CAPITULO 1

INTRODUCCIÓN

1. INTRODUCCIÓN

1.1. Introducción

En la era actual, donde la tecnología avanza a pasos agigantados, la infraestructura de red se ha convertido en un pilar fundamental para el funcionamiento eficiente de cualquier organización. Este hecho es especialmente relevante en el contexto de los hospitales, que no solo deben manejar una gran cantidad de datos médicos y administrativos, sino que también deben garantizar la disponibilidad y seguridad de estos datos para ofrecer una atención de calidad a sus pacientes.

El Hospital Regional San Juan de Dios de Tarija, reconocido como un hospital de tercer nivel y un centro de referencia médica en la región, enfrenta desafíos significativos en la gestión y modernización de su infraestructura de red. A medida que las demandas de comunicación, seguridad y gestión de datos continúan creciendo, la necesidad de una red robusta, confiable y segura se vuelve cada vez más crítica.

Este proyecto se enmarca en una visión integral para transformar la infraestructura tecnológica del hospital, con el fin de mejorar la calidad de atención médica y la eficiencia operativa. El objetivo principal de este proyecto es llevar a cabo un rediseño integral de toda la red del Hospital Regional San Juan de Dios de Tarija, con un enfoque en la implementación de subredes VLAN, la integración de un servidor de telefonía IP para la gestión eficiente de comunicaciones y la implementación de redes Wi-Fi. Este rediseño tiene como propósito mejorar la conectividad, seguridad y eficiencia operativa de la red, proporcionando así un entorno tecnológico robusto y confiable para respaldar las operaciones médicas y administrativas del hospital.

Las subredes VLAN permitirán segmentar el tráfico de la red de manera más eficiente, optimizando el rendimiento y la seguridad al reducir la congestión y mejorar la gestión de los recursos. La integración de un servidor de telefonía IP facilitará la comunicación interna, permitiendo una gestión más flexible y escalable de las llamadas. La implementación de redes Wi-Fi de alto rendimiento asegurará que tanto el personal médico como administrativo puedan acceder a los sistemas y aplicaciones desde cualquier punto del hospital, mejorando así la movilidad y la colaboración. Además, se garantizará que la información sensible del paciente y los datos administrativos estén debidamente protegidos.

Al concluir este proyecto, se espera lograr una infraestructura de red moderna, escalable y segura que permita al Hospital Regional San Juan de Dios de Tarija cumplir con sus objetivos de proporcionar atención médica de calidad, eficiente y accesible a la población.

Además, el proyecto contribuirá a mejorar la experiencia del paciente al reducir los tiempos de espera y facilitar una atención más coordinada. En última instancia, la modernización de la infraestructura de red será un paso fundamental hacia la creación de un entorno más seguro, eficiente y tecnológicamente avanzado que respalde el compromiso del hospital con la excelencia en el cuidado de la salud.

1.2. Planteamiento del problema

El Hospital Regional San Juan de Dios de Tarija enfrenta una serie de desafíos relacionados con su infraestructura de red actual. Esta infraestructura, que no ha experimentado una actualización significativa en varios años, carece de las características necesarias para satisfacer las demandas de un entorno de atención médica moderna y eficiente.

1.3. Justificación

1.3.1. Tecnológico

La implementación de VLAN permite una segmentación efectiva de la red, mejorando la seguridad y el rendimiento al facilitar la gestión del tráfico de datos. La incorporación de Asterisk como solución de comunicaciones unificadas proporciona una plataforma versátil y escalable para gestionar llamadas internas de manera eficiente.

1.3.2. Económico

La optimización del rendimiento de la red y la mejora en las comunicaciones internas conducirán a una mayor eficiencia operativa, reduciendo los costos asociados con tiempos de inactividad y errores de comunicación.

1.3.3. Social

La provisión de Wi-Fi para pacientes no solo mejora su comodidad durante su estancia en el hospital, sino que también facilita la comunicación con familiares y amigos, brindando un apoyo emocional crucial durante momentos difíciles.

1.3.4. Desarrollo Sostenible

La implementación de una solución de comunicaciones unificadas minimiza la necesidad de hardware y recursos físicos adicionales para la gestión de llamadas.

1.3.5. Medioambiental

La implementación de tecnologías más eficientes y la optimización de la infraestructura de red ayudarán a reducir la huella de carbono del hospital, contribuyendo así a la conservación del medio ambiente y a la sostenibilidad a largo plazo.

1.4. Objetivos

1.4.1. Objetivo General

Optimizar el rendimiento y la eficiencia del tráfico de datos de la red del Hospital mediante la implementación de tecnologías de red avanzadas, incluyendo la segmentación de la red con VLAN y la integración de un servidor de telefonía IP.

1.4.2. Objetivos Específicos

• Rediseñar la red del Hospital Regional San Juan de Dios de Tarija mediante una segmentación de red utilizando la tecnología VLAN y desplegar una red Wi-Fi para proporcionar conectividad inalámbrica.
• Configurar un servidor de comunicaciones unificadas basado en Asterisk para mejorar la eficiencia y centralización de las comunicaciones en la red del hospital.

1.5. Metodología

En este proyecto, se empleará la metodología del Diseño Top-Down para abordar el rediseño de la infraestructura de red del Hospital San Juan de Dios de Tarija. 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.
Las restricciones del proyecto no nos permiten llegar a la etapa de implementación, por lo cual llegamos hasta la fase 4.

Fase 1 Análisis de Requisitos: Se identificaron las necesidades específicas del hospital, incluyendo servicios como redes seguras, telefonía IP, Wi-Fi de alta calidad y segmentación mediante VLAN, garantizando el soporte adecuado para las operaciones críticas.

Fase 2 Diseño Lógico: Se definió la topología de red jerárquica como base de la infraestructura, junto con la estructura de VLAN para optimizar el tráfico de datos y garantizar el rendimiento. Además, se diseñaron los servicios que serán soportados por la red, priorizando eficiencia y escalabilidad.

Fase 3 Diseño Físico: Se especificaron los equipos y materiales necesarios, tales como routers, switches, puntos de acceso y cableado estructurado según el estándar TIA/EIA-568-B, además de sus ubicaciones estratégicas en las instalaciones del hospital.

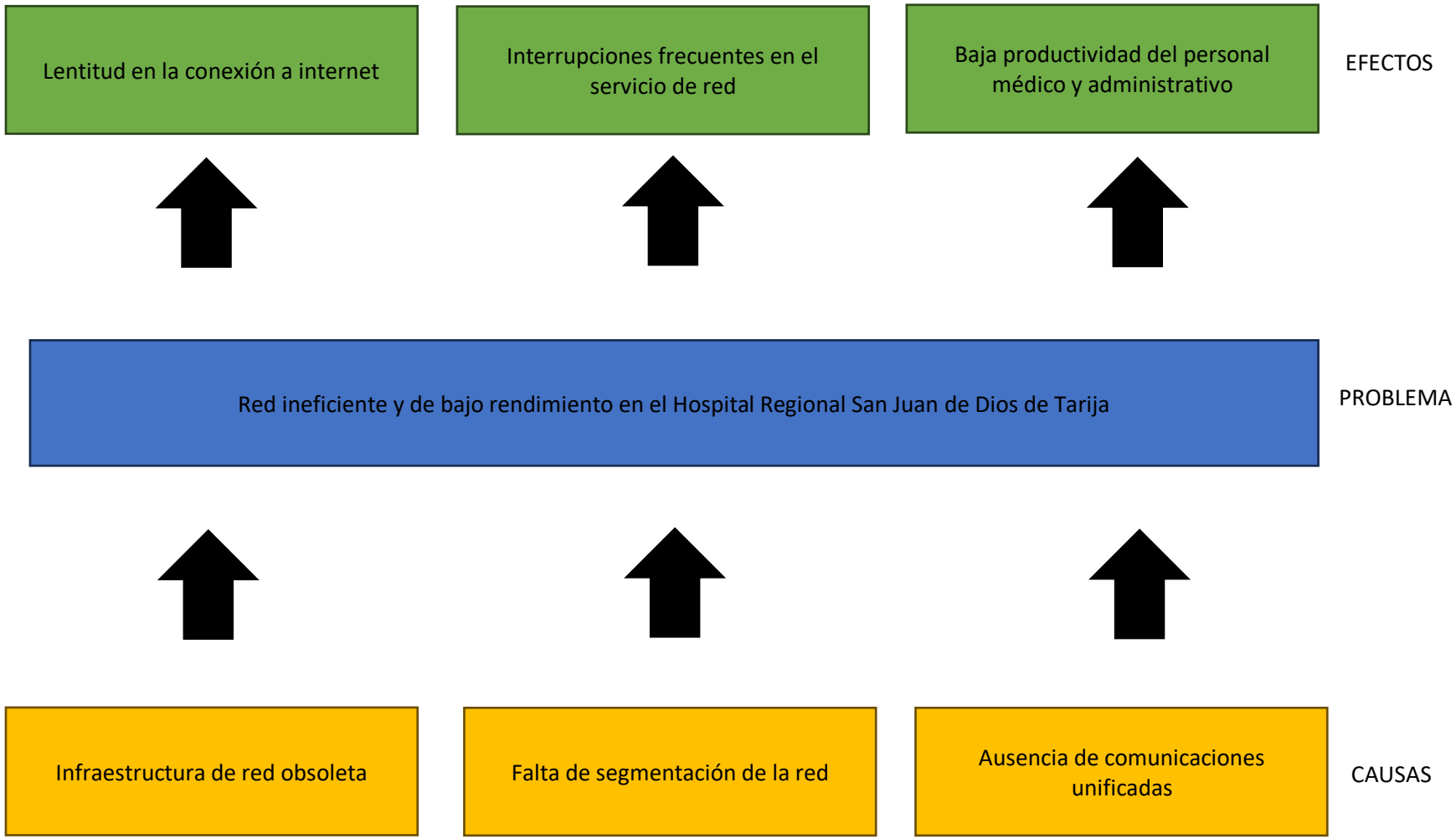
Fase 4 Planificación de la Implementación: Se elaboró un plan detallado que incluye cronogramas, asignación de recursos, medidas de mitigación de riesgos y pruebas previstas para validar cada etapa del proyecto antes de su ejecución.

1.6. Sistema de Marco Lógico

1.6.1. Árbol de Problemas

Figura 1

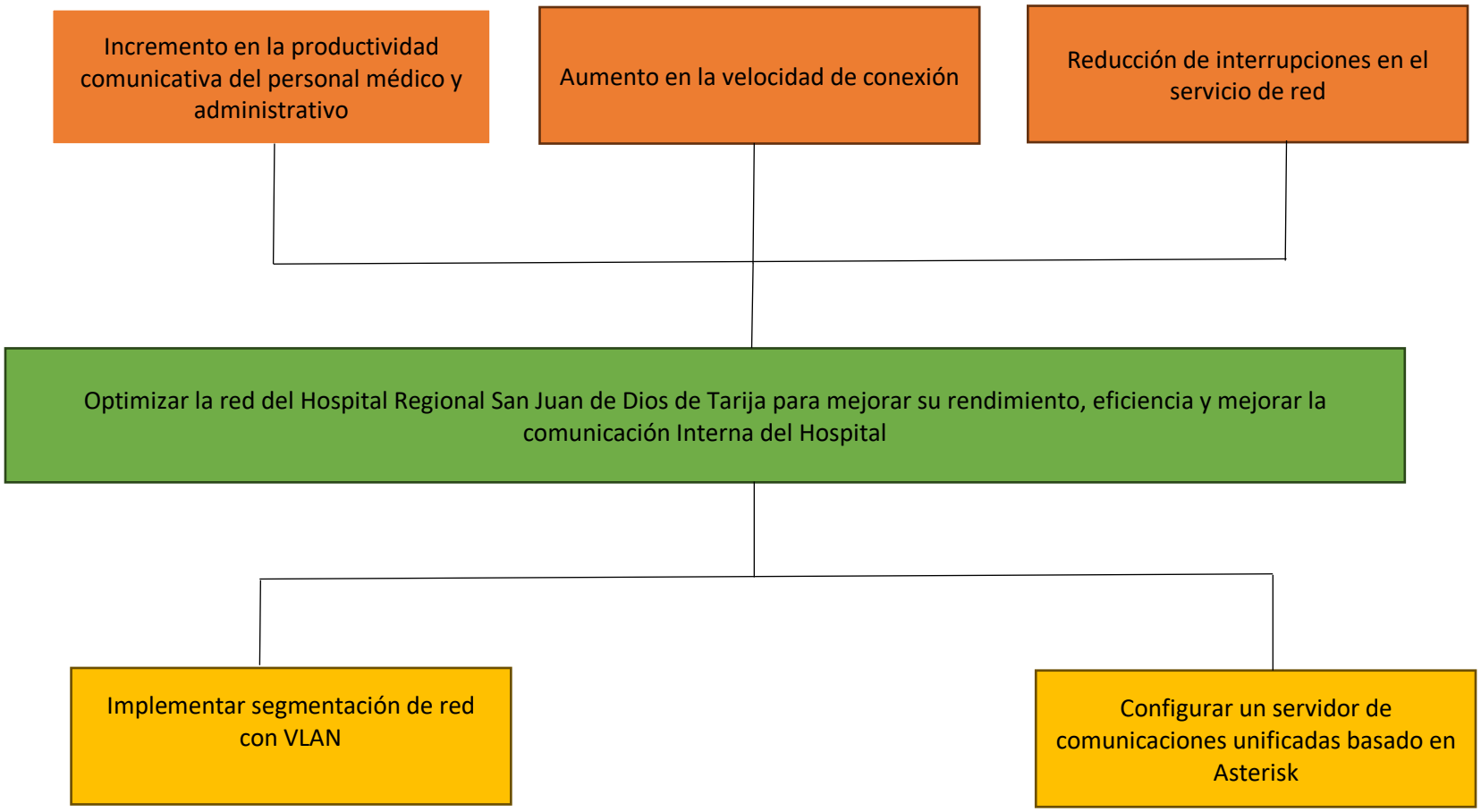
Árbol de Problemas



1.6.2. Árbol de Objetivos

Figura 2

Árbol de Objetivos



1.6.3. Matriz de Marco Lógico

Tabla 1

Matriz de Marco Lógico

Resumen Narrativo del Proyecto	Indicadores	Medios de Verificación	Supuestos
Fin Mejora de la red del hospital mediante las tecnologías de red avanzadas	Red del Hospital optimizada y servidor de telefonía IP implementado y funcional tras 8 meses de ejecución.	Diagramas de red actualizados, Informe de Monitoreo de Tráfico de Datos	Apoyo del personal de sistemas del hospital en el rediseño de la mejora de la red y la comunicación interna
Propósito Optimizar el rendimiento y la eficiencia del tráfico de datos de la red del Hospital mediante la implementación de tecnologías de red avanzados, incluyendo la segmentación de la red con VLAN y la integración de un servidor de telefonía IP.	Expectativa de mejora en tiempos de respuesta en un 50%; Y mejoramiento de la comunicación interna del hospital en un 80%	Registro de Incidencias de la Red en el Hospital	Apoyo institucional y financiero del hospital para una futura implementación del proyecto.
Componentes • Rediseñar la red del Hospital Regional San Juan De Dios de	Equipos de red actualizados al 60% y con capacidad para soportar redes VLAN.	Inventario actualizado de equipos, Resultados de testeo de red	Disponibilidad de fondos del hospital para la adquisición de nuevos dispositivos de red.

