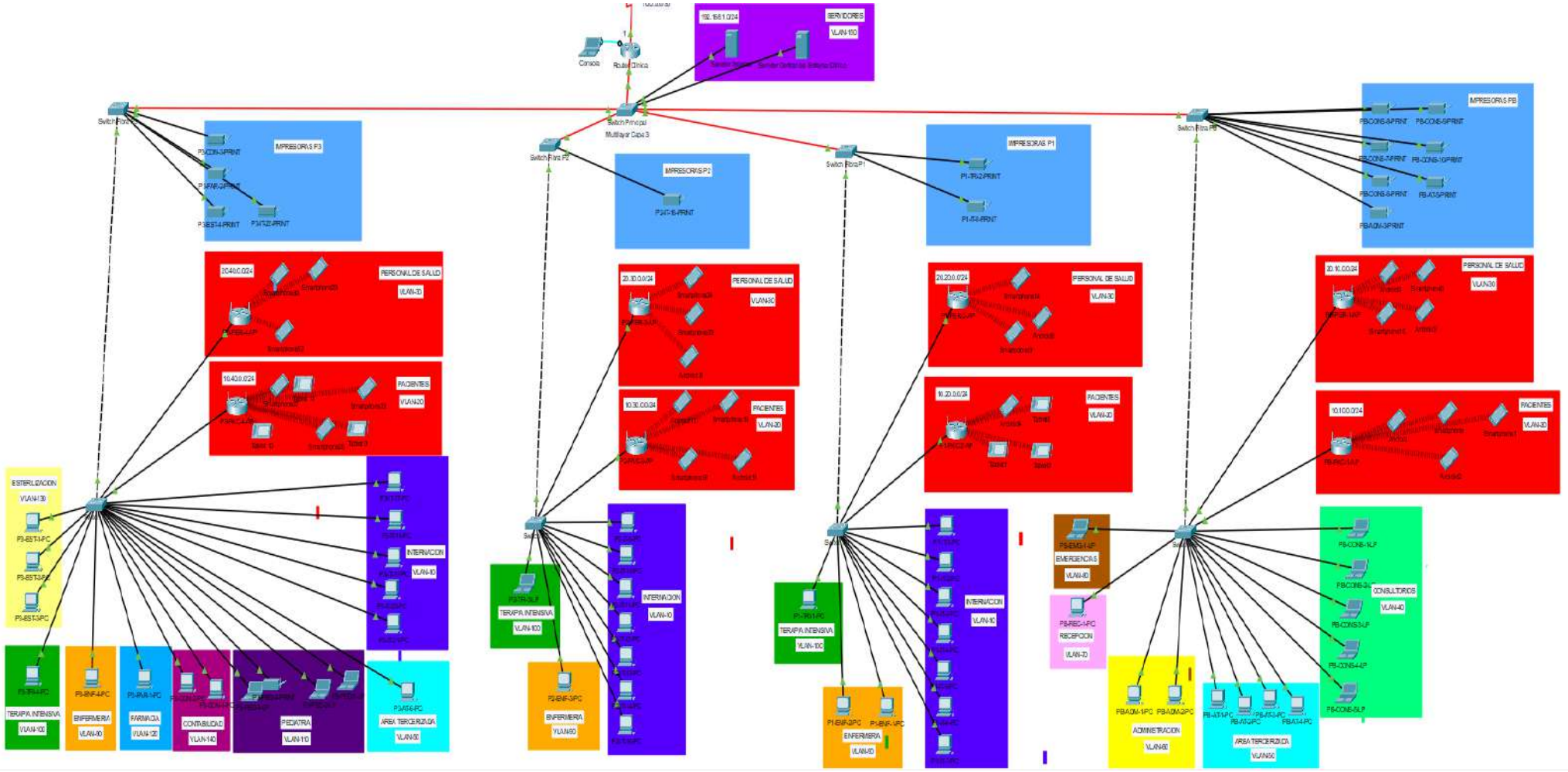

Figura 110. Prototipo de Red por Áreas y VLAN

En el tercer piso, las impresoras de las diferentes áreas se encuentran interconectadas al Switch de Fibra P3, permitiendo una administración centralizada y eficiente del servicio de impresión. Cada equipo está configurado dentro de su respectiva VLAN (140, 120, 130 y 10), garantizando el aislamiento del tráfico y la comunicación segura entre sectores. Las PC de cada área tendrán acceso a estas impresoras según su VLAN correspondiente, permitiendo la impresión directa y controlada dentro de la red.

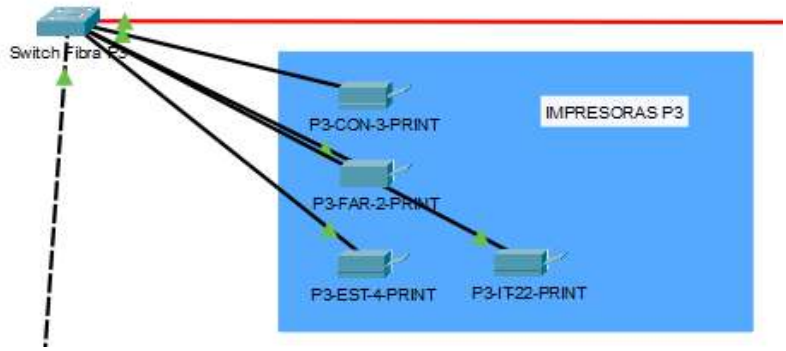

Figura 111. VLAN140,120,130,10 Impresoras

En el segundo piso, la impresora asignada a la VLAN 10 se encuentra conectada al Switch de Fibra P2, asegurando una comunicación estable y controlada dentro de la red. Esta configuración permite que las PC pertenecientes a la misma VLAN puedan acceder a la impresora para la realización de trabajos de impresión, manteniendo la segmentación y seguridad del tráfico en el entorno de red.

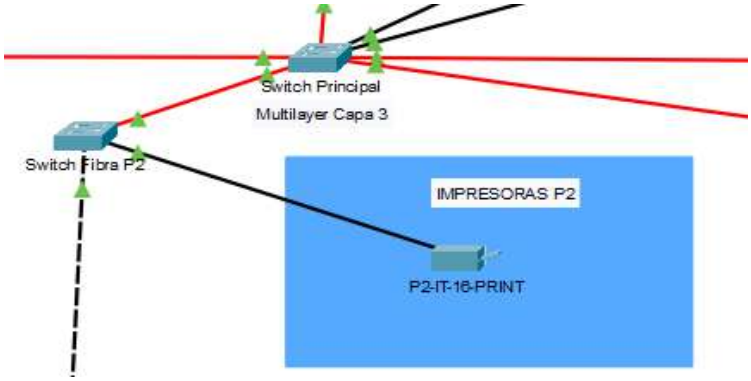

Figura 112. VLAN 10 Impresora

En el primer piso, las impresoras pertenecientes a las VLAN 100 y 10 se encuentran conectadas al Switch de Fibra P1, permitiendo una gestión eficiente y segmentada del servicio de impresión. Cada impresora está asignada a su respectiva VLAN, lo que garantiza la comunicación exclusiva con las PC autorizadas de cada área, asegurando así el acceso controlado y la estabilidad del tráfico en la red local.

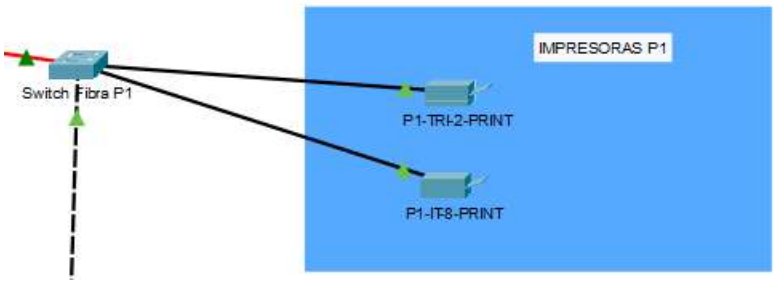

Figura 113. VLAN 100,10 Impresoras

En la planta baja, las impresoras asignadas a las VLAN 50, 60 y 40 están conectadas al Switch de Fibra PB, lo que permite una distribución ordenada y segmentada del servicio de impresión por áreas. Cada impresora está configurada dentro de su VLAN correspondiente, brindando acceso exclusivo a las PC de administración, consultorios y áreas tercerizadas, garantizando así un tráfico eficiente, seguro y una gestión centralizada de los dispositivos.

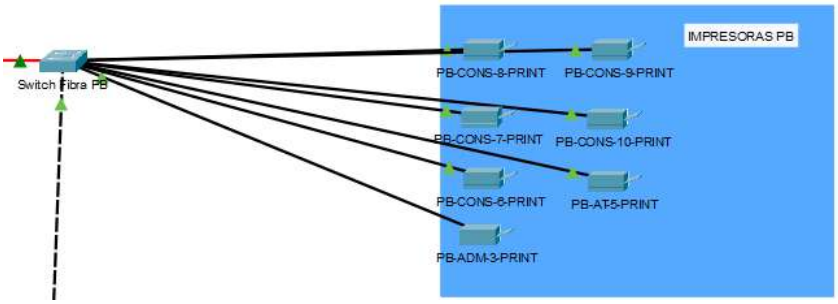

Figura 114. VLAN 50,60,40 Impresoras

Se muestra la distribución del prototipo de red por áreas y VLAN en la planta baja, primer, segundo y tercer piso del edificio. Cada nivel está segmentado mediante VLAN específicas, lo que permite una mejor organización del tráfico de red y una administración más eficiente de los recursos tecnológicos. Esta estructura asegura que los dispositivos de cada área estén correctamente conectados y comunicados dentro de su propio dominio lógico, garantizando rendimiento, seguridad y estabilidad en toda la infraestructura de red.

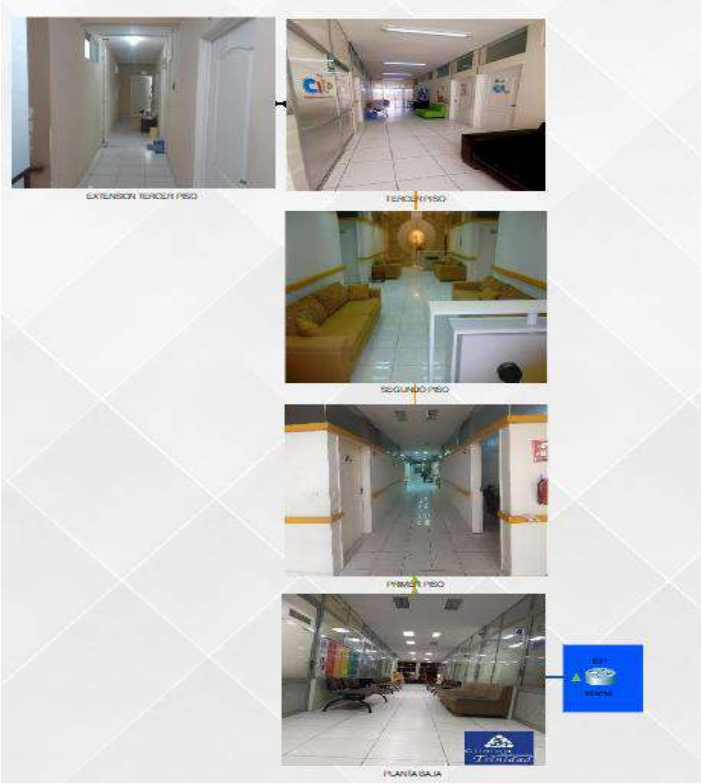

Figura 115. Prototipo de Red por Áreas y VLAN Planta Baja 1er 2do y 3er Piso

Ubicación geográfica de la red de la Clínica Santísima Trinidad Tarija

Se muestra la ubicación geográfica de la Clínica Santísima Trinidad en la ciudad de Tarija, situada en la calle Alejandro Del Carpio #850, entre las calles Ejército y Padilla. Este punto representa el área donde se implementará la infraestructura de red, permitiendo una correcta planificación y conexión de los equipos en las distintas plantas del edificio.

Figura 116. Ubicación de la Clínica Santísima Trinidad

III.1.4.1.1.- Diseño de la red Planta Baja

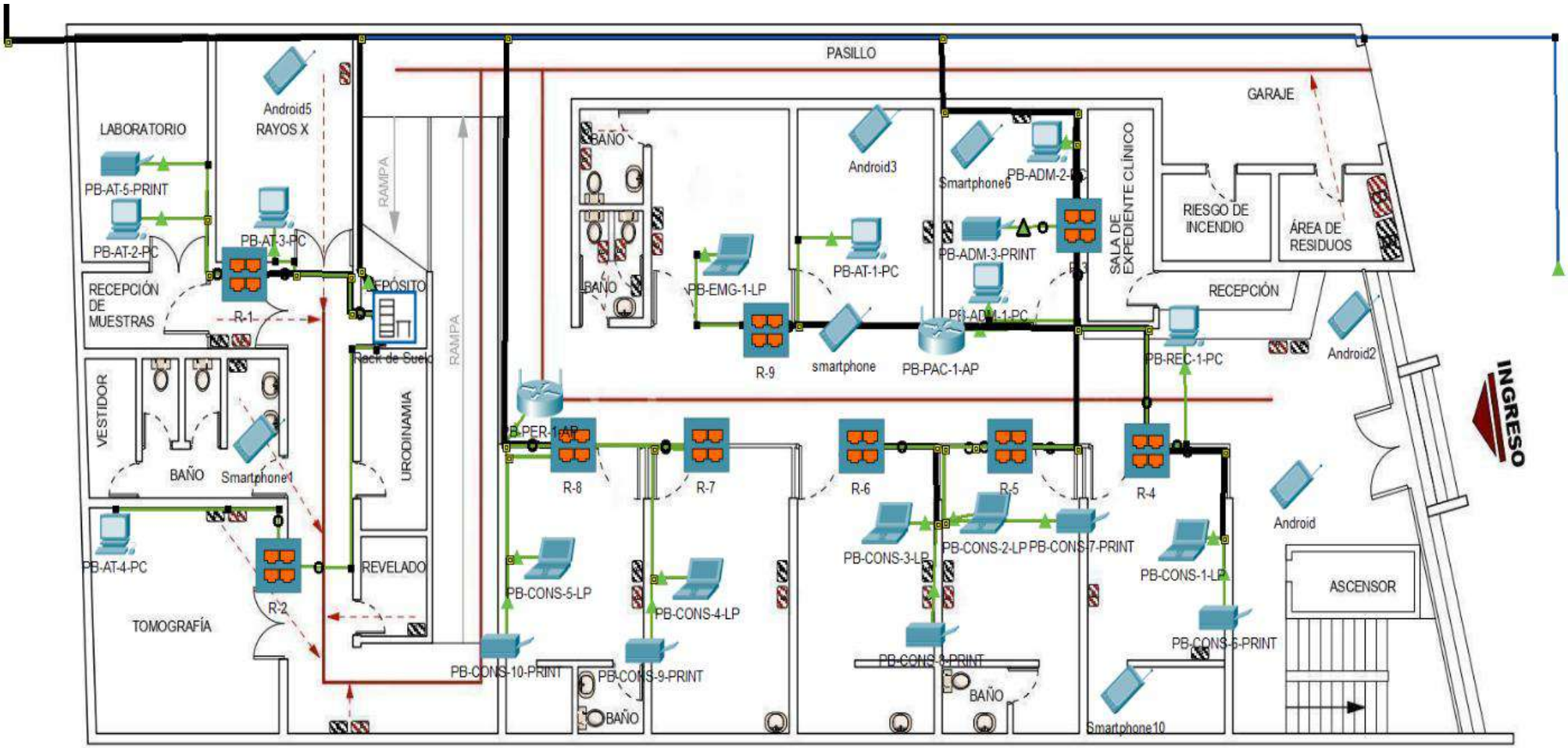

Figura 117. Simulación completa Planta Baja

Se muestra la simulación del área tercerizada ubicada en la planta baja, la cual dispone de una VLAN propia con comunicación hacia otras VLAN dentro de la red general. En esta planta, todos los equipos como computadoras, impresoras y dispositivos del personal están conectados al “Rack de Suelo”, que centraliza las conexiones y distribuye la red hacia los diferentes puntos del área. Esta infraestructura permite una gestión eficiente del tráfico de datos, asegurando la interconexión controlada entre las distintas áreas y plantas del edificio.

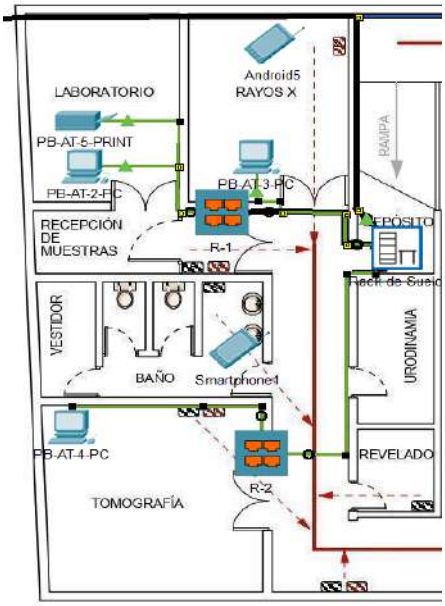

Figura 118. Simulación del Area Tercerizada

Se muestra la simulación del área de consultorios en la planta baja, conectada a una VLAN propia con enlace a otras VLAN. Los equipos informáticos se integran al Rack de Suelo, lo que permite una conexión eficiente y coordinada entre los consultorios.

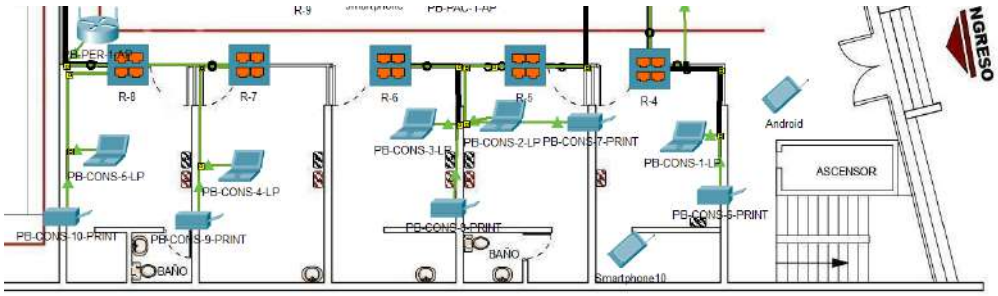

Figura 119. Simulación del Área de Consultorios

Se muestra la simulación del área de emergencias, área tercerizada, administración y recepción, todas integradas en VLANs interconectadas. Estas zonas son vitales para la atención y coordinación del personal y pacientes dentro del edificio. Además, los puntos de acceso (AP) están estratégicamente ubicados para brindar una cobertura óptima, asegurando una conexión estable tanto para el personal de salud como para los pacientes.

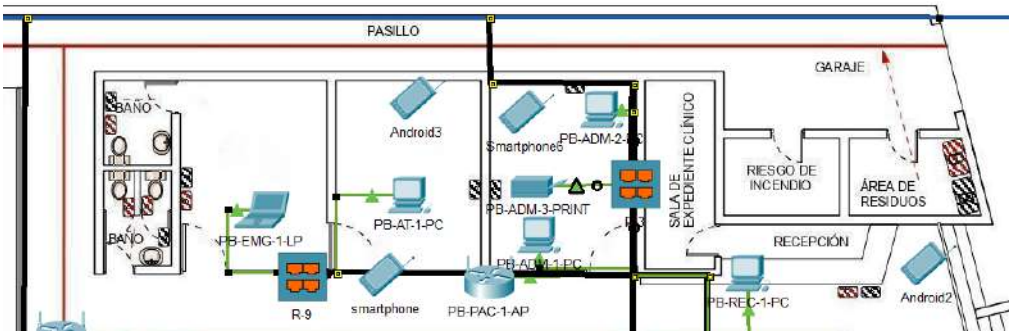

Figura 120. Simulación del Área de Emergencias, Área Tercerizada, Administración y Recepción

Se muestra la simulación del Rack de Piso, que actúa como el centro principal de la red. Contiene un patch panel, un switch de fibra óptica, dos switches cableados, un router y dos servidores, encargados de comunicar y gestionar la red con los demás gabinetes de la clínica.

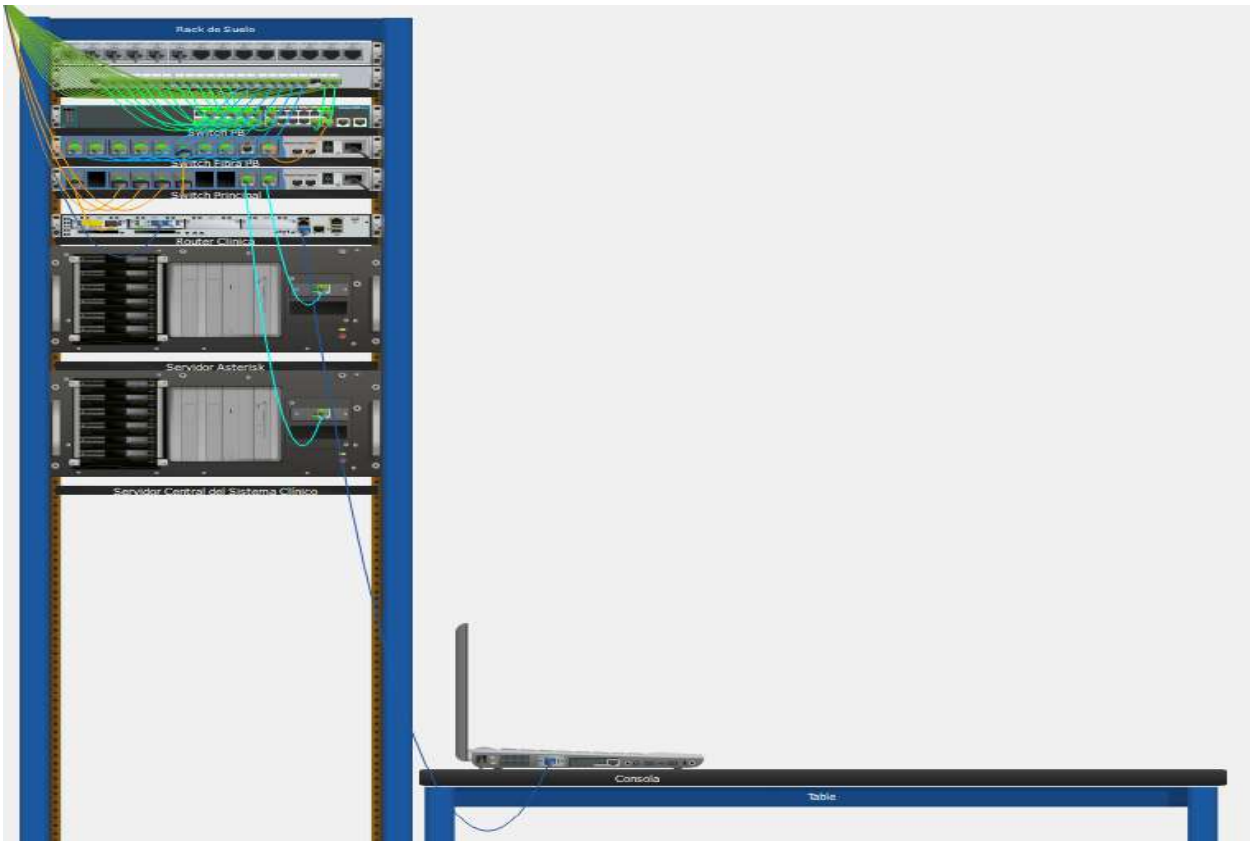

Figura 121. Simulación Rack de Piso

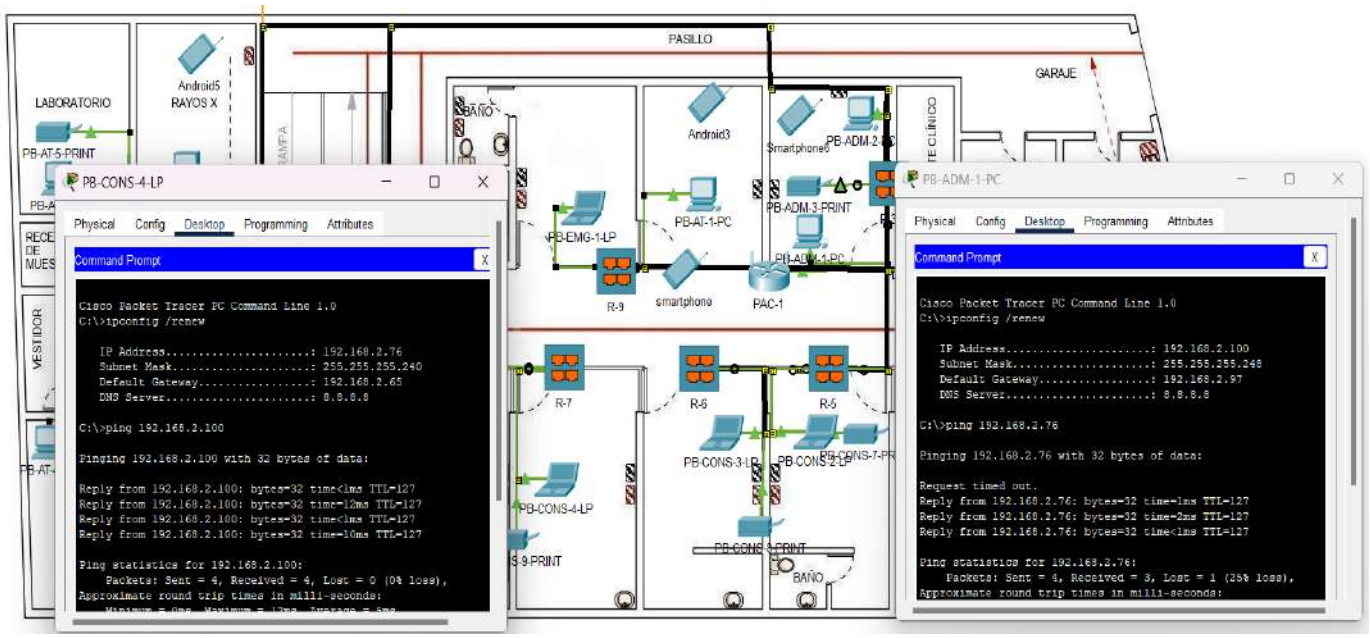

Figura 122. Ping entre LP-VLAN40 y PC-VLAN60 Planta Baja

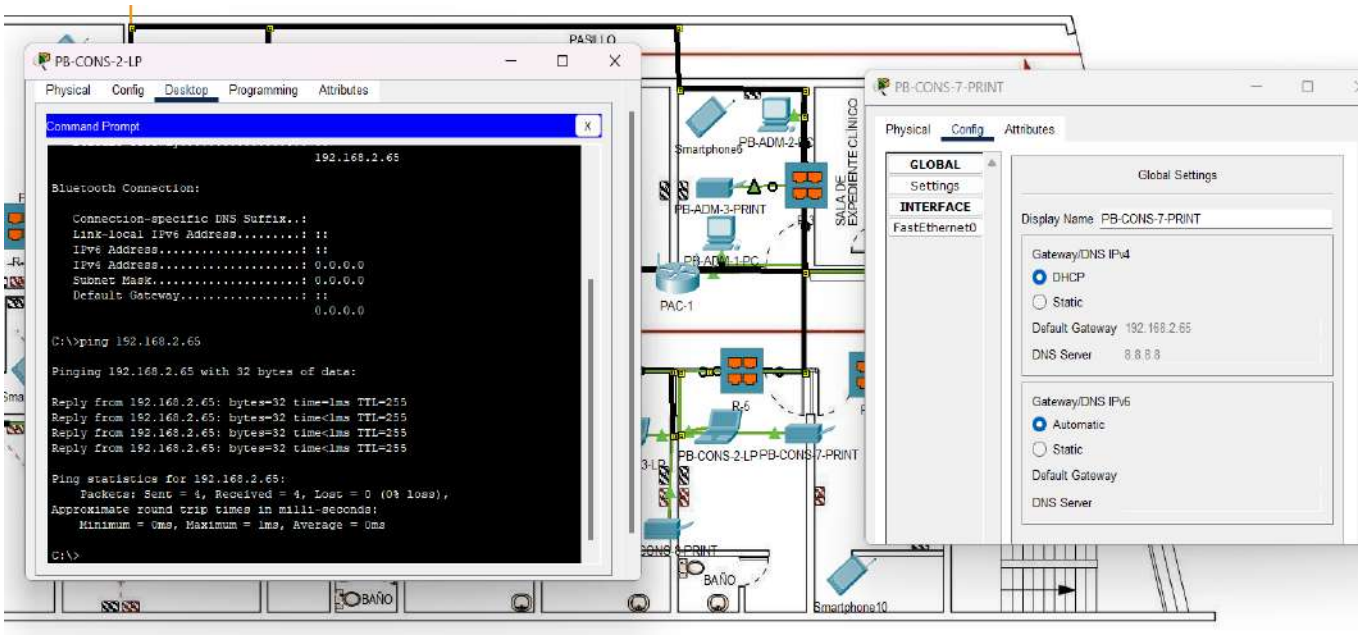

Figura 123. Ping entre LP-VLAN40 y PRINT-VLAN40 Planta Baja

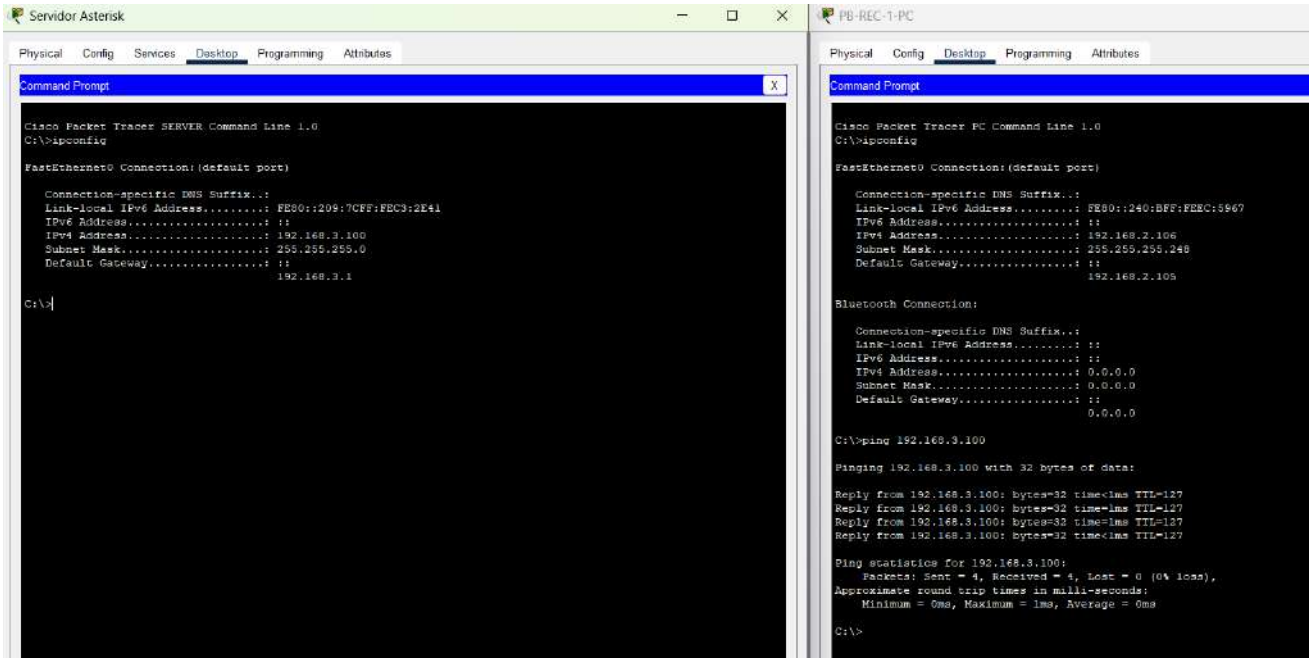

Figura 124. Ping hacia el Servidor Asterisk Planta Baja(VLAN150)

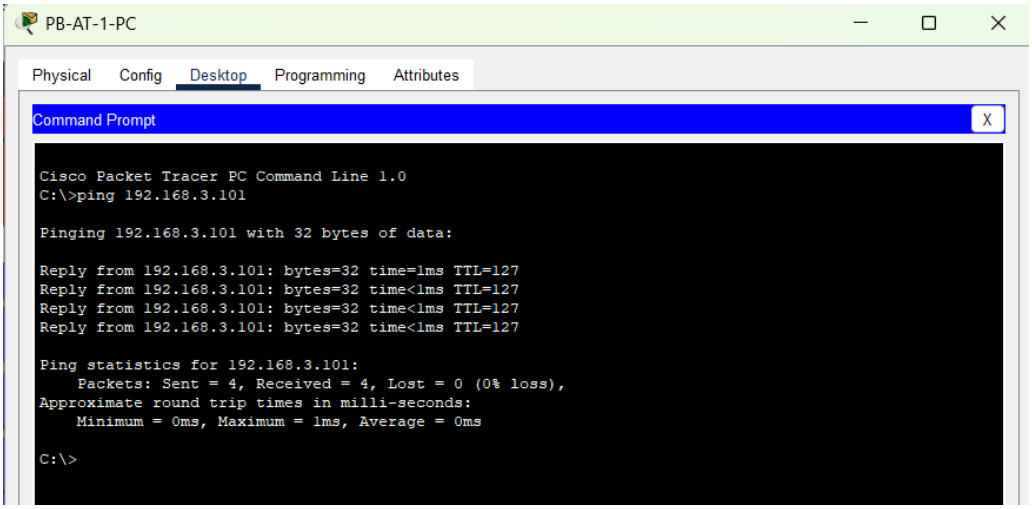

Figura 125. Ping al Servidor Central del Sistema Clínico(VLAN150)

III.1.4.1.2.- Diseño de la red Primer Piso

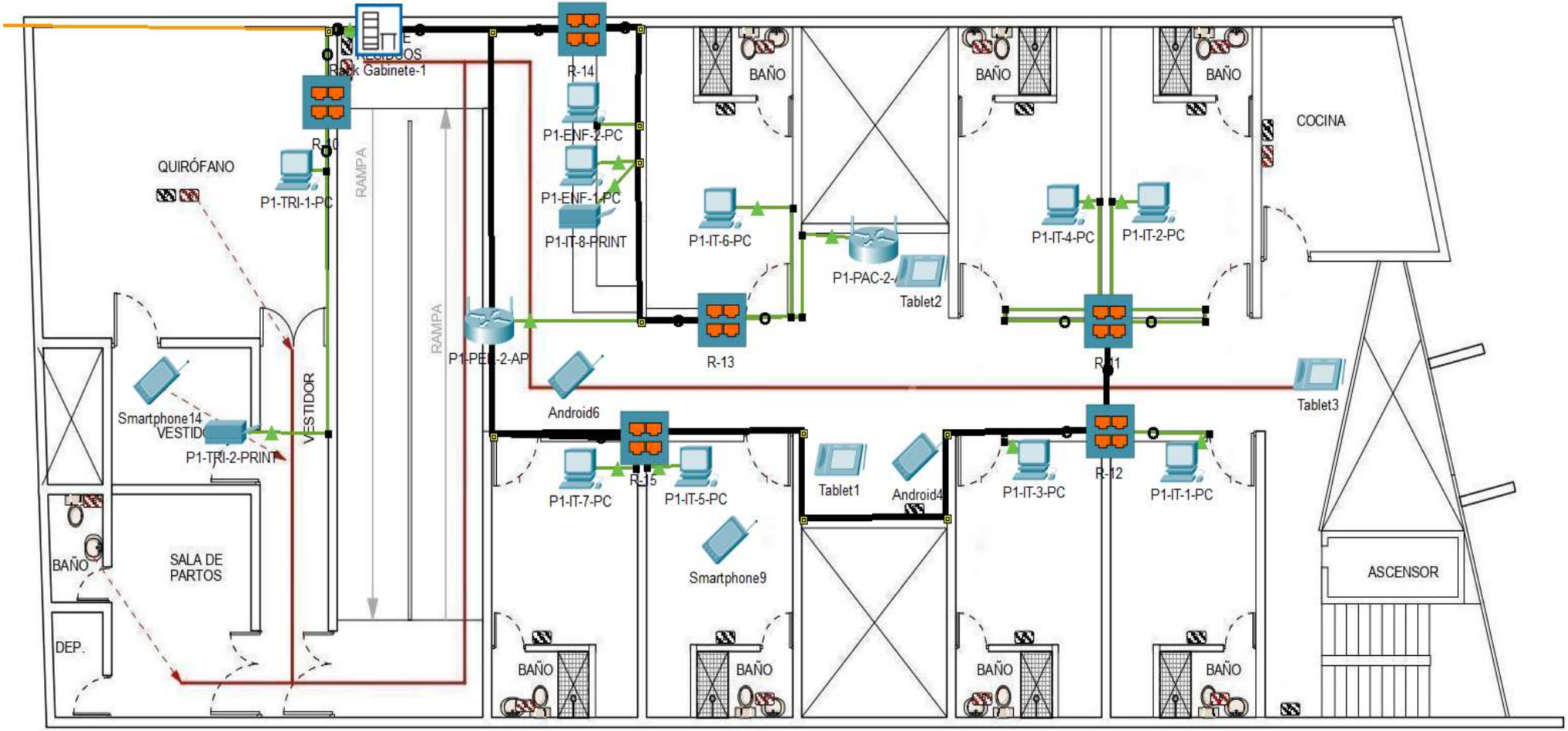

Figura 126. Simulación completa Primer Piso

Se muestra la simulación del área de Terapia Intensiva, Enfermería y Personal de Salud ubicadas en el primer piso, conformadas por VLANs interconectadas. Todas las conexiones de esta planta se concentran en el Rack Gabinete-1, el cual está enlazado al Rack principal de la planta baja.

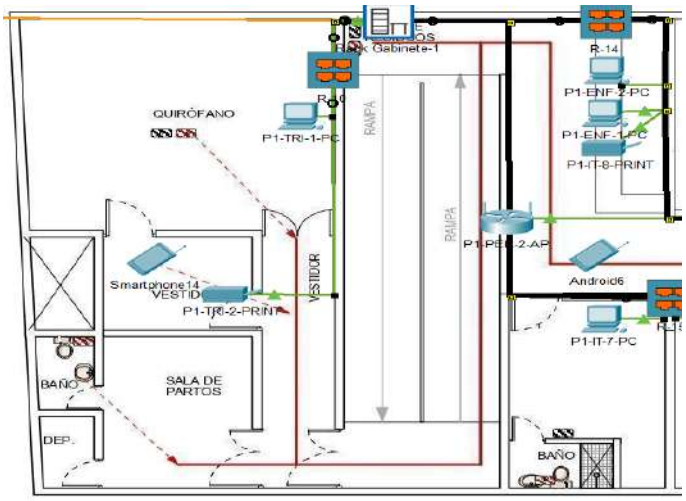

Figura 127. Simulación del Área de Terapia Intensiva Enfermería , Personal de salud

Se muestra la simulación del área de internación de pacientes en el primer piso, conectada al Rack Gabinete-1 y al Rack principal de planta baja. Las VLANs interconectadas permiten una comunicación eficiente entre los equipos y dispositivos médicos para un mejor seguimiento de los pacientes.

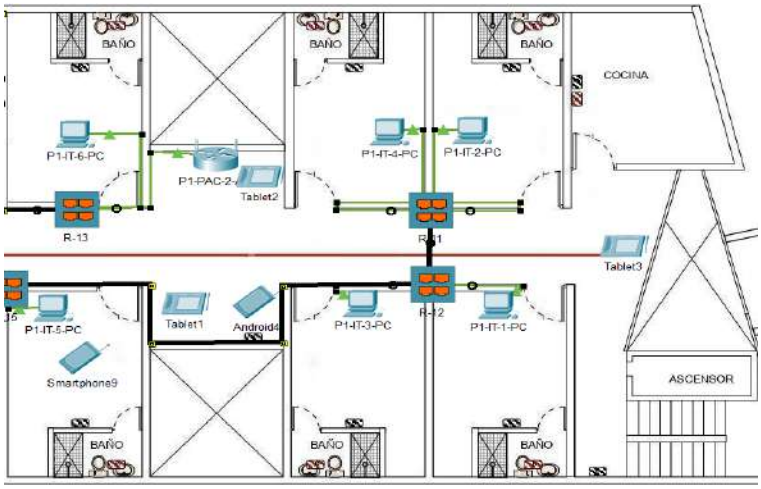

Figura 128. Simulación del Área de Internación, Pacientes

Se muestra la prueba de conectividad (ping) entre PCs del primer piso, comprobando la correcta comunicación entre dispositivos dentro de la VLAN. Los resultados reflejan una conexión estable, con respuestas exitosas y mínima latencia, lo que confirma el buen funcionamiento de la red asociada al Rack Gabinete-1.

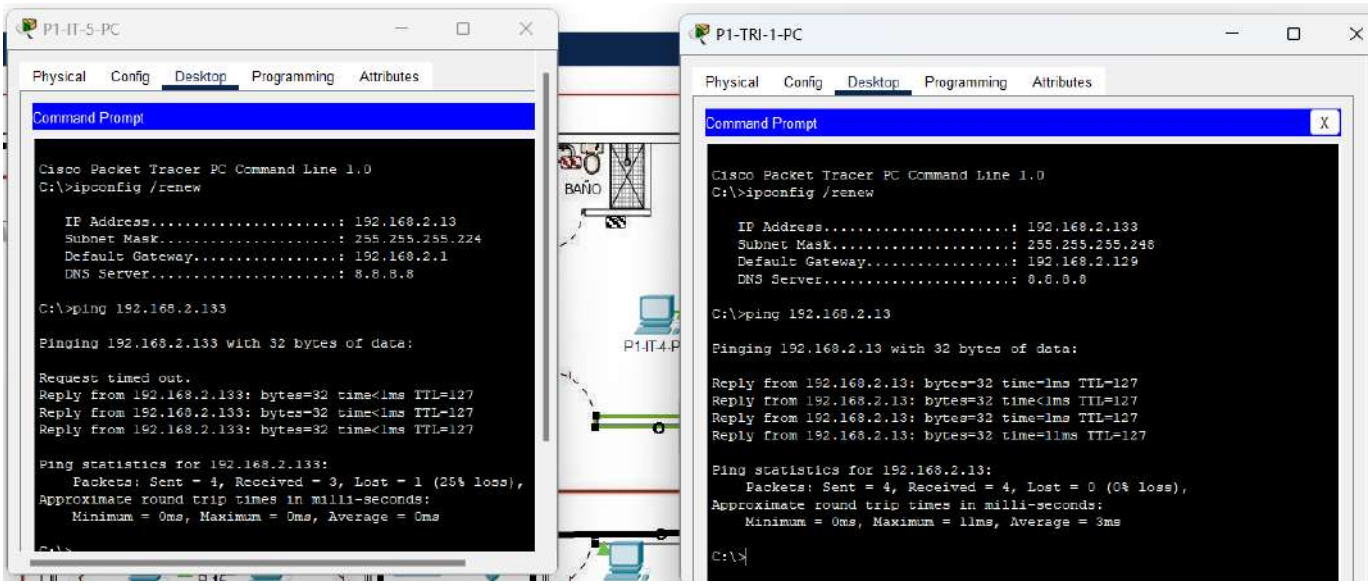

Figura 129. Ping entre PC-VLAN10 y PC-VLAN100 Primer Piso

III.1.4.1.3.- Diseño de la red Segundo Piso

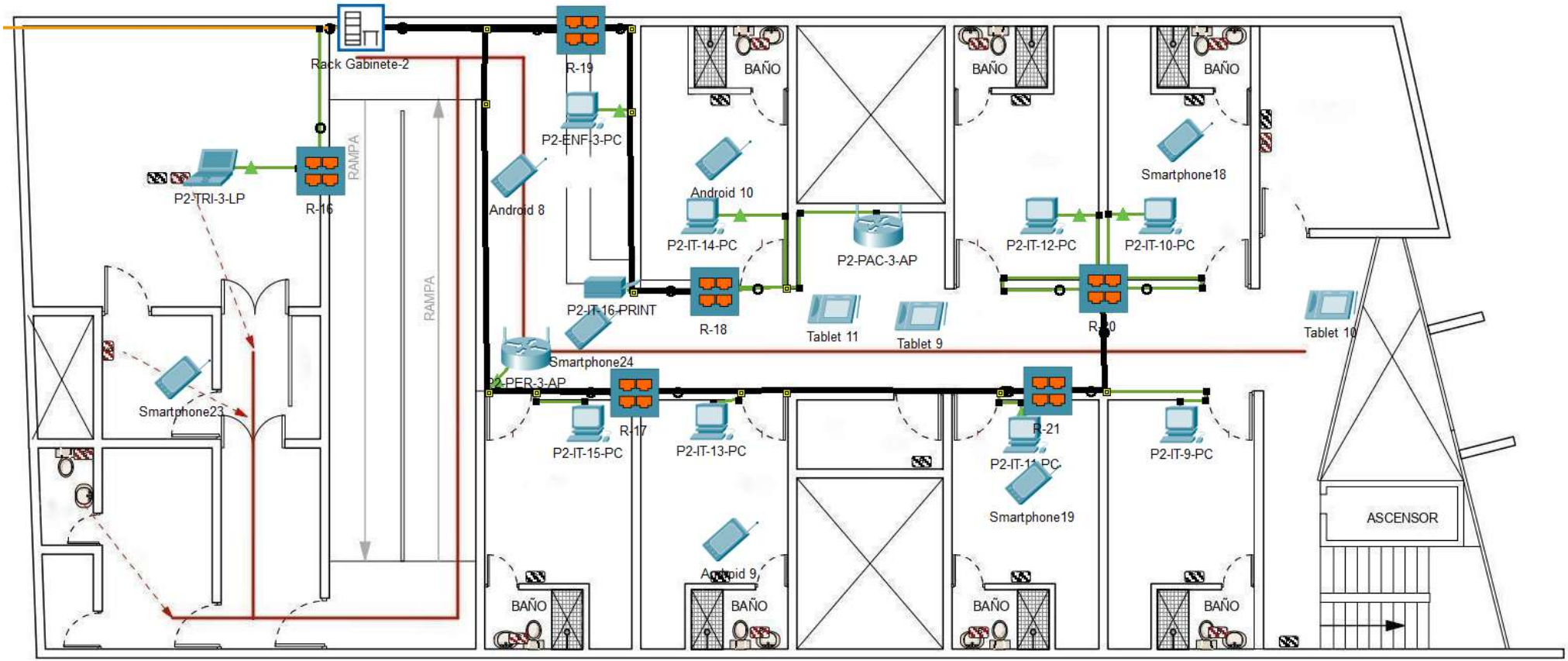

Figura 130. Simulación completa Segundo Piso

Se muestra la simulación del área de Terapia Intensiva, Enfermería y Personal de Salud en el segundo piso, conectada al Rack Gabinete-2, el cual se comunica con el Rack principal de la planta baja. Estas VLANs interconectadas permiten una transmisión estable y segura, facilitando el trabajo del personal y el uso de los puntos de acceso (AP) para mantener una conectividad eficiente.