Tarija mediante una segmentación de red utilizando la tecnología VLAN y desplegar una red WIFI para proporcionar conectividad inalámbrica.	Redes segmentadas en un 90%, reducción de tráfico innecesario en al menos un 40%.		
• Configurar un servidor de comunicaciones unificadas basado en Asterisk para mejorar la eficiencia y centralización de las comunicaciones en la red del hospital.	Servidor de comunicaciones implementado y funcionando al 80%.	Registro de llamadas y comunicaciones del servidor de Telefonía IP	Adaptación del personal administrativo y médico del hospital al nuevo sistema de comunicación.
Actividades 1 **Actividades para el Rediseño de Red mediante VLAN y el Despliegue de Red Wi-Fi:** 1.1 Realizar un análisis de la infraestructura de red existente 1.2 Definir los requisitos de segmentación de red basados	Resumen de Presupuesto Total, del rediseño 188962,82 Bs Total, del servidor 1461,6 Bs Total, Proyecto 190.424,42Bs	Tabla de Costos actuales para el rediseño Reporte de uso del servidor de telefonía IP	Apoyo del personal del hospital con planos y datos de componentes actuales

en las necesidades del hospital. 1.3 Diseñar un esquema de segmentación de red utilizando VLAN. 1.4 Configurar VLAN en los dispositivos de red, como switches y routers. 1.5 Realizar un estudio de cobertura y capacidad para determinar la ubicación de los puntos de acceso Wi-Fi. 1.6 Configurar la autenticación y el acceso a la red Wi-Fi para pacientes y administrativos. **2 Actividades para la Implementación de Sistema de Comunicaciones Unificadas Asterisk:** 2.1 Instalar y configurar el servidor Asterisk en el centro de datos del hospital.			

2.2 Configurar extensiones telefónicas para el personal médico y administrativo. 2.3 Implementar funcionalidades adicionales, como buzón de voz y menú de teléfonos. 2.4 Probar la funcionalidad y la calidad de las llamadas internas.			

CAPITULO 2

MARCO TEÓRICO

2. MARCO TEÓRICO

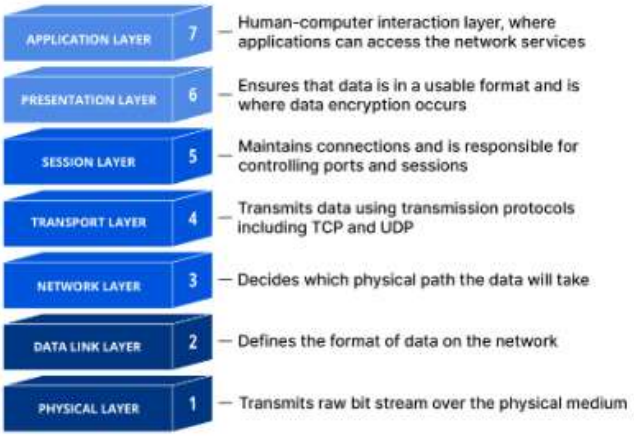
Modelo OSI

El modelo Open Systems Interconnection (OSI) 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.[1]

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.[1]

Figura 3

Modelo OSI



Cada capa del modelo OSI tiene una función específica y se comunica con las capas superiores e inferiores. Los ataques DDoS se dirigen a capas específicas de una conexión de red, los ataques a la capa de aplicación se dirigen a la capa 7, mientras que los ataques a la capa de protocolo se dirigen a las capas 3 y 4.[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

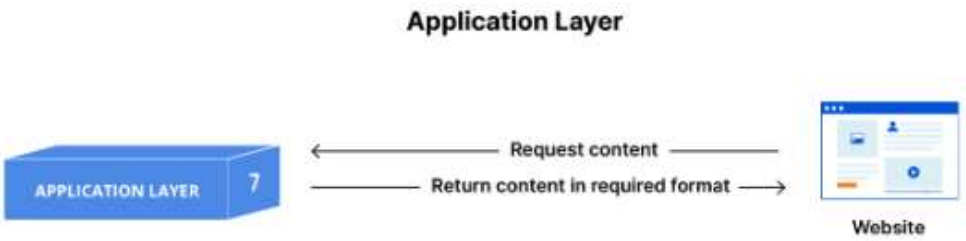
fuente. Si el problema puede reducirse a una capa específica del modelo, se puede evitar mucho trabajo innecesario.[1]

Las 7 capas del Modelo OSI

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

Figura 4

Capa de Aplicación

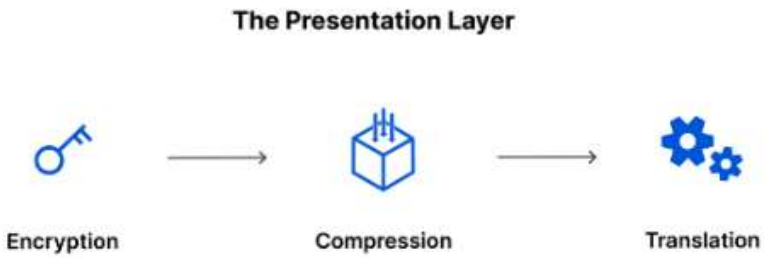


Esta es la única capa que interactúa directamente con los datos del usuario. Las aplicaciones de software, como navegadores web y clientes de correo electrónico, dependen de la capa de aplicación para iniciar comunicaciones. Sin embargo, debe quedar claro que las aplicaciones de software cliente no forman 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.[1]

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).[1]

Figura 5

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.[1]

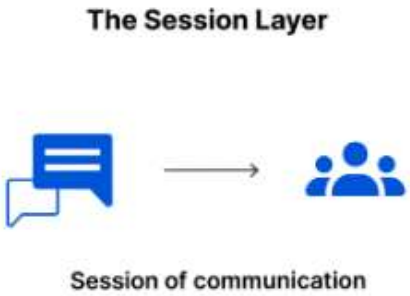
Dos dispositivos de comunicación que se conectan entre sí podrían estar usando distintos métodos de codificación, por lo que la capa 6 es la responsable de traducir los datos entrantes en una sintaxis que la capa de aplicación del dispositivo receptor pueda comprender.[1]

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.[1]

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.[1]

Figura 6

Capa de Sesión

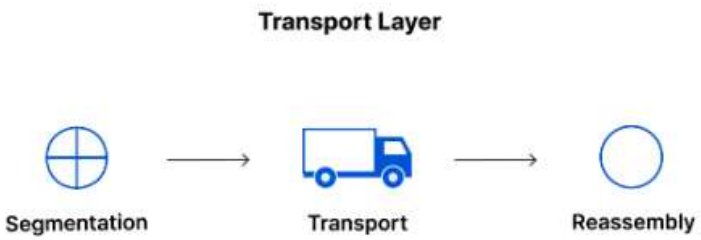


La capa de sesión es la responsable de la apertura y cierre de comunicaciones entre dos dispositivos. Ese tiempo que transcurre entre la apertura de la comunicación y el cierre de esta se conoce como sesión. La capa de sesión garantiza que la sesión permanezca abierta el tiempo suficiente como para transferir todos los datos que se están intercambiando; tras esto, cerrará sin demora la sesión para evitar desperdicio de recursos.[1]

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.[1]

Figura 7

Capa de Transporte



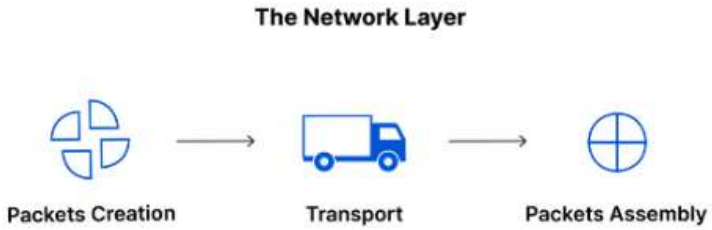
La capa 4 es la responsable de las comunicaciones de extremo a extremo entre dos dispositivos. Esto implica, antes de proceder a ejecutar el envío a la capa 3, tomar datos de la capa de sesión y fragmentarlos seguidamente en trozos más pequeños llamados segmentos. La capa de transporte del dispositivo receptor es la responsable luego de rearmar tales segmentos y construir con ellos datos que la capa de sesión pueda consumir.[1]

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.[1]

Los protocolos de la capa de transporte incluyen el Protocolo de control de transmisión (TCP) y el User Datagram Protocol (UDP).[1]

Figura 8

Capa de Red

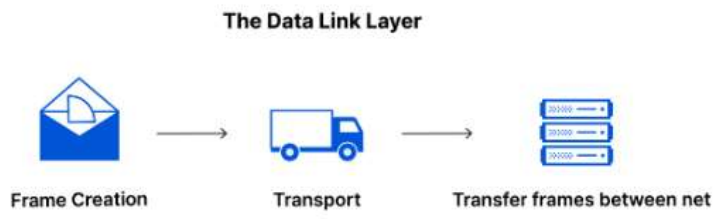


La capa de red es responsable de facilitar la transferencia de datos entre dos redes diferentes. Si los dispositivos que se comunican se encuentran en la misma red, entonces la capa de red no es necesaria. Esta capa divide los segmentos de la capa de transporte en unidades más pequeñas, llamadas paquetes, 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.[1]

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.[1]

Figura 9

Capa de Enlace de Datos

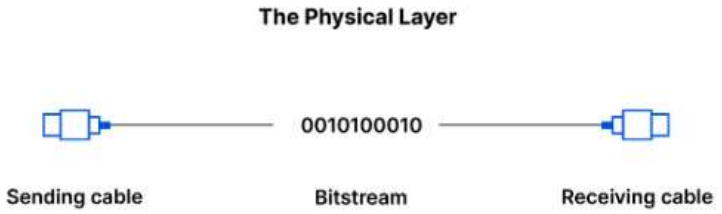


La capa de enlace de datos es muy similar a la capa de red, excepto que la capa de enlace de datos facilita la transferencia de datos entre dos dispositivos dentro la misma red. La capa de enlace de datos toma los

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).[1]

Figura 10

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.[1]

Cómo transitan los datos a través del modelo OSI

Para que la información 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.[1]

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.[1]

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.[1]

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.[1]

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.[1]

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”.[2]

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.[2]

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.[2]

El proceso de planificación de todo el proyecto se lleva a cabo a nivel de 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).[2]

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.[2]

Cable 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.[3]

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.[3]

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.[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.[4]

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. ¿Cuál es la diferencia entre estos dos, entonces? [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.[4]

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.[4]

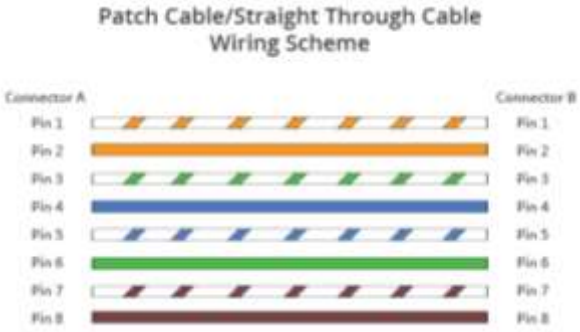
Algunas aplicaciones de red requieren un cable cruzado Ethernet, con un conector T-568A en un extremo y uno T-568B en el otro. Este tipo de cable se usa generalmente para conexiones directas de ordenador a ordenador. En la siguiente sección hablaremos más detalladamente sobre las características del cable directo y el cable cruzado.[4]

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.[4]

Figura 11

Cable de Red Directo



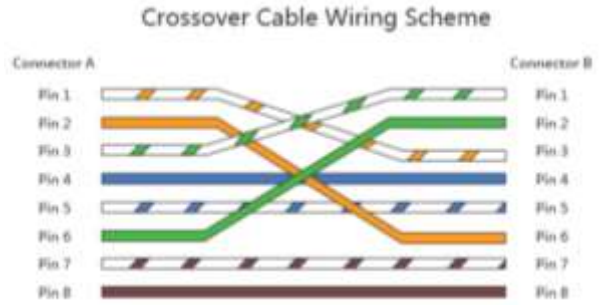
El cable cruzado

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.[4]

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).[4]

Figura 12

Cable de Red Cruzado



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.[5]

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.[5]

Figura 13

Categorías de Cables de Red

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

Cable de red para empresas

Un usuario algo más avanzado, con todo equipamiento Multigigabit e incluso equipos 10G, nuestra recomendación es usar como mínimo cables Cat6, además, sería aconsejable comprar cableado Cat 7 que tiene un precio muy bueno si tenemos en cuenta la calidad-precio, este tipo de cableado Cat7 no solamente te proporcionará una gran velocidad, sino que es de tipo S/FTP, por tanto, tenemos la máxima protección posible. Este tipo de cables de red son nuestros favoritos cuando necesitamos comprar un latiguillo de poca longitud para conectar un router 10G o switch 10G a un servidor o PC con este tipo de conectividad, son bastante baratos para lo bien que funcionan y la calidad que tienen.[5]

Computadora personal (PC)

Una computadora personal, computador personal u ordenador, conocida como PC (siglas en inglés de Personal Computer), es un tipo de microcomputadora diseñada en principio para ser utilizada por una sola persona. Habitualmente, la sigla PC se refiere a las computadoras IBM PC compatibles. Una computadora personal es generalmente de tamaño medio y es usada por un solo usuario (aunque hay sistemas operativos que permiten varios usuarios simultáneamente, lo que es conocido como multiusuario). Suele denominarse ordenador de sobremesa, debido a su posición estática e imposibilidad de transporte a diferencia de un ordenador portátil.[6]

Una computadora personal suele estar equipada para cumplir tareas comunes de la informática moderna, es decir, permite navegar por Internet, estudiar, escribir textos y realizar otros trabajos de oficina o

educativos, como editar textos y bases de datos, además de actividades de ocio, como escuchar música, ver videos, jugar, etc.[6]

En cuanto a su movilidad podemos distinguir entre computadora de escritorio y computadora portátil.[6]

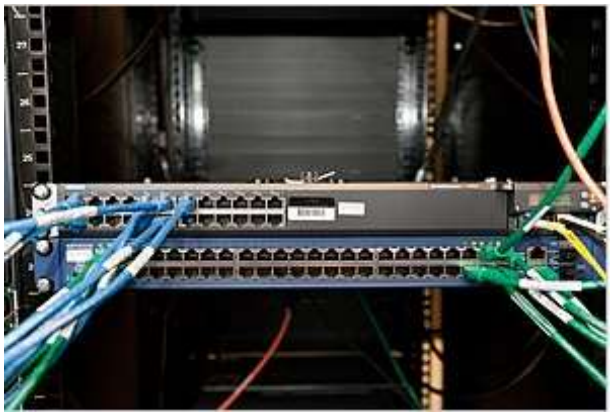
Conmutador (switch)

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.[7]

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).[7]

Figura 14

Switch



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.[7]

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.[7]

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.).[7]

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.[7]

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.[7]

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.[7]

Patch panel

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.[8]

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).[8]

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.[8]

Figura 15

Patch Panel

Rack 9U montaje en pared

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.[9]

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.[9]

Figura 16

Rack

Placa de pared Cat6 de 4 puertos

Los cables y los cables no necesitan ser desordenados.[10]

Ahora puedes mantener tu hogar limpio y ordenado, sin cables corriendo, pero puedes disfrutar de conexiones de datos Cat6 en tu habitación u oficina a alta velocidad.[10]

Rápido y fácil de instalar.[10]

Sin la necesidad de demasiadas conexiones, todo lo que necesitas es un destornillador estándar y conecta el cable Ethernet en la parte delantera y trasera. A continuación, conecta el cable a tu enrutador o interruptor de Internet. El paquete contiene una placa de pared de una sola banda de tamaño estándar.[10]

Combina bien con el estilo de decoración.[10]

La placa de pared Keystone de una sola banda está hecha de plástico ABS flexible y duradero con una superficie moderna y lisa. Diseñado para blanco, combina bien con el color de decoración existente y el estilo de decoración, uso en casa o en la oficina no causará abrupto, será muy armonioso, mantiene un esquema de color consistente.[10]

Práctico puede ahorrar costos.[10]

Rj45 trapezoidal detrás de la placa de pared diseñada para encajar fácilmente en el clip de retención garantiza una conexión segura y no corrosiva, pero también para el conector en la placa de pared, se puede quitar para futuras actualizaciones, después del reemplazo simplemente reemplace la piedra angular, ahorros de costos.[10]

Figura 17

Placa de Pared

Access Point (puntos de acceso)

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. Conoce el significado de ap y todos sus detalles.[11]

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.[11]

Ventajas de un punto de acceso

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

Se basan en emisiones de ondas de radio, capaces de traspasar muros, por lo que son perfectos para conectar edificios cercanos dentro de la misma red, con antenas potentes es posible crear una red WLAN de hasta a un kilómetro de distancia.

Tienen un radio de acción de entre 30 metros a 100 metros.

Proporciona información del estado de red y descongestionan la red dividiendo las redes y enviando la información de manera paralela más rápidamente que de forma convencional.

Si dispone de conexiones PoE es posible con un único cable Ethernet RJ-45 dar acceso a internet sin la necesidad de conectarlo a un enchufe convencional.

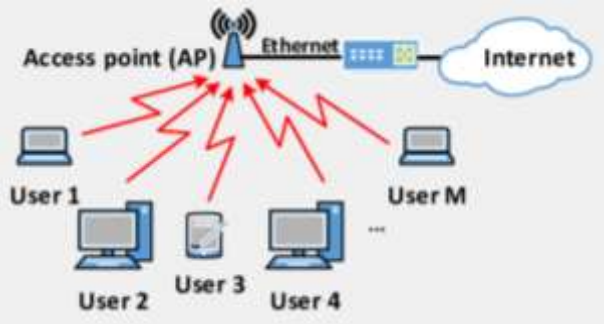
Permite más usuarios conectados, al mismo tiempo.[11]

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 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.[11]

Figura 18

Ubicación Punto de Acceso



Router

En primer lugar, un Router se utiliza para conectar varias redes. Por ejemplo, puede utilizar un Router para conectar sus Ordenadores en red a Internet, por lo tanto, compartir una conexión de Internet entre varios usuarios.[12]

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.[12]

Conectan 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.[12]

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.[12]

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.[12]

Figura 19
Router

Definición de dirección IP

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.[13]

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.[13]

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.[13]

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.[13]

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.[13]

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.[14]

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.[14]

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.[14]

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[14]

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.[14]

Figura 20

Mascara de Red

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	

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.[15]

Su propósito es traducir la información del protocolo utilizado en una red inicial, al protocolo usado en la red de destino.[15]

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.[15]

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.[15]

Un equipo que haga de puerta de enlace en una red debe tener necesariamente dos tarjetas de red (Network Interface Card, NIC).[15]

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.[15]

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.[15]

VLAN

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.[16]

Pero, ¿por qué son importantes las VLANs? 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.[16]

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.[17]

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.[17]

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.[18]

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.[18]

Wi-Fi

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.[19]

La mayoría de las redes inalámbricas se configuran mediante un router, 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.[19]

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.[19]

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.[19]

Las redes wifi funcionan como un mecanismo de comunicación bidireccional entre un dispositivo y el router. 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 router, 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).[19]

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.[19]

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.[20]

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.[20]

WEP

Dado que las redes inalámbricas transmiten datos a través de ondas de radio, los datos se pueden interceptar fácilmente, a menos que se implementen medidas de seguridad. La privacidad equivalente al cableado (WEP) fue el primer intento de protección inalámbrica, el cual fue introducido en 1997. El objetivo era agregar seguridad a las redes inalámbricas mediante el cifrado de datos.[20]

Si los datos inalámbricos fueran interceptados, los interceptores no podrían reconocerlos, ya que estaban encriptados. Sin embargo, los sistemas autorizados en la red podrían reconocer y descifrar los datos. Esto se debe a que los dispositivos en la red utilizan el mismo algoritmo de cifrado.[20]

WEP cifra el tráfico con una clave hexadecimal de 64 o 128 bits. Esta es una clave estática, lo que significa que todo el tráfico se cifra con una única clave, sin importar el dispositivo. Una clave WEP permite que las computadoras en una red intercambien mensajes codificados mientras ocultan a los intrusos el contenido de los mensajes.[20]

Esta clave es la que se utiliza para conectarse a una red con seguridad inalámbrica habilitada.[20]

WPA

Posteriormente, surgió WPA o acceso Wi-Fi protegido. Este protocolo fue el reemplazo de Wi-Fi Alliance para WEP, el cual fue integrado en el 2003. Compartía similitudes con WEP, pero ofrecía mejoras en la forma en que manejaba las claves de seguridad y cómo se autoriza a los usuarios.[20]

Mientras que WEP proporciona la misma clave a cada sistema autorizado, WPA usa el protocolo de integridad de clave temporal (TKIP, por sus siglas en inglés), el cual cambia dinámicamente la clave que usan los sistemas.[20]

Esto evita que los intrusos creen su propia clave de cifrado para que coincida con la utilizada por la red protegida. El estándar de cifrado TKIP fue reemplazado posteriormente por el estándar de cifrado avanzado (AES, por sus siglas en inglés).[20]

Además, WPA incluía comprobaciones de integridad de los mensajes para determinar si un atacante había capturado o alterado paquetes de datos. Las claves utilizadas por WPA eran de 256 bits, un aumento

significativo por sobre las claves de 64 y 128 bits utilizadas en el sistema WEP. Sin embargo, a pesar de estas mejoras, se empezaron a explotar elementos de WPA, lo cual llevó a crear WPA2.[20]

Es posible que a veces escuches el término “clave WPA” en relación con WPA. Una clave WPA es una contraseña que utilizas para conectarte a una red inalámbrica. Puedes obtener la contraseña WPA desde la persona que maneja la red.[20]

En algunos casos, es posible que haya una contraseña o frase de contraseña WPA predeterminada impresa en un enrutador inalámbrico. Si no puedes determinar la contraseña en tu enrutador, es posible que puedas restablecerla.[20]

WPA2

WPA2 se introdujo en el 2004 y era una versión mejorada de WPA. WPA2 se basa en el mecanismo de red de seguridad robusta (RSN, por sus siglas en inglés) y funciona en dos modos:
Modo personal o clave precompartida (WPA2-PSK): se basa en un código de acceso compartido y generalmente se usa en entornos domésticos.
Modo empresarial (WPA2-EAP): como sugiere el nombre, este modo es más adecuado para uso en empresas u organizaciones.[20]

Ambos modos utilizan CCMP, que significa Protocolo de código de autenticación de mensajes de encadenamiento de bloques de cifrado en modo contador. El protocolo CCMP se basa en el algoritmo estándar de cifrado avanzado (AES), el cual proporciona una verificación de la autenticidad e integridad de los mensajes.[20]

CCMP es más resistente y confiable que el protocolo de integridad de clave temporal (TKIP) original de WPA, lo cual dificulta que los atacantes detecten patrones.[20]

Sin embargo, WPA2 también tiene sus inconvenientes. Por ejemplo, es vulnerable a ataques de reinstalación de claves (KRACK, por sus siglas en inglés). Un ataque KRACK explota una debilidad en WPA2, lo que permite a los atacantes hacerse pasar por una red clonada y obligar a la víctima a conectarse a una red maliciosa.[20]

Esto permite al hacker descifrar una pequeña parte de los datos, la cual se puede agregar a otras para descifrar la clave de cifrado. Sin embargo, los dispositivos se pueden reparar y WPA2 todavía se considera más seguro que WEP o WPA.[20]

WPA3

WPA3 es la tercera iteración del protocolo de acceso Wi-Fi protegido. Wi-Fi Alliance introdujo WPA3 en el año 2018. WPA3 integró nuevas funciones para uso personal y empresarial, que incluyen lo siguiente: Cifrado de datos individualizado: al iniciar sesión en una red pública, WPA3 registra un nuevo dispositivo a través de un proceso distinto a una contraseña compartida. WPA3 utiliza un sistema de protocolo de aprovisionamiento de dispositivos Wi-Fi (DPP, por sus siglas en inglés) que permite a los usuarios usar etiquetas de comunicación de campo cercano (NFC, por sus siglas en inglés) o códigos QR para permitir dispositivos en la red. Además, la seguridad WPA3 utiliza el cifrado GCMP-256 en lugar del cifrado de 128 bits utilizado anteriormente.[20]

Protocolo de autenticación simultánea de iguales: se utiliza para crear un protocolo de enlace seguro, en el cual un dispositivo de red se conectará a un punto de acceso inalámbrico y ambos dispositivos se comunicarán para verificar la autenticación y la conexión. Incluso si la contraseña de un usuario es débil, WPA3 proporciona un protocolo de enlace más seguro mediante Wi-Fi DPP.[20]

Protección contra ataques de fuerza bruta más fuerte: WPA3 protege contra suposiciones aleatorias de contraseña fuera de línea permitiendo al usuario solo una oportunidad para adivinar, lo cual obliga al usuario a interactuar con el dispositivo Wi-Fi directamente; esto significa que tendría que estar físicamente presente cada vez que quiera adivinar la contraseña. WPA2 carece de cifrado integrado y privacidad en las redes públicas abiertas, lo cual hace que los ataques de fuerza bruta sean una amenaza significativa.[20]

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.[21]

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.[21]

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.[21]

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.[21]

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.[21]

Figura 21

Asterisk

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.[22]

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.[22]

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.[22]

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.[22]

Los servidores VoIP, explicados

Si estás buscando maneras de reducir costos en llamadas telefónicas, mejorar la interacción con clientes y colaboradores, y sacar el máximo partido a tu conexión de internet, entonces es momento de considerar los servidores VoIP.[23]

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.[23]

En este artículo, te brindaremos una visión completa sobre qué son los servidores VoIP, su funcionamiento, las ventajas que ofrecen, y cómo puedes implementarlos y asegurarlos en tu

organización. Además, te proporcionaremos ejemplos de algunos proveedores VoIP que presentan soluciones personalizadas para variados tipos de empresas.[23]

Servidor 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.[23]

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.[24]

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. [24]

La tecnología SIP aprovecha las ventajas de la VoIP para mejorar las comunicaciones por voz y vídeo mediante Internet.[24]

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. [24]

- 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. [24]

- 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. [24]

- 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.[24]

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: [24]

- 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. [24]

- 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.[24]

- Permite llamadas múltiples. Al no depender del cableado, soporta mayor volumen de llamadas sin perder calidad. [24]

- 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. [24]

- 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.[24]

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. [25]

Los interlocutores internos y externos utilizan los mismos números de extensión de diferentes formas. [25]

Supón que tienes a Alice y Bob trabajando en la misma oficina. La extensión de Alice es 103 y el número de Bob es 104. Si Alice quiere hablar con Bob, puede levantar su teléfono y marcar 104. No es necesario marcar el número completo de la empresa. [25]

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 Alice o 987-6543-104 para hablar con Bob.[25]

Topología de red

La topología de red se define como un mapa físico o lógico de una red para intercambiar datos. En otras palabras, es la forma en que está diseñada la red, sea en el plano físico o lógico. El concepto de red puede definirse como «conjunto de nodos interconectados». Lo que un nodo es concretamente depende del tipo de red en cuestión.