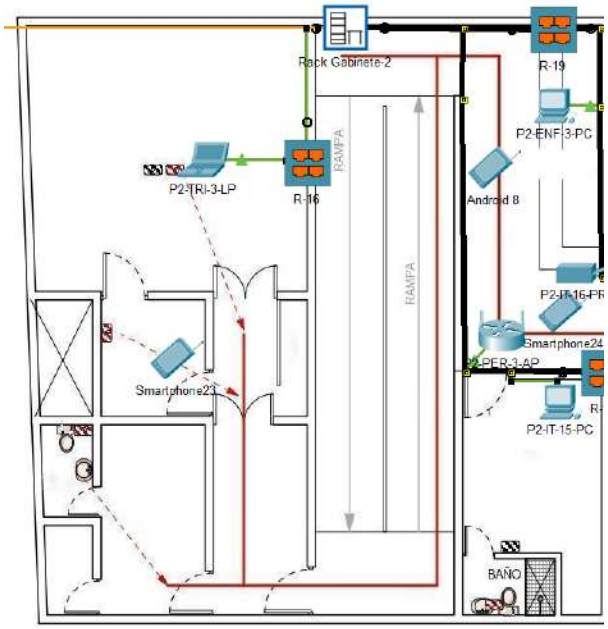

Figura 131. Simulación Área de Terapia Intensiva, Enfermería y Personal de salud

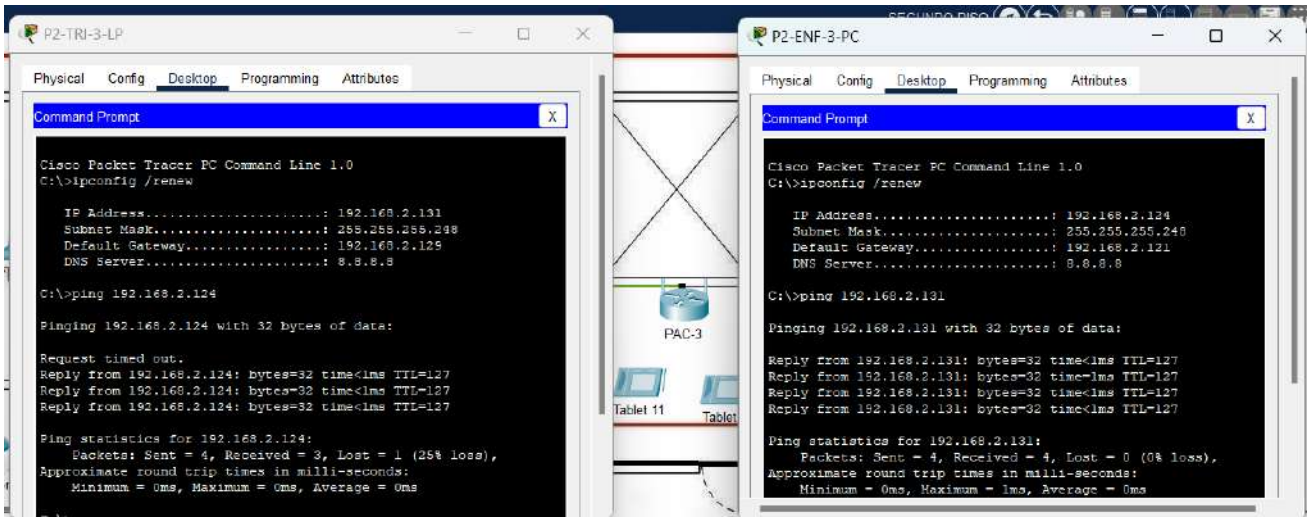

Figura 132. Ping entre PC-VLAN100 y LP-VLAN90 Segundo Piso

III.1.4.1.4.- Diseño de la red Tercer Piso

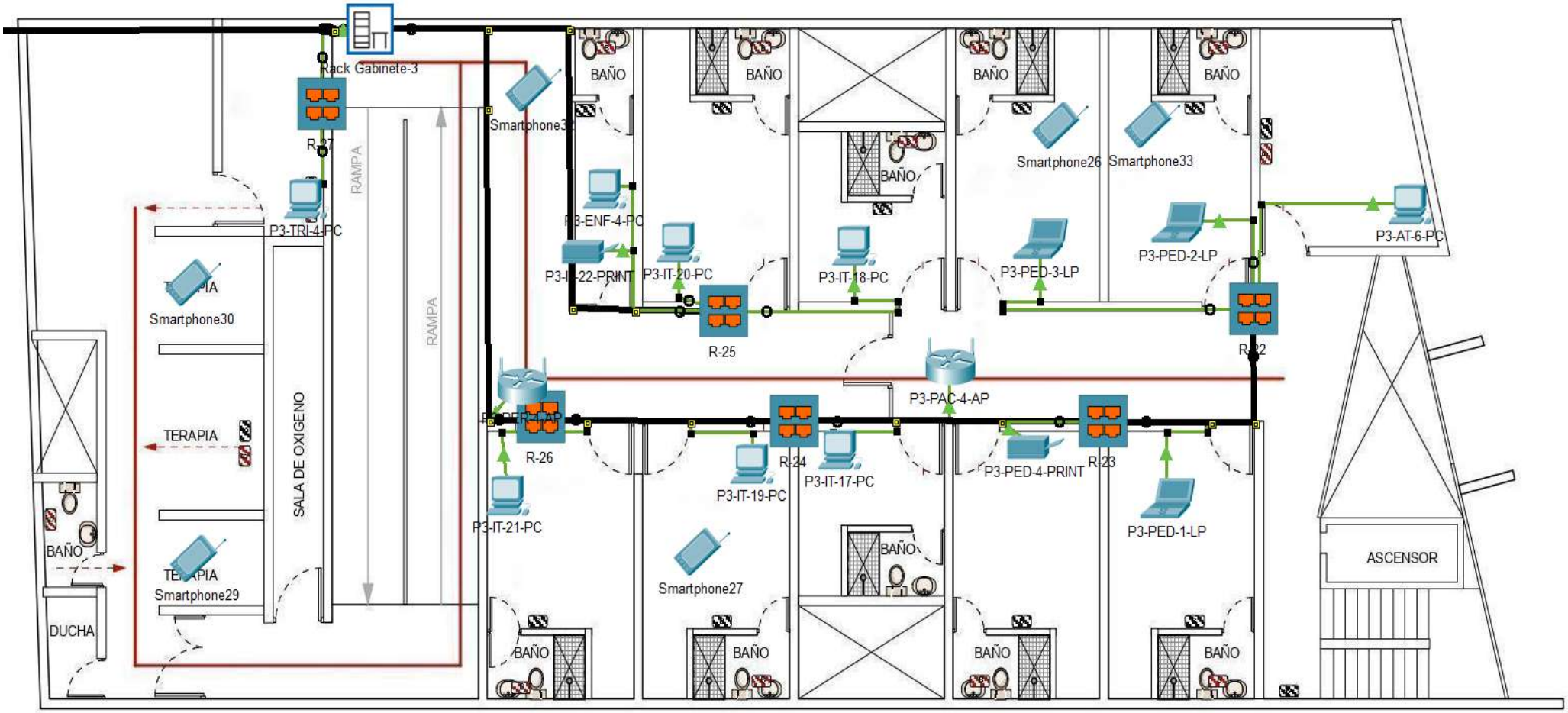

Figura 133. Simulación completa Tercer Piso

Presenta la simulación del área de Terapia Intensiva, Enfermería y Personal de Salud ubicada en el tercer piso, donde todos los equipos están integrados al Rack Gabinete-3, conectado al Rack principal de planta baja. Esta estructura de red, organizada por VLANs interconectadas, permite un flujo de información constante entre los dispositivos médicos y administrativos. Además, los puntos de acceso (AP) están bien ubicados para brindar conectividad estable y cobertura total al personal de salud.

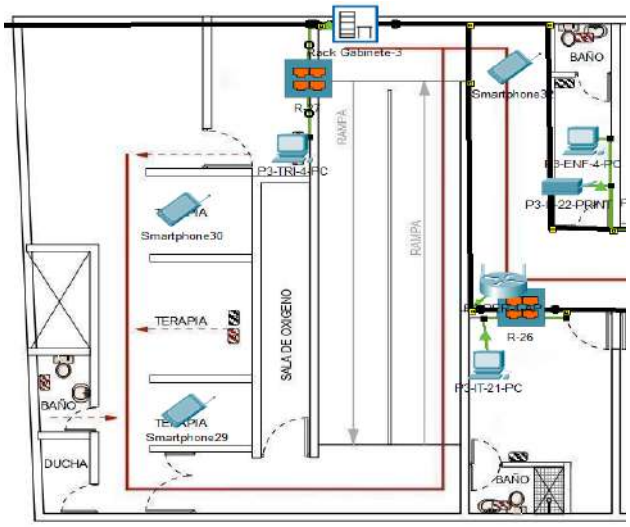

Figura 134. Simulación Área Terapia Intensiva Enfermería y Personal de salud

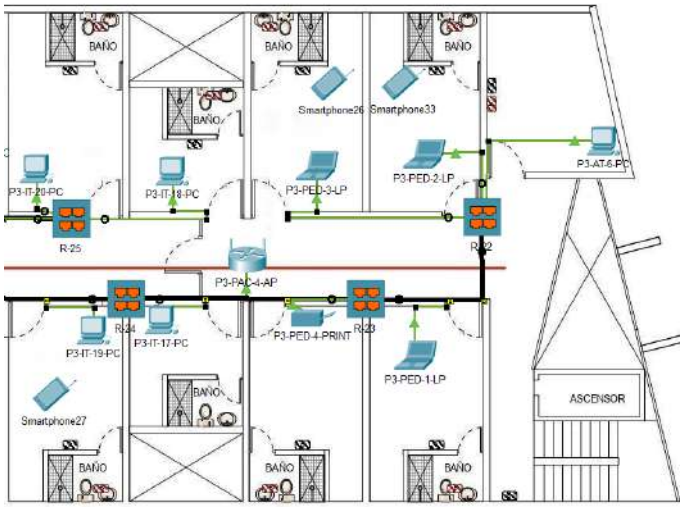

Figura 135. Simulación del Área Tercerizada, Internación y Pacientes

Se muestra la prueba de conectividad (ping) entre equipos del tercer piso, verificando la comunicación correcta dentro de la red VLAN. Los resultados confirman una respuesta exitosa y sin pérdida de paquetes, lo que demuestra una configuración estable y funcional entre los dispositivos conectados al Rack Gabinete-3.

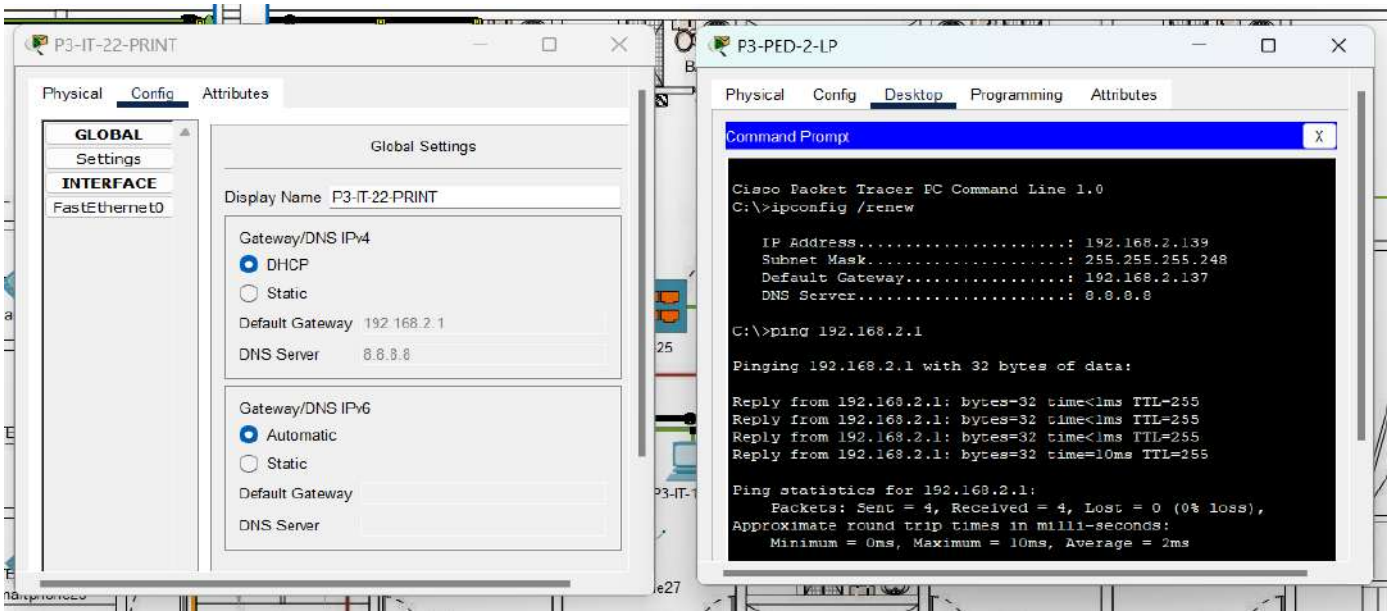

Figura 136. Ping PRINT-VLAN10 y LP-VLAN110 Tercer Piso

III.1.4.1.5.- Diseño de la red Extensión Tercer Piso

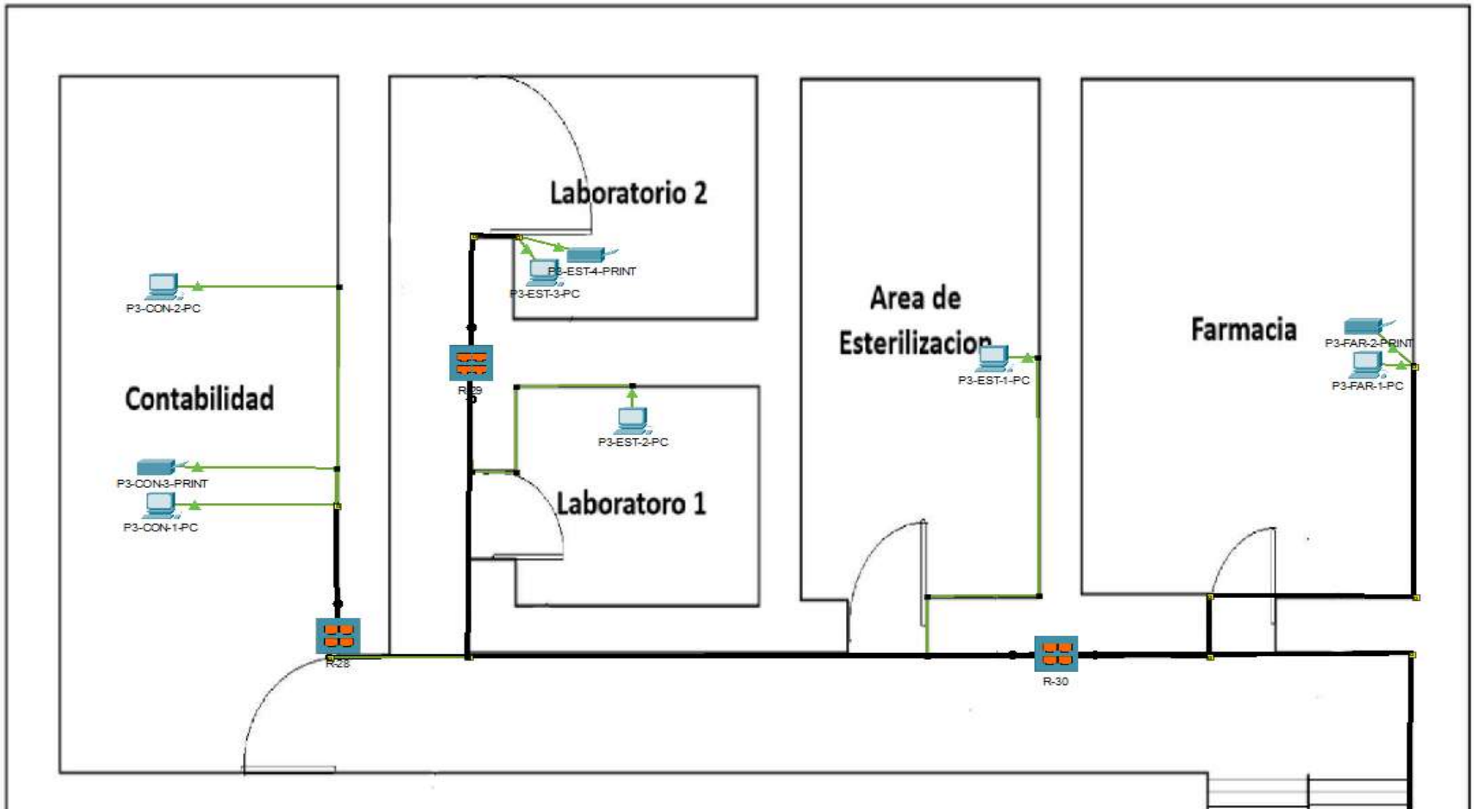

Figura 137. Simulación completa Extensión Tercer Piso

Se muestra la prueba de conectividad (ping) entre PCs del área de extensión en el tercer piso, validando la correcta comunicación dentro de la VLAN asignada. Los resultados evidencian respuestas satisfactorias y mínima pérdida de paquetes, confirmando la estabilidad y funcionamiento adecuado de la red conectada al Rack Gabinete-3.

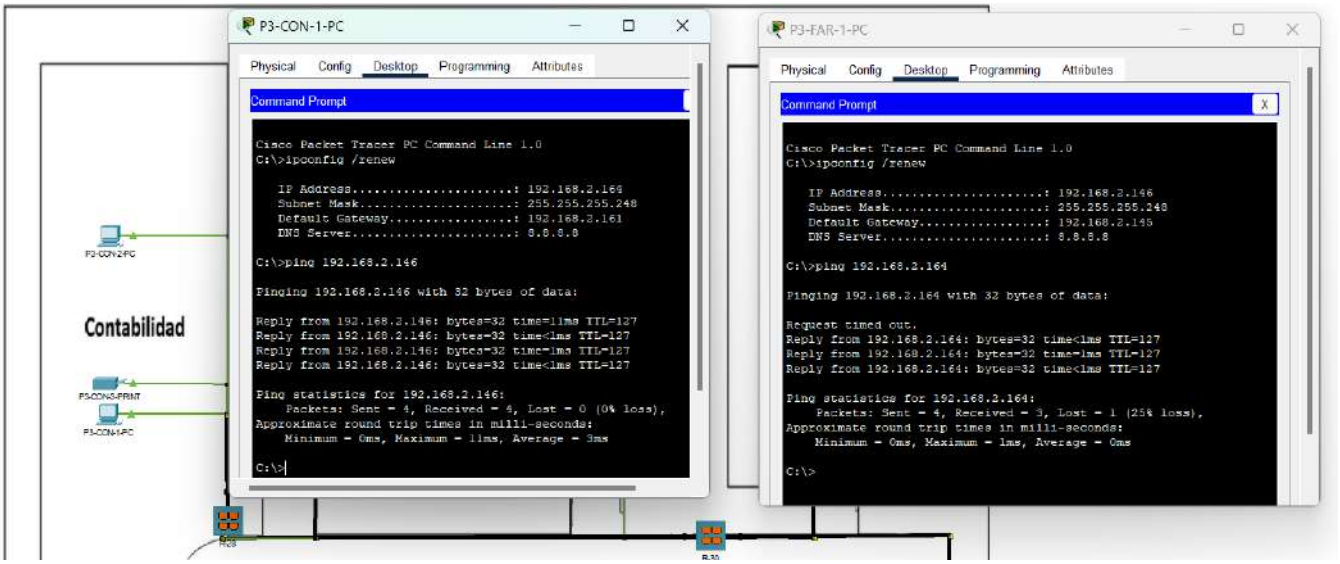

Figura 138. Ping entre PC-VLAN140 y PC-VLAN120 Extensión Tercer Piso

III.1.4.1.6.- Pruebas de los equipos de red

En este apartado se está demostrando que las PCs tienen comunicación exitosa con las otras VLANs a través de los switches, permitiendo el paso de información entre ellas. Además, se muestra que el router tiene acceso a Internet, y que se está aplicando correctamente el NAT (Network Address Translation), lo que asegura que las PCs puedan acceder a recursos externos sin problemas. Las pruebas de conectividad validan que el tráfico fluye adecuadamente entre las VLANs, el router y el acceso a Internet.

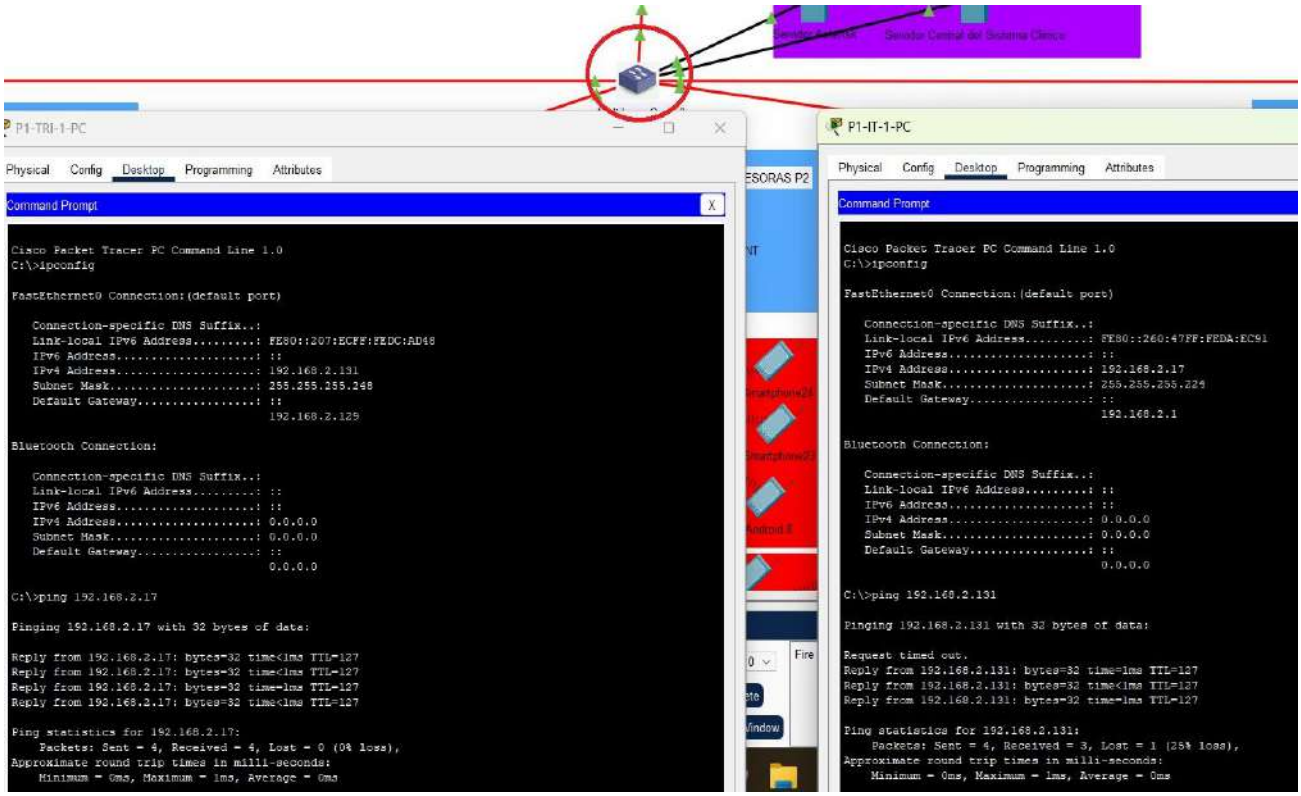

Figura 139. Conectividad pasando por el Switch Principal Capa 3

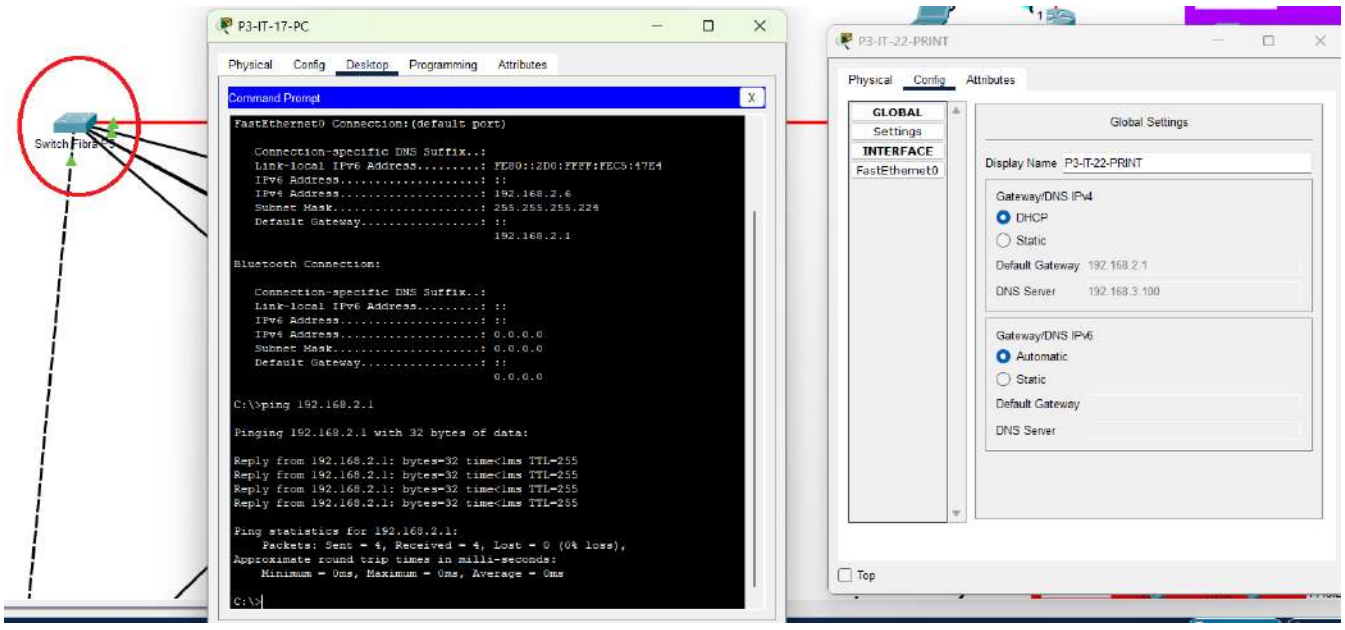

Figura 140. Conectividad pasando por el Switch Fibra

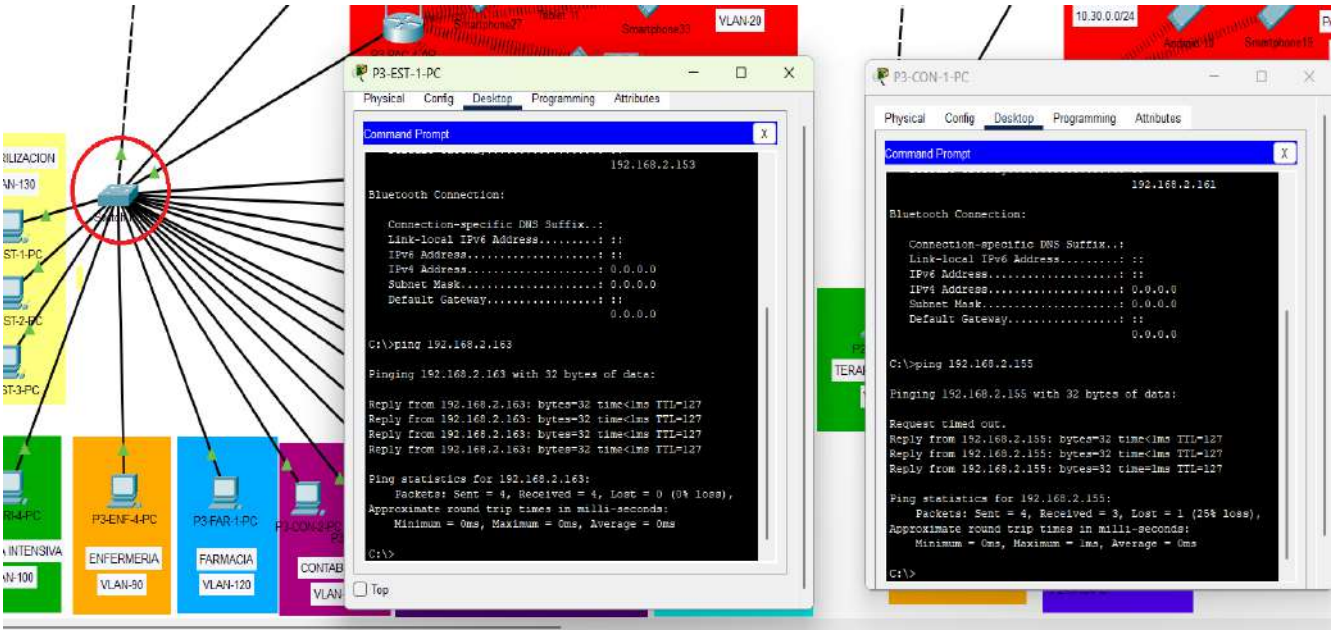

Figura 141. Conectividad pasando por el Switch que usa cable de ethernet

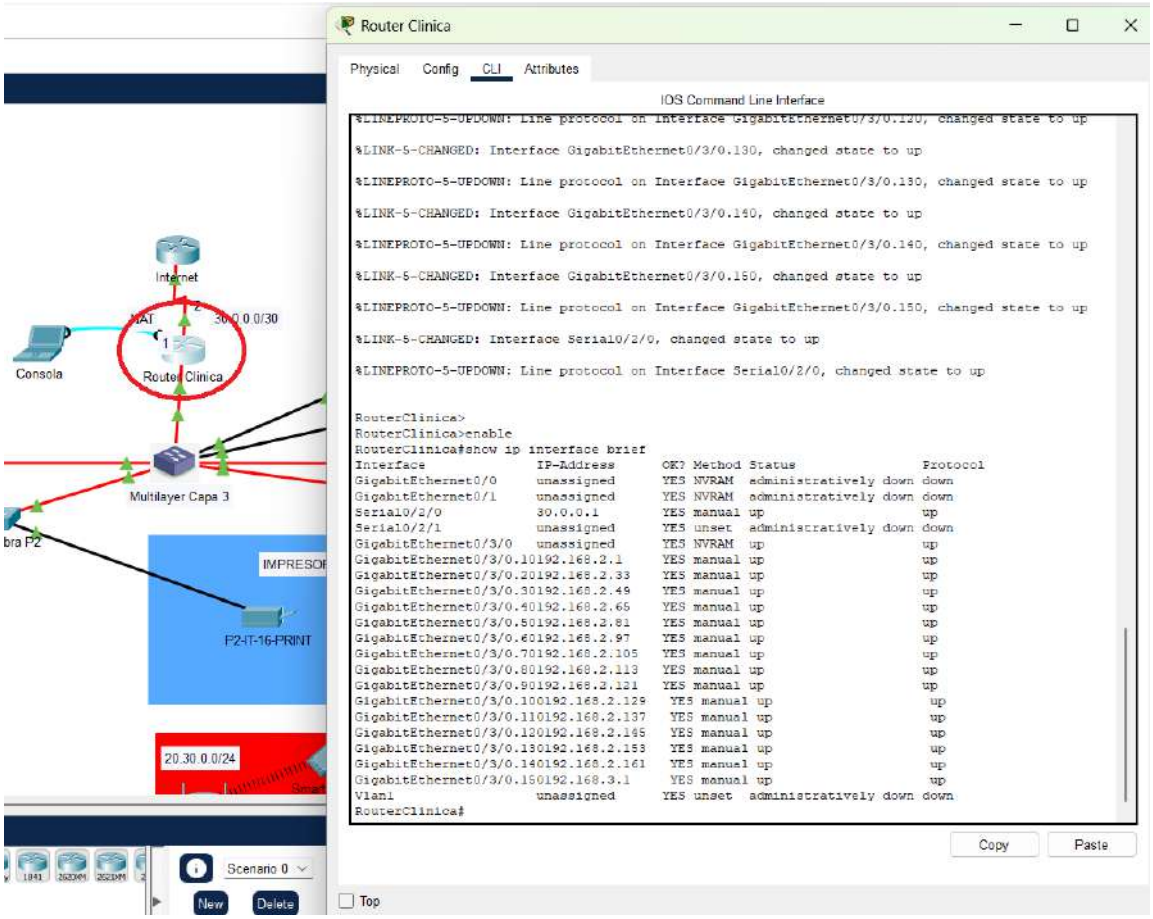

Figura 142. IPs obtenidas del Router de la Clínica

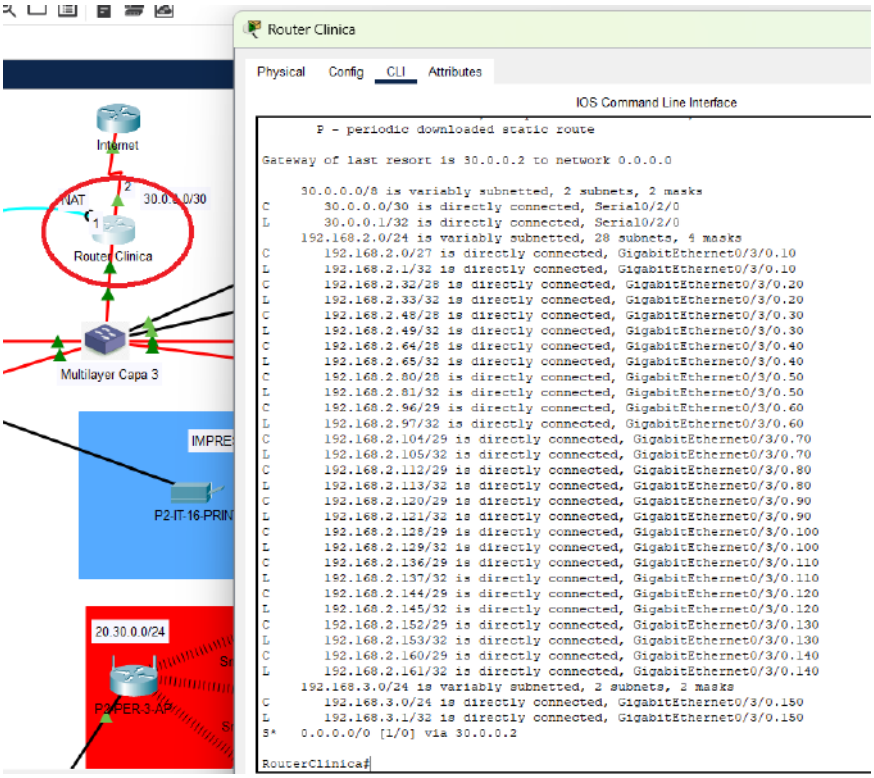

Figura 143.Prueba de enrutamiento

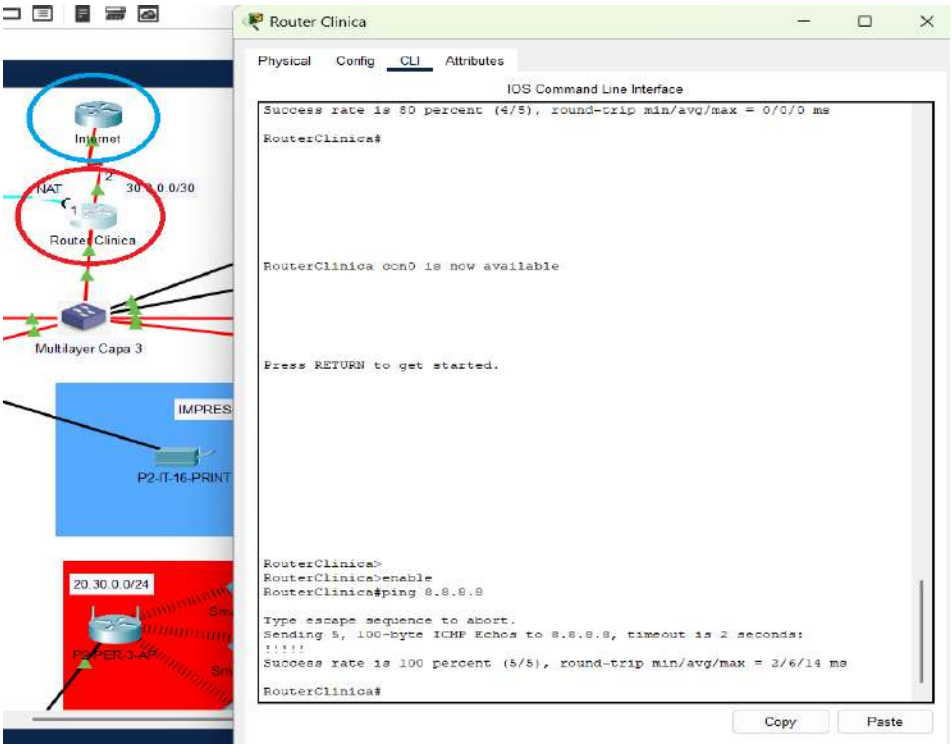

Figura 144. Prueba de NAT

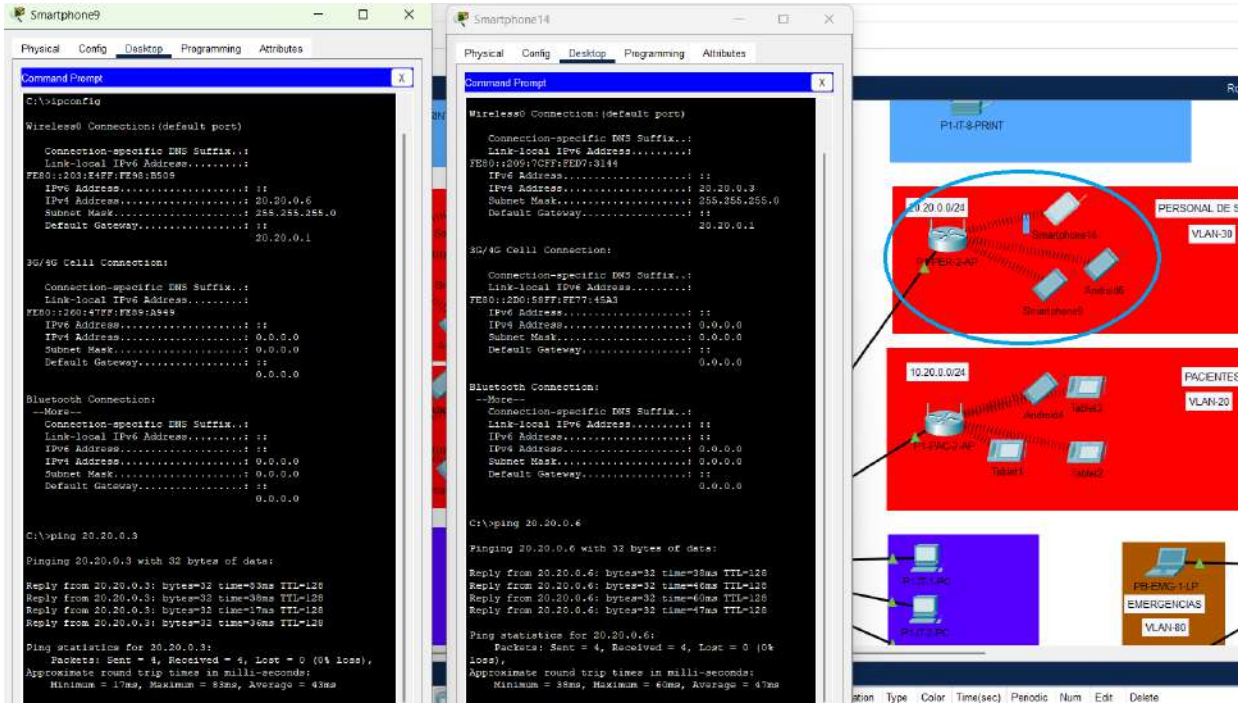

Figura 145. Pruebas de conectividad Wi-Fi (clientes)

III.1.4.1.6.1.- Pruebas de fallo

Cuando se apagó el Switch Fibra PB, se simuló la pérdida total del equipo encargado de distribuir la conectividad en la Planta Baja. Como resultado, todos los dispositivos conectados a ese switch computadoras, impresoras y puntos de acceso quedaron sin servicio; sin embargo, el resto de la red continuó funcionando con normalidad. Esto se debe a que cada área y cada planta cuenta con su propio switch y enlace independiente hacia el switch principal, por lo que una falla local no afecta a los demás sectores. Esta prueba confirma que la red mantiene estabilidad y disponibilidad general incluso ante la caída de un switch específico.

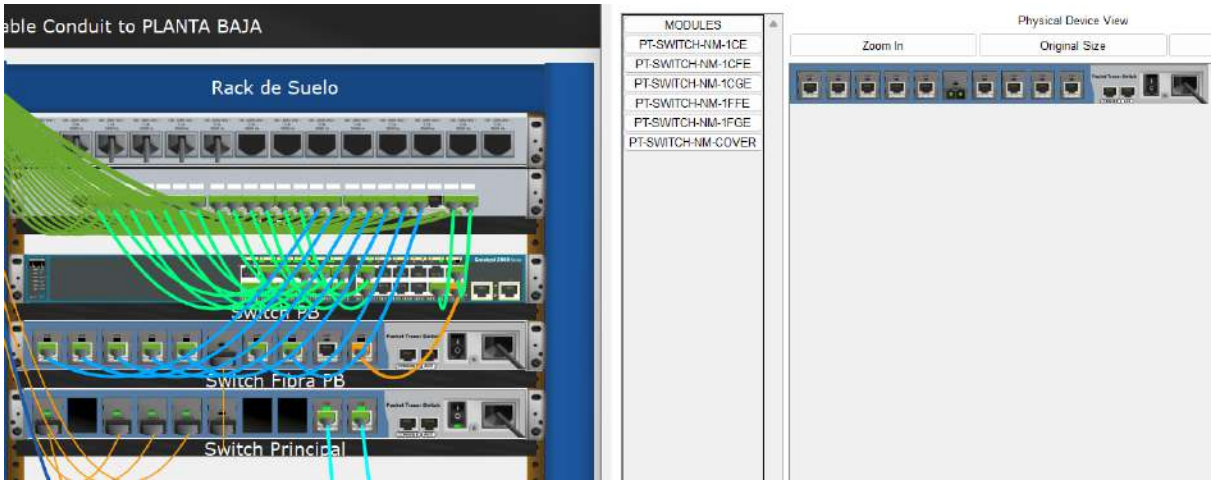

Figura 146. Prueba de fallo switch apagado

Al desconectar el switch, todos los equipos conectados a él perdieron comunicación, pero el resto de la red

siguió funcionando con normalidad. Esto ocurre porque cada área tiene su propio enlace hacia el switch principal, por lo que la falla queda aislada y no afecta a las demás zonas de la clínica.

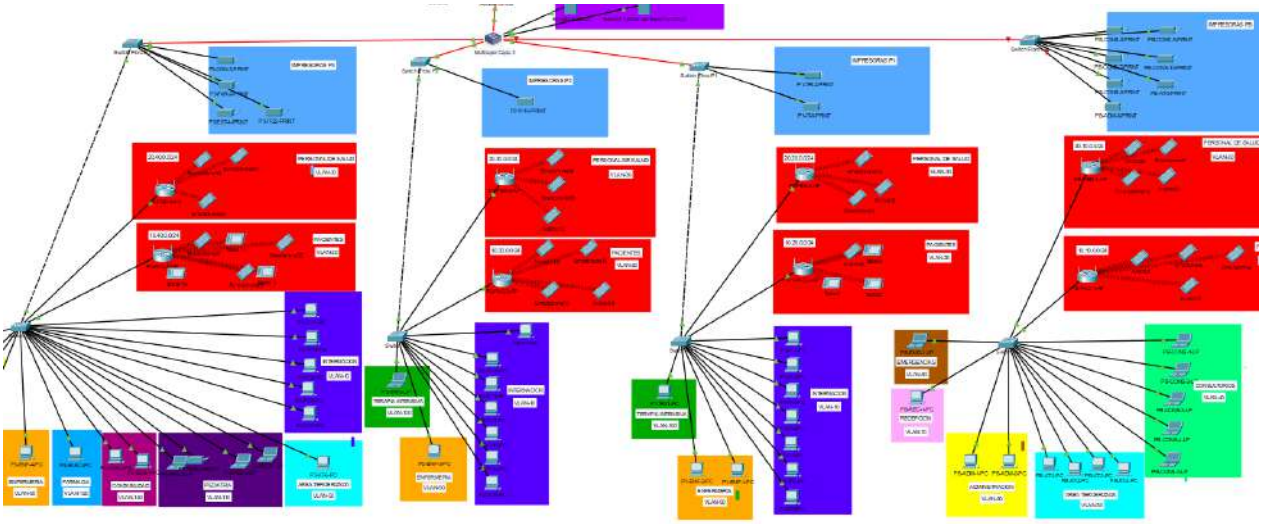

Figura 147. Prueba de fallo desconexión de switch

Al desconectar los servidores, los equipos dejaron de recibir respuesta al realizar pruebas de conexión, lo que confirma que los servicios centrales quedan fuera de operación cuando estos se desconectan. Sin embargo, la red continúa funcionando de manera interna, demostrando que la caída de los servidores afecta solo a los servicios que dependen de ellos, pero no interrumpe la comunicación general entre las áreas.