La topología lógica la determina únicamente la configuración de las conexiones entre nodos. La distancia entre los nodos y las interconexiones físicas que pertenecen a la topología física de la red. [30]

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. [30]

Red en Bus

En una red usando esta topología cada nodo se conecta a un cable central. A este se lo conoce como "bus". Toda la transmisión de datos entre nodos ocurre mediante este canal de comunicación y es recibida por todos los nodos simultáneamente. [30]

Red en estrella

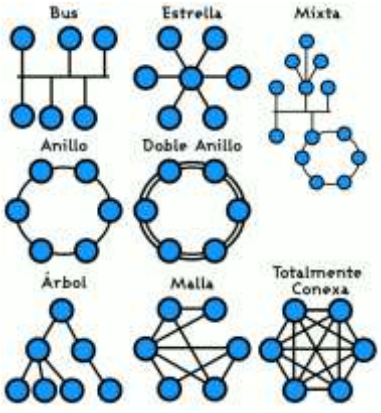
La topología en estrella reduce la posibilidad de fallo de red conectando todos los nodos a un nodo central. Cuando se aplica a una red basada en la topología estrella este concentrador central reenvía todas las transmisiones recibidas de cualquier nodo periférico a todos los nodos periféricos de la red, algunas veces incluso al nodo que lo envió. Todos los nodos periféricos se pueden comunicar con los demás transmitiendo o recibiendo del nodo central solamente. Un fallo en la línea de conexión de cualquier nodo con el nodo central provocaría el aislamiento de ese nodo respecto a los demás, pero el resto de sistemas permanecería intacto. El tipo de concentrador (hub) se utiliza en esta topología, aunque es muy obsoleto; se suele usar comúnmente un switch. [30]

Red en árbol

Una topología en árbol, también conocida como topología jerárquica, puede ser vista como una colección de redes en estrella ordenadas en una jerarquía. Este árbol tiene nodos periféricos individuales —por ejemplo, hojas— que requieren «transmitir a» y «recibir de» otro nodo solamente y no necesitan actuar como repetidores o regeneradores. Al contrario que en las redes en estrella, la función del nodo central se puede distribuir[30]

Figura 22

Topologías de red



María DB

MariaDB es un sistema de gestión de bases de datos relacionales (RDBMS) gratuito y de código abierto. Fue creado por los desarrolladores originales de MySQL por la preocupación de que MySQL pasara a ser comercializado después de que Oracle lo adquiriera en 2009.[36]

MariaDB está escrito en C y C++ y es compatible con varios lenguajes de programación, incluidos C, C#, Java, Python, PHP y Perl. MariaDB también es compatible con todos los principales sistemas operativos, incluidos Windows, Linux y macOS.[36]

Aunque es una base de datos relacional, MariaDB ofrece funciones similares a las de NoSQL en la versión 10. El motor Connect permite acceder fácilmente a datos no estructurados desde MariaDB, mientras que las columnas dinámicas permiten el almacenamiento de tipo NoSQL de diferentes tipos de objetos en la misma fila.[36]

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. [37]

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. [37]

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. [37]

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. [37]

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. [37]

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. [37]

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. [37]

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. [37]

IEEE 802.11

IEEE 802.11 es parte del conjunto IEEE 802 de estándares técnicos de redes de área local (LAN) y especifica el conjunto de protocolos de control de acceso al medio (MAC) y de capa física (PHY) para implementar la comunicación informática de redes de área local inalámbricas (WLAN). El estándar y las modificaciones proporcionan la base para los productos de redes inalámbricas que utilizan la marca Wi-Fi y son los estándares de redes informáticas inalámbricas más utilizados del mundo. IEEE 802.11 se utiliza en la mayoría de las redes domésticas y de oficina para permitir que las computadoras portátiles, impresoras,

teléfonos inteligentes y otros dispositivos se comuniquen entre sí y accedan a Internet sin conectar cables. IEEE 802.11 también es una base para las redes de comunicación basadas en vehículos con IEEE 802.11p.[26]

802.11ax

IEEE 802.11ax es el sucesor de 802.11ac, comercializado como Wi-Fi 6 (2,4 GHz y 5 GHz) y Wi-Fi 6E (6 GHz) por la Wi-Fi Alliance. También se conoce como Wi-Fi de alta eficiencia, por las mejoras generales de los clientes Wi-Fi 6 en entornos densos. Para un cliente individual, la mejora máxima en la tasa de datos (velocidad PHY) en comparación con el predecesor (802.11ac) es solo del 39% (a modo de comparación, esta mejora fue de casi el 500% para los predecesores). Sin embargo, incluso con esta cifra comparativamente menor del 39%, el objetivo era proporcionar 4 veces el rendimiento por área de 802.11ac (de ahí la alta eficiencia). La motivación detrás de este objetivo fue la implementación de WLAN en entornos densos como oficinas corporativas, centros comerciales y apartamentos residenciales densos. Esto se logra mediante una técnica llamada OFDMA, que es básicamente multiplexación en el dominio de frecuencia (a diferencia de la multiplexación espacial, como en 802.11ac). Esto es equivalente a la tecnología celular aplicada a Wi-Fi.[26]

IEEE 802.1Q

IEEE 802.1Q, a menudo denominado Dot1q, es el estándar de redes que admite redes de área local virtuales (VLAN) en una red Ethernet IEEE 802.3. El estándar define un sistema de etiquetado VLAN para tramas Ethernet y los procedimientos que lo acompañan que deben utilizar los puentes y conmutadores para gestionar dichas tramas. El estándar también contiene disposiciones para un esquema de priorización de calidad de servicio conocido comúnmente como IEEE 802.1p y define el Protocolo de registro de atributos genéricos.[27]

Las partes de la red que son compatibles con VLAN (es decir, que cumplen con IEEE 802.1Q) pueden incluir etiquetas VLAN. Cuando un marco ingresa a la parte de la red que es compatible con VLAN, se agrega una etiqueta para representar la membresía de VLAN. Cada marco debe poder distinguirse como perteneciente a exactamente una VLAN. Se supone que un marco en la parte de la red que es compatible con VLAN y que no contiene una etiqueta VLAN fluye en la VLAN nativa.[27]

El estándar fue desarrollado por IEEE 802.1, un grupo de trabajo del comité de estándares IEEE 802, y continúa siendo revisado activamente con modificaciones notables que incluyen IEEE 802.1ad, IEEE

802.1ak e IEEE 802.1s. La revisión 802.1Q-2014 incorporó el estándar IEEE 802.1D-2004.[27]

IEEE 802.3

IEEE 802.3 es un grupo de trabajo y una colección de estándares que definen el control de acceso al medio (MAC) de la capa física y la capa de enlace de datos de Ethernet por cable. Los estándares son producidos por el grupo de trabajo del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE). Se trata generalmente de una tecnología de red de área local (LAN) con algunas aplicaciones de red de área amplia (WAN). Las conexiones físicas se realizan entre nodos y/o dispositivos de infraestructura (concentradores, conmutadores, enrutadores) mediante varios tipos de cable de cobre o fibra.[28]

ANSI/TIA-568

ANSI/TIA-568 es un set de estándares desarrollado por la Telecommunications Industry Association referido al cableado comercial para productos y servicios de telecomunicaciones.[29]

El estándar ANSI/TIA-568 se publicó por primera vez en 1991, luego en 1995, en 2001 y en 2009 las revisiones A, B y C respectivamente. El estándar actual es la versión ANSI/TIA-568D.[29]

Lo más distintivo de esta norma, es la asignación de pines/pares para cable de par trenzado equilibrado de 100 Ω y 8 conductores. Dicha asignación se denomina T568A y T568B.[29]

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. [31]

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. Protocolo de control. Ambos utilizan UDP como protocolo de transporte real, que no ofrece ninguna garantía de que los paquetes se entregarán dentro de un intervalo determinado.[32]

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.[33]

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. [34]

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. [35]

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. [35]

CAPITULO 3

DESARROLLO DEL PROYECTO

3. DESARROLLO DEL PROYECTO

3.1. Análisis de requisitos

3.1.1. Metas del Negocio

Misión

El Hospital Regional San Juan de Dios Tarija como institución de Tercer Nivel con Referencia Departamental y Nacional, es el responsable de dar respuesta a las necesidades de salud de la población del departamento de Tarija, con calidad, equidad y solidaridad a través de procesos Técnico-Administrativos eficientes y eficaces, con participación de la Sociedad Civil Organizadas, y que brinda servicios asistenciales médico quirúrgicos especializados de mediana y alta complejidad a la población en general con eficiencia, eficacia, calidad, equidad, oportunidad, efectividad, calidez y sin ninguna discriminación social.

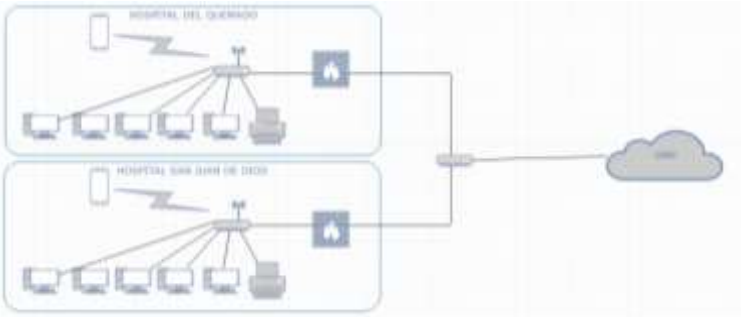
Visión

El Hospital Regional San Juan de Dios Tarija es un modelo de gestión moderna hospitalaria descentralizada en el manejo de recursos materiales, financieros y humanos, con personal suficientemente capacitado y trabajando en equipo, el hospital está integrado a la red de servicios y brinda atención en salud con calidad, calidez a la población del Departamento de Tarija.

3.1.2. Metas técnicas

Figura 23

Creación de una Red WAN para el Hospital del Quemado



3.1.3. Análisis de la red existente

Tabla 2

Dispositivos de la Empresa

Dispositivos	Cantidad	Modelo
Router	1	TP-Link ER605
Switch	10	Tp-link TL-SG1024
Racks de Pared	9	6RU
Rack de Piso	1	18U
Computadoras	165	Delux

Tabla 3

Dispositivos de la Empresa por Áreas

Nº	Nombre Equipo	Modelo	Ubicación	AREA
0	1 Router	Tp-link	Planta Baja	SISTEMAS
1	1 Switch	Tp-link	Planta Baja	EMERGENCIA
2	1 Switch	Tp-link	Planta Baja	CONSULTORIO_1
3	1 Switch	Tp-link	Planta Baja	SISTEMAS
4	1 Switch	Tp-link	Planta Baja	FICHAJE
5	1 Switch	Tp-link	Planta Baja	ADMINISTRATIVOS
6	1 Switch	Tp-link	Planta Baja	RECURSOS HUMANOS
7	1 Switch	Tp-link	Planta Baja	CONSULTORIO_2
8	1 Switch	Tp-link	1er Piso	1er Piso
9	1 Switch	Tp-link	2do Piso	2do Piso
10	1 Switch	Tp-link	3er Piso	3er Piso
11	165 PC	Delux	Toda la empresa	Toda la empresa

Tabla 4

Direccionamiento de las direcciones IP

Nº	Equipo	Dirección IP	Mascara de subred	Puerta de enlace
AREA EMERGENCIA				
0	PC0	192.168.10.9	255.255.255.0	192.168.10.1
1	PC1	192.168.10.10	255.255.255.0	192.168.10.1
2	PC2	192.168.10.11	255.255.255.0	192.168.10.1
3	PC3	192.168.10.12	255.255.255.0	192.168.10.1
4	PC4	192.168.10.13	255.255.255.0	192.168.10.1
5	PC5	192.168.10.14	255.255.255.0	192.168.10.1
6	PC6	192.168.10.15	255.255.255.0	192.168.10.1
7	PC7	192.168.10.16	255.255.255.0	192.168.10.1
8	PC8	192.168.10.17	255.255.255.0	192.168.10.1
9	PC9	192.168.10.18	255.255.255.0	192.168.10.1
10	PC10	192.168.10.19	255.255.255.0	192.168.10.1
11	PC11	192.168.10.20	255.255.255.0	192.168.10.1
12	PC12	192.168.10.21	255.255.255.0	192.168.10.1
13	PC13	192.168.10.22	255.255.255.0	192.168.10.1
14	PC14	192.168.10.23	255.255.255.0	192.168.10.1
15	PC15	192.168.10.24	255.255.255.0	192.168.10.1
16	PC16	192.168.10.25	255.255.255.0	192.168.10.1
17	PC17	192.168.10.26	255.255.255.0	192.168.10.1
18	PC18	192.168.10.27	255.255.255.0	192.168.10.1
19	PC19	192.168.10.28	255.255.255.0	192.168.10.1
20	PC20	192.168.10.29	255.255.255.0	192.168.10.1
AREA CONSULTORIO_1				
21	PC21	192.168.10.30	255.255.255.0	192.168.10.1
22	PC22	192.168.10.31	255.255.255.0	192.168.10.1
23	PC23	192.168.10.32	255.255.255.0	192.168.10.1

24	PC24	192.168.10.33	255.255.255.0	192.168.10.1
25	PC25	192.168.10.34	255.255.255.0	192.168.10.1
26	PC26	192.168.10.35	255.255.255.0	192.168.10.1
27	PC27	192.168.10.36	255.255.255.0	192.168.10.1
28	PC28	192.168.10.37	255.255.255.0	192.168.10.1
29	PC29	192.168.10.38	255.255.255.0	192.168.10.1
30	PC30	192.168.10.39	255.255.255.0	192.168.10.1
31	PC31	192.168.10.40	255.255.255.0	192.168.10.1
32	PC32	192.168.10.41	255.255.255.0	192.168.10.1
33	PC33	192.168.10.42	255.255.255.0	192.168.10.1
34	PC34	192.168.10.43	255.255.255.0	192.168.10.1
35	PC35	192.168.10.44	255.255.255.0	192.168.10.1
36	PC36	192.168.10.45	255.255.255.0	192.168.10.1
37	PC37	192.168.10.46	255.255.255.0	192.168.10.1
38	PC38	192.168.10.47	255.255.255.0	192.168.10.1
39	PC39	192.168.10.48	255.255.255.0	192.168.10.1
40	PC40	192.168.10.49	255.255.255.0	192.168.10.1
41	PC41	192.168.10.50	255.255.255.0	192.168.10.1
42	PC42	192.168.10.51	255.255.255.0	192.168.10.1
AREA SISTEMAS				
43	PC43	192.168.10.52	255.255.255.0	192.168.10.1
44	PC44	192.168.10.53	255.255.255.0	192.168.10.1
45	PC45	192.168.10.54	255.255.255.0	192.168.10.1
46	PC46	192.168.10.55	255.255.255.0	192.168.10.1
47	PC47	192.168.10.56	255.255.255.0	192.168.10.1
48	PC48	192.168.10.57	255.255.255.0	192.168.10.1
49	PC49	192.168.10.58	255.255.255.0	192.168.10.1
50	PC50	192.168.10.59	255.255.255.0	192.168.10.1
51	PC51	192.168.10.60	255.255.255.0	192.168.10.1
52	PC52	192.168.10.61	255.255.255.0	192.168.10.1
53	PC53	192.168.10.62	255.255.255.0	192.168.10.1