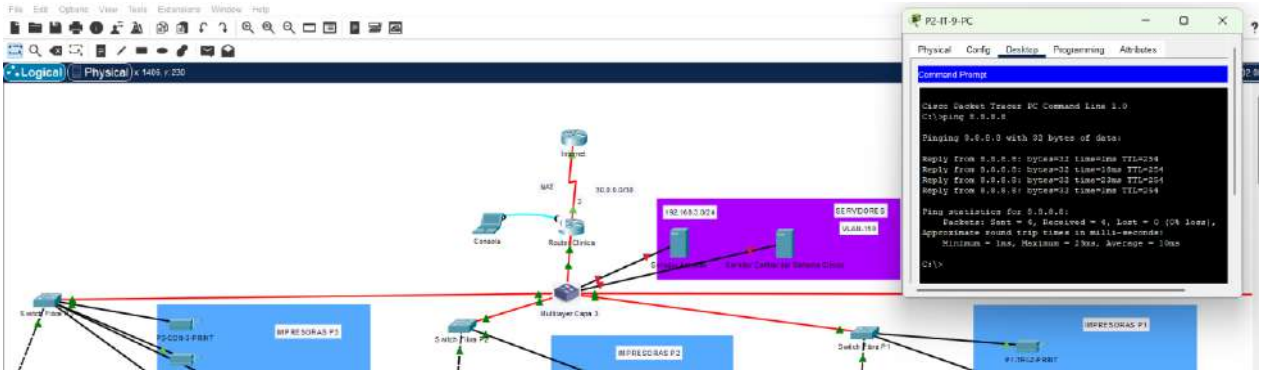

Figura 148. Prueba de fallo desconexión de los servidores

III.1.4.1.7.- Tabla resumen estandarizada de pruebas

VLAN10 | Internación					
Caso de Prueba	**Entrada**	**Salida**	**Resultado Esperado**	**Resultado Obtenido**	**Estado**
CT-01	P1-IT-1-PC	P1-IT-3-PC	Respuesta ICMP exitosa (1ms)	Responde correctamente	Aprobado
CT-02	P2-IT-9-PC	P2-IT-13-PC	Respuesta ICMP exitosa (1ms)	Responde correctamente	Aprobado
CT-03	P1-IT-1-PC	P1-ENF-1-PC (VLAN 90)	Respuesta ICMP exitosa (1ms)	Responde correctamente	Aprobado

CT-04	P1-IT-3-PC	Servidor Clínico (VLAN 150)	Respuesta ICMP exitosa (1ms)	Responde correctamente	Aprobado
CT-05	P3-IT-21-PC	PB-REC-1-PC (VLAN 70)	Respuesta ICMP exitosa (1ms)	Responde correctamente	Aprobado

Tabla 88. Tabla de prueba VLAN10

VLAN20 | Pacientes					
Caso de Prueba	**Entrada**	**Salida**	**Resultado Esperado**	**Resultado Obtenido**	**Estado**
CT-01	Smartphone18	PB-PAC-2-AP	Respuesta ICMP exitosa (1ms)	Responde correctamente	Aprobado
CT-02	Tablet1	Tablet10	Respuesta ICMP exitosa (2-3ms)	Responde correctamente	Aprobado
CT-03	Android	P1-IT-1-PC (VLAN 10)	Comunicación bloqueada hacia otras VLANs	No responde (bloqueado)	Aprobado
CT-04	Android2	PB-ENF-1-PC (VLAN 90)	Comunicación bloqueada hacia otras VLANs	No responde (bloqueado)	Aprobado
CT-05	P3-PAC-3-AP	8.8.8.8 (Internet)	Respuesta ICMP exitosa (<50ms)	Responde correctamente	Aprobado

Tabla 89. Tabla de prueba VLAN20

VLAN30 | Personal de Salud					
Caso de Prueba	**Entrada**	**Salida**	**Resultado Esperado**	**Resultado Obtenido**	**Estado**
CT-01	Smartphone1	Android3	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-02	Android4	Smartphone5	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-03	PB-PERS-AP	Smartphone2	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-04	Android8	P2-ENF-3-PC (VLAN 90 – Enfermería)	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-05	Smartphone1	Android3	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado

Tabla 90. Tabla de prueba VLAN30

VLAN40 | Consultorios					
Caso de Prueba	**Entrada**	**Salida**	**Resultado Esperado**	**Resultado Obtenido**	**Estado**
CT-01	PB-CONS-1-PC	PB-CONS-2-PC	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-02	PB-CONS-3-PC	PB-CONS-4-PC	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-03	PB-CONS-5-PC	PB-CONS-1-PC	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-04	PB-CONS-2-PC	P1-IT-1-PC (VLAN 10 – Internación)	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado

CT-05	PB-CONS-3-PC	P2-ENF-3-PC (VLAN 90 – Enfermería)	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado

Tabla 91. Tabla de prueba VLAN40

VLAN50 | Tercerizados					
Caso de Prueba	**Entrada**	**Salida**	**Resultado Esperado**	**Resultado Obtenido**	**Estado**
CT-01	PB-AT-1-PC	PB-AT-2-PC	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-02	PB-AT-3-PC	P3-AT-6-PC	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-03	P3-AT-6-PC	PB-AT-1-PC	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-04	PB-AT-2-PC	P1-IT-1-PC (VLAN 10 – Internación)	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-05	PB-AT-3-PC	P2-ENF-3-PC (VLAN 90 – Enfermería)	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado

Tabla 92. Tabla de prueba VLAN50

VLAN60 | Administración					
Caso de Prueba	**Entrada**	**Salida**	**Resultado Esperado**	**Resultado Obtenido**	**Estado**
CT-01	PB-ADM-1-PC	PB-ADM-2-PC	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-02	PB-ADM-2-PC	PB-ADM-1-PC	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-03	PB-ADM-1-PC	PB-ADM-3-PC	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-04	PB-ADM-2-PC	P1-IT-1-PC (VLAN 10 – Internación)	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-05	PB-ADM-1-PC	Servidor Clínico (VLAN 150 – Servidores)	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado

Tabla 93. Tabla de prueba VLAN60

VLAN70 | Recepción					
Caso de Prueba	**Entrada**	**Salida**	**Resultado Esperado**	**Resultado Obtenido**	**Estado**
CT-01	PB-REC-1-PC	PB-REC-2-PC	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-02	PB-REC-2-PC	PB-REC-1-PC	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-03	PB-REC-1-PC	PB-REC-3-PC	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-04	PB-REC-2-PC	P1-IT-1-PC (VLAN 10 – Internación)	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-05	PB-REC-1-PC	Servidor Clínico	Respuesta ICMP	Responde	Aprobado

		(VLAN 150 – Servidores)	exitosa (1 ms)	correctamente	

Tabla 94. Tabla de prueba VLAN70

VLAN80 | Emergencias					
Caso de Prueba	**Entrada**	**Salida**	**Resultado Esperado**	**Resultado Obtenido**	**Estado**
CT-01	PB-EMG-1-LP	PB-EMG-2-PC	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-02	PB-EMG-2-PC	PB-EMG-1-LP	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-03	PB-EMG-1-LP	PB-EMG-3-PC	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-04	PB-EMG-2-PC	P2-ENF-3-PC (VLAN 90 – Enfermería)	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-05	PB-EMG-1-LP	P1-TRI-1-PC (VLAN 100 – Terapia Intensiva)	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado

Tabla 95. Tabla de prueba VLAN80

VLAN90 | Enfermería					
Caso de Prueba	**Entrada**	**Salida**	**Resultado Esperado**	**Resultado Obtenido**	**Estado**
CT-01	P1-ENF-1-PC	P1-ENF-2-PC	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-02	P2-ENF-3-PC	P1-ENF-1-PC	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-03	P1-ENF-2-PC	P2-ENF-3-PC	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-04	P1-ENF-1-PC	P1-IT-1-PC (VLAN 10 – Internación)	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-05	P2-ENF-3-PC	PB-ADM-1-PC (VLAN 60 – Administración)	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado

Tabla 96. Tabla de prueba VLAN90

VLAN100 | Terapia Intensiva					
Caso de Prueba	**Entrada**	**Salida**	**Resultado Esperado**	**Resultado Obtenido**	**Estado**
CT-01	P1-TRI-1-PC	P2-TRI-3-LP	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-02	P2-TRI-3-LP	P1-TRI-1-PC	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-03	P1-TRI-1-PC	P1-TRI-2-PC	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-04	P1-TRI-1-PC	P1-IT-1-PC (VLAN 10 – Internación)	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-05	P2-TRI-3-LP	Servidor Clínico	Respuesta ICMP	Responde	Aprobado

		(VLAN 150 – Servidores)	exitosa (1 ms)	correctamente	

Tabla 97. Tabla de prueba VLAN100

VLAN110 | Pediatría					
Caso de Prueba	**Entrada**	**Salida**	**Resultado Esperado**	**Resultado Obtenido**	**Estado**
CT-01	PB-FARM-1-PC	PB-FARM-2-PC	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-02	PB-FARM-2-PC	PB-FARM-1-PC	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-03	PB-FARM-1-PC	PB-FARM-3-PC	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-04	PB-FARM-2-PC	P1-IT-1-PC (VLAN 10 – Internación)	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-05	PB-FARM-1-PC	Servidor Clínico (VLAN 150 – Servidores)	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado

Tabla 98. Tabla de prueba VLAN110

VLAN120 | Farmacia					
Caso de Prueba	**Entrada**	**Salida**	**Resultado Esperado**	**Resultado Obtenido**	**Estado**
CT-01	PB-CONSOL-1-PC	PB-CONSOL-2-PC	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-02	PB-CONSOL-2-PC	PB-CONSOL-1-PC	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-03	PB-CONSOL-1-PC	PB-CONSOL-3-PC	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-04	PB-CONSOL-2-PC	PB-ADM-1-PC (VLAN 60 – Administración)	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-05	PB-CONSOL-1-PC	Servidor Clínico (VLAN 150 – Servidores)	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado

Tabla 99. Tabla de prueba VLAN120

VLAN130 | Esterilización					
Caso de Prueba	**Entrada**	**Salida**	**Resultado Esperado**	**Resultado Obtenido**	**Estado**
CT-01	PB-PED-1-PC	PB-PED-2-PC	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-02	PB-PED-2-PC	PB-PED-3-PC	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-03	PB-PED-3-PC	PB-PED-1-PC	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-04	PB-PED-2-PC	P1-IT-1-PC (VLAN 10 – Internación)	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-05	PB-PED-1-PC	Servidor Clínico (VLAN 150 –	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado

		Servidores)			

Tabla 100. Tabla de prueba VLAN130

VLAN140 | Contabilidad					
Caso de Prueba	**Entrada**	**Salida**	**Resultado Esperado**	**Resultado Obtenido**	**Estado**
CT-01	PB-CONT-1-PC	PB-CONT-2-PC	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-02	PB-CONT-2-PC	PB-CONT-3-PC	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-03	PB-CONT-3-PC	PB-CONT-1-PC	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-04	PB-CONT-2-PC	PB-ADM-1-PC (VLAN 60 – Administración)	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-05	PB-CONT-1-PC	Servidor Clínico (VLAN 150 – Servidores)	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado

Tabla 101. Tabla de prueba VLAN140

VLAN150 | Servidores					
Caso de Prueba	**Entrada**	**Salida**	**Resultado Esperado**	**Resultado Obtenido**	**Estado**
CT-01	Servidor Clínico	Servidor de Backup	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-02	Servidor de Backup	Servidor Clínico	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-03	Servidor Clínico	Gateway VLAN 150	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-04	Servidor Clínico	P1-IT-1-PC (VLAN 10 – Internación)	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado
CT-05	Servidor Clínico	PB-ADM-1-PC (VLAN 60 – Administración)	Respuesta ICMP exitosa (1 ms)	Responde correctamente	Aprobado

Tabla 102. Tabla de prueba VLAN150

III.1.4.1.8.- Simulación del diseño en GNS3

Se muestra el diseño lógico o diagrama final de la red simulado en GNS3, donde se ve la estructura semicompleta del sistema implementado, demostrando en este entorno un firewall Fortinet, switches de capa 3 y 2, PC virtuales con Windows 10 y un servidor de telefonía IP Issabel. GNS3 permite conectar la simulación con el acceso a Internet real del equipo físico, ofreciendo una representación funcional de la red.

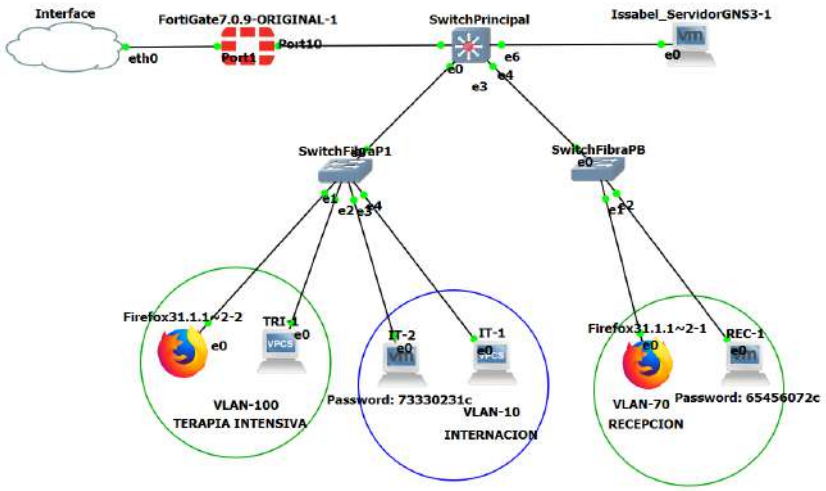

Figura 149. Diseño Lógico GNS3

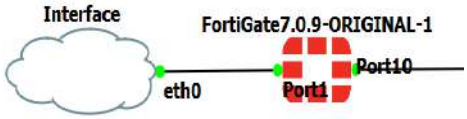

Figura 150. Distribución de Interfaz e Internet Fortinet

Se muestra una simulación de la interfaz de configuración de políticas de seguridad del firewall Fortinet, en la cual se definen las reglas de acceso a Internet para las distintas VLANs. Entre ellas destacan las políticas correspondientes a las áreas de Internación, Recepción y Terapia Intensiva, todas configuradas para permitir el tráfico saliente hacia Internet según los criterios establecidos.

Asimismo, se observa una política implícita de denegación que bloquea todo el tráfico no especificado, garantizando así el control y la seguridad del flujo de datos dentro de la red. Cada política detalla parámetros esenciales como el servicio, la acción (permitir o denegar), y la cantidad de datos procesados, lo que permite una gestión precisa y segura del acceso a los recursos externos.

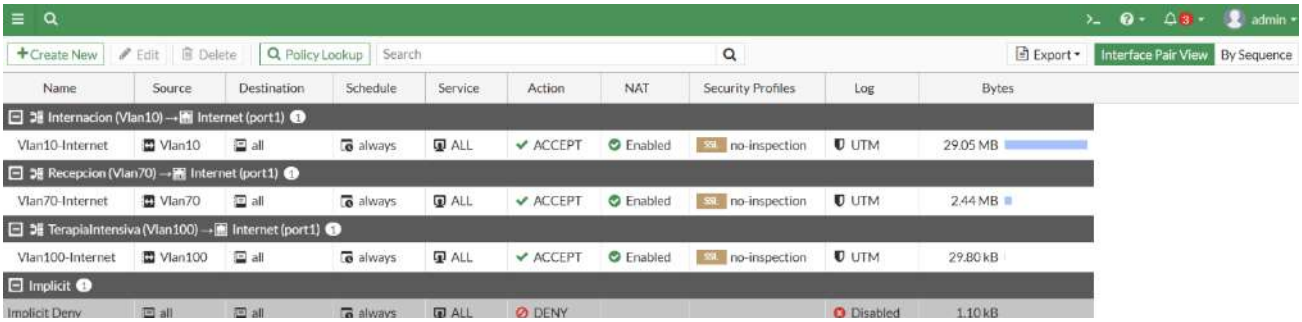

Figura 151. Simulacion de Implementacion de politicas de seguridad

Se presentan las pruebas de conectividad realizadas desde los equipos pertenecientes a la VLAN 70, específicamente desde los hosts VLAN70-PC y VLAN70-Rec-1-Windows.

En ambas simulaciones se ejecutaron pruebas de ping hacia servidores externos (como los DNS de Google 8.8.8.8 y www.google.com), obteniéndose respuestas exitosas sin pérdida de paquetes.
Estos resultados demuestran que la VLAN 70 posee salida efectiva a Internet, validando la correcta configuración del enrutamiento, NAT y políticas de acceso establecidas en el firewall Fortinet y en los routers de la red.

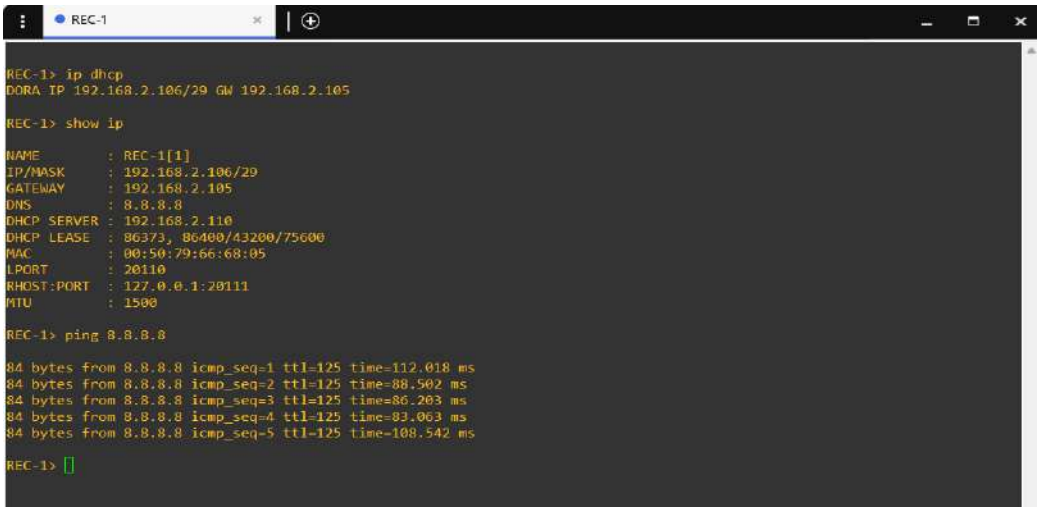

Figura 152. Ping desde Vlan70-PC hacia Servidores DNS de Google

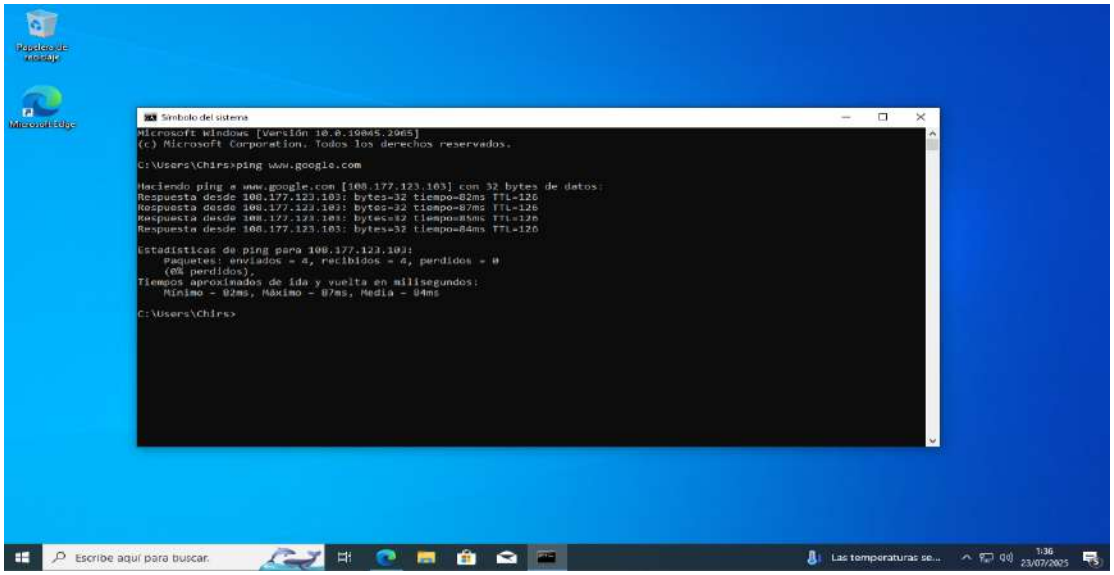

Figura 153. Ping desde VLAN70-Rec-1-Windows a los servicios utilizados

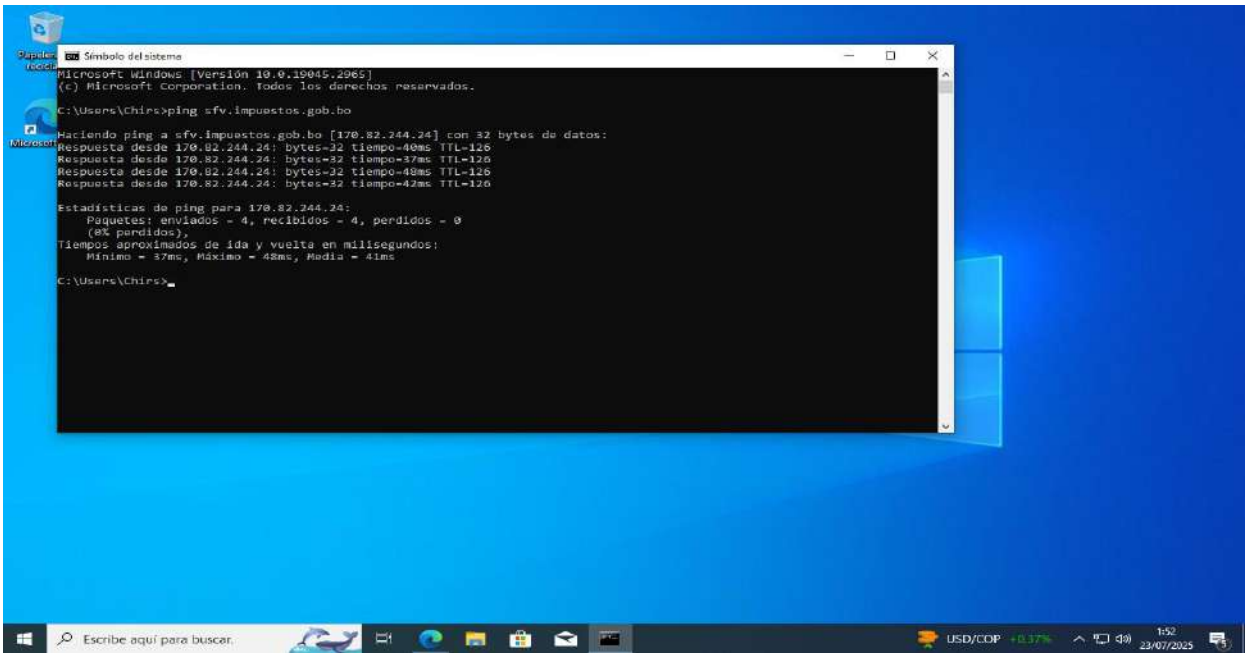

Figura 154. Ping desde VLAN70-Rec-1-Windows a los servicios requeridos

Se muestra la simulación del bloqueo de páginas web mediante los filtros de contenido del firewall Fortinet. En este caso, el acceso al sitio www.youtube.com fue denegado por el sistema de filtrado web FortiGuard, el cual identifica la URL como restringida dentro de las políticas de seguridad configuradas. Este resultado demuestra que las reglas de filtrado y control de navegación están funcionando correctamente, evitando el acceso a páginas no autorizadas y reforzando la seguridad y productividad de la red al limitar contenidos que no son parte de los servicios permitidos.

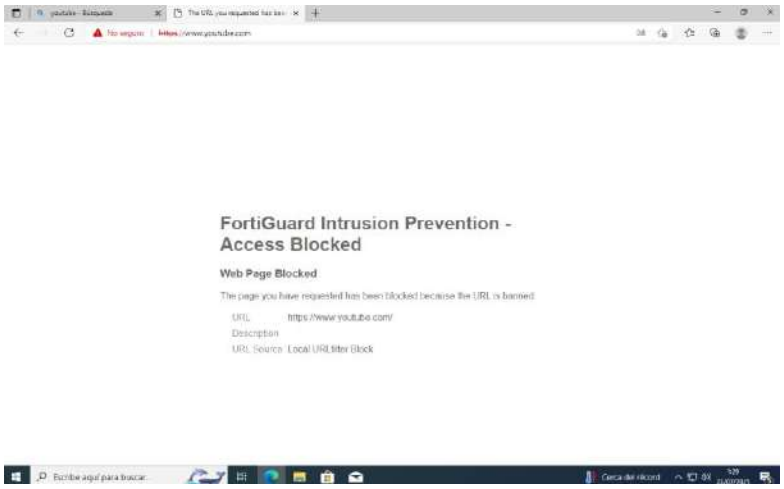

Figura 155. Bloqueo de Paginas web

La simulación muestra una configuración de una dirección IP estática en el servidor de telefonía IP(Issabel) usando una interfaz de terminal en Centos. La IP configurada permite que el servidor se comunique de manera fija con la red local, asegurando que los dispositivos de telefonía siempre lo localicen en la misma dirección. Esto es fundamental para mantener la estabilidad y confiabilidad de las

comunicaciones VoIP.

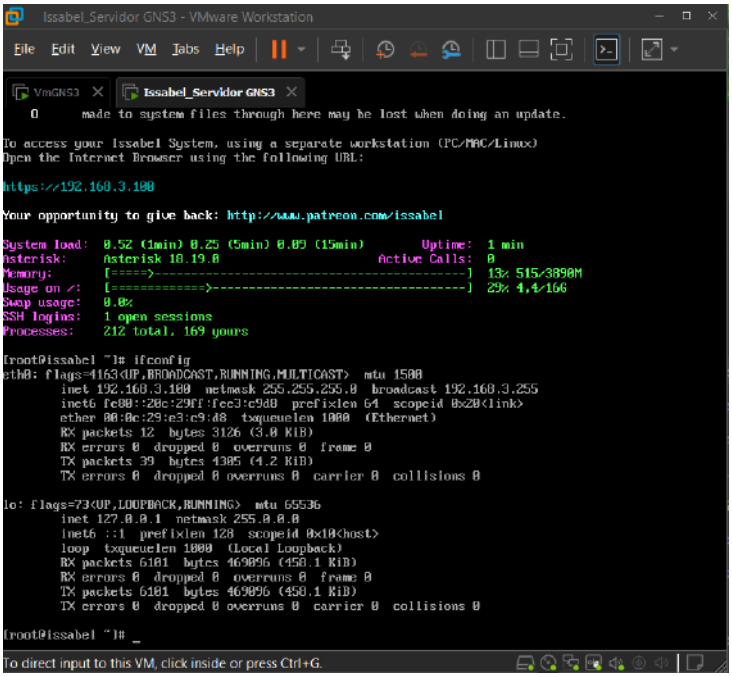

Figura 156. Simulación de Inserción de IP estática hacia el Servidor de telefonía IP

Se muestra la interfaz web de Issabel, donde se añaden y gestionan las extensiones de telefonía IP. Cada extensión representa un teléfono o dispositivo conectado al servidor, y su configuración asegura que las llamadas internas se enruten correctamente. No es necesario que exista conectividad directa (ping) entre los dispositivos; basta con que todos estén conectados al servidor, ya que este actúa como el punto central de comunicación y permite que se realicen las llamadas sin problemas. Esta gestión centralizada simplifica la administración de múltiples dispositivos dentro de la red de la empresa o institución.

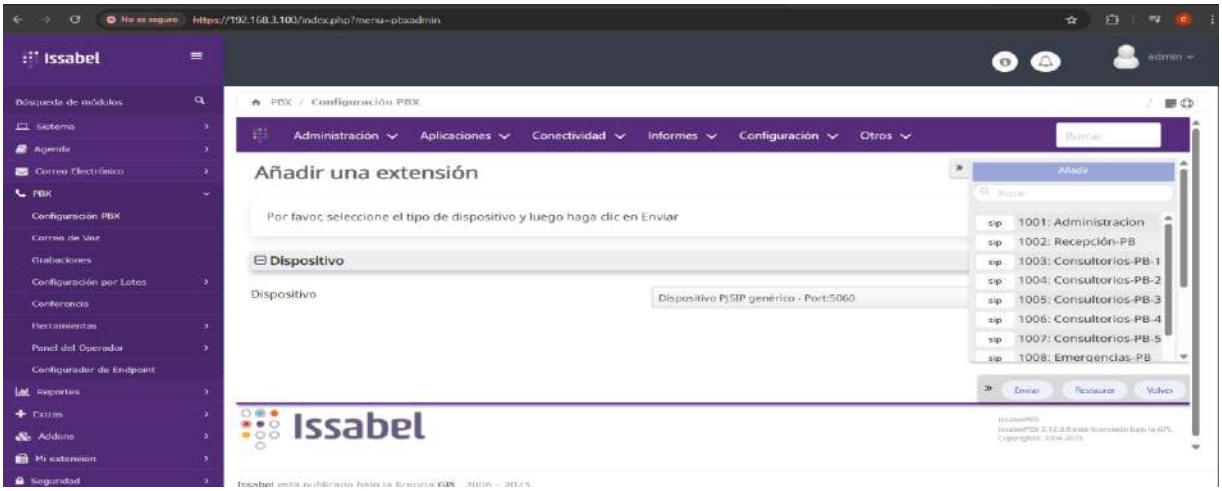

Figura 157. Simulación de las extensiones Servidor de telefonía IP Issabel

III.1.4.1.9.- Nivel de señal Access Point

Con el objetivo de evaluar el alcance de la señal inalámbrica en cada planta de la Clínica, se realizó una

simulación de cobertura Wi-Fi sobre los planos arquitectónicos del edificio.

Las dimensiones aproximadas del área analizada corresponden a 18 metros de largo por 15 metros de ancho del edificio, lo que permitió definir la distribución óptima de los puntos de acceso (AP).

Para la simulación se utilizó la aplicación gratuita NetSpot en su versión para dispositivos móviles, la cual permite:

- ✓ Importar el plano del edificio
- ✓ Definir la ubicación de los Access Points
- ✓ Visualizar la propagación estimada de la señal
- ✓ Medir niveles de potencia en **dBm (decibelios miliwatt)**

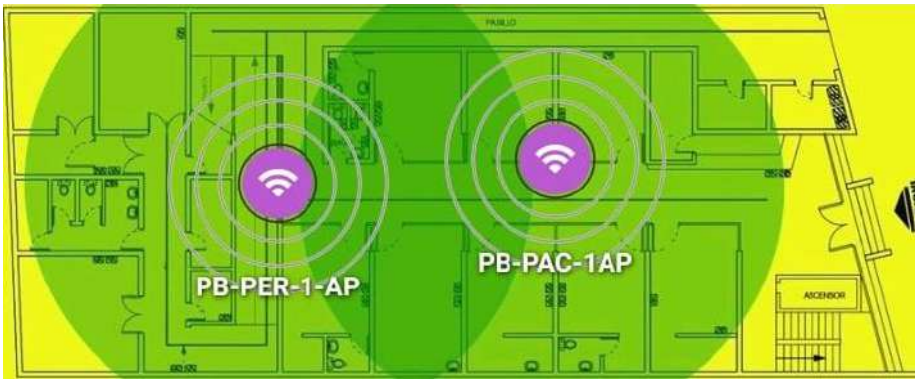

Figura 158. Nivel de señal bajo Planta Baja

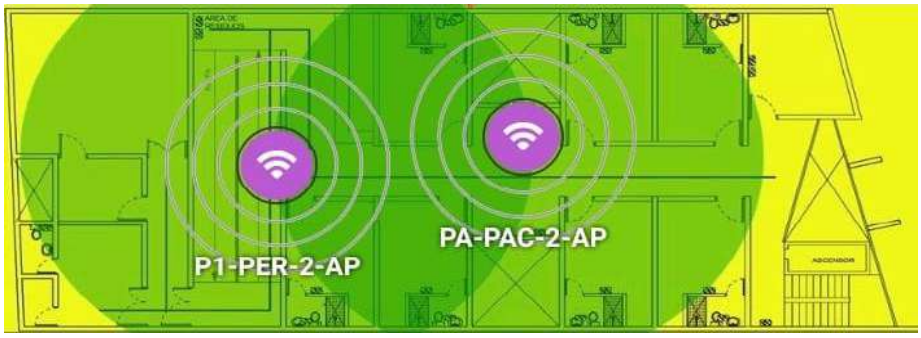

Figura 159. Nivel de señal bajo Primer Piso

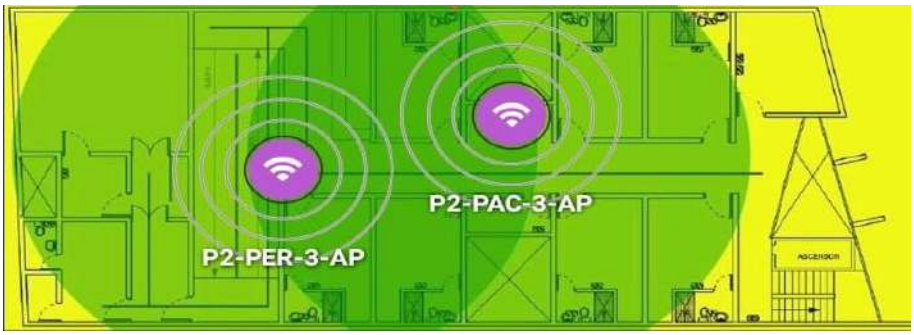

Figura 160. Nivel de señal bajo Segundo Piso

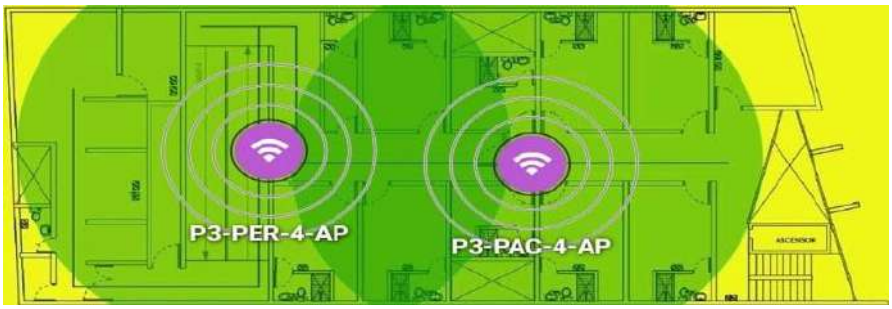

Figura 161. Nivel de señal bajo Tercer Piso

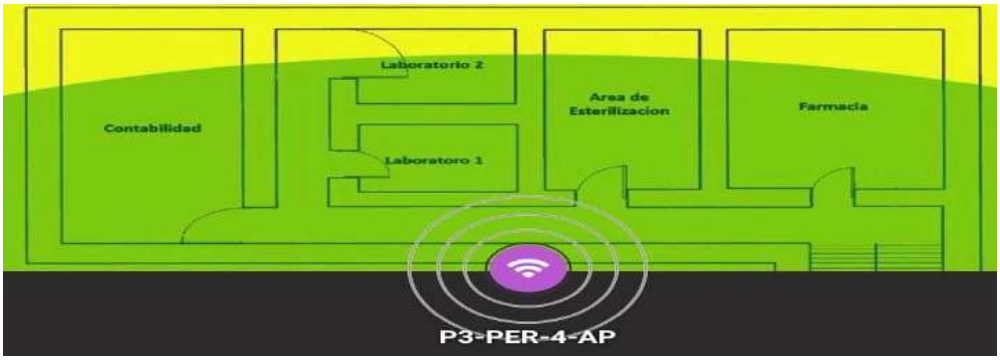

Figura 162. Nivel de señal bajo Extensión Tercer Piso

!!!	!	✓

Nivel de señal mínimo: -70 dBm Nivel de señal máximo: -10 dBm

Potencia de transmisión

La potencia de transmisión de los puntos de acceso 20 dBm (decibelios referenciados a un miliwatt) para el personal y 23 dBm para los pacientes corresponde a la energía con la que el equipo emite la señal. Sin embargo, cuando esta señal llega a los dispositivos, inevitablemente se reduce debido a la distancia, las paredes y otros obstáculos, por lo que se mide en valores negativos como −10 dBm a −70 dBm. En este rango, valores cercanos a −10 dBm indican una señal muy fuerte y estable, mientras que valores cercanos a −70 dBm reflejan una señal débil o al límite de la cobertura.

GHz indica la frecuencia de la señal inalámbrica, es decir, cuántos ciclos por segundo vibra la onda por ejemplo, 2.4 GHz ofrece más cobertura, pero menos velocidad, y 5 GHz menos cobertura pero más velocidad.

#	Nombre de la red	Banda	Máximo TX Power	Fabricante
1	PB-PER-1-AP P1-PER-2-AP P2-PER-3-AP P3-PER-4-AP	2.4GHz 5 GHz	20 dBm	TP-Link Technologies
2	PB-PAC-1-AP P1-PAC-2-AP P2-PAC-3-AP P3-PAC-4-AP	2.4 GHz 5 GHz	23 dBm	TP-Link Technologies

Tabla 103.Potencia de transmisión y banda

III.1.4.1.10.- Plan de Validación Técnica para compatibilidad con equipos físicos

Equipo	Prueba Realizada	Resultado Esperado	Resultado Obtenido	Acciones Correctivas (si es necesario)
Cisco Catalyst 3750X-12S-S	Ping entre equipos	Sin pérdidas de paquetes, latencia < 1ms	Conexión estable	No se requiere acción correctiva
TL-SG2210P V3 (10 puertos)	Ping entre equipos	Sin pérdidas de paquetes, latencia < 1ms	Conexión estable	No se requiere acción correctiva
Cisco WS-C2960S-24PD-L Catalyst 2960S	Ping entre equipos	Sin pérdidas de paquetes, latencia < 1ms	Conexión estable	No se requiere acción correctiva
Cisco 2901 - CISCO2901/K9	Prueba de enrutamiento y NAT	Sin pérdidas de paquetes, latencia < 2/6/14ms	Conexión estable	No se requiere acción correctiva
TP-Link EAP225	Pruebas de conectividad Wi-Fi (clientes)	Cobertura completa, con algunas interferencias, latencia < 83/38/17/36 ms	Conexión estable	Reconfigurar canales Wi-Fi si es necesario
Fortinet 60E	Pruebas de seguridad y firewall	Sin brechas de seguridad, filtrado efectivo	Conexión estable y controlada	No se requiere acción correctiva

Tabla 104. Plan de Validación Técnica para compatibilidad con equipos físicos

III.1.4.2.- 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 trabajará 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: Se usará el tester del sitio web oficial de Tigo para medir la velocidad.

Software de simulación para la configuración de red: Packet tracer y GNS3, Vmware.

Software de monitoreo: Glaswire, Wireshark.

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
- Configuración de parámetros de seguridad pueden afectar el desempeño.
- Tiempos de propagación.

- Elementos de almacenamientos (buffers)
- Elementos de seguridad de la red (Firewall)
- Velocidades de conexión.
- Protocolos de transporte.
- Protocolo TCP
- Protocolo UDP
- Otros protocolos
- IPSEC
- SIP

III.1.5.- Fase 5: Implementación puesta en marcha

En esta fase se llevará a cabo la instalación y configuración de todos los componentes de la red: Fortinet, servidor Issabel, access points, switches y routers.

El desarrollo se presentará de forma detallada y secuencial, similar a un manual de usuario, mostrando qué y cómo configurar cada equipo paso a paso.

Además, se incluirá el cronograma de implementación de la red, donde se especificarán las actividades, responsables y tiempos estimados para cada etapa del proceso.

Finalmente, se mostrarán las pruebas de conectividad, la verificación de servicios y la validación del funcionamiento general de la red, asegurando una puesta en marcha correcta y controlada.

- **Requisitos previos**: parámetros de red (VLAN, IP, DNS, QoS, NAT).
- **Fortinet:** políticas, filtrado web, segmentación y reglas de acceso.
- **Issabel:** extensiones, Colas y softphones (solo llamadas internas).
- **APs:** SSID para personal/pacientes, seguridad y asignación de VLAN.
- **Switches/Routers:** creación de VLAN, trunks, rutas y validaciones.

III.1.5.1.- Cronograma de implementación de la red

Actividad	Nº días	Fecha inicio	Fecha fin	S1	S2	S3	S4	S5
Implementación de los servicios requeridos	**25**	**08/08/2025**	**05/09/2025**	**X**	**X**	**X**	**X**	**X**
Instalación de racks y preparación de la infraestructura para los dispositivos de red.	3	08/08/2025	11/08/2025	X	X			
Instalación y configuración de los equipos de red (routers, switch, servidor DHCP, firewall y Servidor de telefonía IP)	8	12/08/2025	20/08/2025		X	X		
Conexión del cableado estructurado de la red (Cableado ethernet, Fibra Optica)	4	21/08/2025	25/08/2025			X	X	
Configuración de los equipos de computación a la red mediante cableado	3	26/08/2025	28/08/2025				X	X
Configuración de las laptops y dispositivos móviles de manera inalámbrica	2	29/08/2025	30/08/2025					X
Instalación y conexión de Zoiper en los dispositivos móviles	2	01/09/2025	02/09/2025					X
Instalación de programas hacia la red	2	03/09/2025	04/09/2025					X
Pruebas de la red	1	05/09/2025	05/09/2025					X

Tabla 105. Cronograma de implementación de la red

III.1.5.2.- Implementación del diseño de red en Packet tracer

III.1.5.2.1.- Comandos de la configuración de los dispositivos

Servidores

Durante la implementación, se configurarán los servidores principales de la red con direcciones IP estáticas, asegurando su disponibilidad continua y comunicación estable con los demás dispositivos del sistema.

El Servidor Asterisk se configurará con la IP 192.168.3.100, mientras que el Servidor Central del Sistema Clínico usará la 192.168.3.101, ambos dentro del mismo rango de red y conectados al gateway 192.168.3.1. La máscara de subred (255.255.255.0) permitirá la correcta segmentación dentro de su VLAN asignada.

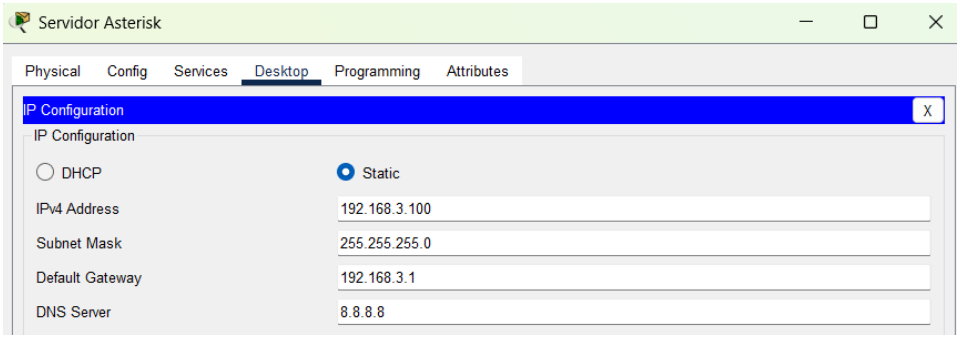

Figura 163. IP Servidor Asterisk

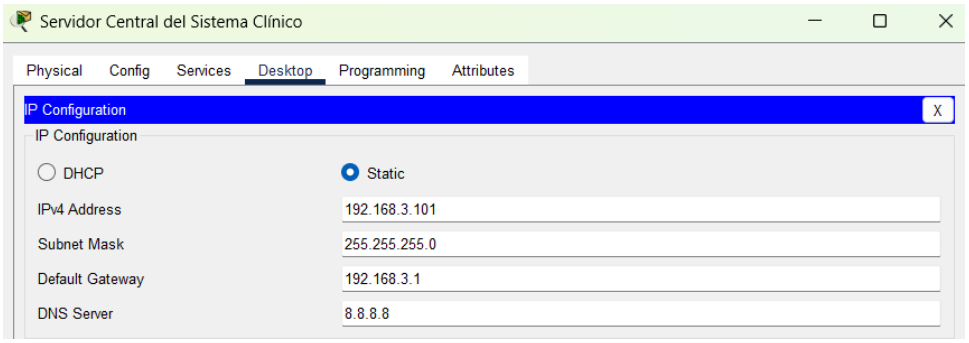

Figura 164. Servidor Central del Sistema Clínico

III.1.5.2.1.1.- Configuración del router

III.1.5.2.1.1.1.- Configuración de calidad de Servicio

En este apartado se realizará la configuración de la Calidad de Servicio (QoS) desde el modo consola del router principal de la clínica. Esta configuración permitirá optimizar el tráfico de red, priorizando los servicios más importantes como la telefonía IP y el sistema clínico para evitar cuellos de botella en la salida del router hacia la red principal. De esta manera, se garantiza un flujo de datos estable, eficiente y con menor latencia, mejorando el rendimiento general de la

infraestructura.

Se creará clases para Voz, Video y Soporte

RouterClinica>enable

RouterClinica#conf ter

RouterClinica(config)#class-map match-any VOZ

RouterClinica(config-cmap)# match protocol skinny

RouterClinica(config-cmap)# match protocol rtp

RouterClinica(config-cmap)#exit

RouterClinica(config)#class-map match-any VIDEO

RouterClinica(config-cmap)# match protocol rtp

RouterClinica(config-cmap)# match protocol udp

RouterClinica(config-cmap)#exit

RouterClinica(config)#class-map match-any SOPORTE

RouterClinica(config-cmap)# match protocol tftp

RouterClinica(config-cmap)# match protocol dhcp

RouterClinica(config-cmap)# match protocol icmp

RouterClinica(config-cmap)#exit

Creando el policy MAP con el nombre de CALIDAD

RouterClinica(config-cmap)#exitpolicy-map CALIDAD

RouterClinica(config-pmap)#class VOZ

RouterClinica(config-pmap-c)#priority percent 20

RouterClinica(config-pmap-c)#exit

RouterClinica(config-pmap)#class VIDEO

RouterClinica(config-pmap-c)#bandwidth percent 25

RouterClinica(config-pmap-c)#exit

RouterClinica(config-pmap)#class SOPORTE

RouterClinica(config-pmap-c)#bandwidth percent 10

RouterClinica(config-pmap-c)#exit

RouterClinica(config-pmap)#class class-default

RouterClinica(config-pmap-c)# fair-queue

Añadiendo hacia la Interfaz de cableado que es Gi 0/3/0 Fibra Óptica

RouterClinica(config)#interface gigabitEthernet 0/3/0

RouterClinica(config-if)#service

RouterClinica(config-if)#service-policy out

RouterClinica(config-if)#service-policy output CALIDAD

RouterClinica#show policy-map interface gigabitEthernet 0/3/0

Verificando la calidad de servicio implementado

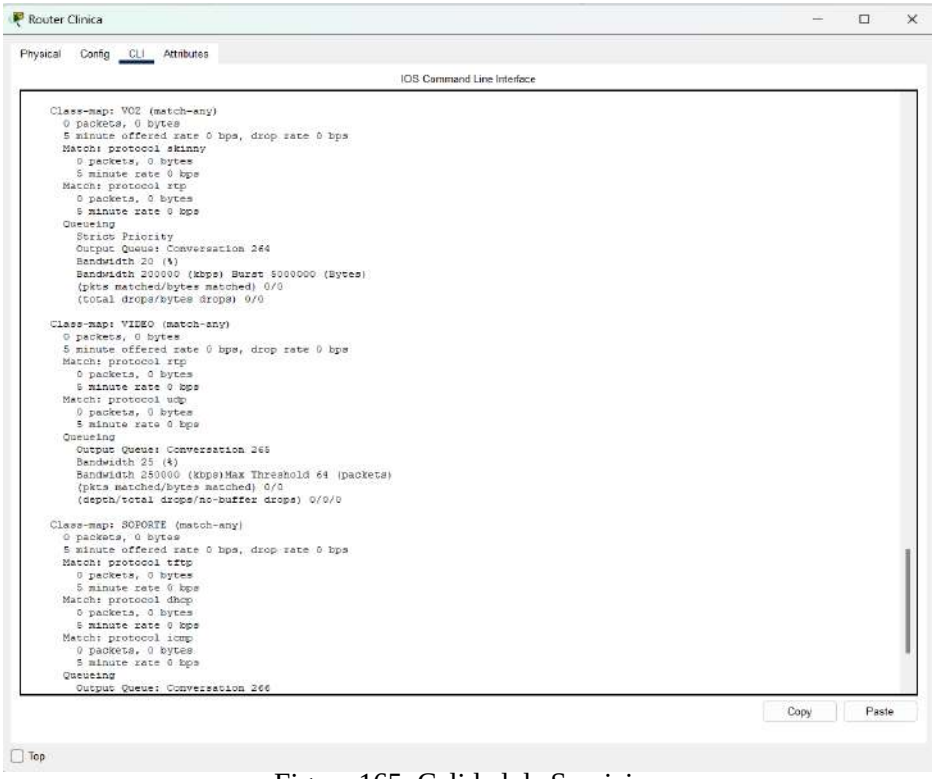

Figura 165. Calidad de Servicio

Lo que se está mostrando en la captura es la aplicación de Calidad de Servicio (QoS) en el router de la clínica, donde el tráfico de voz, video y soporte se clasifica y prioriza. Esto significa que, en caso de existir congestión o cuellos de botella, la red de la Clínica Santísima Trinidad asegurará que los servicios críticos como la telefonía IP y las videollamadas médicas tengan siempre prioridad sobre el resto del tráfico.

Dentro de la política se observan las siguientes clases:

- ✓ **VOZ**: incluye protocolos de telefonía IP como Skinny y RTP, configurados con prioridad estricta para que las llamadas siempre pasen primero en caso de congestión.
- ✓ **VIDEO**: clasifica tráfico de RTP y UDP, asignándole ancho de banda garantizado, de modo que las videollamadas médicas se mantengan estables.
- ✓ **SOPORTE**: agrupa protocolos como TFTP, ICMP, que sirven para transferencias y gestión de equipos, pero con prioridad menor frente a voz y video.

III.1.5.2.1.1.2.- Configuración de subinterfaces para las VLANS

La configuración de las VLANs en el router de la clínica se implementará mediante subinterfaces asignadas al puerto Gi0/3/0, donde cada VLAN contará con su propia puerta de enlace para gestionar el tráfico interno de forma segmentada.

Puerto del router	VLAN	Puerta de enlace
Gi0/3/0.10	VLAN10 INTERNACIÓN	192.168.2.1
Gi0/3/0.20	VLAN20 PACIENTES	192.168.2.33
Gi0/3/0.30	VLAN30 PERSONAL SALUD	192.168.2.49
Gi0/3/0.40	VLAN40 CONSULTORIOS	192.168.2.65
Gi0/3/0.50	VLAN50 ÁREA TERCERIZADA	192.168.2.81
Gi0/3/0.60	VLAN60 ADMINISTRACIÓN	192.168.2.97
Gi0/3/0.70	VLAN70 RECEPCIÓN	192.168.2.105
Gi0/3/0.80	VLAN80 EMERGENCIAS	192.168.2.113
Gi0/3/0.90	VLAN90 ENFERMERÍA	192.168.2.121
Gi0/3/0.100	VLAN100 TERAPIA INTENSIVA	192.168.2.129
Gi0/3/0.110	VLAN110 PEDIATRÍA	192.168.2.137
Gi0/3/0.120	VLAN120 FARMACIA	192.168.2.145
Gi0/3/0.130	VLAN130 ESTERILIZACIÓN	192.168.2.153
Gi0/3/0.140	VLAN140 CONTABILIDAD	192.168.2.161
Gi0/3/0.150	VLAN150 SERVIDORES	192.168.3.1

Tabla 106. Configuración de subinterfaces

Primero se accederá a la interfaz “GigabitEthernet 0/3/0” luego se aplica el comando “encapsulation dot1Q” para asociarla a la VLAN, permitiendo el uso del protocolo 802.1Q.

Después, con “ip address”, se asigna la dirección IP y máscara de subred que servirá como puerta de enlace para esa VLAN.

```
RouterClinica#conf terminal
RouterClinica(config)#interface gigabitEthernet 0/3/0.10
RouterClinica(config-subif)# encapsulation dot1Q 10
RouterClinica(config-subif)# ip address 192.168.2.1 255.255.255.224
RouterClinica(config-subif)#exit
RouterClinica(config)#interface gigabitEthernet 0/3/0.20
RouterClinica(config-subif)#encapsulation dot1Q 20
RouterClinica(config-subif)#ip address 192.168.2.33 255.255.255.240
```

```
RouterClinica(config-subif)#exit
RouterClinica(config)#interface gigabitEthernet 0/3/0.30
RouterClinica(config-subif)#encapsulation dot1Q 30
RouterClinica(config-subif)#ip address 192.168.2.49 255.255.255.240
RouterClinica(config-subif)#exit
RouterClinica(config)#interface gigabitEthernet 0/3/0.40
RouterClinica(config-subif)# encapsulation dot1Q 40
RouterClinica(config-subif)# ip address 192.168.2.65 255.255.255.240
RouterClinica(config-subif)#exit
RouterClinica(config)#interface gigabitEthernet 0/3/0.50
RouterClinica(config-subif)# encapsulation dot1Q 50
RouterClinica(config-subif)# ip address 192.168.2.81 255.255.255.240
RouterClinica(config-subif)#exit
RouterClinica(config)#interface gigabitEthernet 0/3/0.60
RouterClinica(config-subif)# encapsulation dot1Q 60
RouterClinica(config-subif)# ip address 192.168.2.97 255.255.255.248
RouterClinica(config-subif)#exit
RouterClinica(config)#interface gigabitEthernet 0/3/0.70
RouterClinica(config-subif)# encapsulation dot1Q 70
RouterClinica(config-subif)# ip address 192.168.2.105 255.255.255.248
RouterClinica(config-subif)#exit
RouterClinica(config)#interface gigabitEthernet 0/3/0.80
RouterClinica(config-subif)# encapsulation dot1Q 80
RouterClinica(config-subif)# ip address 192.168.2.113 255.255.255.248
RouterClinica(config-subif)#exit
RouterClinica(config)#interface gigabitEthernet 0/3/0.90
RouterClinica(config-subif)# encapsulation dot1Q 90
RouterClinica(config-subif)# ip address 192.168.2.121 255.255.255.248
RouterClinica(config-subif)#exit
RouterClinica(config)#interface gigabitEthernet 0/3/0.100
RouterClinica(config-subif)# encapsulation dot1Q 100
RouterClinica(config-subif)# ip address 192.168.2.129 255.255.255.248
RouterClinica(config-subif)#exit
RouterClinica(config)#interface gigabitEthernet 0/3/0.110
```

RouterClinica(config-subif)# encapsulation dot1Q 110
RouterClinica(config-subif)# ip address 192.168.2.137 255.255.255.248
RouterClinica(config-subif)#exit
RouterClinica(config)#interface gigabitEthernet 0/3/0.120
RouterClinica(config-subif)# encapsulation dot1Q 120
RouterClinica(config-subif)# ip address 192.168.2.145 255.255.255.248
RouterClinica(config-subif)#exit
RouterClinica(config)#interface gigabitEthernet 0/3/0.130
RouterClinica(config-subif)# encapsulation dot1Q 130
RouterClinica(config-subif)# ip address 192.168.2.153 255.255.255.248
RouterClinica(config-subif)#exit
RouterClinica(config)#interface gigabitEthernet 0/3/0.140
RouterClinica(config-subif)# encapsulation dot1Q 140
RouterClinica(config-subif)# ip address 192.168.2.161 255.255.255.248
RouterClinica(config-subif)#exit
RouterClinica(config)#interface gigabitEthernet 0/3/0.150
RouterClinica(config-subif)#encapsulation dot1Q 150
RouterClinica(config-subif)#ip address 192.168.3.1 255.255.255.0
RouterClinica(config-subif)#exit

III.1.5.2.1.1.3.- Configuración del NAT

En esta etapa se realizará la simulación de la conexión a Internet del Router de la Clínica hacia el Router del ISP. Dado que Packet Tracer no tiene acceso real a Internet, se implementará una simulación funcional del NAT (Network Address Translation) para representar el proceso de salida de las direcciones IP privadas hacia una red externa.

Se configurará la interfaz Serial 0/2/0 como NAT outside, las subinterfaces VLAN como NAT inside, y una lista de acceso que identifique las IP privadas permitidas. También se aplicará NAT con sobrecarga (overload) para optimizar la conexión y una ruta por defecto hacia el ISP.

Finalmente, el router del ISP simulará el DNS de Google (8.8.8.8) y el enrutamiento estático, completando la simulación del tráfico externo.

Asignación de IP para el Serial 0/2/0

RouterClinica#conf terminal
RouterClinica(config)#interface serial 0/2/0
RouterClinica(config-if)#ip address 30.0.0.1 255.255.255.252

Configurando el NAT de tipo outside (salida)

RouterClinica(config-if)#ip nat outside

RouterClinica(config-if)#no shutdown

RouterClinica(config-if)#exit

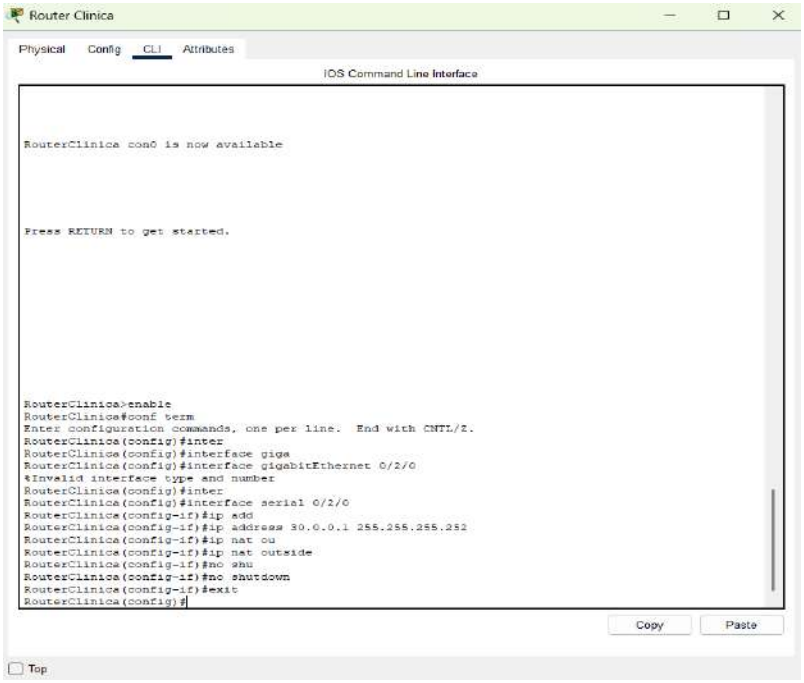

Figura 166. NAT outside (salida)

Configurando las Subinterfaces de tipo Inside (entrada)

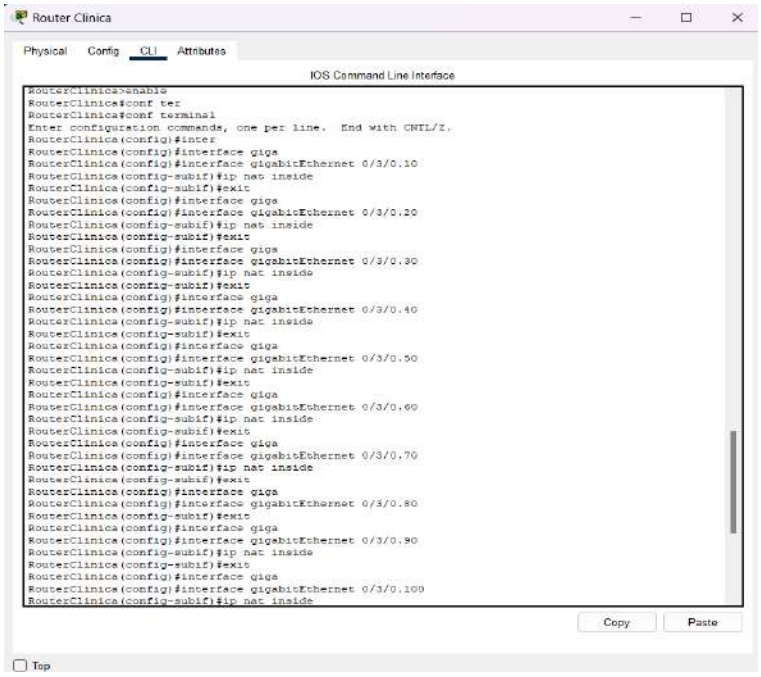

Figura 167. NAT inside (entrada)

Creando el acceso a listas que identifique qué direcciones privadas que se van a traducir

RouterClinica>enable

RouterClinica#conf terminal

RouterClinica(config)#access-list 1 permit 192.168.0.0 0.0.255.255

Figura 168. Cubre todas las VLANs en 192.168.x.x.

Salida de IPs privadas con la pública por el Serial 0/2/0

Overload indica que cada IP agarre diferentes puertos para la salida del Serial y así no existan embotellamientos:

RouterClinica(config)#ip nat inside source list 1 interface Serial 0/2/0 overload

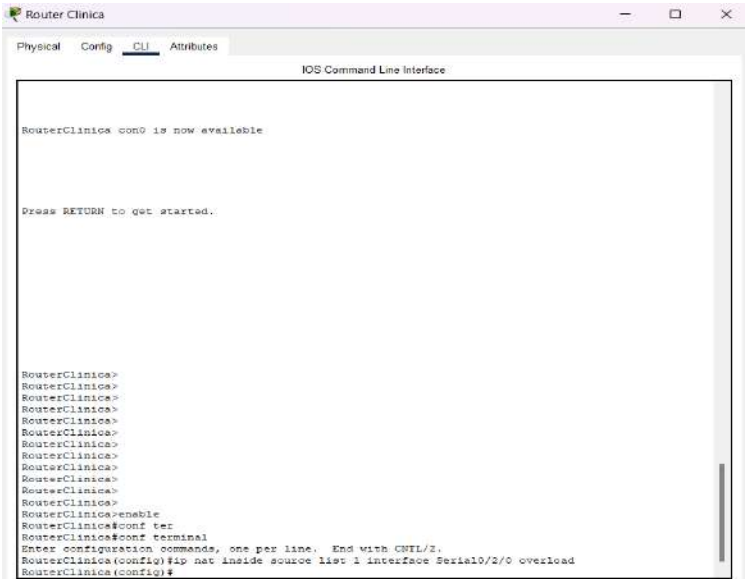

Figura 169. IP NAT Inside Serial

Ruta por defecto hacia el ISP

RouterClinica(config)#ip route 0.0.0.0 0.0.0.0 30.0.0.2

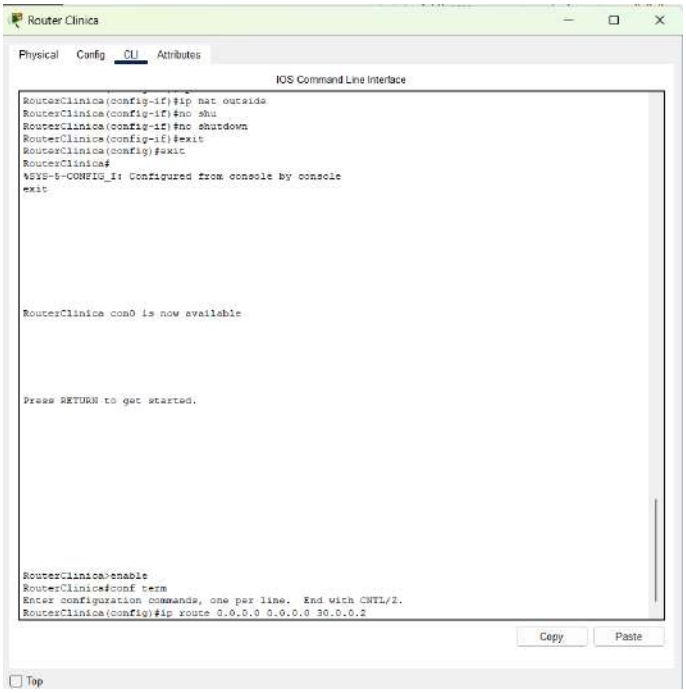

Figura 170. Enrutamiento por defecto

Configuración Simulación del Router ISP(Internet)

Configurando la IP del Serial 0/3/0

Router>enable

Router#conf terminal

Router(config)#interface serial 0/3/0

Router(config-if)#ip address 30.0.0.2 255.255.255.252

Router(config-if)#no shutdown

Router(config-if)#exit

Simular DNS de Google

Router(config)#interface Loopback0

Router(config-if)#ip address 8.8.8.8 255.255.255.255

Router(config-if)#exit

Enrutamiento Stático

Router(config)#ip route 192.168.0.0 255.255.0.0 10.0.0.1

Router(config)#

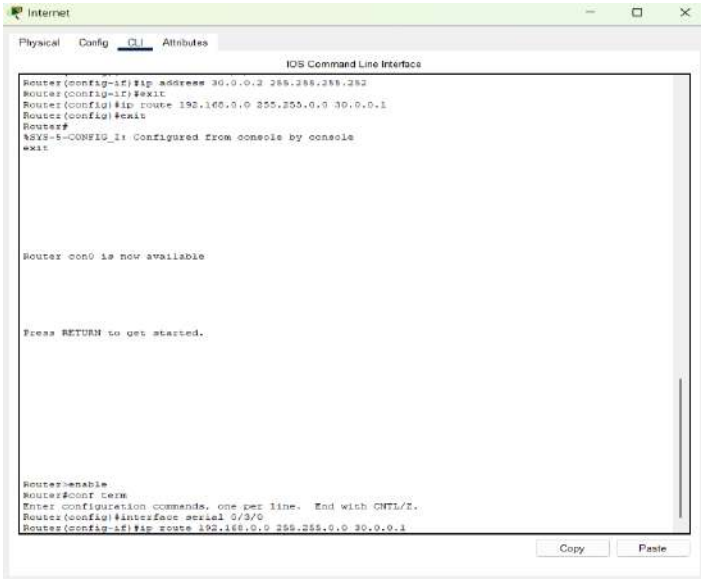

Figura 171. Configuración Simulación ISP

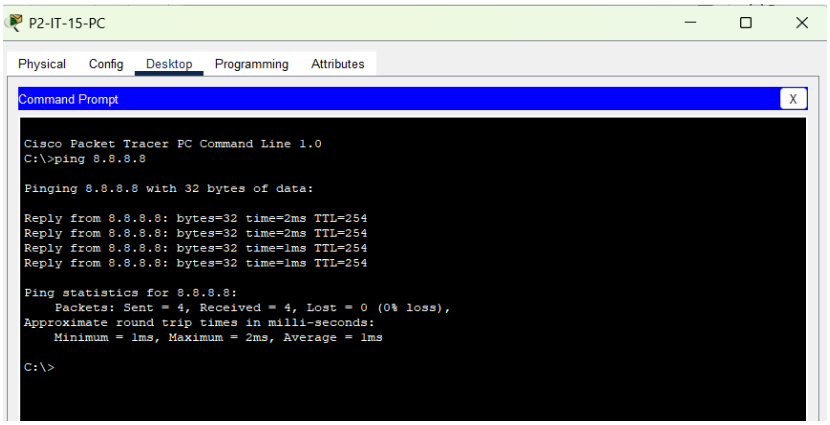

Figura 172. ping hacia los servicios de Google NAT

III.1.5.2.1.2.- Configuración en los Switch

III.1.5.2.1.2.1.- Creando VLAN 150 y accediendo al modo Access

En esta configuración se crea la VLAN 150 denominada *Servidores* y se asignan los puertos FastEthernet 1/1 y 0/1 en modo access, conectando directamente los equipos del área de servidores. Aunque esta VLAN tiene su propio segmento de red, mantiene comunicación con las demás VLANs a través del router y switch de capa 3, permitiendo el intercambio de información entre áreas según las políticas establecidas.

Configuración:

SwitchP>enable

SwitchP#conf terminal

SwitchP(config)#vlan 150

SwitchP(config-vlan)#name Servidores
SwitchP(config-vlan)#exit
SwitchP(config)#interface fastEthernet 1/1
SwitchP(config-if)#switchport mode access
SwitchP(config-if)#switchport access vlan 150
SwitchP(config-if)#exit
SwitchP(config)#interface fastEthernet 0/1
SwitchP(config-if)#switchport mode access
SwitchP(config-if)#switchport access vlan 150
SwitchP(config-if)#exit

III.1.5.2.1.2.2.- Configuración modo troncal con fibra a las interfaces del switch

En esta configuración se establecen los enlaces troncales entre el switch principal y los switches de fibra óptica de cada planta (planta baja, primer, segundo y tercer piso).

El modo trunk permite que un mismo enlace transporte tráfico de múltiples VLANs usando etiquetado 802.1Q, lo que facilita la comunicación entre las diferentes áreas de la clínica a través de la fibra óptica.

De esta forma, los switches de cada piso pueden intercambiar información entre VLANs mediante el router o switch de capa 3, garantizando una conexión estable, rápida y centralizada dentro de toda la red.

Switch Principal

SwitchP(config)#interface gigabitEthernet 9/1
SwitchP(config-if)#switchport mode trunk
SwitchP(config-if)#exit
SwitchP(config)#interface gigabitEthernet4/1
SwitchP(config-if)#switchport mode trunk
SwitchP(config-if)#exit
SwitchP(config)#interface gigabitEthernet 6/1
SwitchP(config-if)#switchport mode trunk
SwitchP(config-if)#exit
SwitchP(config)#interface gigabitEthernet 5/1
SwitchP(config-if)#switchport mode trunk
SwitchP(config-if)#exit
SwitchP(config)#interface gigabitEthernet 7/1
SwitchP(config-if)#switchport mode trunk

SwitchP(config-if)#exit

Switch fibra Planta Baja

SwitchFibraPB#conf terminal

SwitchFibraPB(config)#interface gigabitEthernet 4/1

SwitchFibraPB(config-if)#switchport mode trunk

SwitchFibraPB(config-if)#exit

SwitchFibraPB(config)#interface fastEthernet 0/1

SwitchFibraPB(config-if)#switchport mode trunk

SwitchFibraPB(config-if)#end

Switch Fibra Primer Piso

SwitchFibraP1#conf terminal

SwitchFibraP1(config)#interface gigabitEthernet 6/1

SwitchFibraP1(config-if)#switchport mode trunk

SwitchFibraP1(config-if)#exit

SwitchFibraP1(config)#interface fastEthernet 0/1

SwitchFibraP1(config-if)#switchport mode trunk

SwitchFibraP1(config-if)#exit

Switch Fibra Segundo Piso

SwitchFibraP2#conf terminal

SwitchFibraP2(config)#interface gigabitEthernet 4/1

SwitchFibraP2(config-if)#switchport mode trunk

SwitchFibraP2(config-if)#exit

SwitchFibraP2(config)#interface fastEthernet 0/1

SwitchFibraP2(config-if)#switchport mode trunk

SwitchFibraP2(config-if)#exit

Switch Fibra Tercer Piso

SwitchFribaP3#conf terminal

SwitchFribaP3(config)#interface gigabitEthernet 4/1

SwitchFribaP3(config-if)#switchport mode trunk

SwitchFribaP3(config-if)#exit

SwitchFribaP3(config)#interface fastEthernet 0/1

SwitchFribaP3(config-if)#switchport mode trunk

III.1.5.2.1.2.3.- Configuración de switch modo troncal usando cable de cobre UTP

En esta configuración se establecen los enlaces troncales mediante cable UTP entre los switches de

cada piso. El modo trunk permite el tráfico simultáneo de varias VLANs por un mismo puerto (Fa0/24), garantizando la comunicación entre las áreas y la integración con el resto de la red.

Switch Planta Baja

SwitchPB#conf terminal

SwitchPB(config)#interface fastEthernet 0/24

SwitchPB(config-if)#switchport mode trunk

SwitchPB(config-if)#end

Switch Primer Piso

SwitchP1#conf terminal

SwitchP1(config)#interface fastEthernet 0/24

SwitchP1(config-if)#switchport mode trunk

SwitchP1(config-if)#exit

Switch Segundo Piso

SwitchP2#conf terminal

SwitchP2(config)#interface fastEthernet 0/24

SwitchP2(config-if)#switchport mode trunk

SwitchP2(config-if)#end

Switch Tercer Piso

SwitchP3#conf terminal

SwitchP3(config)#interface fastEthernet 0/24

SwitchP3(config-if)#switchport mode trunk

SwitchP3(config-if)#exit

III.1.5.2.1.2.4.- Configuración de VLAN y servidor DHCP en los switches

En esta etapa se realiza la configuración de las VLANs y DHCP de cada piso.

Cada VLAN representa un área específica (por ejemplo, *Internación, Pacientes, Administración*, etc.) y cuenta con su propia dirección IP, puerta de enlace y rango DHCP, lo que permite asignar direcciones automáticamente a los dispositivos conectados.

Los puertos de los switches se configuran en modo access para cada VLAN según el área correspondiente, mientras que las interfaces VLAN del switch principal actúan como servidores DHCP, distribuyendo las direcciones IP.

Aunque las configuraciones son similares entre VLANs, varían en nombres, rangos de red y parámetros de DNS, garantizando una segmentación ordenada y comunicación eficiente entre las diferentes zonas de la clínica.

Vlan10:

SwitchP#conf terminal

SwitchP(config)#vlan 10

SwitchP(config-vlan)#name Internacion

SwitchP(config-vlan)#exit

SwitchP(config)#interface vlan 10

SwitchP(config-if)#ip address 192.168.2.30 255.255.255.224

SwitchP(config-if)#no shutdown

SwitchP(config-if)#exit

SwitchP(config)#ip dhcp pool vlan10

SwitchP(dhcp-config)#network 192.168.2.0 255.255.255.224

SwitchP(dhcp-config)#default-router 192.168.2.1

SwitchP(dhcp-config)# dns-server 192.168.3.100

SwitchP(dhcp-config)#exit

SwitchP(config)#ip dhcp excluded-address 192.168.2.1

SwitchP(config)#ip dhcp excluded-address 192.168.2.30

P1

SwitchFibraP1#conf terminal

SwitchFibraP1(config)#vlan 10

SwitchFibraP1(config-vlan)#name Internacion

SwitchFibraP1(config-vlan)#exit

Impresora

SwitchFibraP1(config)#interface fastEthernet 8/1

SwitchFibraP1(config-if)#switchport mode access

SwitchFibraP1(config-if)#switchport access vlan 10

SwitchFibraP1(config-if)#exit

SwitchP1#conf terminal

SwitchP1(config)#vlan 10

SwitchP1(config-vlan)#name Internacion

SwitchP1(config-vlan)#exit

SwitchP1(config)#interface range fastEthernet 0/1-7

SwitchP1(config-if-range)#switchport mode access

SwitchP1(config-if-range)#switchport access vlan 10

SwitchP1(config-if-range)#exit

P2

SwitchFibraP2#conf terminal

SwitchFibraP2(config)#vlan 10

SwitchFibraP2(config-vlan)#name Internacion

SwitchFibraP2(config-vlan)#exit

Impresora

SwitchFibraP2(config)#interface fastEthernet 9/1

SwitchFibraP2(config-if)#switchport mode access

SwitchFibraP2(config-if)#switchport access vlan 10

SwitchFibraP2(config-if)#exit

SwitchP2#conf terminal

SwitchP2(config)#vlan 10

SwitchP2(config-vlan)#name Internacion

SwitchP2(config-vlan)#exit

SwitchP2(config)#interface range fastEthernet 0/1-7

SwitchP2(config-if-range)#switchport mode access

SwitchP2(config-if-range)#switchport access vlan 10

SwitchP2(config-if-range)#exit

P3

SwitchFribaP3(config)#conf term

SwitchFribaP3(config)#vlan 10

SwitchFribaP3(config-vlan)#name Internacion

SwitchFribaP3(config-vlan)#exit

Impresora

SwitchFribaP3(config)#interface fastEthernet 6/1

SwitchFribaP3(config-if)#switchport mode access

SwitchFribaP3(config-if)#switchport access vlan 10

SwitchFribaP3(config-if)#exit

SwitchP3(config)#vlan 10

SwitchP3(config-vlan)#name Internacion

SwitchP3(config-vlan)#exit

SwitchP3(config)#interface range fastEthernet 0/6-10

SwitchP3(config-if-range)#switchport mode access

SwitchP3(config-if-range)#switchport access vlan 10

SwitchP3(config-if-range)#end

Vlan20 Wifi:

SwitchP#conf terminal

SwitchP(config)#vlan 20

SwitchP(config-vlan)#name Pacientes

SwitchP(config-vlan)#exit

SwitchP(config)#interface vlan 20

SwitchP(config-if)#ip address 192.168.2.46 255.255.255.240

SwitchP(config-if)#no shutdown

SwitchP(config-if)#exit

SwitchP(config)#ip dhcp pool vlan20

SwitchP(dhcp-config)#network 192.168.2.32 255.255.255.240

SwitchP(dhcp-config)#default-router 192.168.2.33

SwitchP(dhcp-config)#dns-server 8.8.8.8

SwitchP(dhcp-config)#exit

SwitchP(config)#ip dhcp excluded-address 192.168.2.33

SwitchP(config)#ip dhcp excluded-address 192.168.2.46

PB

SwitchFibraPB#conf terminal

SwitchFibraPB(config)#vlan 20

SwitchFibraPB(config-vlan)#name Pacientes

SwitchFibraPB(config-vlan)#exit

SwitchPB#conf terminal

SwitchPB(config)#vlan 20

SwitchPB(config-vlan)#name Pacientes

SwitchPB(config-vlan)#exit

SwitchPB(config)#interface fastEthernet 0/23

SwitchPB(config-if)#switchport mode access

SwitchPB(config-if)#switchport access vlan 20

SwitchPB(config-if)#exit

SwitchPB(config)#interface fastEthernet 0/20

SwitchPB(config-if)#switchport mode access

SwitchPB(config-if)#switchport access vlan 20

SwitchPB(config-if)#exit

P1

SwitchFibraP1#conf terminal

SwitchFibraP1(config)#vlan 20

SwitchFibraP1(config-vlan)#name Pacientes

SwitchFibraP1(config-vlan)#exit

SwitchP1#conf terminal

SwitchP1(config)#vlan 20

SwitchP1(config-vlan)#name Pacientes

SwitchP1(config-vlan)#exit

SwitchP1(config)#interface fastEthernet 0/23

SwitchP1(config-if)#switchport mode access

SwitchP1(config-if)#switchport access vlan 20

SwitchP1(config-if)#end

P2

SwitchFibraP2#conf terminal

SwitchFibraP2(config)#vlan 20

SwitchFibraP2(config-vlan)#name Pacientes

SwitchFibraP2(config-vlan)#exit

SwitchP2#conf terminal

SwitchP2(config)#vlan 20

SwitchP2(config-vlan)#name Pacientes

SwitchP2(config-vlan)#exit

SwitchP2(config)#interface fastEthernet 0/23

SwitchP2(config-if)#switchport mode access

SwitchP2(config-if)#switchport access vlan 20

SwitchP2(config-if)#end

P3

SwitchFribaP3#conf terminal

SwitchFribaP3(config)#vlan 20

SwitchFribaP3(config-vlan)#name Pacientes

SwitchFribaP3(config-vlan)#exit

SwitchP3#conf terminal

SwitchP3(config)#vlan 20

SwitchP3(config-vlan)#name Pacientes

SwitchP3(config-vlan)#exit

SwitchP3(config)#interface fastEthernet 0/23

SwitchP3(config-if)#switchport mode access

SwitchP3(config-if)#switchport access vlan 20

SwitchP3(config-if)#end

Vlan30 Wifi:

SwitchP(config)#vlan 30

SwitchP(config-vlan)#name PersonalSalud

SwitchP(config-vlan)#exit

SwitchP(config)#interface vlan 30

SwitchP(config-if)#ip address 192.168.2.62 255.255.255.240

SwitchP(config-if)#no shutdown

SwitchP(config-if)#exit

SwitchP(config)#ip dhcp pool vlan30

SwitchP(dhcp-config)#network 192.168.2.48 255.255.255.240

SwitchP(dhcp-config)#default-router 192.168.2.49

SwitchP(dhcp-config)# dns-server 192.168.3.100

SwitchP(dhcp-config)#exit

SwitchP(config)#ip dhcp excluded-address 192.168.2.49

SwitchP(config)#ip dhcp excluded-address 192.168.2.62

PB

SwitchFibraPB#conf terminal

SwitchFibraPB(config)#vlan 30

SwitchFibraPB(config-vlan)#name PersonalSalud

SwitchFibraPB(config-vlan)#exit

SwitchPB#conf terminal

SwitchPB(config)#vlan 30

SwitchPB(config-vlan)#name PersonalSalud

SwitchPB(config-vlan)#exit

SwitchPB(config)#interface range fastEthernet 0/21-22

SwitchPB(config-if)#switchport mode access

SwitchPB(config-if)#switchport access vlan 30

SwitchPB(config-if)#end

P1

SwitchFibraP1#conf terminal

SwitchFibraP1(config)#vlan 30

SwitchFibraP1(config-vlan)#name PersonalSalud

SwitchFibraP1(config-vlan)#exit

SwitchP1#conf terminal

SwitchP1(config)#vlan 30

SwitchP1(config-vlan)#name PersonalSalud

SwitchP1(config-vlan)#exit

SwitchP1(config)#interface fastEthernet 0/22

SwitchP1(config-if)#switchport mode access

SwitchP1(config-if)#switchport access vlan 30

SwitchP1(config-if)#end

P2

SwitchFibraP2#conf terminal

SwitchFibraP2(config)#vlan 30

SwitchFibraP2(config-vlan)#name PersonalSalud

SwitchFibraP2(config-vlan)#exit

SwitchP2#conf terminal

SwitchP2(config)#vlan 30

SwitchP2(config-vlan)#name PersonalSalud

SwitchP2(config-vlan)#exit

SwitchP2(config)#interface fastEthernet 0/22

SwitchP2(config-if)#switchport mode access

SwitchP2(config-if)#switchport access vlan 30

SwitchP2(config-if)#end

P3

SwitchFribaP3#conf terminal

SwitchFribaP3(config)#vlan 30

SwitchFribaP3(config-vlan)#name PersonalSalud

SwitchFribaP3(config-vlan)#exit

SwitchP3#conf terminal

SwitchP3(config)#vlan 30

SwitchP3(config-vlan)#name PersonalSalud

SwitchP3(config-vlan)#exit

SwitchP3(config)#interface fastEthernet 0/22

SwitchP3(config-if)#switchport mode access

SwitchP3(config-if)#switchport access vlan 30

SwitchP3(config-if)#end

Vlan40

SwitchP#conf terminal

SwitchP(config)#vlan 40

SwitchP(config-vlan)#name Consultoria

SwitchP(config-vlan)#exit

SwitchP(config)#interface vlan 40

SwitchP(config-if)#ip address 192.168.2.78 255.255.255.240

SwitchP(config-if)#no shutdown

SwitchP(config-if)#exit

SwitchP(config)#ip dhcp pool vlan40

SwitchP(dhcp-config)#network 192.168.2.64 255.255.255.240

SwitchP(dhcp-config)#default-router 192.168.2.65

SwitchP(dhcp-config)# dns-server 192.168.3.100

SwitchP(dhcp-config)#exit

SwitchP(config)#ip dhcp excluded-address 192.168.2.65

SwitchP(config)#ip dhcp excluded-address 192.168.2.78

PB

SwitchFibraPB#conf terminal

SwitchFibraPB(config)#vlan 40

SwitchFibraPB(config-vlan)#name Consultoria

SwitchFibraPB(config-vlan)#exit

SwitchFibraPB(config)#interface fastEthernet 3/1

SwitchFibraPB(config-if)#switchport mode access

SwitchFibraPB(config-if)#switchport access vlan 40

SwitchFibraPB(config-if)#exit

SwitchFibraPB(config)#interface range fastEthernet 5-8/1

SwitchFibraPB(config-if)#switchport mode access

SwitchFibraPB(config-if)#switchport access vlan 40

SwitchFibraPB(config-if)#exit

SwitchPB#conf terminal

SwitchPB(config)#vlan 40

SwitchPB(config-vlan)#name Consultoria

SwitchPB(config-vlan)#exit

SwitchPB(config)#interface range fastEthernet 0/4-8

SwitchPB(config-if-range)#switchport mode access

SwitchPB(config-if-range)#switchport access vlan 40

SwitchPB(config-if-range)#end

Vlan50:

SwitchP(config)#vlan 50

SwitchP(config-vlan)#name AreaTercerizada

SwitchP(config-vlan)#exit

SwitchP(config)#interface vlan 50

SwitchP(config-if)#ip address 192.168.2.94 255.255.255.240

SwitchP(config-if)#no shutdown

SwitchP(config-if)#exit

SwitchP(config)#ip dhcp pool vlan50

SwitchP(dhcp-config)#network 192.168.2.80 255.255.255.240

SwitchP(dhcp-config)#default-router 192.168.2.81

SwitchP(dhcp-config)# dns-server 192.168.3.100

SwitchP(dhcp-config)#exit

SwitchP(config)#ip dhcp excluded-address 192.168.2.81

SwitchP(config)#ip dhcp excluded-address 192.168.2.94

PB

SwitchFibraPB(config)#vlan 50

SwitchFibraPB(config-vlan)#name AreaTercerizada

SwitchFibraPB(config-vlan)#exit

SwitchFibraPB(config)#interface fastEthernet 2/1

SwitchFibraPB(config-if)#switchport mode access

SwitchFibraPB(config-if)#switchport access vlan 50

SwitchPB#conf terminal

SwitchPB(config)#vlan 50

SwitchPB(config-vlan)#name AreaTercerizada

SwitchPB(config-vlan)#exit

SwitchPB(config)#interface range fastEthernet 0/9-12

SwitchPB(config-if-range)#switchport mode access

SwitchPB(config-if-range)#switchport access vlan 50

SwitchPB(config-if-range)#exit

P3

SwitchFribaP3#conf terminal

SwitchFribaP3(config)#vlan 50

SwitchFribaP3(config-vlan)#name AreaTercerizada

SwitchFribaP3(config-vlan)#exit

SwitchP3#conf terminal

SwitchP3(config)#vlan 50

SwitchP3(config-vlan)#name AreaTercerizada

SwitchP3(config-vlan)#exit

SwitchP3(config)#interface fastEthernet 0/1

SwitchP3(config-if)#switchport mode access

SwitchP3(config-if)#switchport access vlan 50

SwitchP3(config-if)#end

Vlan60:

SwitchP(config)#vlan 60

SwitchP(config-vlan)#name Administracion

SwitchP(config-vlan)#exit

SwitchP(config)#interface vlan 60

SwitchP(config-if)#ip address 192.168.2.102 255.255.255.248

SwitchP(config-if)#no shutdown

SwitchP(config-if)#exit

SwitchP(config)#ip dhcp pool vlan60

SwitchP(dhcp-config)#network 192.168.2.96 255.255.255.248

SwitchP(dhcp-config)#default-router 192.168.2.97

SwitchP(dhcp-config)# dns-server 192.168.3.100

SwitchP(dhcp-config)#exit

SwitchP(config)#ip dhcp excluded-address 192.168.2.97

SwitchP(config)#ip dhcp excluded-address 192.168.2.102

PB

SwitchFibraPB#conf terminal

SwitchFibraPB(config)#vlan 60

SwitchFibraPB(config-vlan)#name Administracion

SwitchFibraPB(config-vlan)#exit

Impresoras

SwitchFibraPB(config)#interface fastEthernet 9/1

SwitchFibraPB(config-if)#switchport mode access

SwitchFibraPB(config-if)#switchport access vlan 60

SwitchFibraPB(config-if)#exit

SwitchPB(config)#vlan 60

SwitchPB(config-vlan)#name Administracion

SwitchPB(config-vlan)#exit

SwitchPB(config)#interface range fastEthernet 0/1-3

SwitchPB(config-if-range)#switchport mode access

SwitchPB(config-if-range)#switchport access vlan 60

SwitchPB(config-if-range)#end

Vlan70:

SwitchP(config)#vlan 70

SwitchP(config-vlan)#name Recepcion

SwitchP(config-vlan)#exit

SwitchP(config)#interface vlan 70

SwitchP(config-if)#ip address 192.168.2.110 255.255.255.248

SwitchP(config-if)#no shutdown

SwitchP(config-if)#exit

SwitchP(config)#ip dhcp pool vlan70

SwitchP(dhcp-config)#network 192.168.2.104 255.255.255.248

SwitchP(dhcp-config)#default-router 192.168.2.105

SwitchP(dhcp-config)# dns-server 192.168.3.100

SwitchP(dhcp-config)#exit

SwitchP(config)#ip dhcp excluded-address 192.168.2.105

SwitchP(config)#ip dhcp excluded-address 192.168.2.110

SwitchP(config)#end

PB

SwitchFibraPB(config)#vlan 70

SwitchFibraPB(config-vlan)#name Recepcion

SwitchFibraPB(config-vlan)#exit

SwitchPB#conf terminal

SwitchPB(config)#vlan 70

SwitchPB(config-vlan)#name Recepcion

SwitchPB(config-vlan)#exit

SwitchPB(config)#interface range fastEthernet 0/14-15

SwitchPB(config-if)#switchport mode access

SwitchPB(config-if)#switchport access vlan 70

SwitchPB(config-if)#end

Vlan80:

SwitchP#conf terminal

SwitchP(config)#vlan 80

SwitchP(config-vlan)#name Emergencias

SwitchP(config-vlan)#exit

SwitchP(config)#interface vlan 80

SwitchP(config-if)#ip address 192.168.2.118 255.255.255.248

SwitchP(config-if)#no shutdown

SwitchP(config-if)#exit

SwitchP(config)#ip dhcp pool vlan80

SwitchP(dhcp-config)#network 192.168.2.112 255.255.255.248

SwitchP(dhcp-config)#default-router 192.168.2.113

SwitchP(dhcp-config)# dns-server 192.168.3.100

SwitchP(dhcp-config)#exit

SwitchP(config)#ip dhcp excluded-address 192.168.2.113

SwitchP(config)#ip dhcp excluded-address 192.168.2.118

PB

SwitchFibraPB#conf terminal

SwitchFibraPB(config)#vlan 80

SwitchFibraPB(config-vlan)#name Emergencias

SwitchFibraPB(config-vlan)#exit

SwitchPB(config)#vlan 80

SwitchPB(config-vlan)#name Emergencias

SwitchPB(config-vlan)#exit

SwitchPB(config)#interface fastEthernet 0/13

SwitchPB(config-if)#switchport mode access

SwitchPB(config-if)#switchport access vlan 80

SwitchPB(config-if)#exit

Vlan90:

SwitchP(config)#vlan 90

SwitchP(config-vlan)#name Enfermeria

SwitchP(config-vlan)#exit

SwitchP(config)#interface vlan 90

SwitchP(config-if)#ip address 192.168.2.126 255.255.255.248

SwitchP(config-if)#no shutdown

SwitchP(config-if)#exit

SwitchP(config)#ip dhcp pool vlan90

SwitchP(dhcp-config)#network 192.168.2.120 255.255.255.248

SwitchP(dhcp-config)#default-router 192.168.2.121

SwitchP(dhcp-config)# dns-server 192.168.3.100

SwitchP(dhcp-config)#exit

SwitchP(config)#ip dhcp excluded-address 192.168.2.121

SwitchP(config)#ip dhcp excluded-address 192.168.2.126

P1

SwitchFibraP1(config)#vlan 90

SwitchFibraP1(config-vlan)#name Enfermeria

SwitchFibraP1(config-vlan)#exit

SwitchP1(config)#vlan 90

SwitchP1(config-vlan)#name Enfermeria

SwitchP1(config-vlan)#exit

SwitchP1(config)#interface fastEthernet 0/8

SwitchP1(config-if)#switchport mode access

SwitchP1(config-if)#switchport access vlan 90

SwitchP1(config-if)#end

P2

SwitchFibraP2(config)#vlan 90

SwitchFibraP2(config-vlan)#name Enfermeria

SwitchFibraP2(config-vlan)#exit

SwitchP2(config)#vlan 90

SwitchP2(config-vlan)#name Enfermeria

SwitchP2(config-vlan)#exit

P3

SwitchFribaP3(config)#vlan 90

SwitchFribaP3(config-vlan)#name Enfermeria

SwitchFribaP3(config-vlan)#exit

SwitchP3#conf terminal

SwitchP3(config)#vlan 90

SwitchP3(config-vlan)#name Enfermeria

SwitchP3(config-vlan)#exit

SwitchP3(config)#interface fastEthernet 0/12

SwitchP3(config-if)#switchport mode access

SwitchP3(config-if)#switchport access vlan 90

SwitchP3(config-if)#end

Vlan100:

SwitchP(config)#vlan 100

SwitchP(config-vlan)#name TerapiaIntensiva

SwitchP(config-vlan)#exit

SwitchP(config)#interface vlan 100

SwitchP(config-if)#ip address 192.168.2.134 255.255.255.248

SwitchP(config-if)#no shutdown

SwitchP(config-if)#exit

SwitchP(config)#ip dhcp pool vlan100

SwitchP(dhcp-config)#network 192.168.2.128 255.255.255.248

SwitchP(dhcp-config)#default-router 192.168.2.129

SwitchP(dhcp-config)# dns-server 192.168.3.100

SwitchP(dhcp-config)#exit

SwitchP(config)#ip dhcp excluded-address 192.168.2.129

SwitchP(config)#ip dhcp excluded-address 192.168.2.134

P1

SwitchFibraP1(config)#vlan 100

SwitchFibraP1(config-vlan)#name TerapiaIntensiva

SwitchFibraP1(config-vlan)#exit

SwitchFibraP1(config)#interface fastEthernet 9/1

SwitchFibraP1(config-if)#switchport mode access

SwitchFibraP1(config-if)#switchport access vlan 100

SwitchFibraP1(config-if)#exit

SwitchP1(config)#vlan 100

SwitchP1(config-vlan)#name TerapiaIntensiva

SwitchP1(config-vlan)#exit

SwitchP1(config)#interface fastEthernet 0/9

SwitchP1(config-if)#switchport mode access

SwitchP1(config-if)#switchport access vlan 100

SwitchP1(config-if)#end

P2

SwitchFibraP2(config)#vlan 100

SwitchFibraP2(config-vlan)#name TerapiaIntensiva

SwitchFibraP2(config-vlan)#exit

SwitchP2(config)#vlan 100

SwitchP2(config-vlan)#name TerapiaIntensiva

SwitchP2(config-vlan)#exit

SwitchP2(config)#interface fastEthernet 0/8

SwitchP2(config-if)#switchport mode access

SwitchP2(config-if)#switchport access vlan 100

SwitchP2(config-if)#end

P3

SwitchFribaP3(config)#vlan 100

SwitchFribaP3(config-vlan)#name TerapiaIntensiva

SwitchFribaP3(config-vlan)#exit

SwitchP3(config)#vlan 100

SwitchP3(config-vlan)#name TerapiaIntensiva

SwitchP3(config-vlan)#exit

SwitchP3(config)#interface fastEthernet 0/11

SwitchP3(config-if)#switchport mode access

SwitchP3(config-if)#switchport access vlan 100

SwitchP3(config-if)#end

Vlan110:

SwitchP(config)#vlan 110

SwitchP(config-vlan)#name Pediatria

SwitchP(config-vlan)#exit

SwitchP(config)#interface vlan 110

SwitchP(config-if)#ip address 192.168.2.142 255.255.255.248

SwitchP(config-if)#no shutdown

SwitchP(config-if)#exit

SwitchP(config)#ip dhcp pool vlan110

SwitchP(dhcp-config)#network 192.168.2.136 255.255.255.248

SwitchP(dhcp-config)#default-router 192.168.2.137

SwitchP(dhcp-config)# dns-server 192.168.3.100

SwitchP(dhcp-config)#exit

SwitchP(config)#ip dhcp excluded-address 192.168.2.137

SwitchP(config)#ip dhcp excluded-address 192.168.2.142

P3

SwitchFribaP3(config)#vlan 110

SwitchFribaP3(config-vlan)#name Pediatria

SwitchFribaP3(config-vlan)#exit

SwitchP3#conf terminal

SwitchP3(config)#vlan 110

SwitchP3(config-vlan)#name Pediatria

SwitchP3(config-vlan)#exit

SwitchP3(config)#interface range fastEthernet 0/2-5

SwitchP3(config-if-range)#switchport mode access

SwitchP3(config-if-range)#switchport access vlan 110

SwitchP3(config-if-range)#end

Vlan120:

SwitchP(config)#vlan 120

SwitchP(config-vlan)#name Farmacia

SwitchP(config-vlan)#exit

SwitchP(config)#interface vlan 120

SwitchP(config-if)#ip address 192.168.2.150 255.255.255.248

SwitchP(config-if)#no shutdown

SwitchP(config-if)#exit

SwitchP(config)#ip dhcp pool vlan120

SwitchP(dhcp-config)#network 192.168.2.144 255.255.255.248

SwitchP(dhcp-config)#default-router 192.168.2.145

SwitchP(dhcp-config)# dns-server 192.168.3.100

SwitchP(dhcp-config)#exit

SwitchP(config)#ip dhcp excluded-address 192.168.2.145

SwitchP(config)#ip dhcp excluded-address 192.168.2.150

P3

SwitchFribaP3(config)#vlan 120

SwitchFribaP3(config-vlan)#name Farmacia

SwitchFribaP3(config-vlan)#exit

SwitchFribaP3(config)#interface fastEthernet 8/1

SwitchFribaP3(config-if)#switchport mode access

SwitchFribaP3(config-if)#switchport access vlan 120

SwitchFribaP3(config-if)#exit

SwitchP3(config)#vlan 120

SwitchP3(config-vlan)#name Farmacia

SwitchP3(config-vlan)#exit

SwitchP3(config)#interface fastEthernet 0/13

SwitchP3(config-if)#switchport mode access

SwitchP3(config-if)#switchport access vlan 120

SwitchP3(config-if)#end

Vlan130:

SwitchP(config)#vlan 130

SwitchP(config-vlan)#name Esterilizacion

SwitchP(config-vlan)#exit

SwitchP(config)#interface vlan 130

SwitchP(config-if)#ip address 192.168.2.158 255.255.255.248

SwitchP(config-if)#no shutdown

SwitchP(config-if)#exit

SwitchP(config)#ip dhcp pool vlan130

SwitchP(dhcp-config)#network 192.168.2.152 255.255.255.248

SwitchP(dhcp-config)#default-router 192.168.2.153

SwitchP(dhcp-config)# dns-server 192.168.3.100

SwitchP(dhcp-config)#exit

SwitchP(config)#ip dhcp excluded-address 192.168.2.153

SwitchP(config)#ip dhcp excluded-address 192.168.2.158

P3

SwitchFribaP3(config)#vlan 130

SwitchFribaP3(config-vlan)#name Esterilizacion

SwitchFribaP3(config-vlan)#exit

Impresora

SwitchFribaP3(config)#interface fastEthernet 7/1

SwitchFribaP3(config-if)#switchport mode access

SwitchFribaP3(config-if)#switchport access vlan 130

SwitchFribaP3(config-if)#exit

SwitchP3#conf terminal

SwitchP3(config)#vlan 130

SwitchP3(config-vlan)#name Esterilizacion

SwitchP3(config-vlan)#exit

SwitchP3(config)#interface range fastEthernet 0/14-16

SwitchP3(config-if-range)#switchport mode access

SwitchP3(config-if-range)#switchport access vlan 130

SwitchP3(config-if-range)#end

Vlan140:

SwitchP(config)#vlan 140

SwitchP(config-vlan)#name Contabilidad

SwitchP(config-vlan)#exit

SwitchP(config)#interface vlan 140

SwitchP(config-if)#ip address 192.168.2.166 255.255.255.248

SwitchP(config-if)#no shutdown

SwitchP(config-if)#exit

SwitchP(config)#ip dhcp pool vlan140

SwitchP(dhcp-config)#network 192.168.2.161 255.255.255.248

SwitchP(dhcp-config)#default-router 192.168.2.161

SwitchP(dhcp-config)# dns-server 192.168.3.100

SwitchP(dhcp-config)#exit

SwitchP(config)#ip dhcp excluded-address 192.168.2.161

SwitchP(config)#ip dhcp excluded-address 192.168.2.166

P3

SwitchFribaP3(config)#vlan 140

SwitchFribaP3(config-vlan)#name Contabilidad

SwitchFribaP3(config-vlan)#exit

SwitchFribaP3(config)#interface fastEthernet 9/1

SwitchFribaP3(config-if)#switchport mode access

SwitchFribaP3(config-if)#switchport access vlan 140

SwitchFribaP3(config-if)#exit

SwitchP3(config)#vlan 140

SwitchP3(config-vlan)#name Contabilidad

SwitchP3(config-vlan)#exit

SwitchP3(config)#interface range fastEthernet 0/17-18

SwitchP3(config-if-range)#switchport mode access

SwitchP3(config-if-range)#switchport access vlan 140

SwitchP3(config-if-range)#end

III.1.5.2.1.2.5.- Configuración de las contraseñas al switch

Se realiza la configuración de contraseñas de acceso por consola en todos los switches de la red, tanto principales como de fibra y por piso.

Cada equipo recibe una contraseña única, establecida mediante el comando “line con 0”, seguida de password y login, lo que restringe el acceso no autorizado al modo de configuración.

Finalmente, con el comando “write memory”, se guarda la configuración en la memoria del switch, asegurando que las credenciales permanezcan activas tras un reinicio.

Switch por plantas	**Contraseñas**
Switch Principal	HRSJRE2025PRINC
Switch Fibra Planta Baja	HRSJDD2025FIBRPLANB
Switch Fibra Piso 1	HJRJDD2025FIBRPLAN1
Switch Fibra Piso 2	HDTRD2025FIBRPLAN2
Switch Fibra Piso 3	HSSWRT2025FIBRPLAN3
Switch Planta Baja	HRSCC2025SWITCHPB
Switch Piso 1	HRSTT2025SWITCHP1
Switch Piso 2	HRSTW2025SWITCHP2

Switch Piso 3	HRGHR2025SWITCHP3

Tabla 107. Configuracion de las contraseñas de los switch

Switch Principal

SwitchP>enable

SwitchP#conf term

SwitchP(config)#line con 0

SwitchP(config-line)#password HRSJRE2025PRINC

SwitchP(config-line)#login

SwitchP(config-line)#end

SwitchP#write memory

Switch Fibra Planta Baja

SwitchFibraPB>enable

SwitchFibraPB#conf term

SwitchFibraPB(config)#line con 0

SwitchFibraPB(config-line)#password HRSJDD2025FIBRPLANB

SwitchFibraPB(config-line)#login

SwitchFibraPB(config-line)#end

SwitchFibraPB#write memory

Switch Fibra Piso 1

SwitchFibraP1>enable

SwitchFibraP1#conf ter

SwitchFibraP1(config)#line con 0

SwitchFibraP1(config-line)#password HJRJDD2025FIBRPLAN1

SwitchFibraP1(config-line)#login

SwitchFibraP1(config-line)#end

SwitchFibraP1#write memory

Switch Fibra Piso 2

SwitchFibraP2>enable

SwitchFibraP2#conf term

SwitchFibraP2(config)#line con 0

SwitchFibraP2(config-line)#password HDTRD2025FIBRPLAN2

SwitchFibraP2(config-line)#login

SwitchFibraP2(config-line)#end

SwitchFibraP2#write memory

Switch Fibra Piso 3

SwitchFribaP3>enable

SwitchFribaP3#conf ter

SwitchFribaP3(config)#line con 0

SwitchFribaP3(config-line)#password HSSWRT2025FIBRPLAN3

SwitchFribaP3(config-line)#login

SwitchFribaP3(config-line)#end

SwitchFribaP3#write memory

Switch Planta Baja

SwitchPB>enable

SwitchPB#conf term

SwitchPB(config)#line con 0

SwitchPB(config-line)#password HRSCC2025SWITCHPB

SwitchPB(config-line)#login

SwitchPB(config-line)#end

SwitchPB#write memory

Switch Piso 1

SwitchP1>enable

SwitchP1#conf term

SwitchP1(config)#line con 0

SwitchP1(config-line)#password HRSTT2025SWITCHP1

SwitchP1(config-line)#login

SwitchP1(config-line)#end

SwitchP1#write memory

Switch Piso 2

SwitchP2>enable

SwitchP2#conf term

SwitchP2(config)#line con 0

SwitchP2(config-line)#password HRSTW2025SWITCHP2

SwitchP2(config-line)#login

SwitchP2(config-line)#end

SwitchP2#write memory

Switch Piso 3

SwitchP3>enable

SwitchP3#conf term

SwitchP3(config)#line con 0

SwitchP3(config-line)#password HRGHR2025SWITCHP3

SwitchP3(config-line)#login

SwitchP3(config-line)#end

SwitchP3#write memory

III.1.5.2.1.2.6.- Cómo conectarse a la red mediante las VLANS

Se muestra la configuración del Switch Principal donde se declaran varias direcciones como “ip dhcp excluded-address”. Estas direcciones se reservan para que el servidor DHCP no las asigne de forma automática, ya que se utilizarán para parámetros críticos de la red. En concreto, se apartan IP específicas para el gateway de cada VLAN, es decir, para la interfaz lógica que permitirá la salida de los equipos de ese segmento, y también para la IP de la interfaz que actúa como servidor del DHCP pool, que es la encargada de entregar las direcciones al resto de dispositivos. De esta manera, al reservar normalmente la primera y la última IP utilizable de cada red, se garantiza que las direcciones destinadas al gateway y a la interfaz del pool DHCP no se mezclen con las que recibirán los clientes, evitando conflictos y manteniendo una estructura ordenada en el direccionamiento de la red.

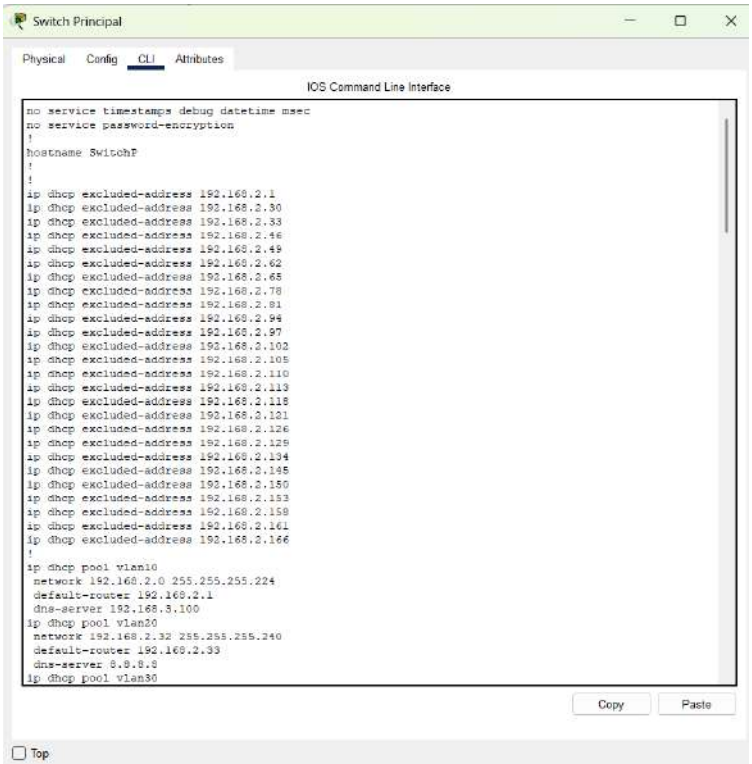

Figura 173. IP excluidas para el DHCP

En esta figura se muestra cómo en el Switch Principal se crean los pools DHCP para cada VLAN, definiendo su red, máscara y la dirección del gateway, que corresponde a la interfaz VLAN de ese segmento. Además, se configura como servidor DNS la IP 192.168.3.100, que pertenece al servidor de telefonía IP Issabel, de modo que los equipos (especialmente los teléfonos IP) reciban automáticamente esta dirección y puedan conectarse correctamente a dicho servidor para registrar sus extensiones y utilizar los servicios de voz. Con esta configuración, cualquier dispositivo que se conecte a una VLAN obtiene una IP válida, su puerta de enlace y el DNS apuntando al servidor Issabel, asegurando la comunicación tanto dentro de la red de datos como con la plataforma de telefonía.

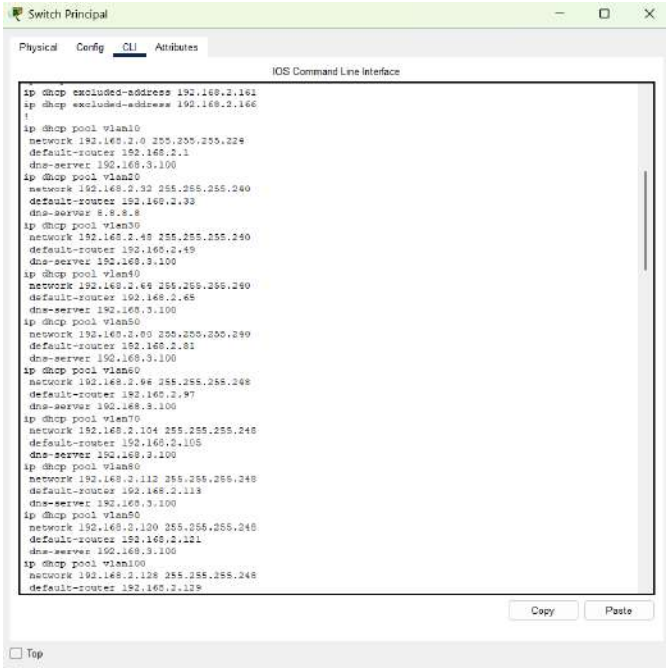

Figura 174. DHCP para cada VLAN

Se muestra la configuración del Switch Principal donde varias interfaces GigabitEthernet se establecen en modo trunk, permitiendo el transporte simultáneo de todas las VLAN entre equipos de la red. Las interfaces FastEthernet se dejan en modo access asociadas, por ejemplo, a la VLAN 150 para conectar dispositivos finales. Al final se observan las interfaces lógicas VLAN10, VLAN20 y VLAN30 con sus direcciones IP correspondientes, que funcionarán como gateway de cada segmento y permitirán el enrutamiento entre VLANs.

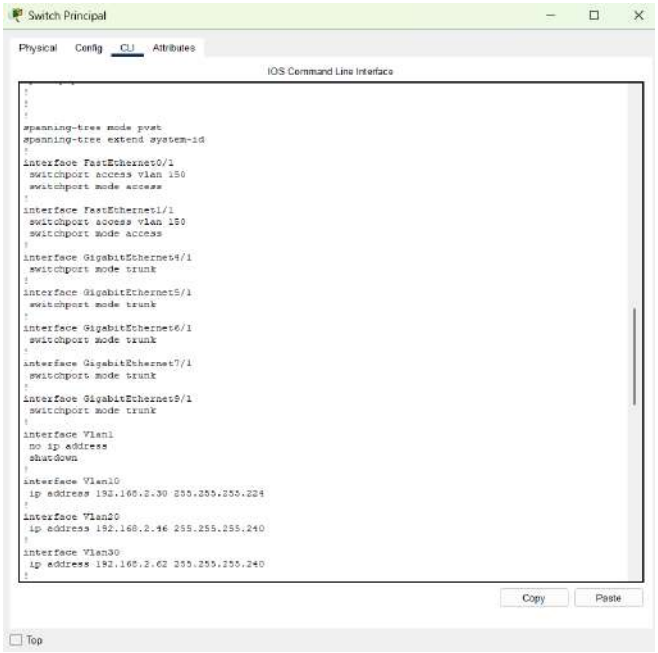

Figura 175. Modo Trunk para cada interface

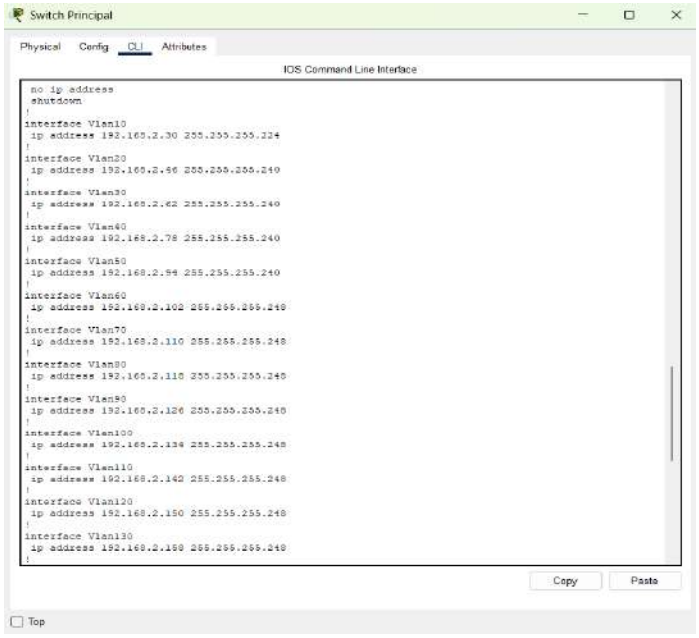

Figura 176. IP unica para cada Interface para HDCP

Se observa el resultado del comando **ipconfig /renew** ejecutado en el PC de la VLAN, donde el equipo solicita una nueva configuración al servidor DHCP. Como respuesta, obtiene automáticamente la dirección IP 192.168.2.11, la máscara 255.255.255.224, el gateway 192.168.2.1 correspondiente a la interfaz de su VLAN y el DNS 192.168.3.100, que es la dirección del servidor de telefonía IP Issabel. De esta manera se comprueba que el DHCP de la VLAN funciona correctamente y que el equipo queda listo para comunicarse tanto con la red de datos como con el

servidor Issabel.

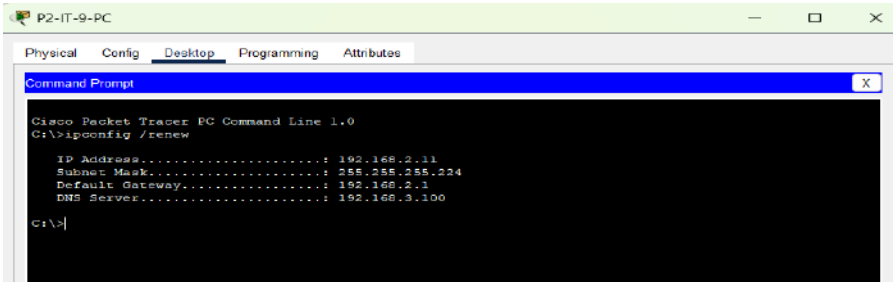

Figura 177. Obteniedo la IP de tipo DHCP para dicha VLAN

III.1.5.2.1.2.7.- Comparativa en el uso de redes VLAN a otras tecnologías

Criterio	**VLANs**	**Subredes**
Segmentación de Red	Segmenta el tráfico dentro de una misma red física a nivel lógico. Permite que los dispositivos en diferentes VLANs no se vean entre sí a nivel de tráfico.	Divide una red IP en múltiples subredes. Aísla dispositivos a nivel de dirección IP.
Aislamiento	Aísla tráfico dentro de la misma infraestructura física, lo que mejora la seguridad. Las VLANs pueden comunicarse solo a través de un router o capa 3.	Aísla tráfico entre diferentes segmentos de red usando enrutadores. No proporciona aislamiento a nivel de capa 2.
Flexibilidad	Alta: Las VLANs pueden ser configuradas y modificadas sin necesidad de reconfigurar la infraestructura física. La reconfiguración es sencilla, ya que solo implica cambios a nivel de software en switches.	Baja: El cambio de subredes implica la reconfiguración de direcciones IP y cambios en la infraestructura de red, lo que puede requerir más trabajo.
Gestión y Configuración	Más fácil y dinámica: Las VLANs son fáciles de crear, eliminar y modificar mediante configuraciones de software en los switches. Esto facilita la administración de redes grandes y cambiantes.	Menos flexible: Las subredes requieren más esfuerzo para modificar, especialmente cuando se requiere reconfiguración de direcciones IP y cambios en los routers.
Escalabilidad	Alta: Las VLANs permiten crear hasta 4096 VLANs en una red, lo que proporciona una segmentación adecuada incluso para redes grandes sin	Limitada: Las subredes están limitadas por la cantidad de direcciones IP disponibles en la red, lo que puede hacer que una red crezca más

	necesidad de aumentar la infraestructura.	lentamente.
Seguridad	Alta: El tráfico entre VLANs está aislado, por lo que se pueden aplicar políticas de seguridad más estrictas para cada VLAN. Además, las VLANs permiten segmentar la red por tipo de usuario o dispositivo (por ejemplo, VLANs para administración, servidores, invitados, etc.).	Baja: Aunque las subredes pueden ayudar a aislar el tráfico a nivel de capa 3, no proporcionan el mismo nivel de control de tráfico que las VLANs, ya que no se puede aplicar la misma segmentación de capa 2.
Costos de Hardware	Bajos: No es necesario invertir en hardware adicional, ya que las VLANs se configuran mediante software en switches. No se requiere equipo extra, solo un switch gestionable.	Más altos: Las subredes requieren más routers o dispositivos de capa 3 para manejar la segmentación, lo que puede aumentar los costos de infraestructura.
Manejo de Tráfico	Las VLANs pueden manejar el tráfico de manera más eficiente, segmentando tráfico de diferentes tipos (por ejemplo, voz, datos, video), y cada tipo puede tener sus propias reglas de priorización.	Las subredes no gestionan el tráfico de manera tan granular; el tráfico entre diferentes subredes se controla mediante enrutadores, pero no existe un control tan detallado como en las VLANs.
Redundancia y Alta Disponibilidad	Las VLANs permiten implementar redundancia y alta disponibilidad fácilmente mediante técnicas como Spanning Tree Protocol (STP), que previene bucles de red.	Las subredes no proporcionan un mecanismo automático de prevención de bucles, y la redundancia suele depender de la implementación manual de rutas y configuraciones.
Rendimiento	Mejor rendimiento en redes grandes: Las VLANs optimizan el uso del ancho de banda y la utilización de la red al aislar diferentes tipos de tráfico, evitando que el tráfico no relacionado se mezcle y afecte el rendimiento.	Las subredes no optimizan el rendimiento de la red de manera tan eficiente, ya que el tráfico de diferentes dispositivos dentro de la misma subred no está aislado.
Soporte para QoS (Calidad de Servicio)	Las VLANs permiten implementar políticas de QoS (Quality of Service) de manera eficiente para priorizar tráfico crítico, como voz o video,	Las subredes no proporcionan un control tan específico de QoS, ya que la segmentación es menos precisa y no se puede aplicar la misma

	mejorando la calidad del servicio en redes de alto tráfico.	granularidad que con las VLANs.

Tabla 108. Comparativa en el uso de redes VLAN a otras tecnologías

III.1.5.2.2.-Configuración de ACL como política de seguridad

RouterClinica>enable

RouterClinica#configure terminal

RouterClinica(config)#access-list 100 deny ip 192.168.2.32 0.0.0.15 192.168.2.0 0.0.0.31

RouterClinica(config)#access-list 100 deny ip 192.168.2.32 0.0.0.15 192.168.2.64 0.0.0.15

RouterClinica(config)#access-list 100 deny ip 192.168.2.32 0.0.0.15 192.168.2.80 0.0.0.15

RouterClinica(config)#access-list 100 deny ip 192.168.2.32 0.0.0.15 192.168.2.96 0.0.0.7

RouterClinica(config)#access-list 100 deny ip 192.168.2.32 0.0.0.15 192.168.2.104 0.0.0.7

RouterClinica(config)#access-list 100 deny ip 192.168.2.32 0.0.0.15 192.168.2.112 0.0.0.7

RouterClinica(config)#access-list 100 deny ip 192.168.2.32 0.0.0.15 192.168.2.120 0.0.0.7

RouterClinica(config)#access-list 100 deny ip 192.168.2.32 0.0.0.15 192.168.2.128 0.0.0.7

RouterClinica(config)#access-list 100 deny ip 192.168.2.32 0.0.0.15 192.168.2.136 0.0.0.7

RouterClinica(config)#access-list 100 deny ip 192.168.2.32 0.0.0.15 192.168.2.144 0.0.0.7

RouterClinica(config)#access-list 100 deny ip 192.168.2.32 0.0.0.15 192.168.2.152 0.0.0.7

RouterClinica(config)#access-list 100 deny ip 192.168.2.32 0.0.0.15 192.168.2.160 0.0.0.7

RouterClinica(config)#access-list 100 deny ip 192.168.2.32 0.0.0.15 192.168.3.0 0.0.0.255

RouterClinica(config)#access-list 100 permit ip any any

RouterClinica(config)#end

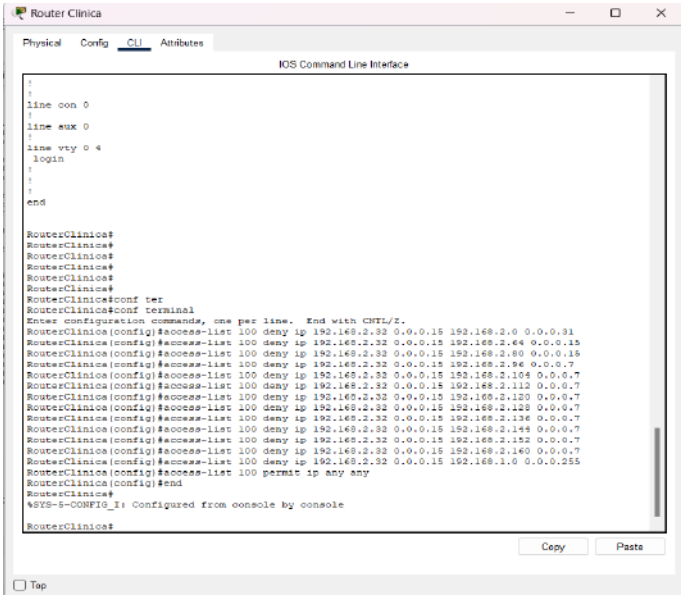

Figura 178. Configuración de ACL como política de seguridad

Se ha implementado una lista de control de acceso (ACL) que bloquea la comunicación entre la VLAN asignada a los pacientes y las demás áreas internas de la clínica. De esta forma, los dispositivos conectados al Access Point de Pacientes únicamente tendrán acceso a internet, sin posibilidad de interactuar con la red interna.

III.1.5.3.- Implementación del diseño de red en GNS3

III.1.5.3.1.- Configuración del Firewall Fortinet

Se muestra la configuración de la interfaz port1 en el firewall Fortinet, donde se activa el modo DHCP y se permiten accesos para ping, http, https, y ssh. Esto asegura que la interfaz pueda obtener una IP dinámica y manejar tráfico básico.

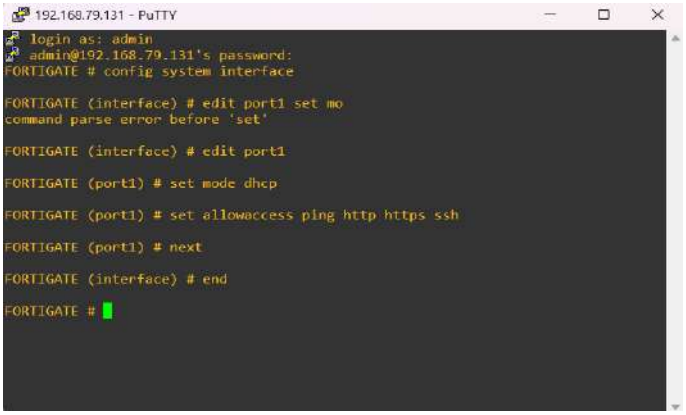

Figura 179. Configuracion port1 DHCP

Aquí se verifica la configuración de la interfaz port1, donde se confirma que ha recibido una dirección IP de 192.168.1.143 con máscara 255.255.255.0 y con conexión “up”. También se muestra el estado de la interfaz y su velocidad de conexión.

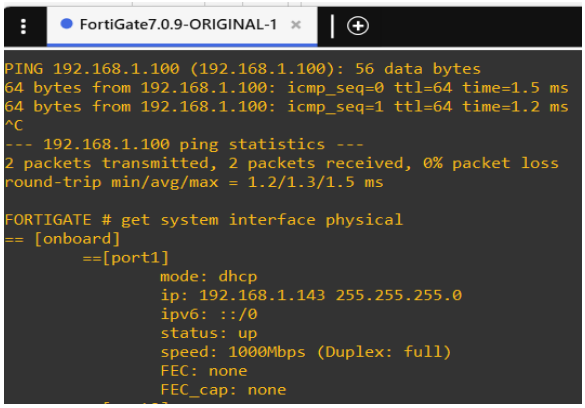

Figura 180. Verificacion de Ips

Se muestra la pantalla de inicio de sesión del firewall Fortinet. El usuario ingresa su nombre de usuario y contraseña para acceder a la interfaz de administración del dispositivo y realizar configuraciones.

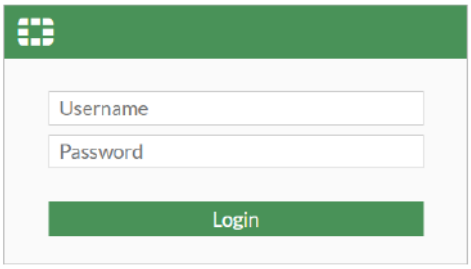

Figura 181. Inicio de sesion Fortinet

En esta captura, se verifica la configuración de la interfaz port1 en el Fortinet, mostrando que está configurada en modo DHCP. Se observa que el dispositivo ha adquirido una dirección IP dinámica (192.168.1.143) con una máscara de subred de 255.255.255.0 y un puerto WAN activo, confirmando la correcta obtención de la configuración de red.

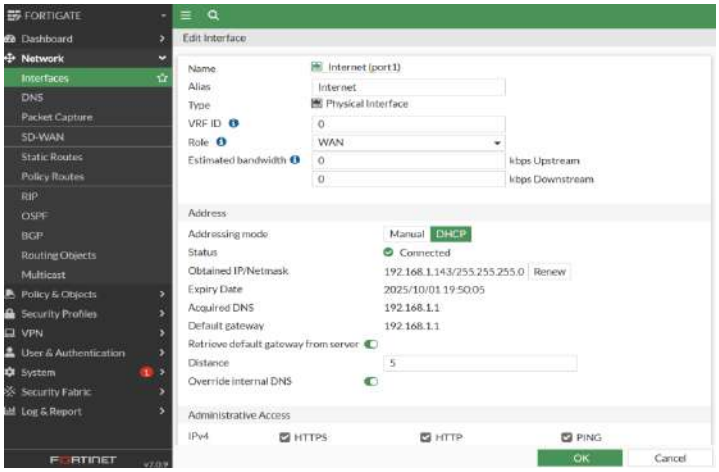

Figura 182. Verificacion de tipo DHCP puerto1

Se está configurando la interfaz Red Interna (port10) en el Fortinet. Se le asigna un nombre (Red Interna) y se configura como una interfaz de tipo LAN, en modo manual para la dirección IP, y otras configuraciones de acceso administrativo habilitadas como HTTPS, PING.

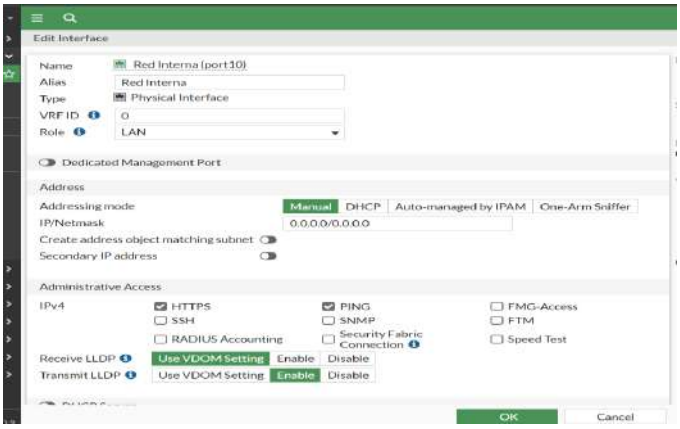

Figura 183. Ingresar nombre puerto10

III.1.5.3.1.1.- Asignación de VLANs en el puerto 10

Se muestra la configuración de la VLAN 70 llamada Recepción, asignada a la interfaz Red Interna (port10). Se especifica el protocolo 802.1Q, el ID de VLAN 70, y se asigna la dirección IP 192.168.2.105 con la máscara 255.255.255.248. Esta configuración permite segmentar la red en diferentes VLANs para una mejor gestión del tráfico.

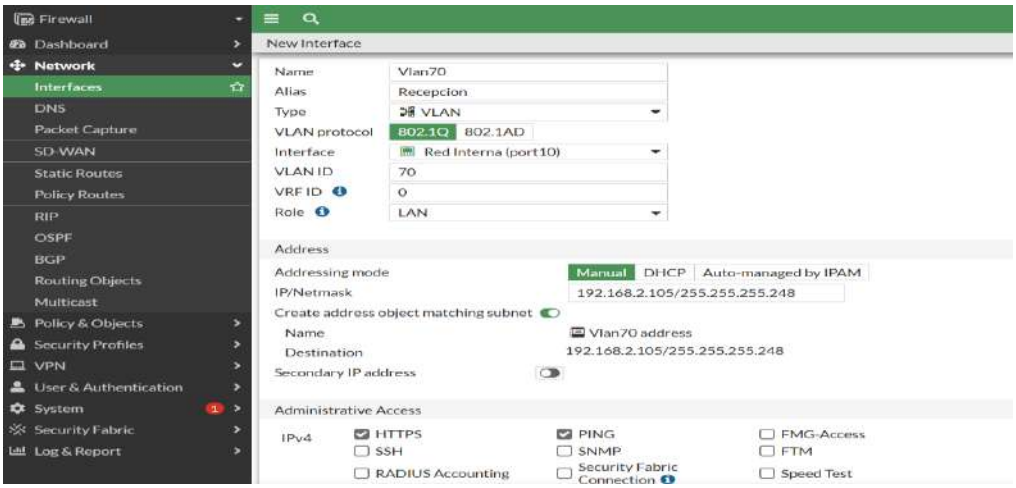

Figura 184. Crear VLAN 70 tipo Interface

Se muestra la configuración de la VLAN 10 llamada Internación, asignada a la interfaz Red Interna (port10). Se configura el protocolo 802.1Q para la VLAN, con el ID de VLAN 10 y la dirección IP 192.168.2.1/255.255.255.224. Esta configuración segmenta la red para un área específica, permitiendo un control de tráfico eficiente.

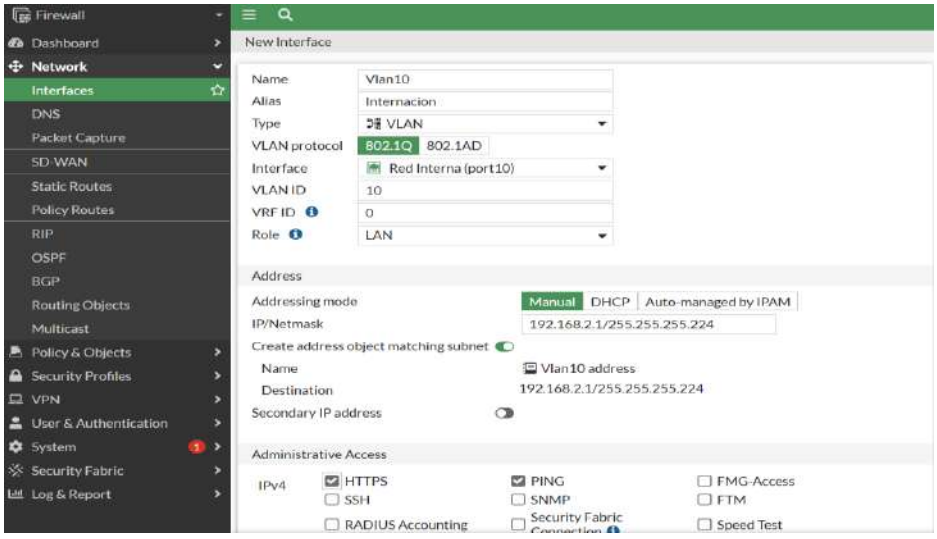

Figura 185. Crear VLAN 10 tipo Interface

Se configura la VLAN 100 llamada TerapiaIntensiva, también asignada a la interfaz Red Interna (port10). La VLAN tiene el ID 100, se utiliza el protocolo 802.1Q, y se asigna la dirección IP

192.168.2.129/255.255.255.248, lo que también crea una red separada para gestionar el tráfico de la zona correspondiente.

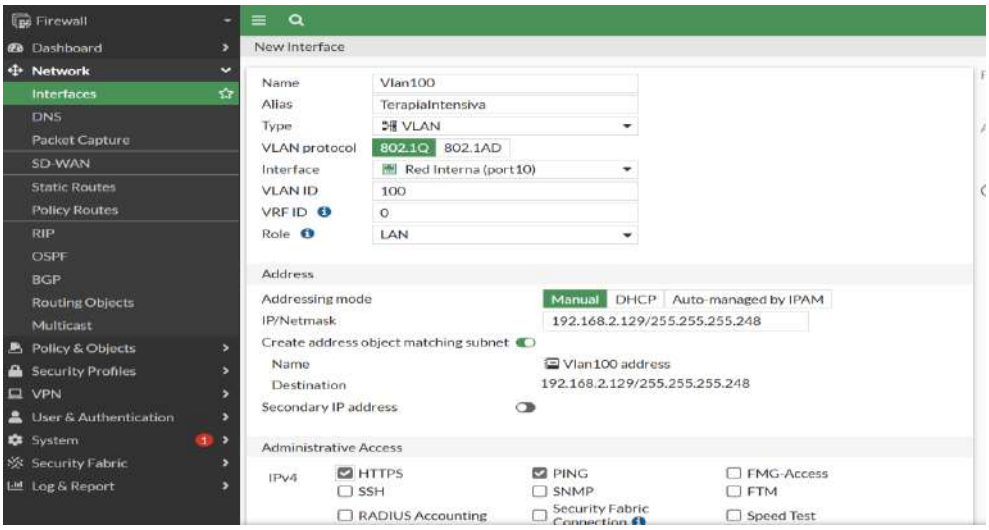

Figura 186. Crear VLAN 100 tipo Interface

Se muestra la configuración de la VLAN 150 llamada Servidores, asignada a la interfaz Red Interna (port10). Se configura el protocolo 802.1Q para esta VLAN y se asigna la dirección IP 192.168.3.1/255.255.255.0, lo que crea una subred específica para los servidores de la red, segmentando el tráfico para optimizar el rendimiento y la seguridad.

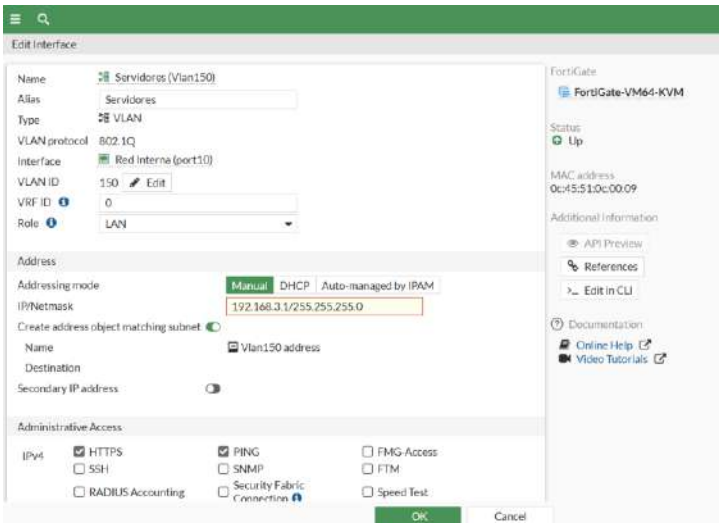

Figura 187. Crear VLAN 150 tipo Interface

III.1.5.3.1.2.- Configuración de Objetos de Dirección (Address)

Se configurarán los Address Objects en Fortinet para controlar los rangos de IPs en diferentes VLANs. Se crearán los objetos para Vlan70, Vlan10 y Vlan100, asignando rangos de IPs específicos a cada uno, lo que permite gestionar y segmentar el tráfico dentro de cada subred

asociada a las VLANs correspondientes. Esto facilita el control y la organización del tráfico en la red.