54	PC54	192.168.10.63	255.255.255.0	192.168.10.1
55	PC55	192.168.10.64	255.255.255.0	192.168.10.1
56	PC56	192.168.10.65	255.255.255.0	192.168.10.1
57	PC57	192.168.10.66	255.255.255.0	192.168.10.1
58	PC58	192.168.10.67	255.255.255.0	192.168.10.1
59	PC59	192.168.10.68	255.255.255.0	192.168.10.1
60	PC60	192.168.10.69	255.255.255.0	192.168.10.1
61	PC61	192.168.10.70	255.255.255.0	192.168.10.1
62	PC62	192.168.10.71	255.255.255.0	192.168.10.1
63	PC63	192.168.10.72	255.255.255.0	192.168.10.1
AREA FICHAJE				
64	PC64	192.168.10.73	255.255.255.0	192.168.10.1
65	PC65	192.168.10.74	255.255.255.0	192.168.10.1
66	PC66	192.168.10.75	255.255.255.0	192.168.10.1
67	PC67	192.168.10.76	255.255.255.0	192.168.10.1
68	PC68	192.168.10.77	255.255.255.0	192.168.10.1
69	PC69	192.168.10.78	255.255.255.0	192.168.10.1
70	PC70	192.168.10.79	255.255.255.0	192.168.10.1
71	PC71	192.168.10.80	255.255.255.0	192.168.10.1
72	PC72	192.168.10.81	255.255.255.0	192.168.10.1
73	PC73	192.168.10.82	255.255.255.0	192.168.10.1
74	PC74	192.168.10.83	255.255.255.0	192.168.10.1
75	PC75	192.168.10.84	255.255.255.0	192.168.10.1
76	PC76	192.168.10.85	255.255.255.0	192.168.10.1
77	PC77	192.168.10.86	255.255.255.0	192.168.10.1
78	PC78	192.168.10.87	255.255.255.0	192.168.10.1
79	PC79	192.168.10.88	255.255.255.0	192.168.10.1
80	PC80	192.168.10.89	255.255.255.0	192.168.10.1
81	PC81	192.168.10.90	255.255.255.0	192.168.10.1
82	PC82	192.168.10.91	255.255.255.0	192.168.10.1
83	PC83	192.168.10.92	255.255.255.0	192.168.10.1

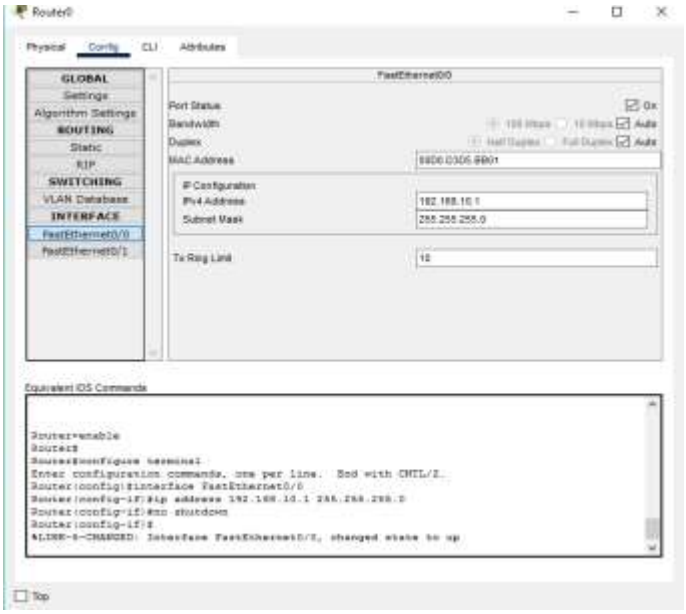
84	PC84	192.168.10.93	255.255.255.0	192.168.10.1
85	PC85	192.168.10.94	255.255.255.0	192.168.10.1
86	PC86	192.168.10.95	255.255.255.0	192.168.10.1
AREA ADMINISTRATIVOS				
87	PC87	192.168.10.96	255.255.255.0	192.168.10.1
88	PC88	192.168.10.97	255.255.255.0	192.168.10.1
89	PC89	192.168.10.98	255.255.255.0	192.168.10.1
90	PC90	192.168.10.99	255.255.255.0	192.168.10.1
91	PC91	192.168.10.100	255.255.255.0	192.168.10.1
92	PC92	192.168.10.101	255.255.255.0	192.168.10.1
93	PC93	192.168.10.102	255.255.255.0	192.168.10.1
94	PC94	192.168.10.103	255.255.255.0	192.168.10.1
95	PC95	192.168.10.104	255.255.255.0	192.168.10.1
96	PC96	192.168.10.105	255.255.255.0	192.168.10.1
97	PC97	192.168.10.106	255.255.255.0	192.168.10.1
98	PC98	192.168.10.107	255.255.255.0	192.168.10.1
99	PC99	192.168.10.108	255.255.255.0	192.168.10.1
100	PC100	192.168.10.109	255.255.255.0	192.168.10.1
101	PC101	192.168.10.110	255.255.255.0	192.168.10.1
102	PC102	192.168.10.111	255.255.255.0	192.168.10.1
103	PC103	192.168.10.112	255.255.255.0	192.168.10.1
104	PC104	192.168.10.113	255.255.255.0	192.168.10.1
105	PC105	192.168.10.114	255.255.255.0	192.168.10.1
106	PC106	192.168.10.115	255.255.255.0	192.168.10.1
107	PC107	192.168.10.116	255.255.255.0	192.168.10.1
108	PC108	192.168.10.117	255.255.255.0	192.168.10.1
AREA RECURSOS HUMANOS				
109	PC109	192.168.10.118	255.255.255.0	192.168.10.1
110	PC110	192.168.10.119	255.255.255.0	192.168.10.1
111	PC111	192.168.10.120	255.255.255.0	192.168.10.1
112	PC112	192.168.10.121	255.255.255.0	192.168.10.1

113	PC113	192.168.10.122	255.255.255.0	192.168.10.1
114	PC114	192.168.10.123	255.255.255.0	192.168.10.1
115	PC115	192.168.10.124	255.255.255.0	192.168.10.1
116	PC116	192.168.10.125	255.255.255.0	192.168.10.1
117	PC117	192.168.10.126	255.255.255.0	192.168.10.1
118	PC118	192.168.10.127	255.255.255.0	192.168.10.1
119	PC119	192.168.10.128	255.255.255.0	192.168.10.1
120	PC120	192.168.10.129	255.255.255.0	192.168.10.1
121	PC121	192.168.10.130	255.255.255.0	192.168.10.1
122	PC122	192.168.10.131	255.255.255.0	192.168.10.1
123	PC123	192.168.10.132	255.255.255.0	192.168.10.1
124	PC124	192.168.10.133	255.255.255.0	192.168.10.1
125	PC125	192.168.10.134	255.255.255.0	192.168.10.1
126	PC126	192.168.10.135	255.255.255.0	192.168.10.1
127	PC127	192.168.10.136	255.255.255.0	192.168.10.1
128	PC128	192.168.10.137	255.255.255.0	192.168.10.1
129	PC129	192.168.10.138	255.255.255.0	192.168.10.1
130	PC130	192.168.10.139	255.255.255.0	192.168.10.1
131	PC131	192.168.10.140	255.255.255.0	192.168.10.1
132	PC132	192.168.10.141	255.255.255.0	192.168.10.1
AREA CONSULTORIO_2				
133	PC133	192.168.10.142	255.255.255.0	192.168.10.1
134	PC134	192.168.10.143	255.255.255.0	192.168.10.1
135	PC135	192.168.10.144	255.255.255.0	192.168.10.1
136	PC136	192.168.10.145	255.255.255.0	192.168.10.1
137	PC137	192.168.10.146	255.255.255.0	192.168.10.1
138	PC138	192.168.10.147	255.255.255.0	192.168.10.1
1ER PISO				
139	PC139	192.168.10.148	255.255.255.0	192.168.10.1
140	PC140	192.168.10.149	255.255.255.0	192.168.10.1
141	PC141	192.168.10.150	255.255.255.0	192.168.10.1

142	PC142	192.168.10.151	255.255.255.0	192.168.10.1
143	PC143	192.168.10.152	255.255.255.0	192.168.10.1
144	PC144	192.168.10.153	255.255.255.0	192.168.10.1
145	PC145	192.168.10.154	255.255.255.0	192.168.10.1
146	PC146	192.168.10.155	255.255.255.0	192.168.10.1
147	PC147	192.168.10.156	255.255.255.0	192.168.10.1
148	PC148	192.168.10.157	255.255.255.0	192.168.10.1
149	PC149	192.168.10.158	255.255.255.0	192.168.10.1
150	PC150	192.168.10.159	255.255.255.0	192.168.10.1
151	PC151	192.168.10.160	255.255.255.0	192.168.10.1
2DO PISO				
152	PC152	192.168.10.161	255.255.255.0	192.168.10.1
153	PC153	192.168.10.162	255.255.255.0	192.168.10.1
154	PC154	192.168.10.163	255.255.255.0	192.168.10.1
155	PC155	192.168.10.164	255.255.255.0	192.168.10.1
156	PC156	192.168.10.165	255.255.255.0	192.168.10.1
157	PC157	192.168.10.166	255.255.255.0	192.168.10.1
158	PC158	192.168.10.167	255.255.255.0	192.168.10.1
3ER PISO				
159	PC159	192.168.10.168	255.255.255.0	192.168.10.1
160	PC160	192.168.10.169	255.255.255.0	192.168.10.1
161	PC161	192.168.10.170	255.255.255.0	192.168.10.1
162	PC162	192.168.10.171	255.255.255.0	192.168.10.1
163	PC163	192.168.10.172	255.255.255.0	192.168.10.1
164	PC164	192.168.10.173	255.255.255.0	192.168.10.1

Figura 24

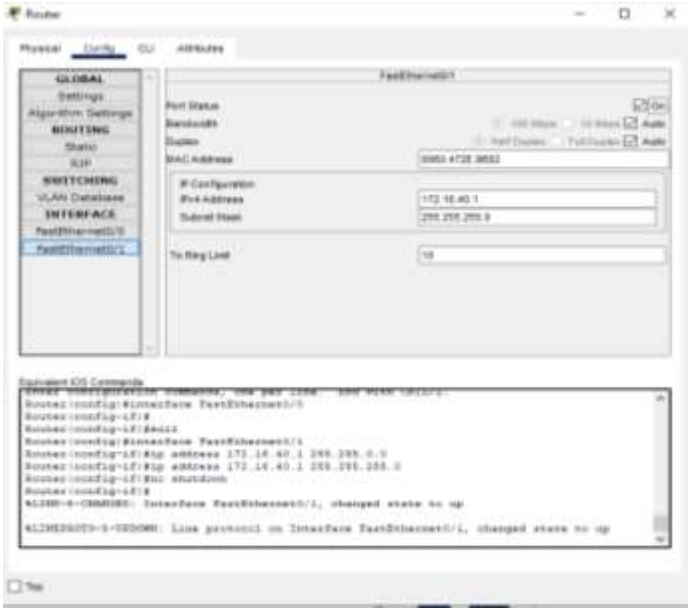
Simulación de la Configuración del Router