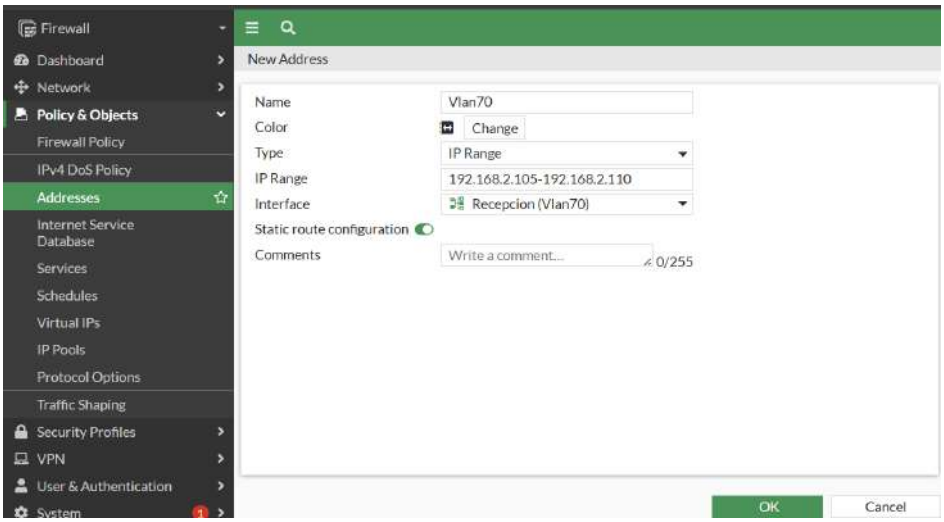

Figura 188. Crear Address para controlar el rango de la subred VLAN70

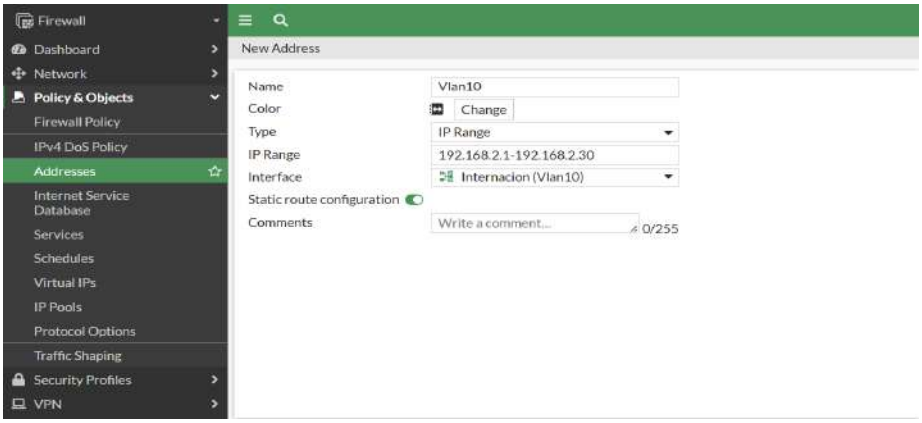

Figura 189. Crear Address para controlar el rango de la subred VLAN10

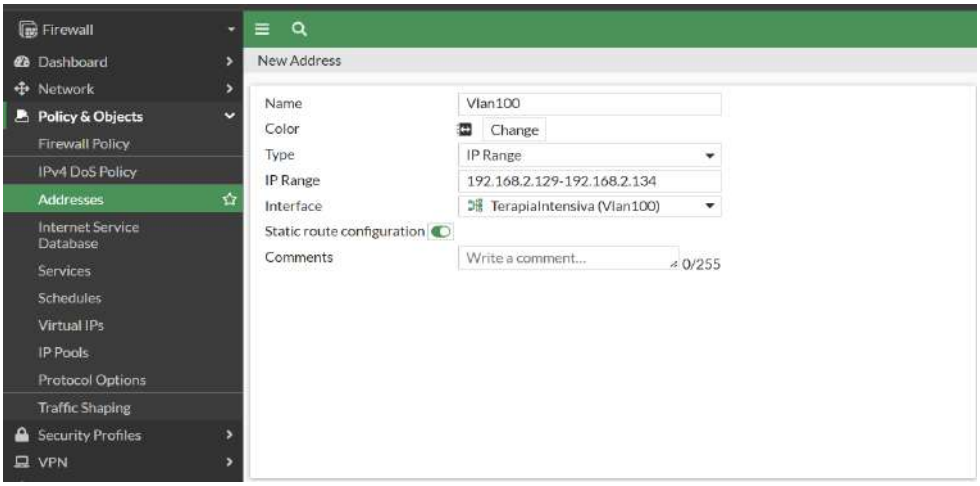

Figura 190. Crear Address para controlar el rango de la subred VLAN100

III.1.5.3.1.3.- Configuración de las Políticas de seguridad perimetral

Se configura una política de seguridad para la VLAN 10, que permite la comunicación entre la VLAN 10 y el Internet. La política define las interfaces de entrada y salida, el tipo de tráfico permitido y la acción que se debe tomar (permitir o denegar).

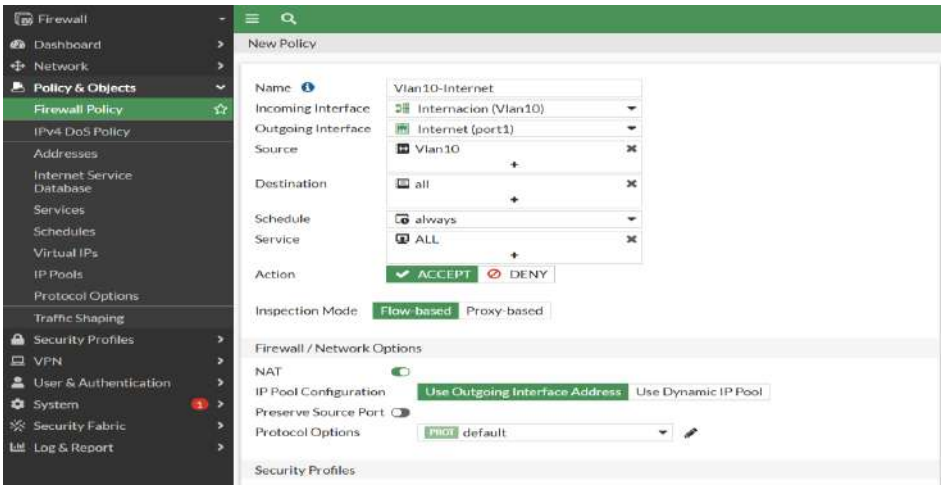

Figura 191. Politica de Seguridad Vlan10-Internet

Esta es otra política de seguridad, pero en este caso para la VLAN 70, permitiendo la comunicación entre VLAN 70 y Internet. La configuración sigue la misma lógica que la política de la VLAN 10, asegurando que el tráfico deseado se permita.

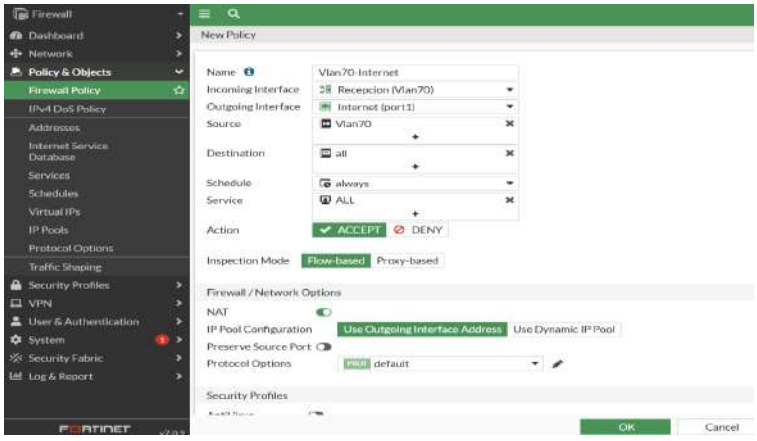

Figura 192. Política de Seguridad Vlan70-Internet

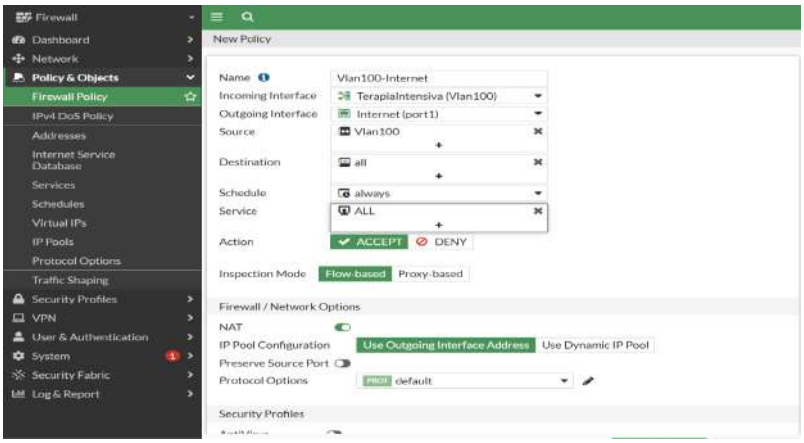

Figura 193. Política de Seguridad Vlan100-Internet

Aquí se configura una política que permite el tráfico entre la VLAN 70 y un sistema específico llamado Issabel. Esta política se utiliza para controlar el acceso entre una VLAN 150 Servidor.

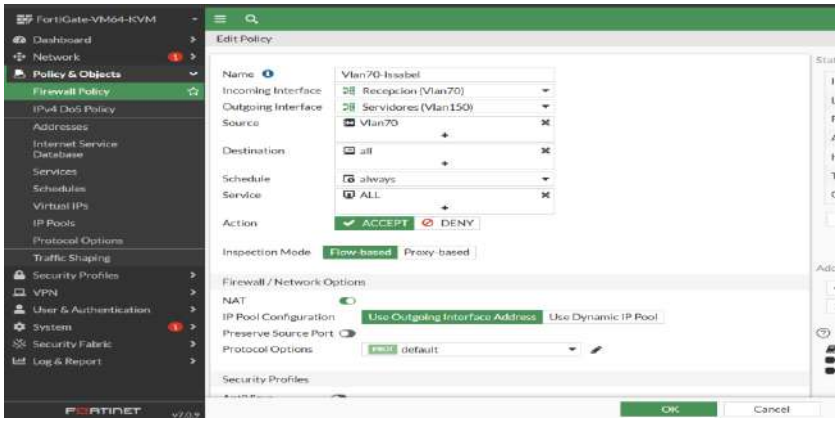

Figura 194. Politica de Seguridad Vlan70 a Issabel

Se muestra la configuración de un filtro web para bloquear el acceso a redes sociales como Facebook, YouTube y TikTok. Este filtro se aplica a una política de seguridad que controla el acceso a Internet y asegura que los usuarios no puedan acceder a estas plataformas.

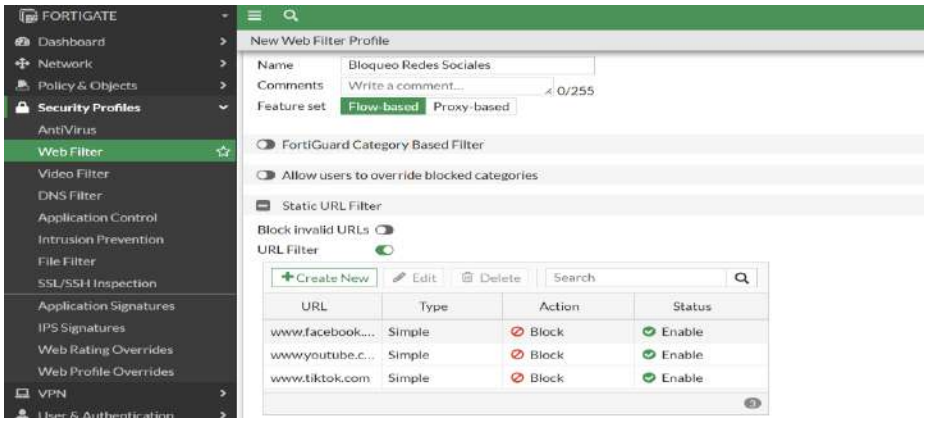

Figura 195. Bloqueo de redes sociales

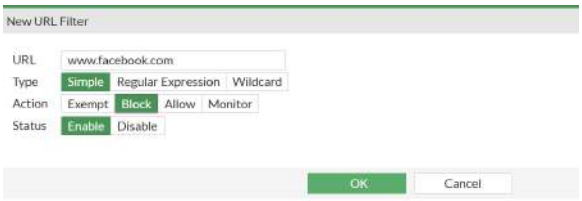

Figura 196. Bloqueo por URL

Aquí se configura el sensor de aplicaciones para bloquear ciertas aplicaciones en la red, como Redes Sociales, Juegos, y P2P. Esto se aplica a través de una política de seguridad que permite controlar el acceso a aplicaciones específicas.

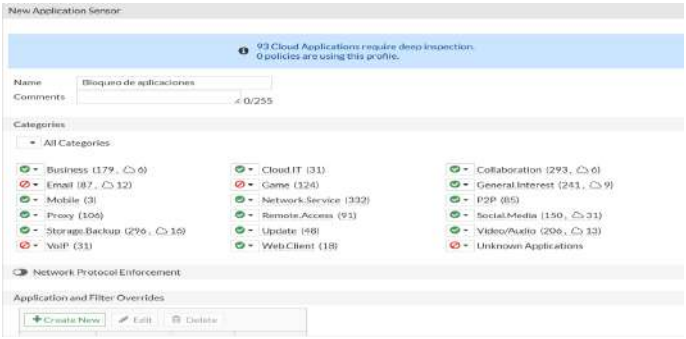

Figura 197. Bloqueo de Aplicaciones por el Fortinet

Finalmente, se muestra cómo añadir un filtro web a una política de seguridad. Este filtro permite bloquear el acceso a categorías específicas de sitios web (como redes sociales o aplicaciones de entretenimiento), proporcionando una capa adicional de control sobre el tráfico web.

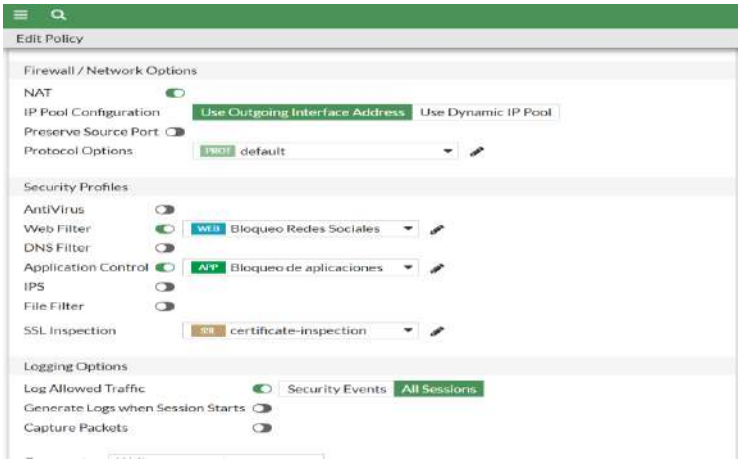

Figura 198. Añadir el filtro web

III.1.5.3.2.- Configuración del Wifi

III.1.5.3.2.1.- Importancia del Wi-Fi en la empresa

Wi-Fi es una tecnología de red inalámbrica a través de la cual los dispositivos, como computadoras,

dispositivos móviles y otros equipos (impresoras y videocámaras), pueden interactuar con Internet. Permite que estos dispositivos, entre tantos otros, intercambien información entre sí y establezcan, de esta manera, una red.

Es muy importante que se diseñe una infraestructura de redes Wi-Fi en hospitales o clínicas, por parte de la administración, que responda a las necesidades específicas de cada unidad de salud, con el fin de aprovechar al máximo la inversión. No está demás comentar que las redes Wi-Fi son más económicas, veloces y confiables que otras tecnologías de conectividad.

Las redes Wi-Fi en clínicas representan la nueva generación de tecnología inalámbrica para modernizar los sistemas de salud, entre otros servicios sociales. Su utilización disminuye los costos de diseño, despliegue y ofrece una mejor experiencia en el uso de datos, voz y aplicaciones médicas críticas para cuidar de la salud de los pacientes que al final, son los más importantes.

Además, es importante mencionar que no es posible realizar un ping directamente a un punto de acceso (AP) desde una VLAN cableada, ya que muchos AP trabajan en modo capa 2 (bridge) y no exponen una interfaz IP interna para cada VLAN, o tienen bloqueo de ICMP por razones de seguridad. En varios modelos, el dispositivo tiene deshabilitada la respuesta ICMP (ping), por lo que no responde a solicitudes de eco aun estando en la misma red. Sin embargo, sí es posible hacer ping desde un dispositivo conectado al AP hacia una PC en otra VLAN, porque el tráfico del cliente sí atraviesa la red como tráfico normal, respetando el enrutamiento y las políticas de firewall configuradas.

III.1.5.3.2.2.- Configuración de la red Wifi

Se muestra la configuración del router donde la conexión a Internet está ajustada en modo DHCP automático, permitiendo que el dispositivo obtenga su dirección IP de forma dinámica. Esto garantiza que la red WiFi reciba parámetros de red sin configuración manual.

Figura 199. Configuramos la Conexión DHCP de la VLAN para la Red Wifi

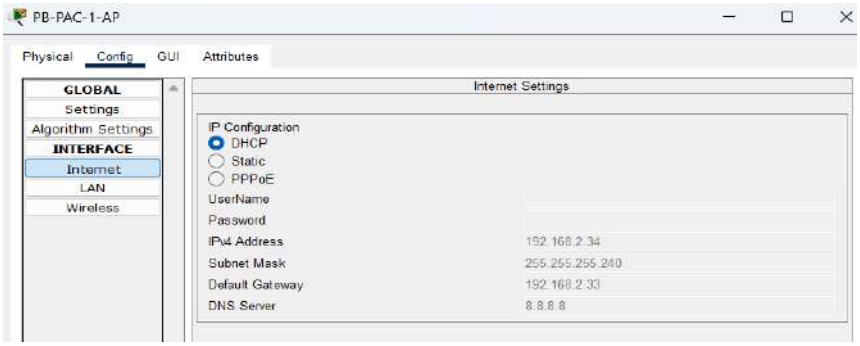

Figura 200. Verificamos que nos esté Accediendo Dinámicamente a la Red VLAN 20 de Wifi

Se configura el servidor DHCP que asignará direcciones IP automáticamente a los usuarios de la red WiFi. Se define el rango de direcciones 10.10.0.1 - 10.10.0.50, así como la máscara y la cantidad máxima de clientes que podrán recibir servicio.

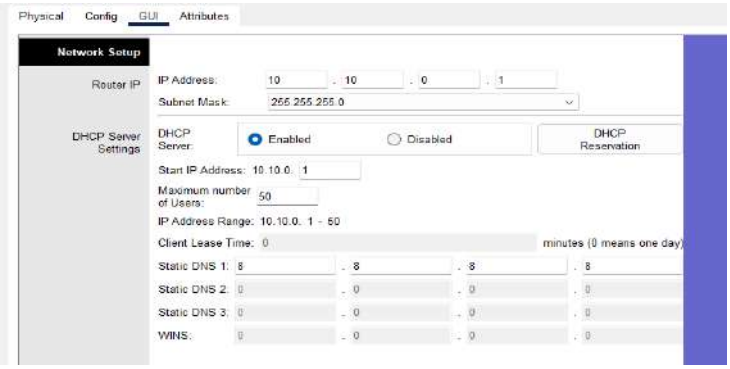

Figura 201. Configuramos la Red del DHCP que Repartiremos a los Usuarios

Se confirma que la interfaz LAN del punto de acceso está configurada correctamente con la dirección 10.10.0.1 y su respectiva máscara de subred. Esto asegura que el AP pueda administrar la red local y repartir DHCP según lo establecido.

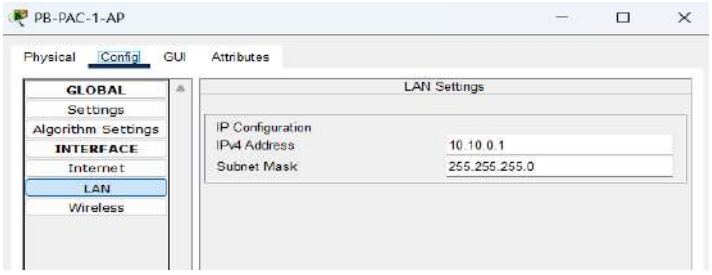

Figura 202. Verificamos la Configuración LAN

Se asigna el nombre **PacientesPB** a la red inalámbrica, permitiendo que los usuarios identifiquen el SSID al momento de conectarse. También se mantiene la emisión del SSID habilitada para que la red sea visible.

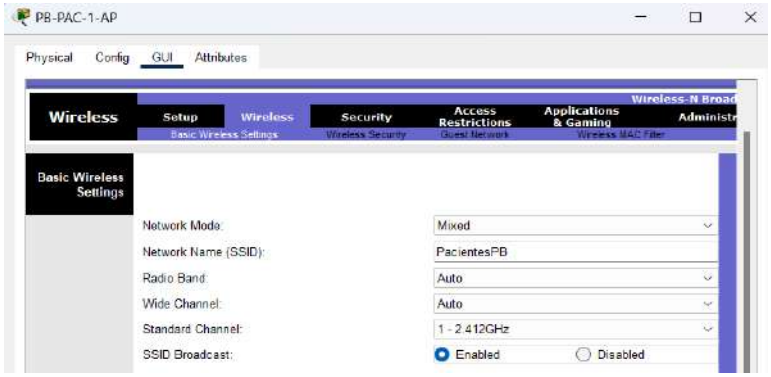

Figura 203. Configuramos el Nombre al Wifi (SSID) en este caso Pacientes PB

Se establece el modo de operación en **Mixed**, permitiendo compatibilidad con diferentes estándares WiFi (b/g/n). Esto garantiza que dispositivos antiguos y nuevos puedan conectarse sin problemas a la red.

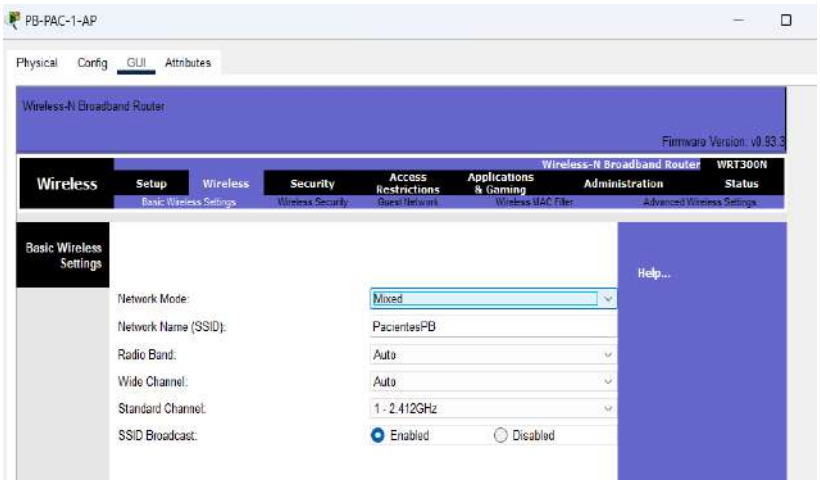

Figura 204. La configuración Network Mode la Mantenemos en Mixed

Se mantiene la opción **Radio Band** en Auto, permitiendo que el punto de acceso seleccione automáticamente la banda adecuada (2.4 GHz o 5 GHz) según el entorno y los dispositivos conectados, optimizando así el rendimiento inalámbrico.

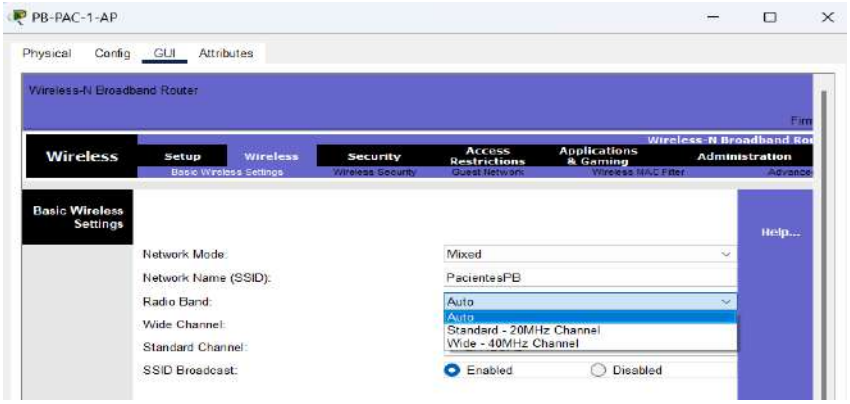

Figura 205. La configuración Radio Band la Mantenemos en Auto

La opción **Wide Channel** también se deja en Auto, permitiendo que el AP elija automáticamente el ancho de canal más eficiente (20 MHz o 40 MHz). Esto mejora la estabilidad y evita interferencias con otras redes cercanas.

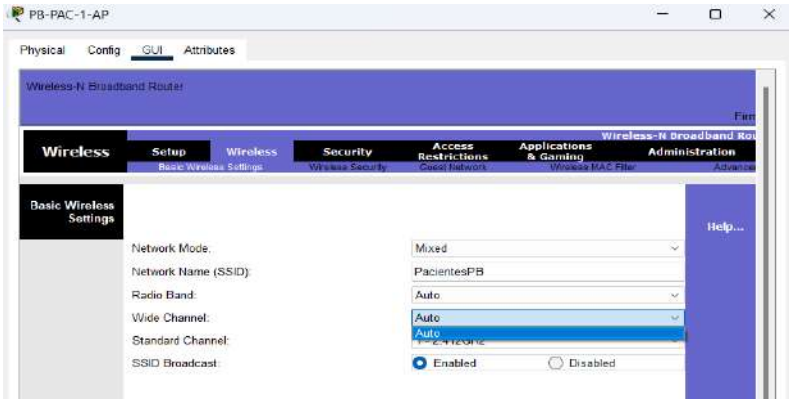

Figura 206. La Configuración Wide Channel la Mantenemos en Auto

Se selecciona el canal **1 (2.412 GHz)** para la red WiFi, una opción común que reduce interferencias y mejora la estabilidad, especialmente en entornos con múltiples redes inalámbricas.

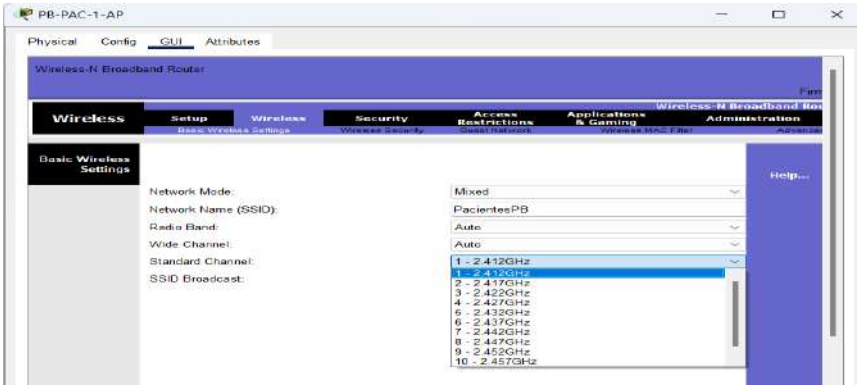

Figura 207. La configuración Standard Chanel la Mantenemos en el 1 - 2.412 GHz

El parámetro **SSID Broadcast** se mantiene en Enabled, lo que permite que el nombre de la red (SSID) sea visible para los usuarios y pueda ser detectado fácilmente por sus dispositivos.

Figura 208. La configuración SSID Broadcast la Mantenemos en Enabled

Se establece una contraseña para la red WiFi utilizando el modo de seguridad **WPA2 Personal** (el

simulador solo soporta hasta WPA2). Esto garantiza una conexión protegida mediante autenticación segura para los usuarios.

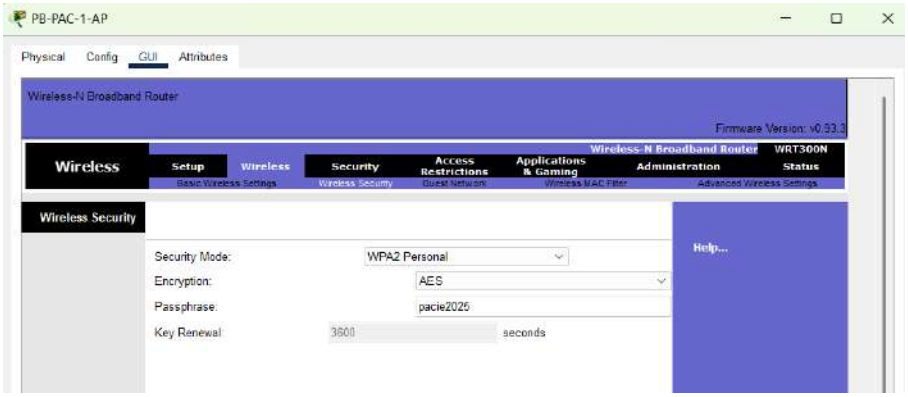

Figura 209. Configuramos una Contraseña con la seguridad de WPA3 Personal en este caso pacie123 (en este caso el simulador cuenta hasta WPA2)

La encriptación se configura en **AES**, el estándar más seguro y recomendado para redes inalámbricas. Esto ofrece mayor protección frente a ataques y asegura que los datos transmitidos por WiFi viajen cifrados correctamente.

Figura 210. Configuramos la encriptación en AES

Se verifica la configuración inalámbrica aplicada, confirmando que el SSID, canal, autenticación y cifrado coinciden con los parámetros definidos. Esto asegura que la red WiFi esté funcionando correctamente según las especificaciones del diseño de red.

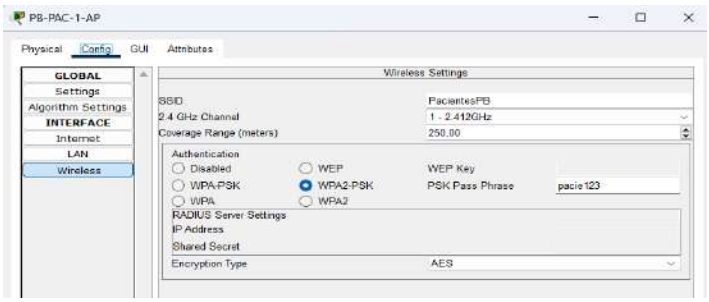

Figura 211. Verificamos la configuración asignada

Se muestra las contraseñas asignadas a cada punto de acceso (AP) según la planta y el tipo de usuario Médicos o Pacientes. Cada planta cuenta con una clave distinta para mejorar la seguridad, evitar accesos no autorizados y facilitar la gestión por segmentos, permitiendo controlar quién se conecta y desde dónde. Esta separación también ayuda a identificar y administrar mejor el tráfico de cada área dentro de la clínica.

Switch por plantas	**Contraseñas**
MédicosPB	medic2025
MédicosP1	medicP12025
MédicosP2	medicP22025
MédicosP3	medicP32025
PacientesPB	pacie2025
PacientesP1	pacieP12025
PacientesP2	pacieP22025
PacientesP3	pacieP32025

Tabla 109. Configuración de las contraseñas de los Access Point de la Clinica

III.1.5.3.2.2.1.- Autenticación de la red wifi

Se observa el proceso de autenticación del dispositivo inalámbrico para ingresar a la red WiFi. El usuario selecciona el SSID correspondiente e introduce la contraseña configurada bajo el método de seguridad WPA2-PSK(WPA3 limitado por packet tracer). Las credenciales utilizadas están autorizadas únicamente para el personal de salud, ya que pertenecen a la VLAN 30, la cual es una red privada destinada exclusivamente a personal autorizado. De esta manera, solo dispositivos validados pueden acceder a los recursos internos definidos para esta VLAN.

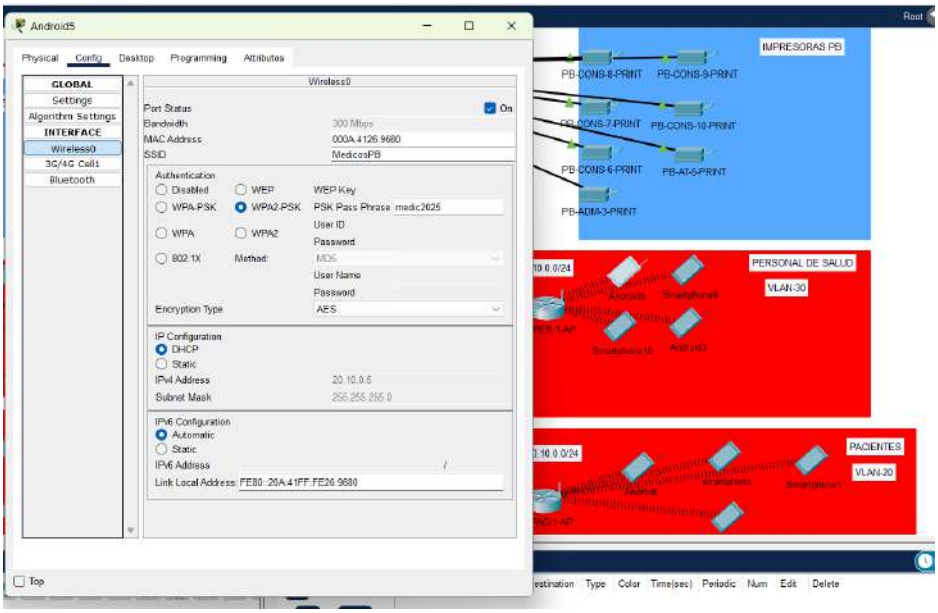

Figura 212. Autentificar dispositivo

Aquí se configura el Access Point donde se definen los parámetros de autenticación de la red WiFi, como el SSID, el tipo de seguridad (WPA2/WPA2-PSK), el cifrado AES y la clave de acceso. La contraseña asignada está limitada únicamente al personal de salud, perteneciente a la VLAN 30, que es una red privada y restringida. Por otro lado, la VLAN 20 es configurada como una red pública, destinada a los pacientes, con credenciales distintas y acceso limitado para mayor seguridad.

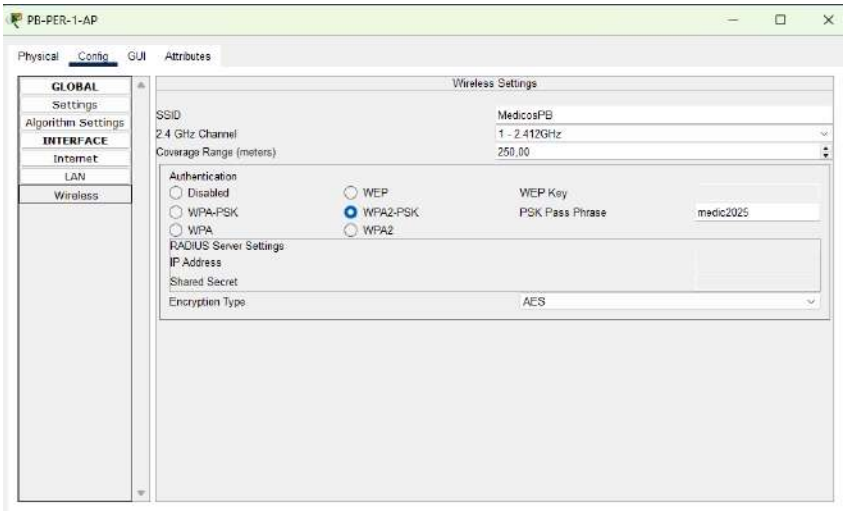

Figura 213. Access Poit a cual conectarse

III.1.5.3.2.2.2.- Seguridad de la red Wifi

Para implementar mejoras en la seguridad de la red Wi-Fi de la clínica, vamos a utilizar WPA3, que es la tercera versión del protocolo de acceso protegido para redes Wi-Fi, introducidas por la Wi-Fi Alliance en 2018. WPA3 trae varias innovaciones tanto para uso personal como empresarial,

incluyendo:

Cifrado de datos individualizado: En redes públicas, cuando un dispositivo se conecta, WPA3 utiliza un proceso de registro más seguro, que no depende de una contraseña compartida. Emplea un protocolo llamado DPP (Device Provisioning Protocol) que permite conectar dispositivos mediante etiquetas NFC o códigos QR, mejorando así la seguridad en la conexión inicial. Además, WPA3 usa un cifrado más fuerte,

GCMP-256, reemplazando el cifrado de 128 bits que se usaba anteriormente.

Autenticación simultánea de iguales: Este protocolo crea un enlace seguro al conectarse un dispositivo a un punto de acceso inalámbrico, verificando tanto la autenticación como la conexión de forma más robusta. Incluso si una contraseña es débil, WPA3 establece un protocolo de enlace seguro gracias al uso del Wi-Fi DPP.

Protección contra ataques de fuerza bruta: WPA3 evita los ataques de fuerza bruta fuera de línea al permitir solo una oportunidad de adivinanza por intento. Esto requiere que el usuario interactúe directamente con el dispositivo Wi-Fi cada vez, evitando la vulnerabilidad de redes abiertas de WPA2.

	WEP	WPA	WPA2	WPA3
Año salida	1997	2003	2004	2018
Cifrado	RC4	TKIP con RC4	AES-CCMP	AES-CCMP y AES-GCMP
Tamaño de clave	64 y 128 bits	128 bits	128 bits	128 y 256 bits
Tipo de cifrado	Flujo	Flujo	Bloque	Bloque
Autenticación	Sistema abierto y clave compartida	Clave precompartida (PSK) y 802.1x con variante EAP	Clave precompartida (PSK) y 802.1x con variante EAP	Simultaneous Authentication of Equals (SAE) y 802.x con variante EAP

Figura 214. Seguridad de la red Wifi

III.1.5.3.2.2.3.- Aproximado de cuantas personas acceden a la clínica por turnos

Se evaluó cuantas personas ingresan al Clínica tomando en cuenta los horarios de trabajo Turno Mañana inicia alas 7am hasta las 1pm

Turno Tarde inicia alas 1pm hasta las 7pm

Turno Noche inicia alas 7pm hasta las 7am

De igual manera tomando en cuenta todo el personal de la clínica y los pacientes para ver la capacidad de cuantas personas accederán a la red inalámbrica que tiene un aproximado de 180 personas.

Turno	Personal Administrativo y Médicos	Pacientes, Pasantes, Internos, Residentes	Total
Mañana	25	45	70

Tarde	15	60	75
Noche	7	28	35
Total	**47**	**133**	**180**

Tabla 110. Personas que acceden a la clinica

Ancho de banda

Para evitar la congestión y asegurar una experiencia más estable para 300 personas, lo ideal es contar con un ancho de aproximadamente 500 Mbps.

III.1.5.3.2.2.4.- Servicios del Access Point

El TP-Link Omada EAP225 es un punto de acceso de clase empresarial de doble banda (2,4 y 5GHz) montado en el techo o pared que soporta Wi-Fi 5 (802.11ac) y ofrece velocidades combinadas de hasta 1350 Mbps. Equipado con MU-MIMO, Beamforming, WPA3 (según firmware), QoS y AirTime Fairness, este dispositivo está diseñado para entornos de alta densidad y tráfico intenso.

Wi-Fi AC1350 de doble banda

- 450 Mbps simultáneos en 2.4 GHz
- 867 Mbps simultáneos en 5 GHz
- Velocidades combinadas de hasta 1350 Mbps
- Conectividad de alta densidad
- Gracias a MU-MIMO y Beamforming, el EAP225 puede atender múltiples dispositivos de manera eficiente, optimizando la cobertura y estabilidad de la red.

Integración en Omada SDN

- Provisionamiento sin intervención (ZTP)
- Administración centralizada en la nube
- Monitorización inteligente
- Control mediante aplicación Omada App

Roaming sin interrupciones

- Compatible con 802.11k/v
- Permite movilidad fluida entre puntos de acceso sin cortes en videollamadas o transmisiones de voz.

Soporte PoE

- Compatible con 802.3af PoE para una instalación sencilla y flexible sin necesidad de alimentación adicional.

Red de invitados segura

- Múltiples opciones de autenticación: Portal cautivo, SMS, Facebook Wi-Fi, Voucher, etc.
- Seguridad avanzada con WPA3 (según firmware disponible) y tecnologías de aislamiento de clientes.

Características relevantes del TP-Link Omada EAP225:

- Compatibilidad con Omada SDN: Control unificado desde hardware, software o nube.
- Roaming rápido: transición fluida entre APs con 802.11k/v.
- Dual-Band AC1350: cobertura estable en 2.4 GHz y 5 GHz.
- Modo Mesh (con Omada): Permite crear redes Mesh cuando no se dispone de cableado entre APs.

Protocolo	Frecuencia	Ancho del canal	MIMO	Velocidad de datos máxima (en teoría)
802.11ax	2,4 o 5 GHz	20, 40, 80, 160 MHz	Usuario múltiple (MIMO-MU)	2,4 Gbps[1]
802.11ac wave2	5 GHz	20, 40, 80, 160 MHz	Usuario múltiple (MIMO-MU)	1,73 Gbps[1]
802.11ac wave1	5 GHz	20, 40, 80 MHz	Un solo usuario (SU-MIMO)	866,7 Mbps[2]
802.11n	2,4 o 5 GHz	20, 40 MHz	Un solo usuario (SU-MIMO)	450 Mbps[2]
802.11g	2,4 GHz	20 MHz	No se aplica	54 Mbps
802.11a	5 GHz	20 MHz	No se aplica	54 Mbps
802.11b	2,4 GHz	20 MHz	No se aplica	11 Mbps
Tradicional 802.11	2,4 GHz	20 MHz	No se aplica	2 Mbps

Figura 215. Estándares de Wi-Fi

III.1.5.3.2.2.5.- Descripción de la instalación

En este apartado se demostró como debe ser una instalación de un AP ya que la demás configuración tanto para el Personal de salud y Pacientes o Invitados en las diferentes plantas serán de la misma forma. Se configuro diferentes direcciones IP exclusivas para los Access Points (AP), iniciando con el ubicado en la Planta Baja. En cada planta se permitirá la conexión de hasta 50 dispositivos, tanto de pacientes como del personal de salud. La red destinada a los pacientes estará completamente aislada: no tendrá ningún tipo de comunicación con las demás áreas de la clínica ni con los servidores, garantizando así la seguridad, el control del tráfico y la privacidad de los servicios internos.

III.1.5.3.3.-Extensiones SIP para diferentes áreas

N.º	Nombre de Área	Número de teléfono
1	Administración-PB	1001
2	Recepción-PB	1002
3	Consultorios-PB-1	1003
4	Consultorios-PB-2	1004
5	Consultorios-PB-3	1005

6	Consultorios-PB-4	1006
7	Consultorios-PB-5	1007
8	Emergencias-PB	1008
9	Área Tercerizada-PB	1009
10	Enfermería-P1-1	1010
11	Enfermería-P2-2	1011
12	Enfermería-P3-3	1012
13	Terapia Intensiva-P1-1	1013
14	Terapia Intensiva-P2-2	1014
15	Terapia Intensiva-P3-3	1015
16	Pediatría-P3-1	1016
17	Pediatría-P3-2	1017
18	Farmacia-P3	1018
19	Esterilización-P3	1019
20	Contabilidad-P3	1020
21	Internación-P1-1	1021
22	Internación-P2-2	1022
23	Internación-P3-3	1023

Tabla 111. Extensiones para diferentes áreas

III.1.5.3.3.1.- Restricción Del Servidor

El acceso al servidor Issabel está diseñado exclusivamente para el personal del área de sistemas, garantizando que solo ellos puedan gestionar y administrar el sistema. Esto asegura un control estricto, evita accesos no autorizados y protege la integridad de los servicios críticos que dependen del servidor.

III.1.5.3.3.2.- Ventajas de Issabel

Ventajas clave:

- Facilidad de uso: Ofrece una interfaz amigable, ideal para equipos no especializados en IT.
- Integración completa: Incluye funcionalidades empresariales como correo de voz, reportes y administración de extensiones.
- Soporte comunitario: Amplia base de usuarios y documentación gratuita.
- Costo cero: Al ser de código abierto, no requiere licencias costosas.
- Versatilidad: Compatible con hardware existente y VoIP.

Alternativas comparadas:

- FreePBX: Similar en funcionalidad, pero Issabel es más robusta para call centers.
- 3CX: Es más fácil de usar, pero requiere licencias pagas.
- Cisco Unified Communications: Solución propietaria más costosa.