IP de puerta de enlace del hospital a salida de internet

Figura 25

Simulación de la Conexión con el Proveedor de Servicio



IP del proveedor de servicio Tigo para brindar internet al hospital

Figura 26

Simulación del Switch del Área de Emergencias

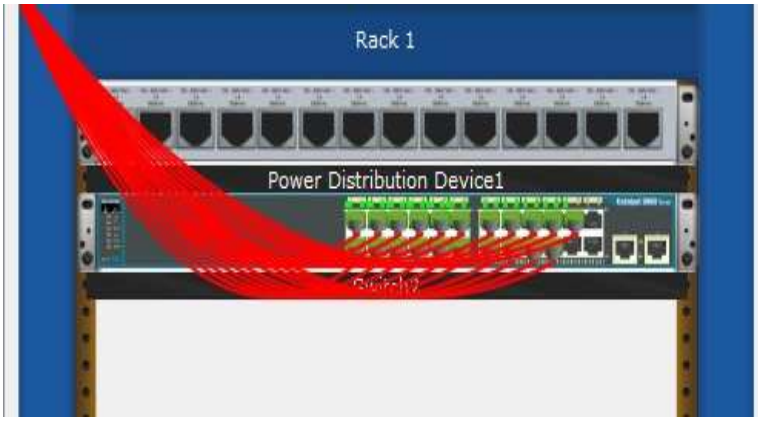


Figura 27

Simulación del Switch del Área de Consultorios_1

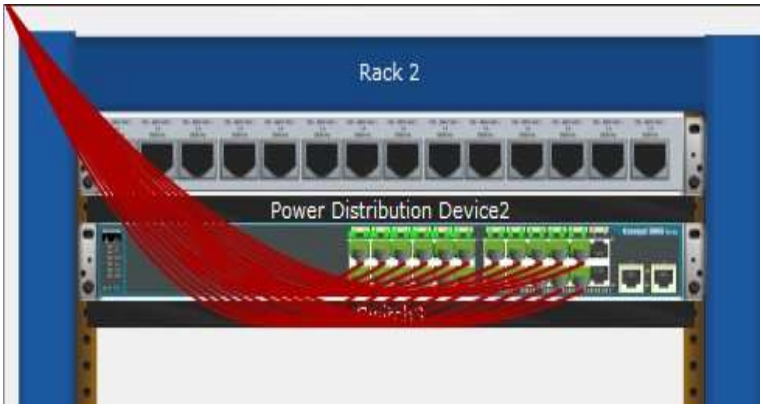


Figura 28

Simulación del Switch del Área de Consultorios_2

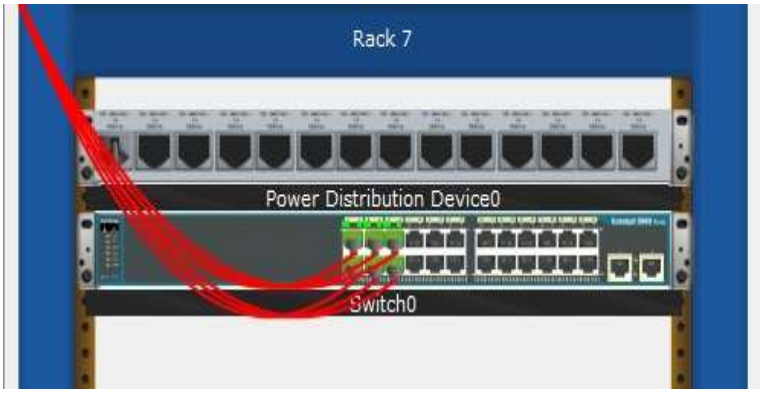


Figura 29

Simulación del Switch del Área de Sistemas

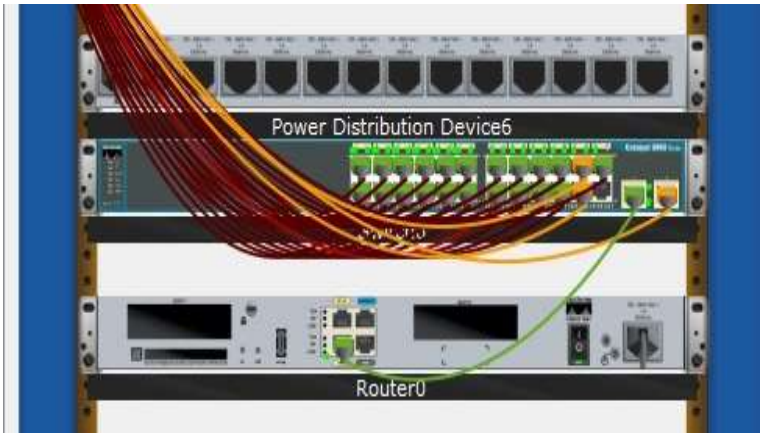


Figura 30

Simulación del Switch del Área de Fichaje

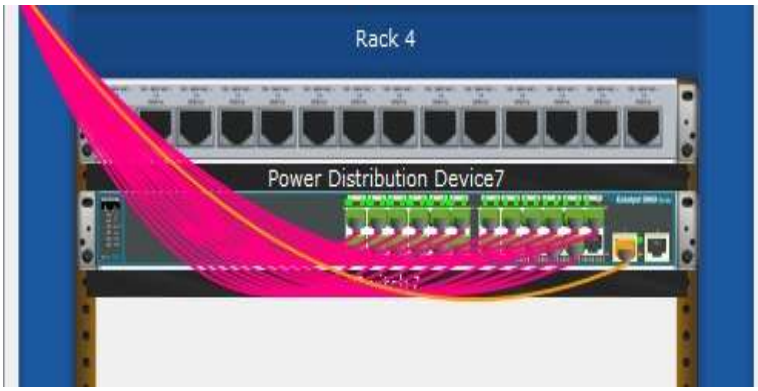


Figura 31

Simulación del Switch del Área de Recursos Humanos

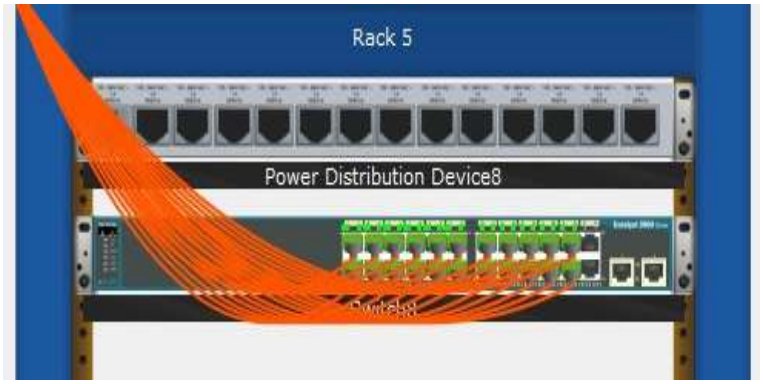


Figura 32

Simulación del Switch del Área Administrativa

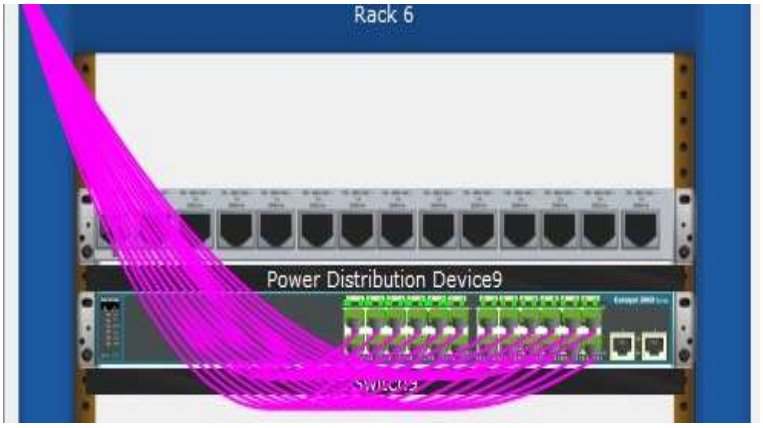


Figura 33

Simulación del Switch del Área del 1er Piso

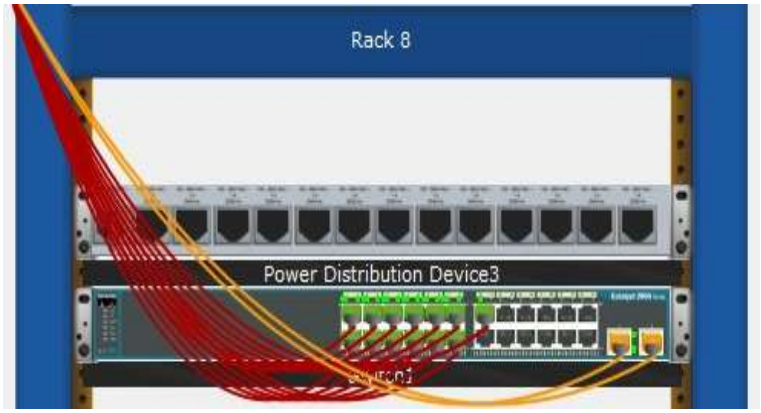


Figura 34

Simulación del Switch del Área del 2do Piso

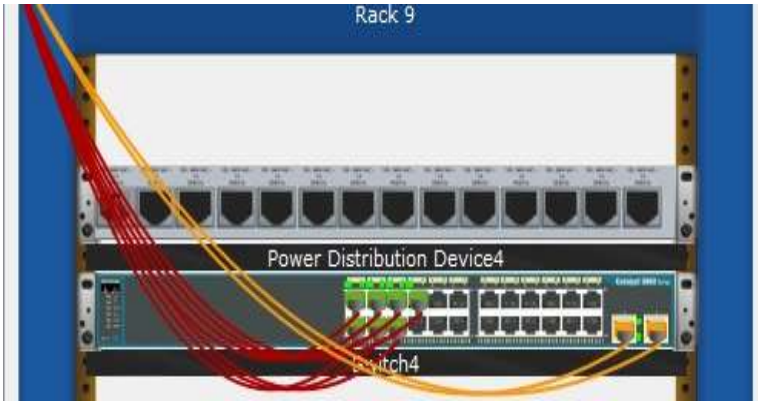


Figura 35

Simulación del Switch del Área del 3er Piso

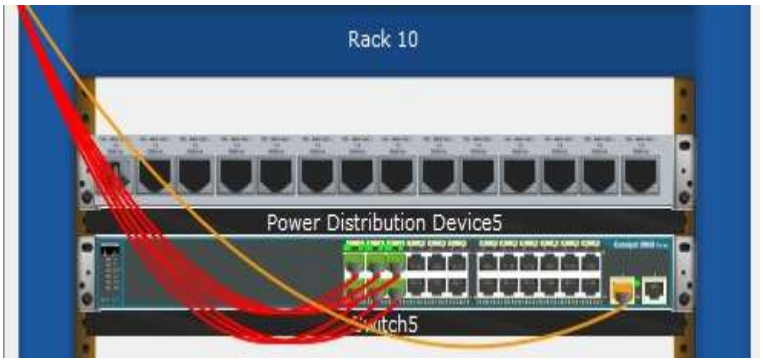


Figura 36

Rack Nº1 de Pared Accesible del Hospital

Figura 37

Rack Nº2 de Pared Accesible del Hospital

Figura 38

Rack Nº3 de Pared Accesible del Hospital

3.1.4. Análisis de tráfico existente

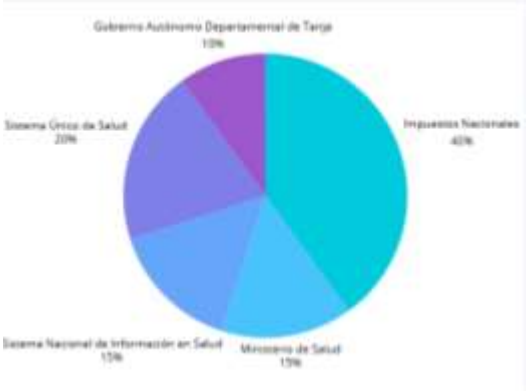
Mediante una medición de tráfico existente en la prueba que se realizó en el hospital Regional San Juan De Dios se pudieron obtener los siguientes enlaces y porcentajes de uso del ancho de banda.

Lista de Trafico existente

1. https://www.impuestos.gob.bo/
2. https://sus.minsalud.gob.bo/
3. https://www.minsalud.gob.bo/
4. https://snis.minsalud.gob.bo/siaf
5. https://www.tarija.gob.bo/

Figura 39

Trafico de Red



3.1.5. Ancho de Banda actual de la red

Mediante un testeo de ancho de banda se pudo analizar el ancho de banda actual del proveedor de servicio Tigo.

Figura 40

Ancho de Banda Actual de la Red

3.1.6. Estado de la red Actual

El estado actual de la red del hospital presenta múltiples limitaciones tanto en términos de rendimiento como de seguridad. La falta de segmentación, la obsolescencia de los equipos y la insuficiente capacidad de ancho de banda representan los principales desafíos.

Infraestructura de red

Equipos de red: La infraestructura actual es una simple red LAN con topología de bus, compuesta principalmente por routers y switches de generación pasada, sin soporte para tecnologías avanzadas como VLAN. Además, no se ha implementado una segmentación de red efectiva y no cuenta con conexión inalámbrica. Esta configuración, aunque simple, presenta importantes desventajas: al depender de un único cable troncal, existe un punto único de falla, lo que significa que, si el cable principal se daña, toda la red podría verse afectada. 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

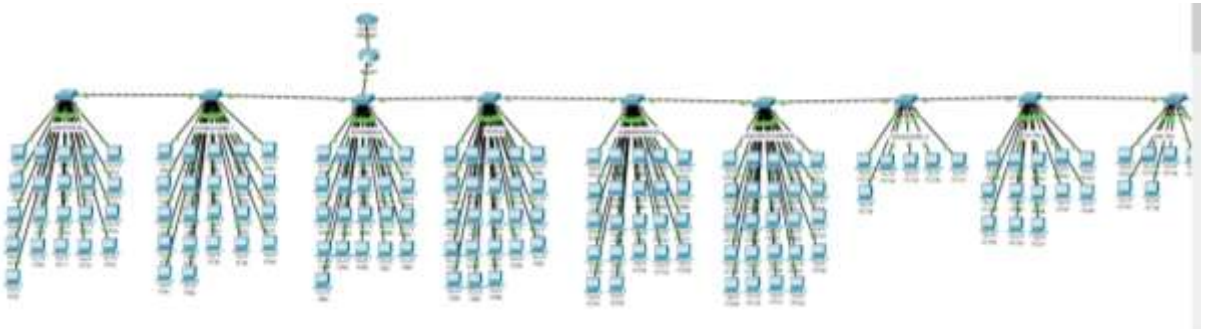
Velocidad y latencia: Se han detectado velocidades inestables en la red interna, lo que afecta a los sistemas de gestión hospitalaria, como la actualización de historiales médicos y la comunicación entre dispositivos médicos. Las latencias registradas son altas durante las horas pico, afectando los sistemas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

Seguridad de la red

Falta de segmentación: La red no está segmentada adecuadamente, 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 41

Simulación de su Topología de Bus



Problemas detectados

-Componentes desactualizados y sin soporte

-Falta de segmentación

-Topología de red bus

-Ausencia de conexión inalámbrica

-Caídas de red

-No cumple con estándares

-Direccionamiento Estático susceptible a incidentes de seguridad.

Análisis de Riesgos para el Hospital Regional San Juan de Dios de Tarija

Identificación de Riesgos

Riesgos Tecnológicos

Fallo de la infraestructura tecnológica (servidores, red, comunicaciones)

- Descripción: La infraestructura de red y servidores del hospital 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)

Fallo en los sistemas de telefonía IP o comunicaciones

- Descripción: La interrupción en los sistemas de comunicación internos, como la telefonía IP o el correo electrónico, puede afectar la coordinación entre los departamentos, lo cual es crucial en situaciones de emergencia.
- Impacto: Alta
- Probabilidad: Moderada (depende de la calidad de la infraestructura tecnológica)

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)

Tabla 5

Evaluación de Riesgos

Riesgo	**Probabilidad**	**Impacto**	**Puntaje de Riesgo (Probabilidad x Impacto)**
Fallo de la	Moderada	Alta	6 (Alto)

infraestructura tecnológica			
Fallo en los sistemas de comunicación	Moderada	Alta	6 (Alto)
Interrupción en el suministro eléctrico	Baja	Alta	4 (Moderado)
Accidentes o desastres naturales	Baja	Alta	4 (Moderado)

Plan de Mitigación de Riesgos para el Hospital Regional San Juan de Dios de Tarija

Riesgos Tecnológicos

Fallo de Infraestructura Tecnológica (Red, Servidores, Comunicaciones)

Estrategias de Mitigación:

- Redundancia de Infraestructura: Implementar redes y servidores redundantes para evitar puntos únicos de fallo. Esto incluye 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.