III.1.5.3.3.3.- Instalación de Issabel

Figura 216. Una vez Cargada la Imagen ISO Colocamos Test this media & install

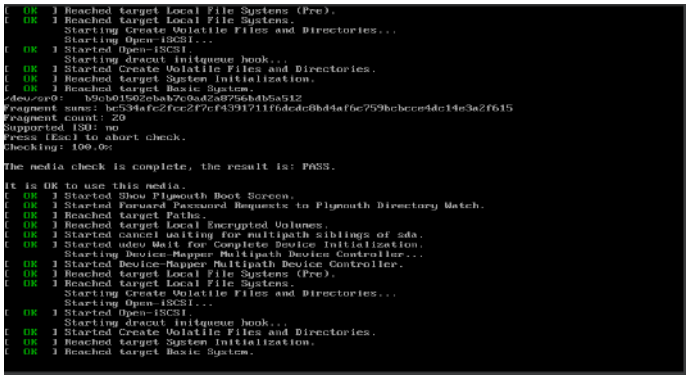

Figura 217. Esperamos la instalación

Figura 218. Seleccionamos el Idioma Español

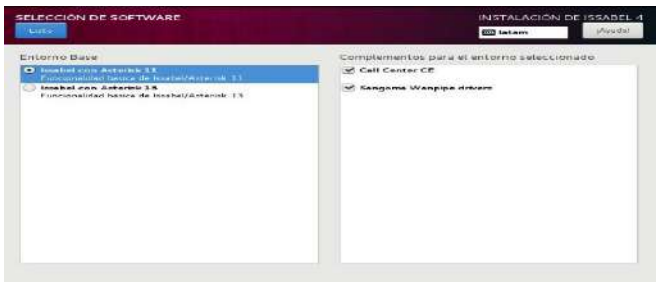

Figura 219. Seleccionamos el Software de Asterisk 11

Figura 220. Colocamos una Contraseña Root

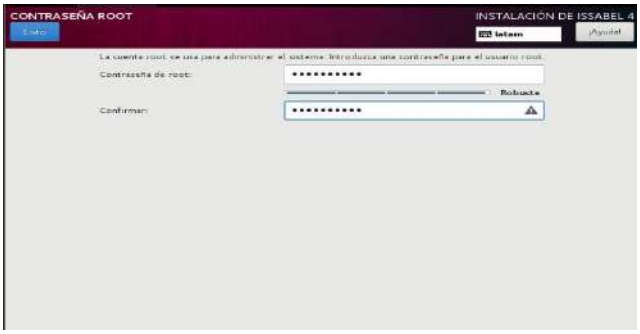

Figura 221. Colocamos una Contraseña Administrativa Root 12623385c

Figura 222. Continua la Instalación

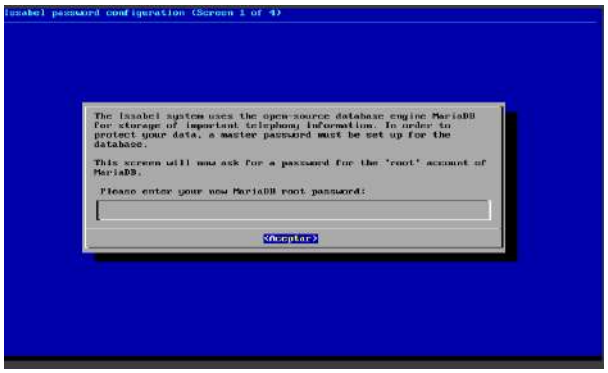

Figura 223. Luego de Instalar Pedirá que Coloquen la Contraseña de Root de la base de datos 12623385c

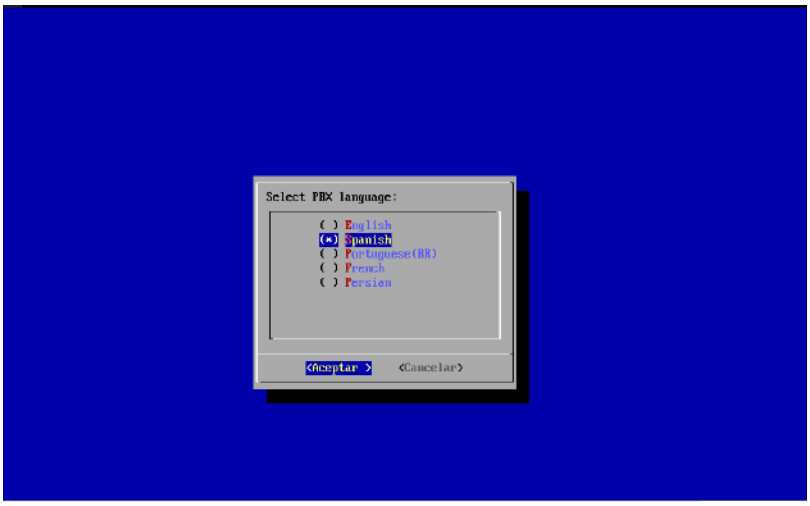

Figura 224. Seleccionamos el Idioma Español

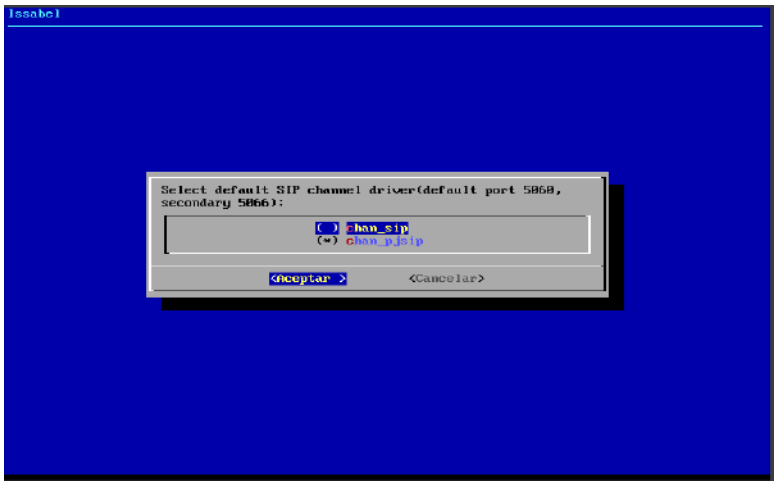

Figura 225. Selecciona el tipo de SIP Chanel chan_pjsip

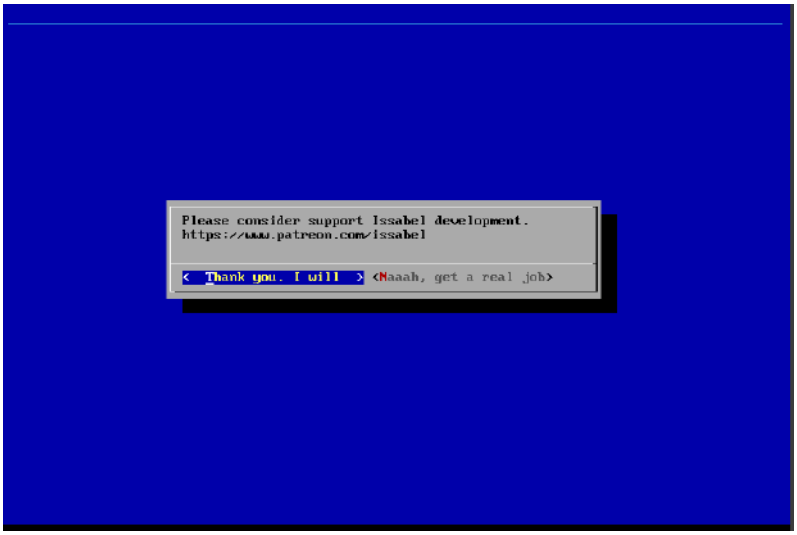

Figura 226. Desea Acceder a su Página Oficial

Figura 227. Iniciamos Sesión login: root password: 12623385c

Figura 228. Direccion IP tipo Estatico

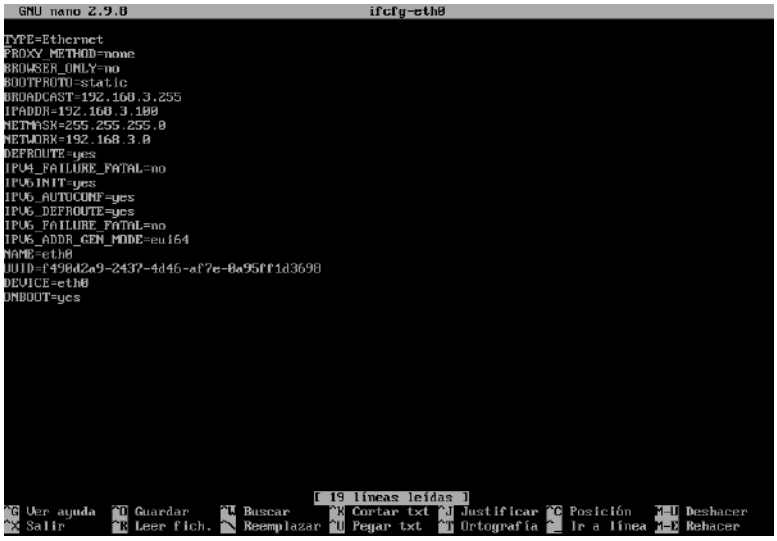

Figura 229. Configuramos la IP 192.168.3.100 para el servidor Asterisk

```
[root@issabel network-scripts]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.3.100  netmask 255.255.255.0  broadcast 192.168.3.255
        inet6 fe80::20c:29ff:fe7c:37e3  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:7c:37:e3  txqueuelen 1000  (Ethernet)
        RX packets 102  bytes 35110 (34.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 117  bytes 47406 (46.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 6210  bytes 475707 (464.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6210  bytes 475707 (464.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@issabel network-scripts]# _
```

Figura 230. Verificar el cambio de IP

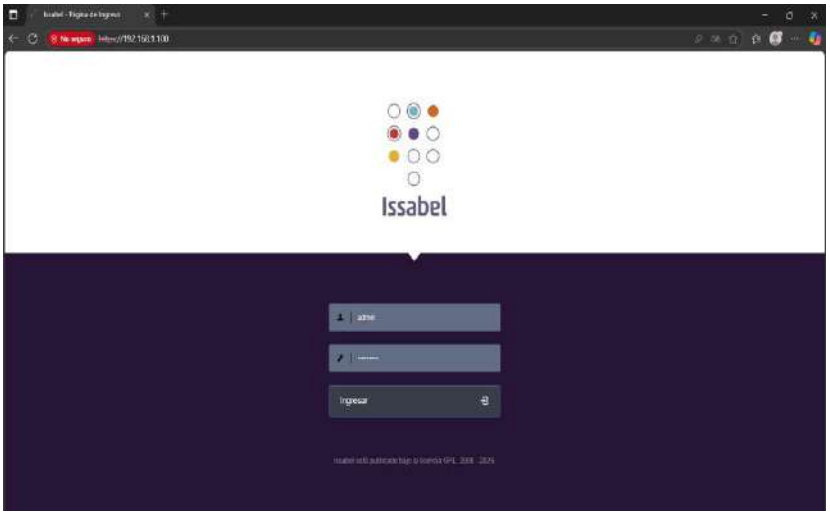

Figura 231. Inicio de Sesión por Interfaz ingresando la IP 192.168.3.100

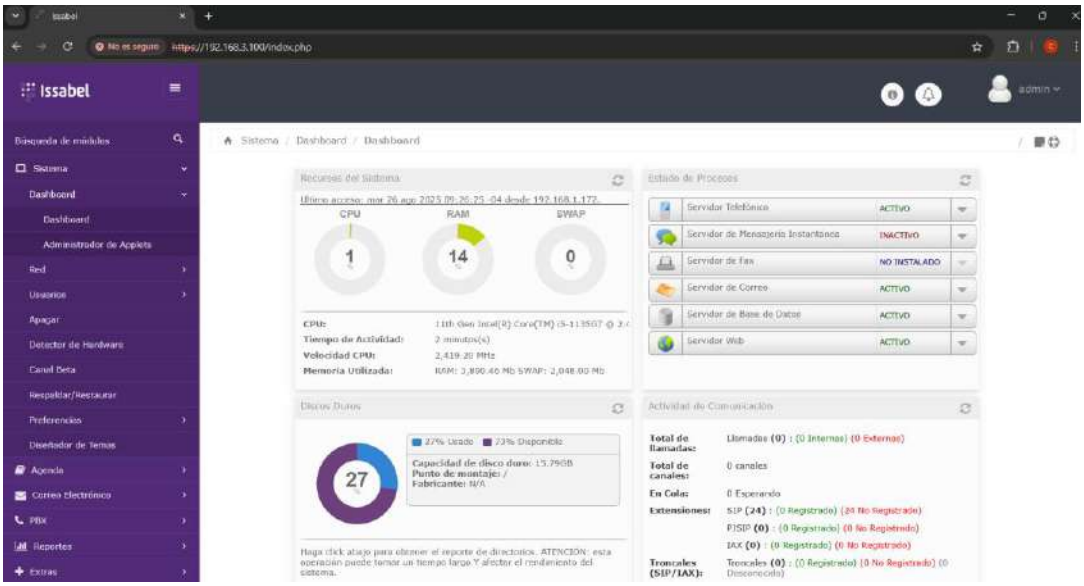

Figura 232. Iniciamos Sesión con Nombre de Usuario: admin contraseña: 12623385c

III.1.5.3.3.4.- Añadir una extensión(número) al servidor

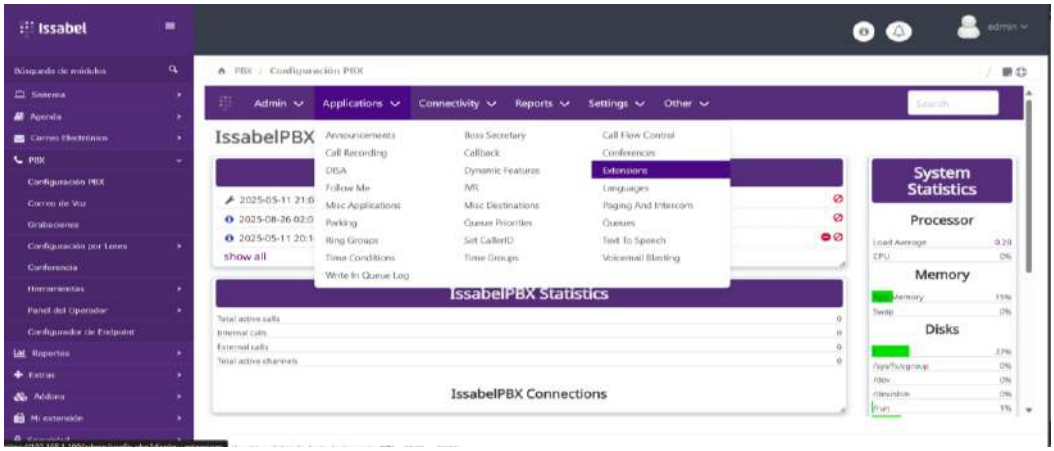

Figura 233. Entramos a PBX -> Configuración PBX, Dejamos por Defecto SIP y Damos Enviar

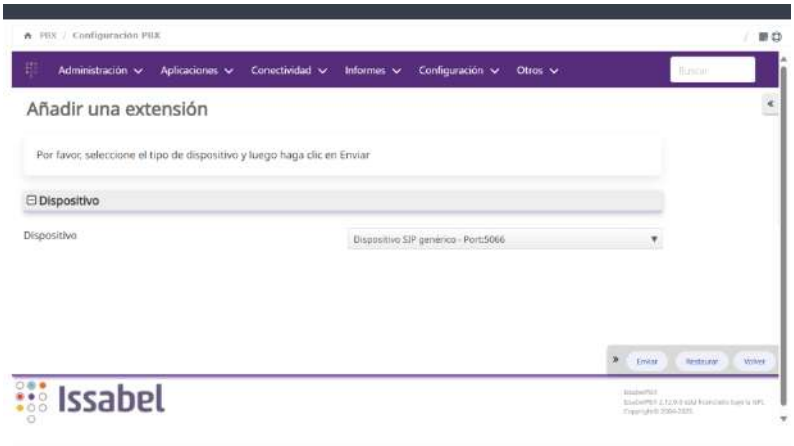

Figura 234. Protocolo de inicio de sesión SIP

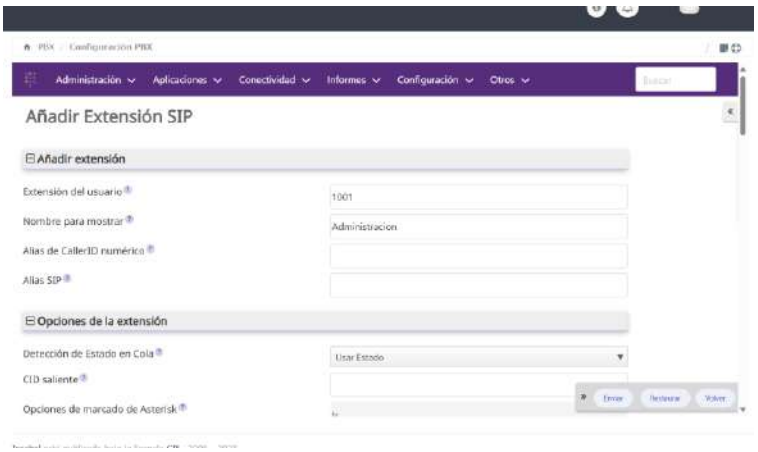

Figura 235. Llenamos los datos Extensión de Usuario: 1001 Nombre para mostrar: Administración

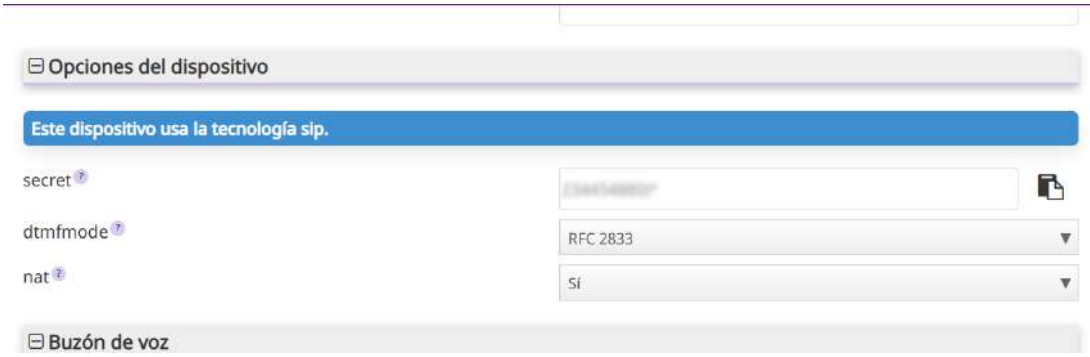

Figura 236. Contraseña con la cual iniciara sesión para los dispositivos

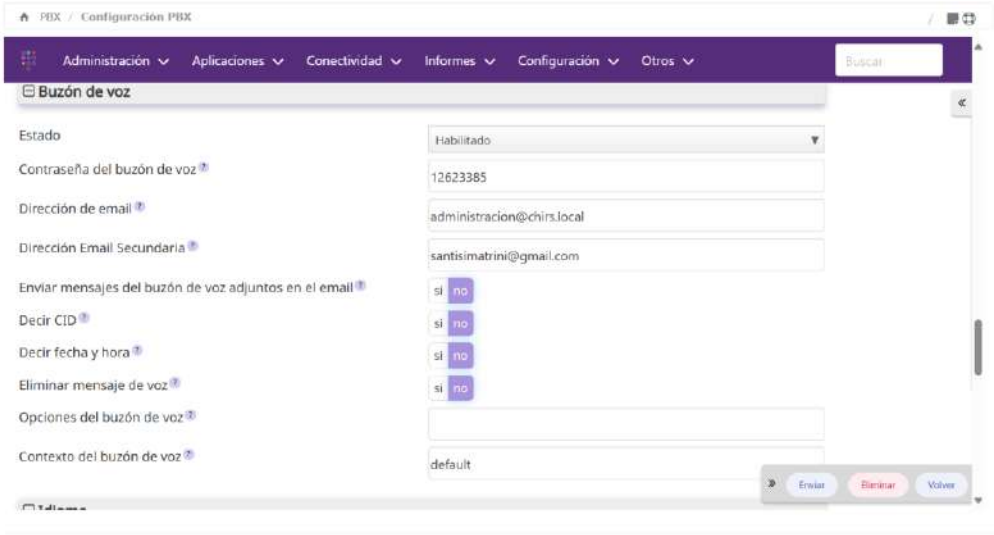

Figura 237. Habilitamos el Buzón de Voz para poder escuchar los mensajes de voz guardados

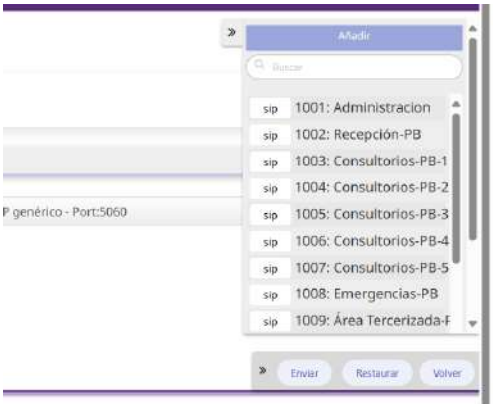

Figura 238. Verificamos las Extensiones Creadas

III.1.5.3.3.5.- Instalación de video llamadas

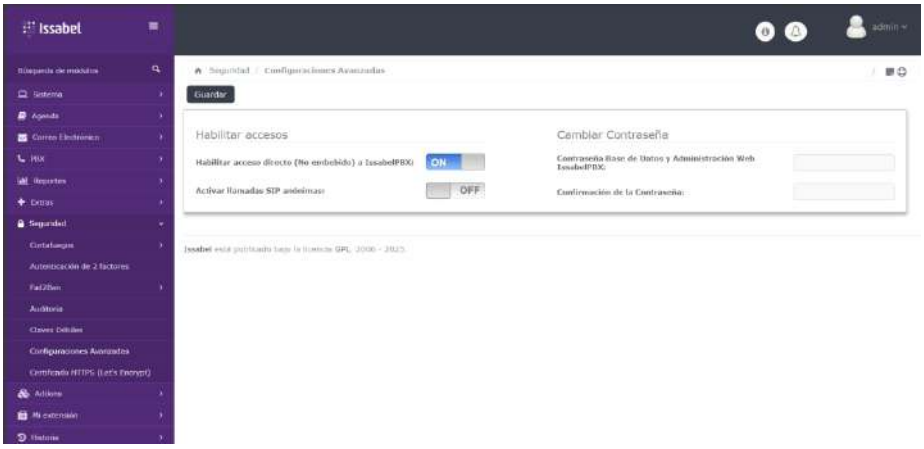

Figura 239. Entramos a Seguridad y Después Configuraciones Avanzadas

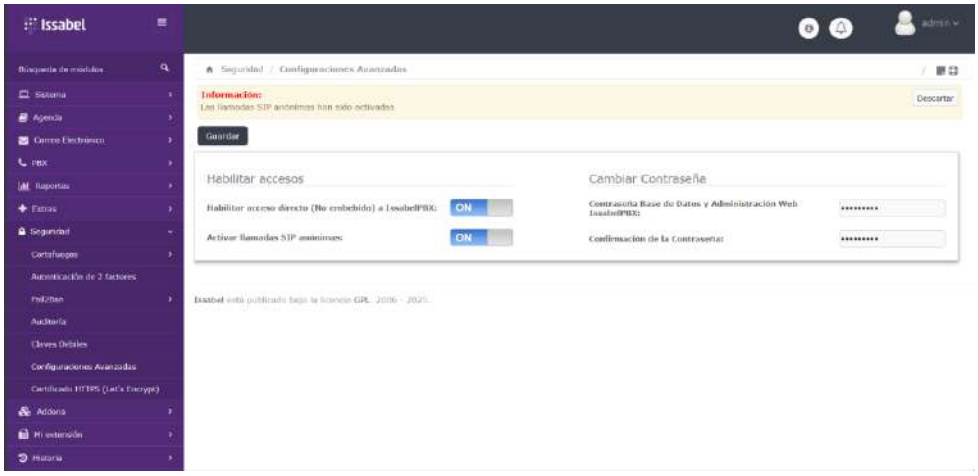

Figura 240. Activamos el Acceso Directo no Integrado y Colocamos la Contraseña: 12623385c para Guardar Cambios

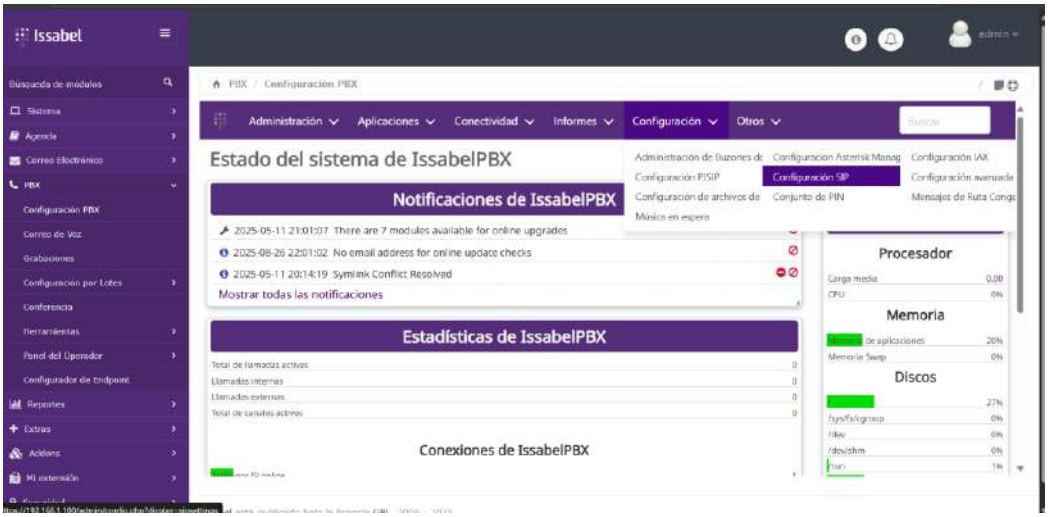

Figura 241. Volvemos a PBX>Configuración PBX>Configuración SIP

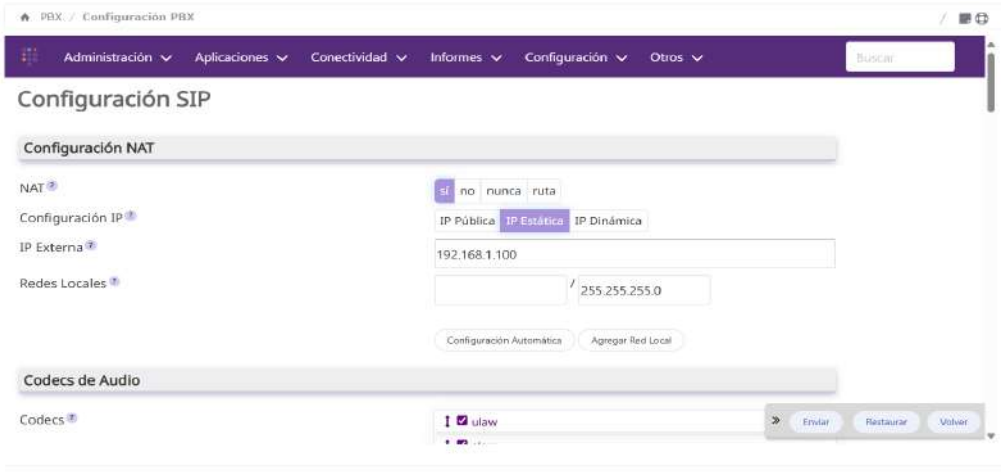

Figura 242. En este apartado añadimos la IP del servidor 192.168.3.100

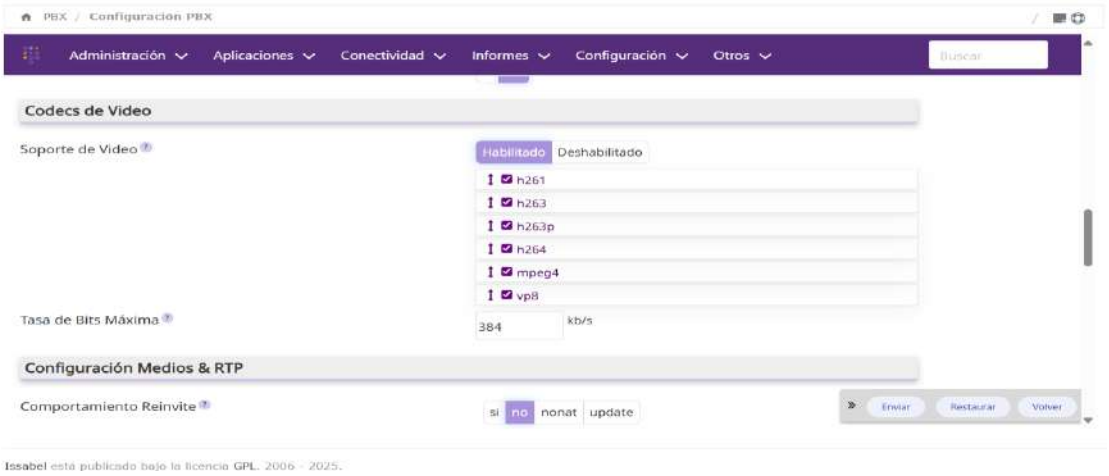

Figura 243. Video Suport lo Activamos y Seleccionamos Todos los Formatos de Video

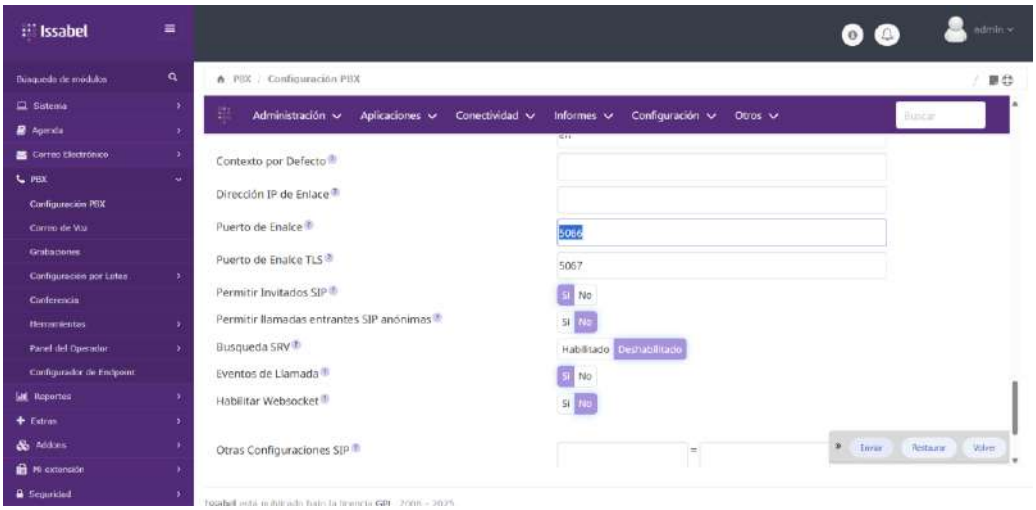

Figura 244. Verificamos el puerto 5066 y presionamos Enviar

III.1.5.3.3.6.- Colas de llamadas

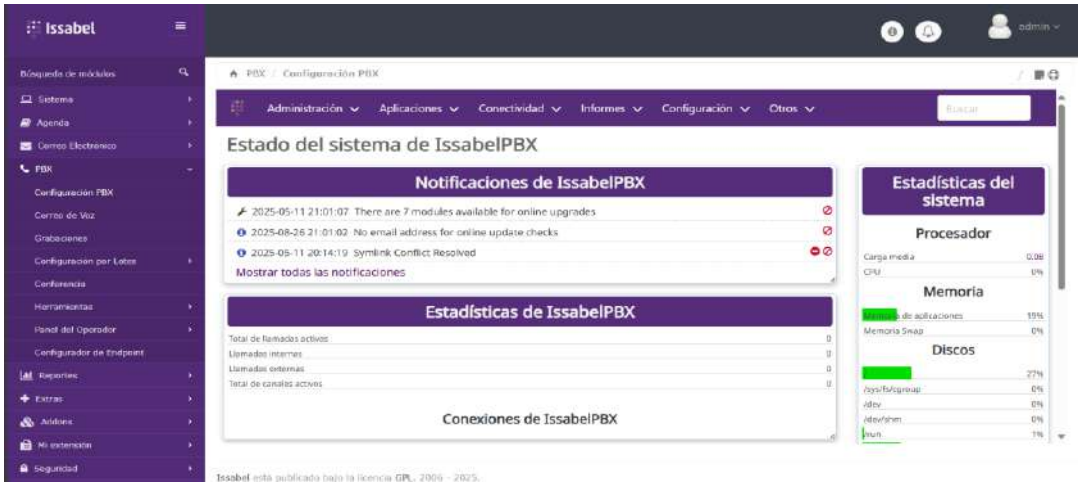

Figura 245. Entramos a PBX -> Configuración PBX

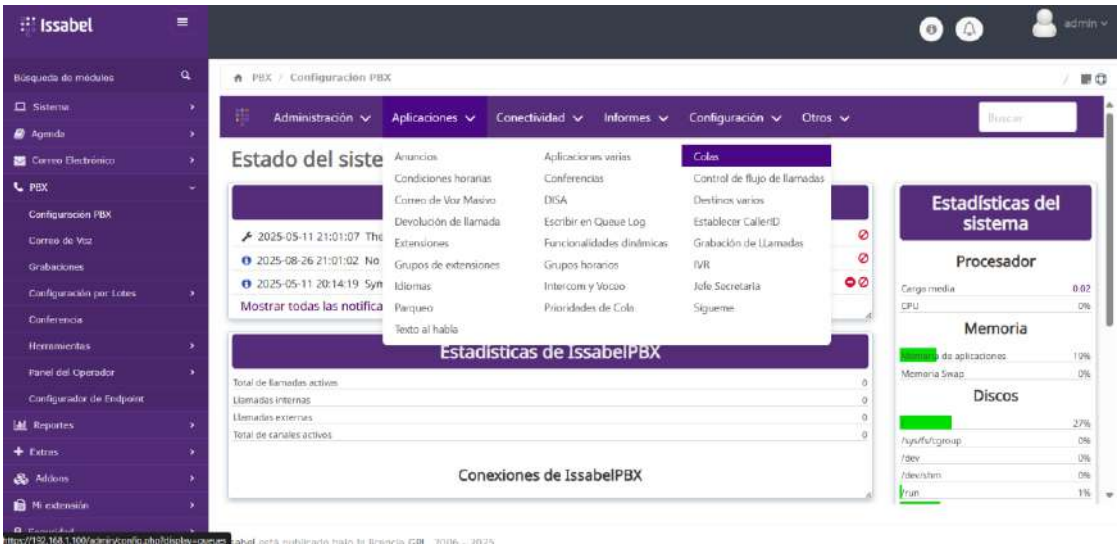

Figura 246. Entramos a Colas

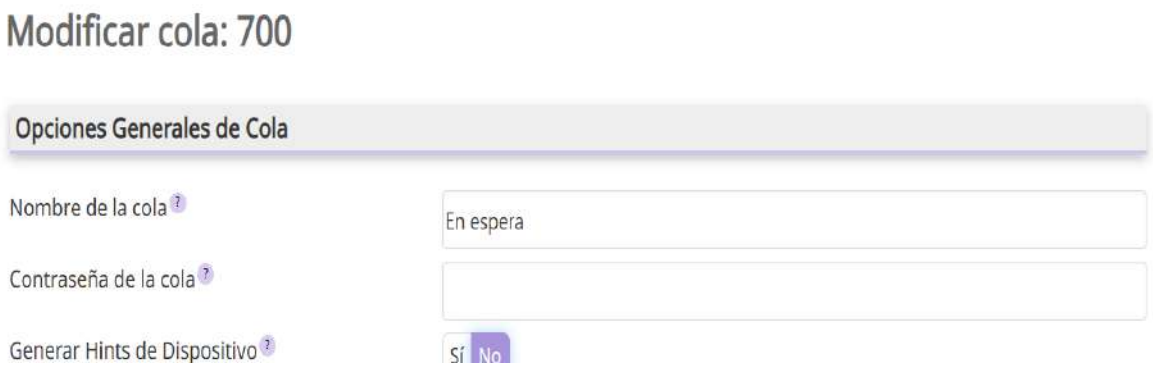

Figura 247. Creamos el grupo y el numero de cola

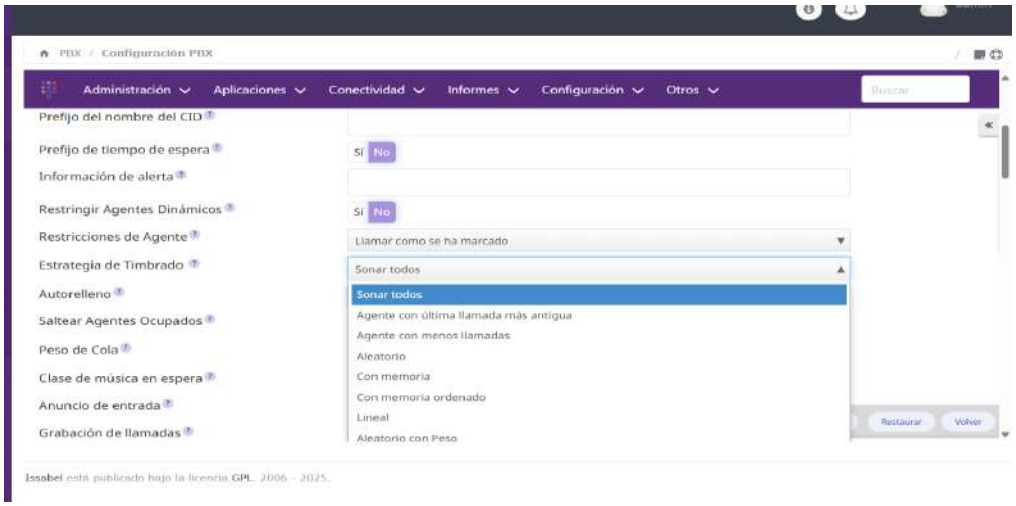

Figura 248. En estrategia de timbrado sonar todos

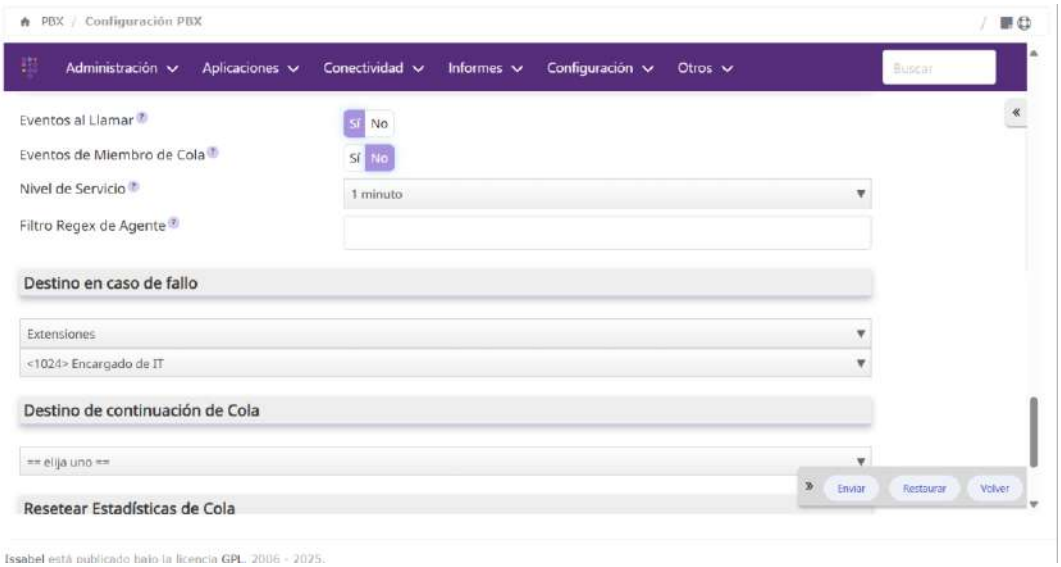

Figura 249. En caso de fallos

III.1.5.3.3.7.- Correo de voz

Figura 250. Entramos a Correo de voz

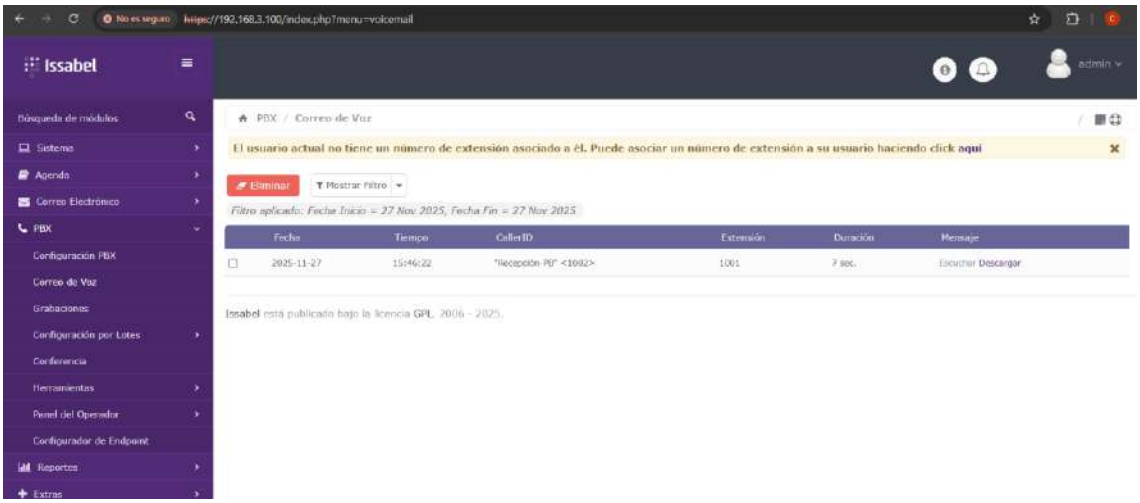

Figura 251. Se encuentra registrado todas las grabaciones de llamadas a las diferentes extensions

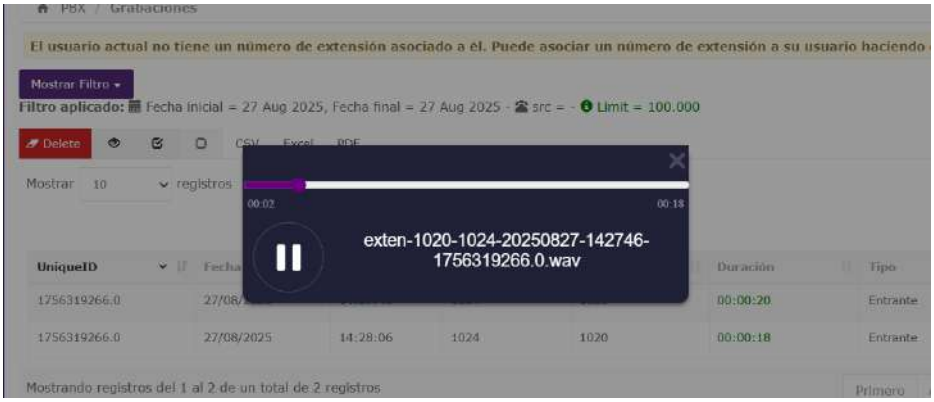

Figura 252. Escuchando la grabacion

III.1.5.3.3.8.- Buzón de voz

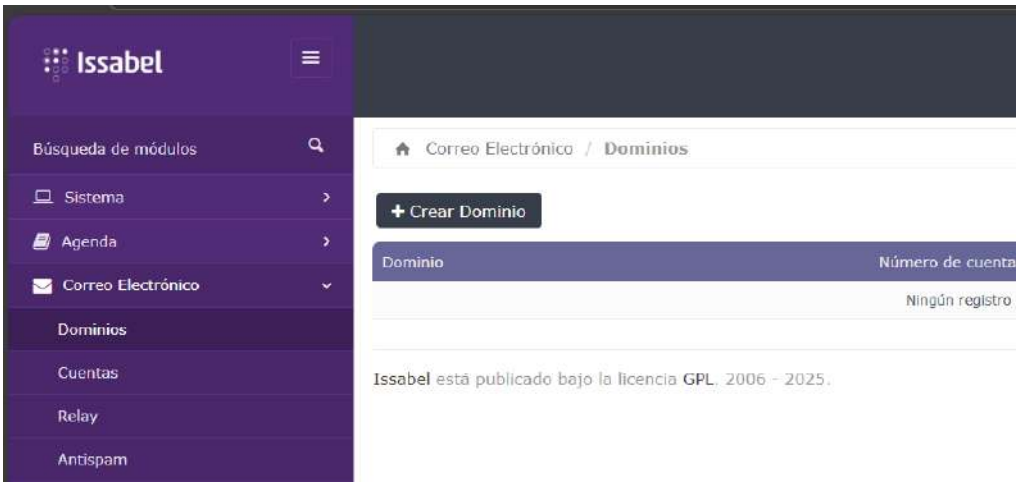

Figura 253. Nos dirigimos hacia Correo Electronico -> Dominios

Figura 254. Creamos el Dominio como "santisimatrinidad.local"

Figura 255. Nos dirigimos a cuentas

Figura 256. Seleccionamos el Dominio y creamos una nueva cuenta

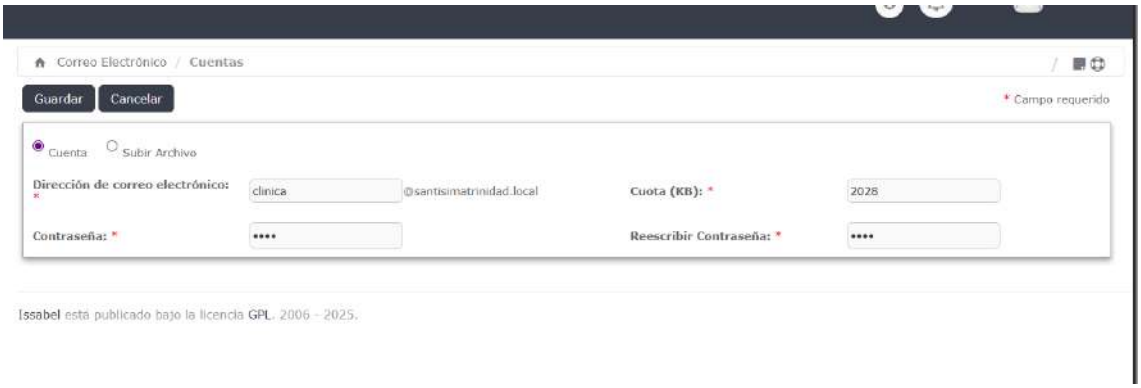

Figura 257. Seleccionamos el Dominio y Creamos una Cuenta

clinica@santisimatrinidad.local Contraseña: 6545

Cuota (KB): * 2028 Guardamos

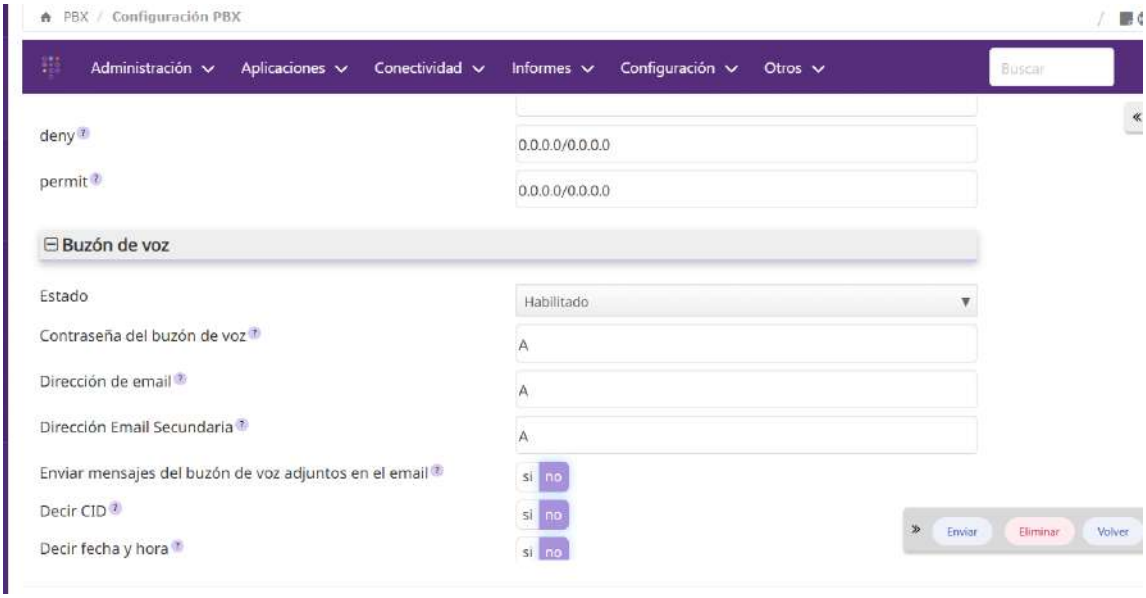

Figura 258. Volvemos al apartado de buzon de voz en dichas extensiones

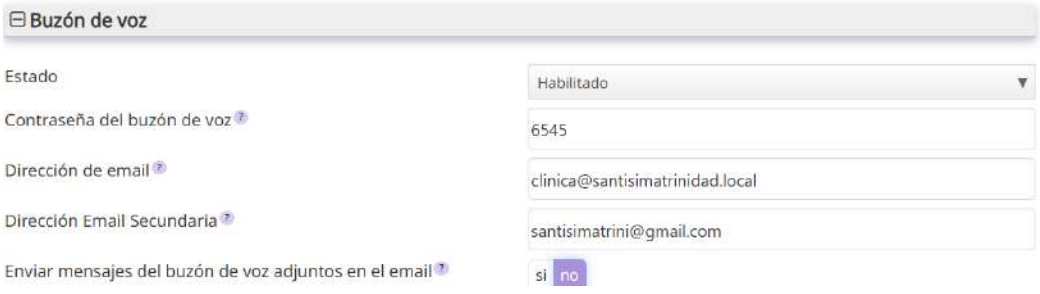

Figura 259.Habilitamos y empezamos a añadir dichas direcciones

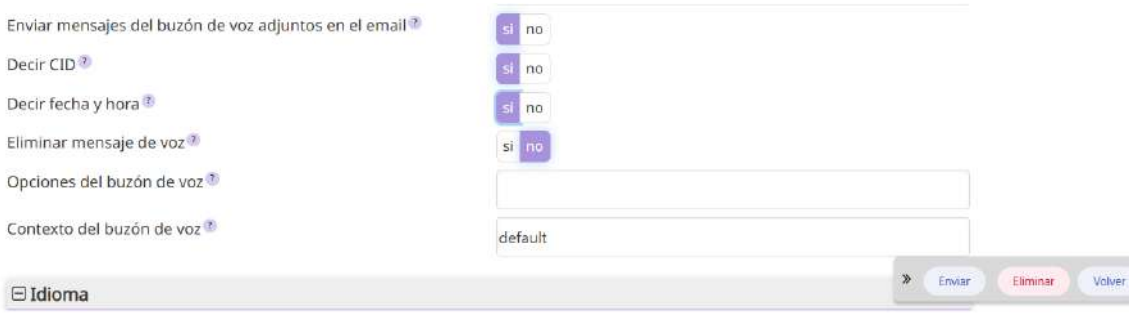

Figura 260. Enviar Mensajes del Buzón de Voz Adjuntos en el Email: yes, Decir CID: yes, Decir Fecha y Hora: yes y Enviar