Fallo en los Sistemas de Comunicación Internos

Estrategias de Mitigación:

- Mantenimiento y Monitoreo: Establecer un sistema de monitoreo constante de las comunicaciones y la infraestructura tecnológica para detectar posibles fallos antes de que ocurran.

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 del hospital (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 (Terremotos, Inundaciones, Incendios)

Estrategias de Mitigación:

- Infraestructura Resistente: Asegurar que las instalaciones físicas del hospital 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.

3.2. Planificación

Tabla 6

Cronograma de Actividades

Actividad	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre
Planificación y análisis	x	x	x					
Implementación de VLAN			x	x	x			
Despliegue de wifi					x	x	x	
Configuración telefonía IP						x	x	x

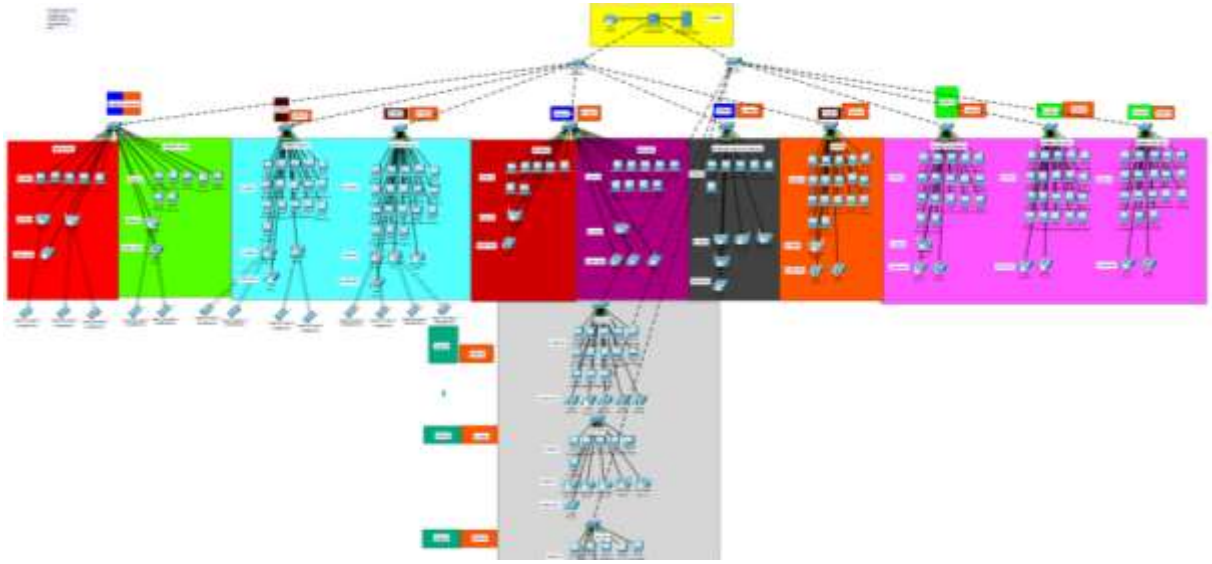
3.3. Diseño Lógico

Diseñar topología de red

En el contexto de esta red, la topología jerárquica se implementará organizando los dispositivos en niveles. Los switches de acceso se conectarán a switches de distribución, que a su vez estarán enlazados a un switch central o de core. Cada dispositivo se conectará a los switches de acceso mediante cables Ethernet de categoría 6, garantizando así una conexión rápida y fiable. El switch central estará configurado para gestionar el tráfico de la red, priorizando ciertos tipos de datos para optimizar el rendimiento.

Figura 42

Simulación de la Topología Jerárquica



3.3.1. VLAN

Las VLAN (Virtual LAN), o también conocidas como redes de área local virtuales, es una tecnología de redes que nos permite crear redes lógicas independientes dentro de la misma red física. El objetivo de usar VLAN en un entorno doméstico o profesional, es para segmentar adecuadamente la red y usar cada subred de una forma diferente, además, al segmentar por subredes usando VLANs se puede permitir o denegar el tráfico entre las diferentes VLAN El uso de VLANs nos proporciona lo siguiente:

Seguridad. Las VLAN nos permiten crear redes lógicamente independientes, por tanto, podemos aislarlas

para que solamente tengan conexión a Internet, y denegar el tráfico de una VLAN a otra. Por defecto no se permite a las VLANs intercambiar tráfico con otra VLAN, es totalmente necesario ascender a nivel de red (L3) con un router o un switch multicapa, con el objetivo de activar el inter-vlan routing, es decir, el enrutamiento entre VLANs para sí permitir la comunicación entre ellas siempre que lo necesitemos.

Segmentación. Las VLAN nos permiten segmentar todos los equipos en diferentes subredes, a cada subred le asignaremos una VLAN diferente. Por ejemplo, podremos crear una subred de gestión interna de todos los routers, switches y puntos de acceso, podremos crear una subred principal para los administradores, otra subred para dispositivos IoT y otra subred diferente para invitados. Es decir, podremos segmentar la red principal en subred con el objetivo de que cada subred haga uso de las comunicaciones como deseen. Gracias a la segmentación, podremos agrupar una gran cantidad de equipos dentro del mismo dominio de broadcast, aunque estén muy lejos físicamente.

Flexibilidad. Gracias a las VLAN podremos colocar a los diferentes equipos en una subred o en otra, de manera fácil y rápida, y tener unas políticas de comunicación donde permitimos o denegamos el tráfico hacia otras VLANs o hacia Internet. Por ejemplo, si creamos una VLAN de invitados, podríamos prohibirles el uso de servicios de streaming de vídeo.

Optimización de la red. Al tener subredes más pequeñas, en entornos donde tengamos cientos o miles de equipos conectados, contendremos el broadcast en dominios más pequeños, por tanto, el rendimiento de la red será óptimo, sin tener que transmitir los mensajes de broadcast a todos los equipos conectados, lo que haría que el rendimiento de la red baje radicalmente e incluso podría llegar a colapsar. Al usar VLAN, tendremos varios dominios de 56 difusión en el mismo switch. En redes donde el tráfico consiste en un alto porcentaje de transmisiones y multidifusiones, las VLAN pueden reducir la necesidad de enviar dicho tráfico a destinos innecesarios.

Asignación de Direcciones IP

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

VLAN 10 (Administrativos)

Se implementará esta vlan para las áreas de Administración y Recursos humanos con un rango DHCP con

el segmento de red 192.168.10.6 hasta el 192.168.10.254 con mascará de subred 255.255.255.0 su puerta de enlace 192.168.10.1

VLAN 20 (Consultas)

Se implementará esta vlan para las áreas de Fichaje y Consultorios con un rango DHCP con el segmento de red 192.168.20.6 hasta el 192.168.20.254 con mascará de subred 255.255.255.0 su puerta de enlace 192.168.20.1

VLAN 30 (Emergencias)

Se implementará esta vlan para las áreas de Emergencias, Laboratorios, Farmacia, Imagen con un rango DHCP con el segmento de red 192.168.30.6 hasta el 192.168.30.254 con mascará de subred 255.255.255.0 su puerta de enlace 192.168.30.1

VLAN 40 (Internación)

Se implementará esta vlan para las áreas de Primer Piso, Segundo Piso, Tercer Piso con un rango DHCP con el segmento de red 192.168.40.6 hasta el 192.168.40.254 con mascará de subred 255.255.255.0 su puerta de enlace 192.168.40.1

VLAN 50 (AccessPoint)

Se implementará esta vlan para todos los Access Points con un rango DHCP con el segmento de red 192.168.50.16 hasta el 192.168.50.254 con mascará de subred 255.255.255.0 su puerta de enlace 192.168.50.1

Identificadores de Componentes

PC – EM 1

PC = Identificador que es una computadora

- = Separador Componente - Área

EM = Área de EMERGENCIAS

1 = Numero de PC

AC – 1

AC = Identificador que es un Access Point

- = Separador de Componente – Numero

1 = Numero de Access Point

TEL-1

TEL = Identificador que es Teléfono IP

- = Separador de Componente – Numero

1 = Número de Teléfono IP

Tabla 7

Segmentación IPV4 con VLAN de direccionamiento dinámico

Nombre	Equipos	Rango de Ip (DHCP)	Mascara de Subred	Puerta de enlace
VLAN 10 Administrativos 55 PC	PC-RE1 PC-RE2 PC-RE3 PC-RE4 PC-RE5 PC-RE6 PC-RE7 PC-RE8 PC-RE9 PC-RE10 PC-RE11 PC-RE12 PC-RE13 PC-RE14	192.168.10.6- 192.168.10.254	255.255.255.0	192.168.10.1

	PC-RE15 PC-RE16 PC-RE17 PC-AD1 PC-AD2 PC-AD3 PC-AD4 PC-AD5 PC-AD6 PC-AD7 PC-AD8 PC-AD9 PC-AD10 PC-AD11 PC-AD12 PC-AD13 PC-AD14 PC-AD15 PC-AD16 PC-AD17 PC-AD18 PC-AD19 PC-AD20 PC-AD21 PC-AD22 PC-AD23 PC-AD24 PC-AD25 PC-AD26 PC-AD27 PC-AD28			

	PC-AD29 PC-AD30 PC-AD31 PC-AD32 PC-AD33 PC-AD34 PC-AD35 PC-AD36 PC-AD37 PC-AD38			
VLAN 20 Consultas 51 PC	PC-CO1 PC-CO2 PC-CO3 PC-CO4 PC-CO5 PC-CO6 PC-CO7 PC-CO8 PC-CO9 PC-CO10 PC-CO11 PC-CO12 PC-CO13 PC-CO14 PC-CO15 PC-CO16 PC-CO17 PC-CO18 PC-CO19 PC-CO20 PC-CO21 PC-CO22	192.168.20.6- 192.168.20.254	255.255.255.0	192.168.20.1

	PC-CO23 PC-CO24 PC-CO25 PC-CO26 PC-CO27 PC-CO28 PC-CO29 PC-CO30 PC-CO31 PC-CO32 PC-CO33 PC-CO34 PC-FI1 PC-FI2 PC-FI3 PC-FI4 PC-FI5 PC-FI6 PC-FI7 PC-FI8 PC-FI9 PC-FI10 PC-FI11 PC-FI12 PC-FI13 PC-FI14 PC-FI15 PC-FI16 PC-FI17			

VLAN 30 Emergencias 34 PC	PC-EM1 PC-EM2 PC-EM3 PC-EM4 PC-EM5 PC-LA1 PC-LA2 PC-LA3 PC-LA4 PC-LA5 PC-LA6 PC-LA7 PC-FA1 PC-FA2 PC-FA3 PC-FA4 PC-FA5 PC-FA6 PC-FA7 PC-IM1 PC-IM2 PC-IM3 PC-IM4 PC-IM5 PC-IM6 PC-IM7 PC-IM8 PC-IM9	192.168.30.6- 192.168.30.254	255.255.255.0	192.168.30.1

	PC-AL1 PC-AL2 PC-AL3 PC-AL4 PC-AL5 PC-AL6			
VLAN 40 Internación 25PC	PC-1ER1 PC-1ER2 PC-1ER3 PC-1ER4 PC-1ER5 PC-1ER6 PC-1ER7 PC-1ER8 PC-1ER9 PC-1ER10 PC-1ER11 PC-1ER12 PC-1ER13 PC-2DO1 PC-2DO2 PC-2DO3 PC-2DO4 PC-2DO5 PC-2DO6 PC-3ER1 PC-3ER2 PC-3ER3 PC-3ER4 PC-3ER5	192.168.40.6- 192.168.40.254	255.255.255.0	192.168.40.1

	PC-3ER6			
VLAN 50 AccessPoint 21AC	AC-1 AC-2 AC-3 AC-4 AC-5 AC-6 AC-7 AC-8 AC-9 AC-10 AC-11 AC-12 AC-13 AC-14 AC-15 AC-16 AC-17 AC-18 AC-19 AC-20 AC-21	192.168.50.16- 192.168.50.254	255.255.255.0	192.168.50.1
VLAN voice 25 TEL	TEL-1 TEL-2 TEL-3 TEL-4 TEL-5 TEL-6 TEL-7 TEL-8 TEL-9	10.17.77.10- 10.17.77.254	255.255.255.0	10.17.77.1

	TEL-10			
	TEL-11			
	TEL-12			
	TEL-13			
	TEL-14			
	TEL-15			
	TEL-16			
	TEL-17			
	TEL-18			
	TEL-19			
	TEL-20			
	TEL-21			
	TEL-22			
	TEL-23			
	TEL-24			
	TEL-25			

Tabla 8

Direccionamiento de la VLAN a puertos del switch

Rack	**VLAN**	**Puertos**	**N.º de componentes**
	VLAN30	F0/1-17	12PC
Emergencias-Laboratorios	VLAN50	F0/18-20	3AC
	TEL	F0/21-24	2TEL
	VLAN20	F0/1-18	16PC
Consultorios_1	VLAN50	F0/19-21	2AC
	TEL	F0/22-24	1TEL
	VLAN20	F0/1-18	18PC
Consultorios_2	VLAN50	F0/19-21	3AC
	TEL	F0/22-24	1TEL
	VLAN30	F0/1-17	16PC

Farmacia-Imágenes	VLAN50	F0/18-20	2AC
	TEL	F0/21-24	4TEL
	VLAN30	F0/1-17	6PC
Almacén (Área Restringida)	VLAN50	F0/18-21	4AC
	TEL	F0/22-24	1TEL
	VLAN20	F0/1-18	18PC
Fichaje	VLAN50	F0/19-21	1AC
	TEL	F0/22-24	2TEL
	VLAN10	F0/1-20	17PC
Recursos Humanos	VLAN50	F0/21-22	1AC
	TEL	F0/23-24	2TEL
	VLAN10	F0/1-20	20PC
Administracion_1	VLAN50	F0/21-22	
	TEL	F0/23-24	2TEL
	VLAN10	F0/1-20	18PC
Administracion_2	VLAN50	F0/21-22	
	TEL	F0/23-24	2TEL
	VLAN40	F0/1-14	13PC
PISO 1	VLAN50	F0/15-19	
	TEL	F0/20-24	5TEL
	VLAN40	F0/1-14	6PC
PISO 2	VLAN50	F0/15-19	5AC
	TEL	F0/20-24	1TEL
	VLAN40	F0/1-14	6PC
PISO 3	VLAN50	F0/15-19	
	TEL	F0/20-24	2TEL