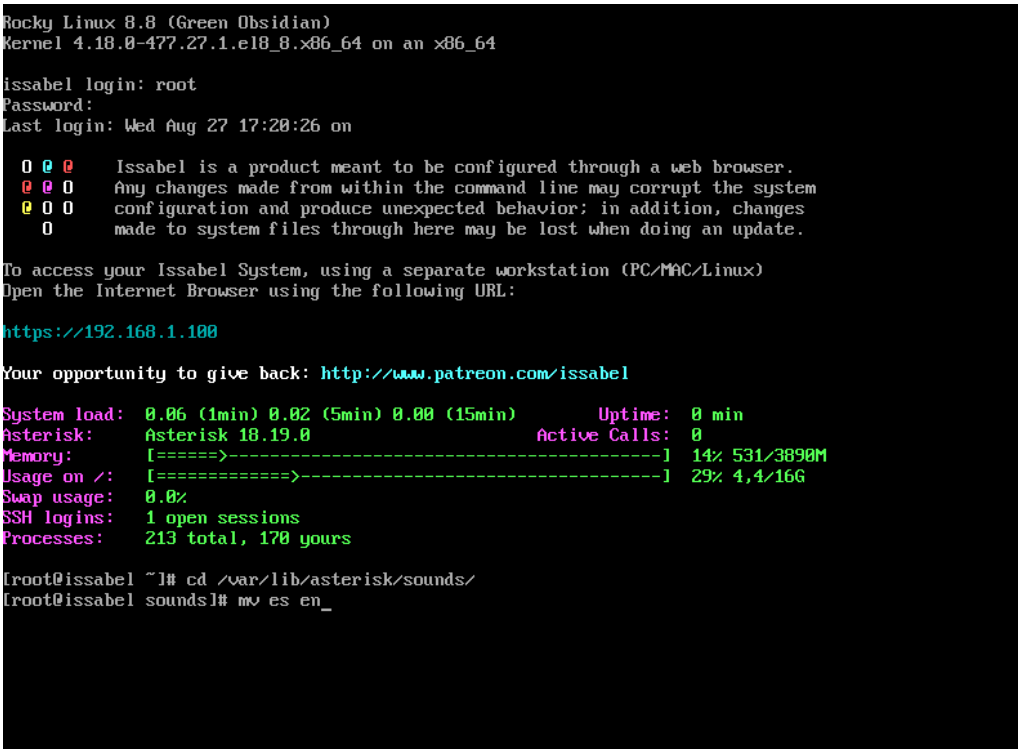

Figura 261. Configuramos para cambiar al operador a español

III.1.5.3.3.9.- Configuración dispositivo móvil con el servidor

Figura 262. Tenemos que estar Conectados a la red Wifi de la clínica en el área de Personal de salud

Figura 263. Descargamos la Aplicación Zoiper del Google Play

Figura 264. Dentro de la Aplicación Necesitamos Colocar la Extensión Creada Seguido de @ y la Dirección del Servidor de Telefonía IP agregando: el puerto que se está utilizando y la Contraseña Creada en el Servidor

Figura 265. En Hostname Dejamos la IP del Servidor de Telefonía IP

Figura 266. Mantenemos por defecto la Configuración del Proxy

Figura 267. Esperamos la Conexión SIP UDP (si marco verde) la Configuración fue Todo un Éxito

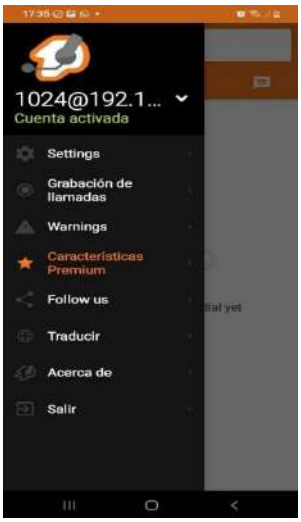

Figura 268. Verificamos que la Cuenta Este Activada

Figura 269. Podemos Comenzar a Usar los Teléfonos Mediante la Telefonía IP

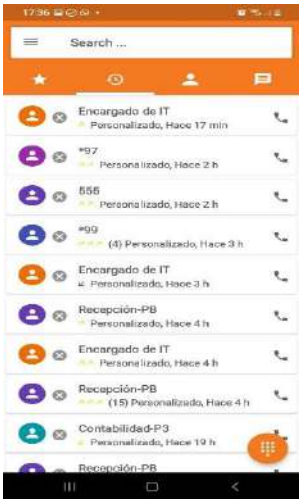

Figura 270. Podemos ver el Historial de Llamadas

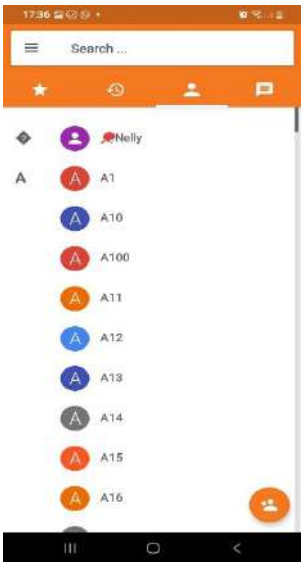

Figura 271. Podemos Vincular Nuestros Contactos

Figura 272. Prueba de Llamada Entramos al Teléfono

Figura 273. Marcamos *60 Para Escuchar la Hora

Figura 274. Interfaz de Llamada Entrante

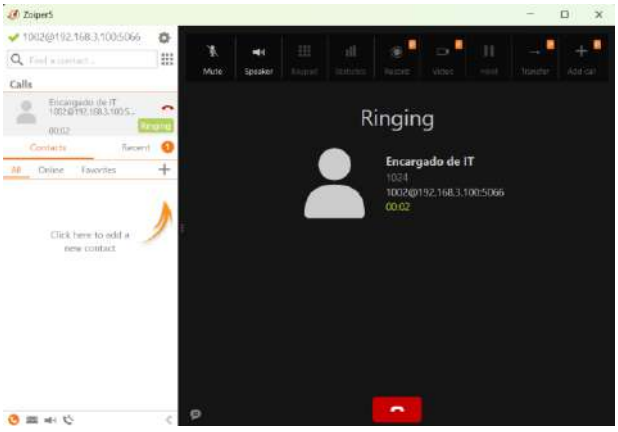

Figura 275. Interfaz de Llamada en Espera a Contestar

III.1.5.3.3.10.- Beneficios y comparativa al usar el servidor de telefonía IP Issabel

Características	Central de Telefonía IP Externa (3CX, RingCentral)	Servidor de Telefonía IP Issabel (Local)
Costo	Elevado (licencias y soporte propietarios)	Gratuito (código abierto, sin licencias costosas)
Costo inicial	Bajo, generalmente basado en suscripciones.	Mayor, ya que requiere hardware y configuración inicial. Sin embargo, es una inversión que elimina pagos recurrentes a largo plazo.
Costo a largo plazo	Pago mensual o anual basado en el número de extensiones o usuarios.	Mucho menor, ya que no hay suscripciones continuas. Solo necesitas mantenimiento interno, lo que resulta en ahorros significativos con el tiempo.
Control sobre los datos	Limitado. Los datos de llamadas	Totalmente local, los datos

	y configuraciones están alojados en los servidores del proveedor, lo que puede ser un riesgo para la privacidad.	permanecen dentro de la red de la organización, garantizando seguridad, privacidad y cumplimiento de normativas internas.
Personalización	Limitada a las opciones que ofrece el proveedor.	Altamente personalizable: Issabel permite ajustar cada aspecto del sistema, desde reglas de llamadas hasta integraciones con software existente.
Escalabilidad	Alta, pero los costos aumentan proporcionalmente al agregar extensiones o servicios adicionales.	Escalable internamente según la capacidad del hardware. Los costos son controlables y no aumentan por extensiones adicionales.
Seguridad	La seguridad está en manos del proveedor, lo que implica confiar en terceros para proteger la información.	Seguridad bajo control local, con opciones avanzadas de configuración, como VPN y firewalls personalizados para proteger la red.
Compatibilidad de hardware	Limitada a equipos y servicios compatibles con el proveedor.	Compatible con una amplia gama de dispositivos VoIP y adaptadores, lo que reduce costos y mejora la flexibilidad tecnológica.
Flexibilidad de uso	Rápido de implementar, pero depende de las opciones predefinidas del proveedor.	Completamente flexible: Issabel te permite configurar IVR, grabación de llamadas, integración con CRM y mucho más, sin restricciones de terceros.
Soporte técnico	Incluido en el servicio, pero puede ser limitado a las políticas del proveedor.	Puedes gestionar el soporte con tu equipo interno o recurrir a la activa comunidad de Issabel, reduciendo costos y aumentando la autonomía.
Fiabilidad	Alta si el proveedor es confiable y ofrece redundancia en su infraestructura. Sin embargo, puede ser vulnerable a fallas de internet o problemas con el proveedor.	Muy alta en redes locales, ya que no depende de factores externos. Además, puedes configurar redundancia interna para mayor fiabilidad.
Independencia del proveedor	Baja. Estás atado al proveedor, y cambiar de servicio puede ser complejo y costoso.	Total, independencia tecnológica, ya que Issabel es de código abierto. Puedes modificar, actualizar o migrar según tus necesidades, sin costos ocultos.
Teléfonos IP físicos necesarios	Altamente recomendados. A menudo forman parte del	No necesarios. Puedes usar Zoiper o cualquier softphone.

	sistema.	
Flexibilidad de dispositivos	Media: Teléfonos IP físicos son la opción preferida.	Alta: smartphones, PC, tablets con Zoiper u otros.
Costo inicial	Alto (compra de teléfonos IP físicos o planes más caros).	Muy bajo (solo un servidor Issabel y dispositivos existentes).
Independencia de hardware	Limitada: En muchos casos, debes adquirir hardware compatible.	Total: Issabel no te obliga a un tipo específico de dispositivo.
Precio en compra de teléfonos IP GXP1610 GrandStream	32 teléfonos para cada área precio unitario Bs. 430,11 precio total Bs 13763,52	Sin gasto ya que no requiere comprar teléfonos IP

Tabla 112. Beneficios y comparativa telefonía IP

III.1.5.3.4.- 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 VLAN 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 Fortinet

- 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
- El monitoreo de red se usa principalmente para monitorear el rendimiento, pero también puede ayudar a descubrir amenazas de seguridad dentro del 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
- Dejar un buzón de voz para llamadas perdidas
- Realizar video llamadas
- 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
- Se pueden atender llamadas en movilidad

Mejorar el cuarto de telecomunicaciones

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

III.1.6.- Fase 6: Monitoreo de la red

III.1.6.1.- 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.1.6.1.1.- Monitoreo Clínica

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 están usando en el equipo de computación aquí se puede observar que se tiene un total de 117.7 mb usados en el transcurso del día en la red.

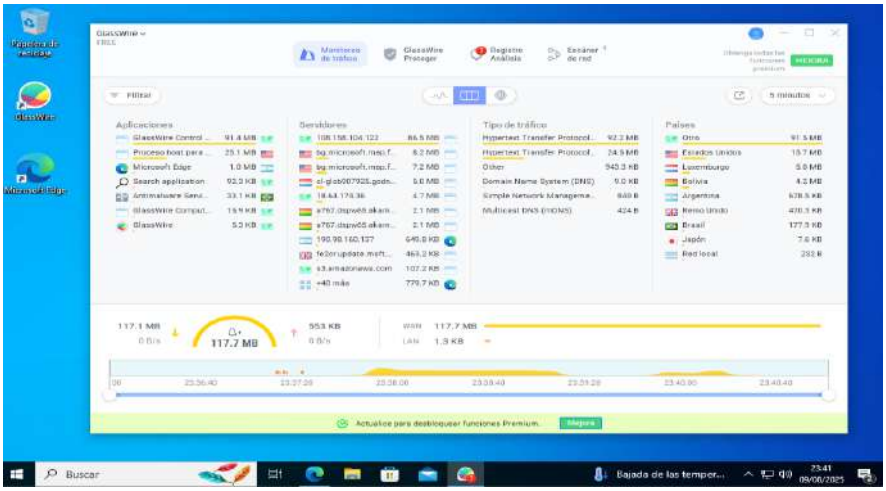

Figura 276. Monitoreo de la red en uso

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 esta en 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.

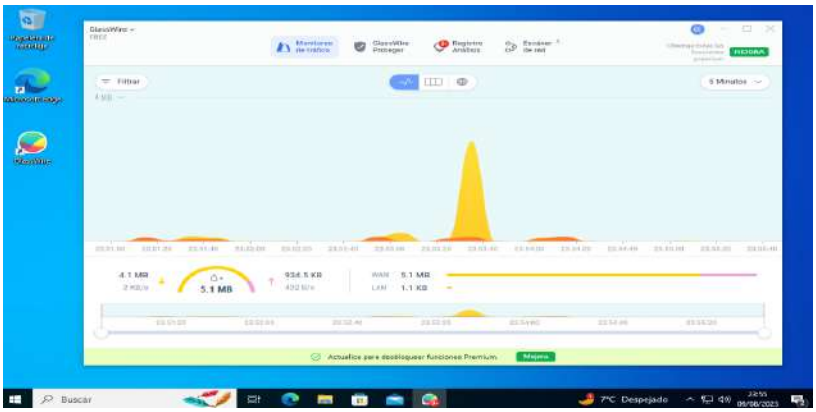

Figura 277. Monitoreo de la red en modo grafico

III.1.6.1.2.- 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 ancho de banda de redes 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 la alta velocidad de la fibra óptica que se dio a cada subred.
- 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.1.6.1.3.- Verificación de Monitoreo de la red

Informe de Monitoreo de Tráfico de Datos

La ventana de conversaciones IPv4 en Wireshark muestra un resumen de todas las comunicaciones que ocurrieron entre direcciones IP durante una captura de red. Cada fila representa un intercambio de datos entre dos equipos, indicando cuántos paquetes se enviaron, cuántos se recibieron, el tamaño de la información transmitida, el tiempo que duró la comunicación y la velocidad promedio. En pocas palabras, esta vista permite identificar qué dispositivos se comunicaron, cuánto tráfico

generó y si las respuestas fueron exitosas o unidireccionales, facilitando así el análisis general del comportamiento de la red.

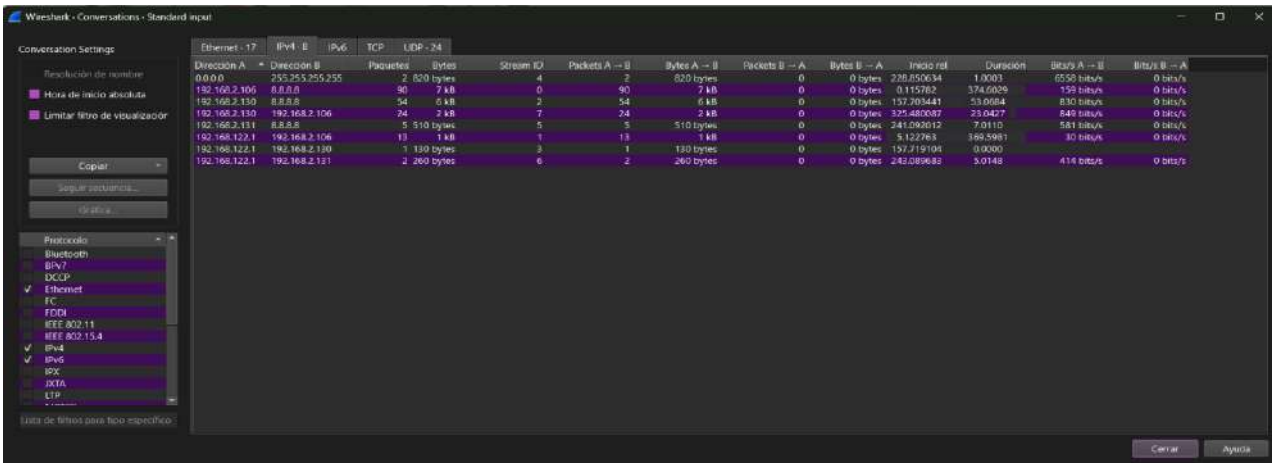

Figura 278. Conversaciones IPV4

El monitoreo del tráfico UDP muestra el intercambio de datos entre equipos de la red sin necesidad de establecer una conexión previa. En la captura se observan principalmente paquetes DNS, usados para resolver nombres de dominio, y DHCP, que asignan direcciones IP automáticamente a los dispositivos. Este tráfico indica que la red está funcionando correctamente, permitiendo la comunicación y el acceso a servicios externos como Internet.

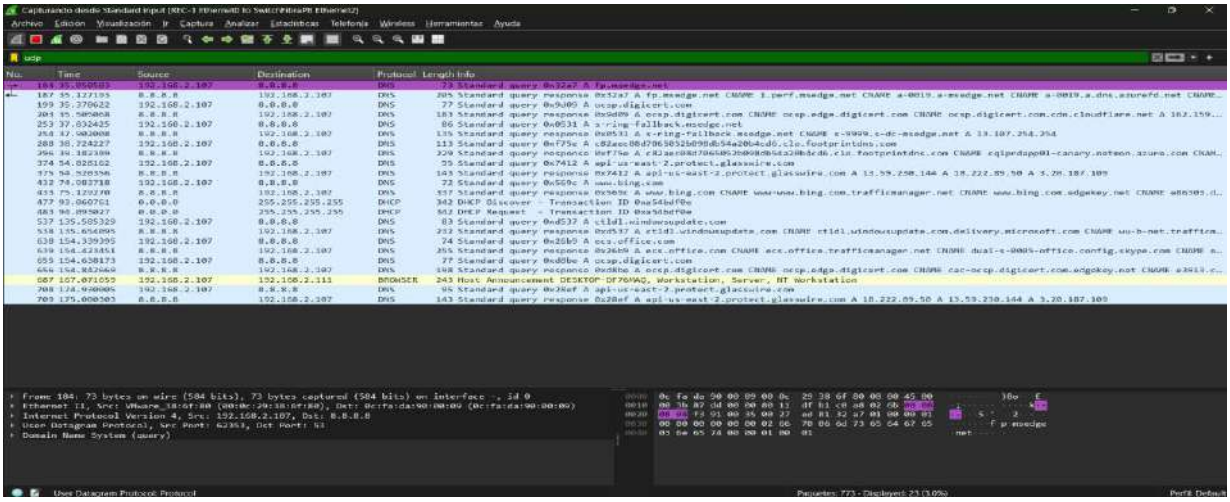

Figura 279. Informe de Monitoreo de Tráfico de Datos UDP

El gráfico de entrada y salida del tráfico de datos muestra la cantidad de paquetes transmitidos y recibidos por segundo en la red durante el monitoreo. La línea negra representa el total de paquetes, mientras que las barras rojas reflejan los paquetes filtrados o analizados (UDP y TCP). Se puede observar un flujo constante de tráfico, con variaciones en la cantidad de paquetes a lo largo del tiempo, lo que indica una actividad de red continua. En resumen, el gráfico evidencia que la red

mantiene un intercambio estable de información sin interrupciones notables.

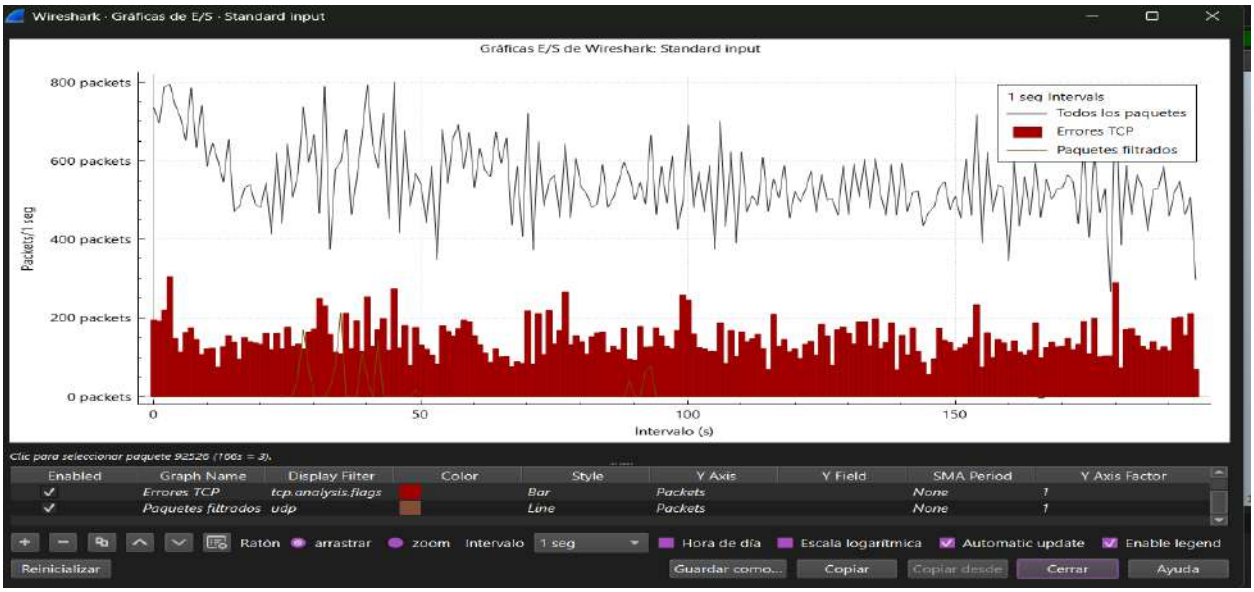

Figura 280. Gráfico de entrada y salida del tráfico de datos

Resultados esperados de testeo de red

Figura 281. Resultados esperados de testeo de red

Registro de llamadas y comunicaciones del servidor de Telefonía IP

El registro de llamadas y comunicaciones del servidor de telefonía IP muestra de forma detallada el historial de llamadas realizadas, recibidas o fallidas, incluyendo datos como fecha, hora, origen, destino, estado de la llamada (contestada, no contestada, ocupada o fallida), duración y canales utilizados, además de ofrecer gráficos estadísticos que permiten analizar visualmente el comportamiento y desempeño de las comunicaciones en el periodo seleccionado.

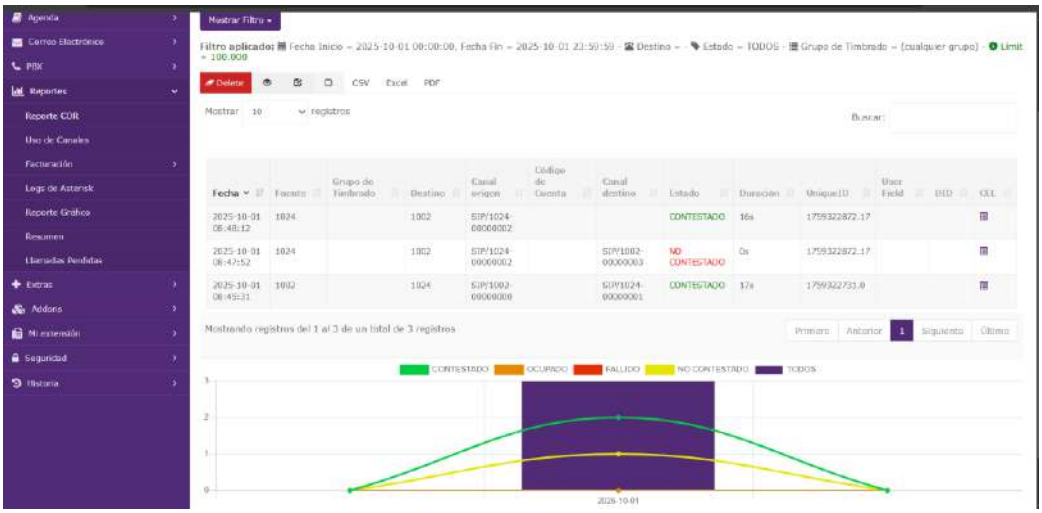

Figura 282. Registro de llamadas y comunicaciones del servidor de Telefonía IP

Reporte de uso de servidor de telefonía IP

El reporte de uso del servidor de telefonía IP muestra el estado general del sistema y los recursos utilizados. Incluye indicadores de consumo de CPU, memoria RAM y SWAP, así como información del hardware, tiempo de actividad y memoria empleada. Además, detalla el estado de los principales servicios del sistema, como el servidor telefónico, de mensajería instantánea, correo, base de datos y web, indicando si están activos o no instalados. Este resumen permite supervisar el rendimiento y funcionamiento del servidor para garantizar su operatividad eficiente.

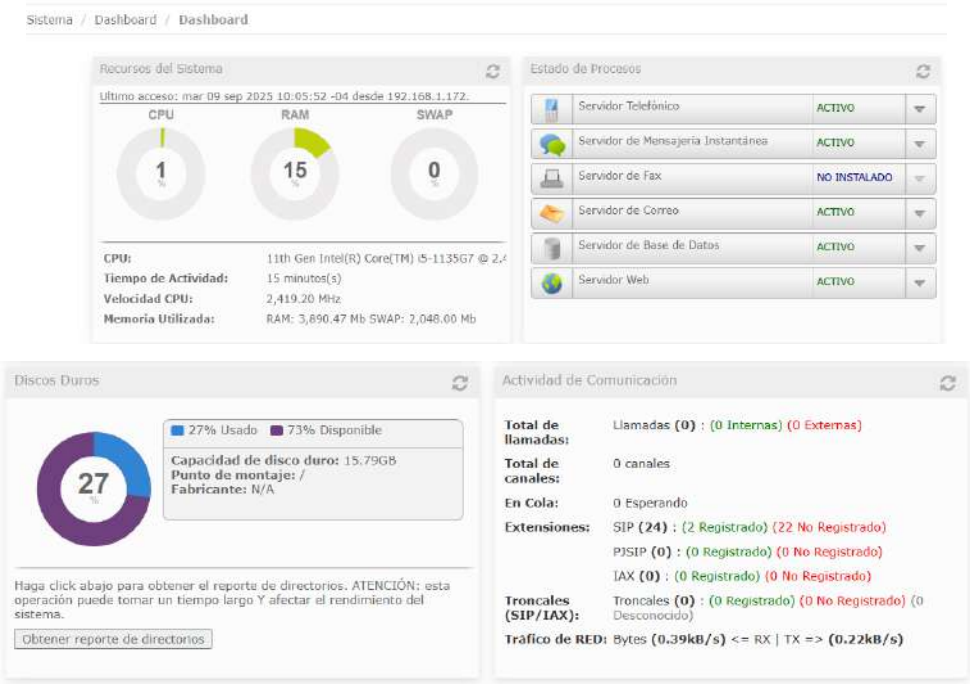

Figura 283. Reporte de uso de servidor de telefonía IP

Registro y Supervisión de Tráfico Denegado por el Firewall

Muestra las políticas de seguridad configuradas para el control de tráfico entre redes internas (VLANS) e Internet, indicando el origen, destino, servicios permitidos, acción aplicada (ACCEPT o DENY), uso de NAT, perfiles de seguridad, registros de actividad y la cantidad de datos transferidos; destacando la regla "Implicit Deny", que bloquea automáticamente cualquier tráfico no autorizado por políticas anteriores, lo que permite monitorear intentos de acceso no permitidos y garantizar la protección de la red.

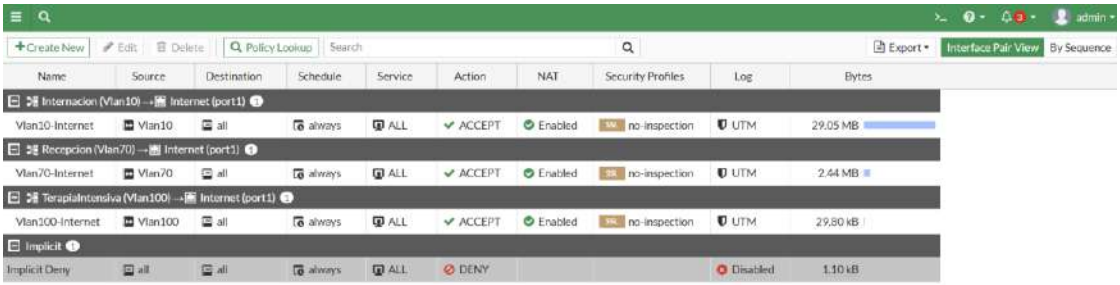

Figura 284. Registro y Supervisión de Tráfico Denegado por el Firewall

III.1.7.- Medio de verificación para el Componente 1

TARIJA, 20 de Octubre de 2025

Señora

Lic. Deysi Beatriz Arancibia Marquez

DIRECTORA a.i CARRERA DE INGENIERIA INFORMATICA FACULTAD DE CIENCIAS Y TECNOLOGIA

Presente.-

De mi mayor consideración:

Por medio de la presente, se hace constar que el proyecto titulado ***"Rediseño y Optimización de la Infraestructura de Red de la Clínica Santísima Trinidad"*** cumple con la norma ERS IEEE 830, aplicada como referencia para la correcta documentación de los requerimientos técnicos y funcionales del sistema de red, garantizando una estructura clara, completa y coherente con los objetivos planteados en el proyecto.

Agradecer de antemano su gentil deferencia, aprovecho la oportunidad para saludarle.

Atentamente,

Ing. SILVANA PAZ RAMIREZ
DOCENTE DE TALLER III
Universidad Autónoma Juan Misael Saracho
Tarija – Bolivia

III. Componente 2: Capacitación del personal en el buen uso y administración de la red

III.2.1.-Análisis

Con el objetivo de concluir el proyecto se brindará la correspondiente capacitación al personal de informática en un entorno real controlado, para probar que las instalaciones y configuraciones de los diferentes servicios estructurados.

El personal que se encuentra a cargo de los gabinetes de telecomunicaciones obtendrá conocimientos sobre el uso fundamental de las tecnologías implementadas en la nueva estructuración, haciendo uso de métodos de enseñanza para el aprendizaje para la administración y mantenimientos requeridos en un futuro.

Este componente asegura la transferencia de conocimientos sobre el trabajo del personal involucrado que conlleva a mejorar los conocimientos del personal que recibe la capacitación.

III.2.2.- Propósito

El propósito del componente es finalizar el proyecto con la capacitación, para contar con personal de informática sepa de la modificación de la red actual y tenga conocimiento de la nueva infraestructura de red por alguna posible falla.

III.2.3.- Objetivos generales

III.2.3.1.- Objetivo

- Capacitar al personal de informática sobre la nueva instalación del cuarto de Telecomunicaciones, sobre la administración de la nueva red en la infraestructura.

III.2.3.2.- Objetivos específicos

- Definición de medios y estrategias de capacitación.
- Capacitación sobre la nueva red.

III.2.4.- Diseño

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 del personal de informática (TI) solo se capacitara al personal técnico debido a que este es el único que tiene acceso y autorización de su uso y administración.

III.2.5.- Propuesta pedagógica

Para la propuesta pedagógica a utilizar sobre los servicios en la nueva infraestructura tecnológica dada las características de los usuarios directos que son el personal técnico administrativo del cuarto de telecomunicaciones.

El método de enseñanza será el aprendizaje Significativo: Debido a que este método se caracteriza que los mismos técnicos de la institución se les incorporará nuevos conocimientos previamente tomando en cuenta que el personal capacitado tenga alguna relación sobre las nuevas tecnologías implementadas que generará interés por aprender el uso de las herramientas para su trabajo cotidiano comprender para fallas.

III.2.5.- Desarrollo

Lo que comprende con el desarrollo o el análisis de las herramientas que se utilizaran para el aprendizaje de los encargados de informática de la institución se usara como herramienta principal de manera visual y el uso de backups hechos durante la configuración de los equipos como medio de explicación cargarla en un equipo o dispositivo pequeño y someterlo a pruebas de su funcionamiento.

III.2.6.- Implementación

III.2.6.1.- Puntos de 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 diferentes servicios del Firewall Fortinet
- Lección 6: Configuración de los equipos de computación para poder compartir archivos entre áreas
- Lección 7: Instalación de programas para los equipos
- Lección 8: Configuración del servidor de telefonía IP
- Lección 9: Administración del cuarto de telecomunicaciones
- Lección 10: Monitoreo de control al rack del cuarto de telecomunicaciones

III.2.6.2.- Plan de capacitación

Nro.	CONTENIDO	OBJETIVO	FECHA	DURACION (horas)	MATERIAL DIDACTICO	MEDIOS DE ENSEÑANZA Y APRENDIZAJE	DESTINATARIO
1	Configuración del router	Que los encargados puedan configurar correctamente y se ubiquen en la red	21/10/ 2025	2	Demostración en tiempo real	Equipo de computación	Encargado del cuarto de telecomunicaciones
2	Configuración del servidor DHCP	Que el personal técnico aprenda el manejo del servidor y pueda asignar direcciones a los usuarios de manera dinámica	22/10/ 2025	2	Demostración en tiempo real	Equipo de computación	Encargado del cuarto de telecomunicaciones
3	Configuración de las VLANs	Que se tenga conocimiento de cómo segmentar y manejar las redes lógicas	23/10/ 2025	2	Demostración en tiempo real	Equipo de computación	Encargado del cuarto de telecomunicaciones
4	Configuración de los Access Point.	Que el personal técnico aprenda a configurar los AP correctamente y con las nuevas configuraciones	24/10/ 2025	2	Demostración en tiempo real	Equipo de computación	Encargado del cuarto de telecomunicaciones
5	Configuración de los diferentes servicios del Firewall Fortinet	Que el personal técnico pueda configurar la interfaz inicial.	25/10/ 2025	2	Demostración en tiempo real	Equipo de computación	Encargado del cuarto de telecomunicaciones
6	Configuración de los equipos de computación para poder compartir	Que el personal técnico domine la administración y	27/10/ 2025	1	Demostración en tiempo real	Equipo de computación	Encargado del cuarto de telecomunicaciones

	archivos entre áreas	configuración de los equipos					
7	Instalación de programas para los equipos	Que el personal técnico pueda instalar los programas de manera correcta	28/10/ 2025	1	Demostración en tiempo real	Equipo de computación	Encargado del cuarto de telecomunicaciones
8	Configuración del servidor de telefonía IP	Que el personal tecnico aprenda la configuración de telefonía IP y pueda administrarla correctamente	29/10/ 2025	2	Demostración en tiempo real	Equipo de computación	Encargado del cuarto de telecomunicaciones
9	Administración del cuarto de telecomunicaciones	Que el personal técnico domine el manejo de la red y del centro de datos	30/10/ 2025	2	Demostración en tiempo real	Equipo de computación	Encargado del cuarto de telecomunicaciones
10	Monitoreo de control al rack del cuarto de telecomunicaciones	Que el personal tecnico aprenda a monitorear y supervisar el tráfico de datos de forma correcta	01/11/ 2025	1	Demostración en tiempo real	Equipo de computación	Encargado del cuarto de telecomunicaciones

Tabla 113. Plan de capacitación

III.2.7.- Evaluación

III.2.7.1.- Resultados

Se tiene como resultados la capacitación al personal técnico del área de informática de la institución, y se tornan capaces en el manejo de los equipos de red en el uso de los dispositivos de redes avanzadas.

III.2.7.2.- Conclusiones

Después que se realice la capacitación se concluirá de esta manera la etapa de capacitación de manera exitosa con la Socialización de la explicación de la infraestructura de red y principalmente con el manejo de los dispositivos de redes avanzadas.

III.2.8.- Medios de verificación para el Componente 2

- Carta de conformidad de informe técnico sobre los servicios prestados en la institución por parte del encargado de Informática.
- Lista de asistentes de la capacitación.

Tarija, 5 de octubre del 2025

Señor:

Lic. Luis German Quispe Hanco

JEFE DE DIVISION-TELECOMUNICACIONES

En mi calidad de jefe de División y encargado del Cuarto de Telecomunicaciones de la Clínica Santísima Trinidad de Tarija, manifiesto nuestra plena conformidad con la ejecución del proyecto ***"Rediseño y optimización de la infraestructura de red de la Clínica Santísima Trinidad"***.

La propuesta desarrollada ha respondido de manera satisfactoria a los requerimientos planteados, cumpliendo con los términos establecidos y dentro del plazo acordado.

Destacamos el compromiso, la responsabilidad y la adecuada aplicación de nuevas tecnologías que han permitido alcanzar los objetivos propuestos con eficiencia y calidad.

Entre los principales logros obtenidos, se destaca:

- ***La optimización de la red*** mediante segmentación por VLAN y acceso inalámbrico, lo que mejora el orden y el rendimiento de las comunicaciones internas.
- ***La implementación de comunicaciones unificadas con Asterisk***, permitiendo la gestión centralizada y eficiente de la telefonía IP en toda la clínica.
- ***El fortalecimiento de la seguridad de la red*** mediante la integración del sistema Fortinet, asegurando un mayor control y protección frente a amenazas externas.

Agradecemos el esfuerzo y la dedicación del responsable del proyecto, reiterando nuestra disposición para cualquier consulta adicional o futura colaboración.

Sin otro particular, me despido cordialmente.

Atentamente,

Luis German Quispe Hanco
Jefe de División – Encargado del Cuarto de Telecomunicaciones
Clínica Santísima Trinidad – Tarija

Figura 286. Carta de conformidad de informe técnico sobre los servicios prestados

Lista de asistencia a la capacitación

Capacitación al encargado del cuarto de telecomunicaciones sobre los servicios de red.

Lista de asistencia a la capacitación.

Lección 1: Configuración de router

N°	NOMBRE	FECHA	FIRMA
1	LUIS GERMAN QUISPE HANCO	03-11-25	

Lección 2: Configuración del servidor DHCP

N°	NOMBRE	FECHA	FIRMA
1	LUIS GERMAN QUISPE HANCO	03-11-25	

Lección 3: Configuración de las VLANs

N°	NOMBRE	FECHA	FIRMA
1	LUIS GERMAN QUISPE HANCO	03-11-25	

Lección 4: Configuración de los Access Point

N°	NOMBRE	FECHA	FIRMA
1	LUIS GERMAN QUISPE HANCO	03-11-25	

Lección 5: Configuración de los diferentes servicios del Firewall Fortinet

N°	NOMBRE	FECHA	FIRMA
1	LUIS GERMAN QUISPE HANCO	03-11-25	

Lección 6: Configuración de los equipos de computación para poder compartir archivos entre áreas

N°	NOMBRE	FECHA	FIRMA
1	LUIS GERMAN QUISPE HANCO	03-11-25	

Lección 7: Instalación de programas para los equipos

N°	NOMBRE	FECHA	FIRMA
1	LUIS GERMAN QUISPE HANCO	03-11-25	

Lección 8: Configuración del servidor de telefonía IP

N°	NOMBRE	FECHA	FIRMA
1	LUIS GERMAN QUISPE HANCO	03-11-25	

Lección 9: Administración del cuarto de telecomunicaciones

N°	NOMBRE	FECHA	FIRMA
1	LUIS GERARDO LUQUE HANCO	03-11-25	

Lección 10: Monitoreo de control al rack del cuarto de telecomunicaciones

N°	NOMBRE	FECHA	FIRMA
1	LUIS GERARDO LUQUE HANCO	03-11-25	

Figura 287. Lista de asistentes de la capacitación.

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

IV.1.-Conclusiones

El proyecto de “Rediseño y optimización de la infraestructura de red de la Clínica Santísima Trinidad” permitió identificar y solucionar varios problemas que afectaban el funcionamiento diario de la institución. Al inicio se detectó que la red estaba desordenada, sin segmentación, con equipos antiguos, cableado poco organizado y sin medidas adecuadas de seguridad, lo que provocaba lentitud, fallas frecuentes y riesgos en la información clínica y administrativa.

Con el diseño elaborado mediante la metodología Top-Down fue posible crear una red más ordenada, escalable y fácil de administrar. La reorganización del cableado siguiendo normas TIA/EIA mejoró la estructura física y permitirá un mantenimiento más simple en el futuro. La implementación de VLANs fue uno de los cambios más importantes, ya que permitió separar la red por áreas, evitar congestiones y mejorar la seguridad interna. Además, la instalación de un firewall Fortinet fortaleció la protección contra accesos no autorizados y amenazas externas.

La incorporación de un servidor central y del sistema de telefonía IP mejoró la comunicación interna y la disponibilidad de servicios esenciales. Las pruebas realizadas demostraron que la red es estable, segura y funciona correctamente en todos sus componentes, incluyendo WiFi, direccionamiento IP y segmentación. Finalmente, la capacitación brindada al personal aseguró que quienes administren la red puedan manejarla adecuadamente y mantener su buen funcionamiento.

Finalmente, el proyecto logró cumplir satisfactoriamente los objetivos planteados: mejorar el rendimiento, la seguridad, la organización y la disponibilidad de la red institucional. La infraestructura optimizada constituye un soporte tecnológico confiable para el funcionamiento de la clínica, incrementa la eficiencia de los procesos y establece bases sólidas para futuras ampliaciones tecnológicas.

IV.2.- Recomendaciones

A partir de la implementación del proyecto y los resultados alcanzados, es posible formular una serie de recomendaciones orientadas a garantizar la sostenibilidad, seguridad y crecimiento de la infraestructura de red de la Clínica Santísima Trinidad.

En primer lugar, se recomienda fortalecer la infraestructura física del cuarto de telecomunicaciones. Actualmente, este espacio no cumple plenamente con las condiciones técnicas necesarias para garantizar la integridad de los equipos instalados. Se sugiere implementar medidas que aseguren ventilación adecuada, control de temperatura, protección contra polvo y acceso restringido, a fin de brindar un entorno óptimo para el funcionamiento y duración de los dispositivos de red.

Asimismo, es fundamental establecer un programa de mantenimiento preventivo con intervalos regulares. Este programa debe incluir limpieza del equipamiento, revisión de conexiones, actualización de firmware, monitoreo de logs, pruebas periódicas de conectividad y verificación de la funcionalidad del firewall y los sistemas de telefonía IP. El mantenimiento preventivo no solo prolonga la vida útil del equipamiento, sino que disminuye el riesgo de interrupciones inesperadas en los servicios clínicos.

Una recomendación prioritaria es la elaboración de un plan formal de contingencia ante fallos de red, caídas del servidor o interrupciones del suministro eléctrico. Dicho plan debe contemplar redundancia en enlaces críticos, respaldos constantes de la configuración, disponibilidad de equipos de reemplazo y procedimientos de recuperación rápida. Para una institución clínica, la continuidad operativa es esencial, por lo que contar con estrategias de resiliencia es indispensable.

También se sugiere implementar un sistema de monitoreo permanente de la red, que permita identificar congestión, consumo de ancho de banda, intentos de acceso no autorizado, variaciones en la cobertura inalámbrica y estados del firewall. Las herramientas de monitoreo facilitan la toma de decisiones basada en datos y permiten detectar fallos antes de que afecten la prestación de servicios.

Respecto al componente humano, es importante continuar con procesos periódicos de capacitación y actualización para el personal de informática y para los responsables de la operación de la red. Las tecnologías evolucionan constantemente, por lo que la actualización continua garantizará el uso responsable, seguro y eficiente de la infraestructura tecnológica.

Finalmente, se recomienda planificar un proceso gradual de renovación de equipos informáticos y de red que, por su tiempo de uso o capacidades limitadas, puedan convertirse en puntos vulnerables o en cuellos de botella. La infraestructura instalada es escalable, por lo que futuras ampliaciones pueden integrarse sin necesidad de reemplazar lo ya implementado, siempre que se mantenga una política de renovación tecnológica.