Tabla 9

Direccionamiento de componente a puertos del switch

RACK EMERGENCIAS-LABORATORIOS							
	CONECTOR DE PARED			PATCH PANEL			
COMPONENTE	JACK		PUNCHDOWN	PUNCHDOWN	JACK	SWITCH	VLAN
PC-EM1	J1	Emer 01	PD1	PD1	J1	F0/1	30
PC-EM2	J2		PD2	PD2	J2	F0/2	30
PC-EM5	J3		PD3	PD3	J3	F0/3	30
PC-EM4	J4		PD4	PD4	J4	F0/4	30
PC-EM3	J1	Emer 02	PD1	PD5	J5	F0/5	30
AC-1	J2		PD2	PD18	J18	F0/18	50
TEL-1	J3		PD3	PD21	J21	F0/21	
AC-2	J4		PD4	PD19	J19	F0/19	50
PC-LA1	J1	Lab 01	PD1	PD6	J6	F0/6	30
PC-LA2	J2		PD2	PD7	J7	F0/7	30
PC-LA3	J3		PD3	PD8	J8	F0/8	30
PC-LA4	J4		PD4	PD9	J9	F0/9	30
TEL-2	J1	Lab 02	PD1	PD22	J22	F0/22	
PC-LA5	J2		PD2	PD10	J10	F0/10	30
	J3		PD3	PD	J	F0/	
	J4		PD4	PD	J	F0/	
AC-3	J1	Lab 03	PD1	PD20	J20	F0/20	50
PC-LA7	J2		PD2	PD11	J11	F0/11	30
PC-LA6	J3		PD3	PD12	J12	F0/12	30
	J4		PD4	PD	J	F0/	
RACK CONSULTORIOS_1							
	CONECTOR DE PARED			PATCH PANEL			
COMPONENTE	JACK		PUNCHDOWN	PUNCHDOWN	JACK	SWITCH	VLAN
AC-4	J1	Con	PD1	PD19	J19	F0/19	50
PC-CO1	J2		PD2	PD1	J1	F0/1	20

PC-CO2	J3	01	PD3	PD2	J2	F0/17	20
PC-CO3	J4		PD4	PD3	J3	F0/3	20
PC-CO4	J1		PD1	PD4	J4	F0/1	20
TEL-3	J2	Con	PD2	PD22	J22	F0/22	
PC-CO5	J3	02	PD3	PD5	J5	F0/5	20
	J4		PD4	PD	J	F0/	
PC-CO6	J1		PD1	PD6	J6	F0/6	20
PC-CO7	J2	Con	PD2	PD7	J7	F0/7	20
PC-CO8	J3	03	PD3	PD8	J8	F0/8	20
AC-5	J4		PD4	PD20	J20	F0/20	50
PC-CO9	J1		PD1	PD9	J9	F0/9	20
PC-CO10	J2	Con	PD2	PD10	J10	F0/10	20
PC-CO11	J3	04	PD3	PD11	J11	F0/11	20
PC-CO12	J4		PD4	PD12	J12	F0/12	20
PC-CO13	J1		PD1	PD13	J13	F0/13	20
PC-CO14	J2	Con	PD2	PD14	J14	F0/14	20
PC-CO15	J3	05	PD3	PD15	J15	F0/15	20
PC-CO16	J4		PD4	PD16	J16	F0/16	20
RACK CONSULTORIOS_2							
	CONECTOR DE PARED			PATCH PANEL			
COMPONENTE	JACK		PUNCHDOWN	PUNCHDOWN	JACK	SWITCH	VLAN
PC-CO17	J1		PD1	PD1	J1	F0/1	20
AC-6	J2	Con	PD2	PD19	J19	F0/19	50
PC-CO18	J3	06	PD3	PD2	J2	F0/2	20
PC-CO19	J4		PD4	PD3	J3	F0/3	20
PC-CO20	J1		PD1	PD4	J4	F0/4	20
PC-CO21	J2	Con	PD2	PD5	J5	F0/5	20
PC-CO22	J3	07	PD3	PD6	J6	F0/6	20
	J4		PD4	PD	J	F0/	
PC-CO23	J1		PD1	PD7	J7	F0/7	20

PC-CO24	J2	Con 08	PD2	PD8	J8	F0/8	20
PC-CO25	J3		PD3	PD9	J9	F0/9	20
AC-7	J4		PD4	PD20	J20	F0/20	50
PC-CO26	J1	Con 09	PD1	PD10	J10	F0/10	20
PC-CO27	J2		PD2	PD11	J11	F0/11	20
PC-CO28	J3		PD3	PD12	J12	F0/12	20
TEL-4	J4		PD4	PD22	J22	F0/22	
PC-CO29	J1	Con 10	PD1	PD13	J13	F0/13	20
PC-CO30	J2		PD2	PD14	J14	F0/14	20
AC-8	J3		PD3	PD21	J21	F0/21	50
	J4		PD4	PD	J	F0/	
PC-CO31	J1	Con 11	PD1	PD15	J15	F0/15	20
PC-CO32	J2		PD2	PD16	J16	F0/16	20
PC-CO33	J3		PD3	PD17	J17	F0/17	20
PC-CO34	J4		PD4	PD18	J18	F0/18	20
RACK FARMACIA-IMÁGENES							
	CONECTOR DE PARED			PATCH PANEL			
COMPONENTE	JACK		PUNCHDOWN	PUNCHDOWN	JACK	SWITCH	VLAN
PC-FA1	J1	Far 01	PD1	PD1	J1	F0/1	30
PC-FA2	J2		PD2	PD2	J2	F0/2	30
PC-FA3	J3		PD3	PD3	J3	F0/3	30
PC-FA4	J4		PD4	PD4	J4	F0/4	30
PC-FA5	J1	Far 02	PD1	PD5	J5	F0/5	30
PC-FA6	J2		PD2	PD6	J6	F0/6	30
PC-FA7	J3		PD3	PD7	J7	F0/7	30
AC-9	J4		PD4	PD18	J18	F0/18	50
TEL-5	J1	Far 03	PD1	PD21	J21	F0/21	
PC-IM8	J2		PD2	PD8	J8	F0/8	30
PC-IM9	J3		PD3	PD9	J9	F0/	30
TEL-7	J4		PD4	PD22	J22	F0/22	

PC-IM1	J1	Far 04	PD1	PD10	J10	F0/10	30
PC-IM7	J2		PD2	PD11	J11	F0/11	30
TEL-6	J3		PD3	PD23	J23	F0/23	
TEL-8	J4		PD4	PD24	J24	F0/24	
PC-IM2	J1	Far 05	PD1	PD12	J12	F0/12	30
PC-IM3	J2		PD2	PD13	J13	F0/13	30
PC-IM4	J3		PD3	PD14	J14	F0/14	30
PC-IM5	J4		PD4	PD15	J15	F0/15	30
PC-IM6	J1	Far 06	PD1	PD16	J16	F0/16	30
AC-10	J2		PD2	PD19	J19	F0/19	50
	J3		PD3	PD	J	F0/	
	J4		PD4	PD	J	F0/	
RACK ALMACEN (AREA RESTRINGIDA)							
	CONECTOR DE PARED			PATCH PANEL			
COMPONENTE	JACK		PUNCHDOWN	PUNCHDOWN	JACK	SWITCH	VLAN
PC-AL1	J1	Alm 01	PD1	PD1	J1	F0/1	30
PC-AL2	J2		PD2	PD2	J2	F0/2	30
PC-AL3	J3		PD3	PD3	J3	F0/3	30
AC-11	J4		PD4	PD18	J18	F0/18	50
PC-AL4	J1	Alm 02	PD1	PD4	J4	F0/4	30
AC-16	J2		PD2	PD19	J19	F0/19	50
AC-15	J3		PD3	PD20	J20	F0/20	50
	J4		PD4	PD	J	F0/	
PC-AL5	J1	Alm 03	PD1	PD5	J5	F0/5	30
PC-AL6	J2		PD2	PD6	J6	F0/6	30
AC-12	J3		PD3	PD21	J21	F0/21	50
TEL-9	J4		PD4	PD22	J22	F0/22	
RACK FICHAJE							
	CONECTOR DE PARED			PATCH PANEL			

COMPONENTE	JACK		PUNCHDOWN	PUNCHDOWN	JACK	SWITCH	VLAN
PC-FI3	J1	Fic 01	PD1	PD1	J1	F0/1	20
PC-FI11	J2		PD2	PD2	J2	F0/2	20
PC-FI5	J3		PD3	PD3	J3	F0/3	20
PC-FI15	J4		PD4	PD4	J4	F0/4	20
PC-FI16	J1	Fic 02	PD1	PD5	J5	F0/5	20
PC-FI17	J2		PD2	PD6	J6	F0/6	20
	J3		PD3	PD	J	F0/	
PC-FI2	J4		PD4	PD8	J8	F0/8	20
PC-FI4	J1	Fic 03	PD1	PD9	J9	F0/9	20
PC-FI10	J2		PD2	PD10	J10	F0/10	20
PC-FI14	J3		PD3	PD11	J11	F0/11	20
TEL-11	J4		PD4	PD22	J22	F0/22	50
PC-FI7	J1	Fic 04	PD1	PD12	J12	F0/12	20
PC-FI6	J2		PD2	PD13	J13	F0/13	20
PC-FI8	J3		PD3	PD14	J14	F0/14	20
AC-13	J4		PD4	PD19	J19	F0/19	50
PC-FI13	J1	Fic 05	PD1	PD15	J15	F0/15	20
PC-FI9	J2		PD2	PD16	J16	F0/16	20
PC-FI12	J3		PD3	PD17	J17	F0/17	20
	J4		PD4	PD	J	F0/	
PC-FI1	J1	Fic 06	PD1	PD18	J18	F0/18	20
TEL-10	J2		PD2	PD23	J23	F0/23	
	J3		PD3	PD	J	F0/	
	J4		PD4	PD	J	F0/	
RACK RECURSOS HUMANOS							
	CONECTOR DE PARED			PATCH PANEL			
COMPONENTE	JACK		PUNCHDOWN	PUNCHDOWN	JACK	SWITCH	VLAN
PC-RE1	J1	Rec	PD1	PD1	J1	F0/1	10
PC-RE2	J2		PD2	PD2	J2	F0/2	10

PC-RE3	J3	01	PD3	PD3	J3	F0/3	10
PC-RE4	J4		PD4	PD4	J4	F0/4	10
PC-RE10	J1		PD1	PD5	J5	F0/5	10
PC-RE11	J2	Rec	PD2	PD6	J6	F0/6	10
AC-14	J3	02	PD3	PD21	J21	F0/21	50
TEL-12	J4		PD4	PD23	J23	F0/23	
PC-RE5	J1		PD1	PD7	J7	F0/7	10
PC-RE6	J2	Rec	PD2	PD8	J8	F0/8	10
	J3	03	PD3	PD	J	F0/	
	J4		PD4	PD	J	F0/	
PC-RE7	J1		PD1	PD9	J9	F0/9	10
PC-RE8	J2	Rec	PD2	PD10	J10	F0/10	10
PC-RE9	J3	04	PD3	PD11	J11	F0/11	10
	J4		PD4	PD	J	F0/	
PC-RE12	J1		PD1	PD12	J12	F0/12	10
PC-RE13	J2	Rec	PD2	PD13	J13	F0/13	10
PC-RE16	J3	05	PD3	PD14	J14	F0/14	10
TEL-13	J4		PD4	PD24	J24	F0/24	
PC-RE17	J1		PD1	PD15	J15	F0/15	10
PC-RE15	J2	Rec	PD2	PD16	J16	F0/16	10
PC-RE14	J3	06	PD3	PD17	J17	F0/17	10
	J4		PD4	PD	J	F0/	
RACK ADMINISTRACION_1							
	CONECTOR DE PARED			PATCH PANEL			
COMPONENTE	JACK		PUNCHDOWN	PUNCHDOWN	JACK	SWITCH	VLAN
PC-AD1	J1		PD1	PD1	J1	F0/1	10
PC-AD2	J2	Adm	PD2	PD2	J2	F0/2	10
PC-AD3	J3	01	PD3	PD3	J3	F0/3	10
PC-AD4	J4		PD4	PD4	J4	F0/4	10
PC-AD5	J1		PD1	PD5	J5	F0/5	10

PC-AD6	J2	Adm 02	PD2	PD6	J6	F0/6	10
PC-AD7	J3		PD3	PD7	J7	F0/7	10
PC-AD8	J4		PD4	PD8	J8	F0/8	10
PC-AD9	J1	Adm 03	PD1	PD9	J9	F0/9	10
PC-AD10	J2		PD2	PD10	J10	F0/10	10
PC-AD11	J3		PD3	PD11	J11	F0/11	10
TEL-15	J4		PD4	PD23	J23	F0/23	
PC-AD12	J1	Adm 04	PD1	PD12	J12	F0/12	10
PC-AD13	J2		PD2	PD13	J13	F0/1	10
PC-AD14	J3		PD3	PD14	J14	F0/14	10
	J4		PD4	PD	J	F0/	
PC-AD15	J1	Adm 05	PD1	PD15	J15	F0/15	10
PC-AD19	J2		PD2	PD16	J16	F0/16	10
PC-AD20	J3		PD3	PD17	J17	F0/17	10
TEL-14	J4		PD4	PD24	J24	F0/24	
PC-AD16	J1	Adm 06	PD1	PD18	J18	F0/18	10
PC-AD17	J2		PD2	PD19	J19	F0/19	10
PC-AD18	J3		PD3	PD20	J20	F0/20	10
	J4		PD4	PD	J	F0/	
RACK ADMINISTRACION_2							
	CONECTOR DE PARED			PATCH PANEL			
COMPONENTE	JACK		PUNCHDOWN	PUNCHDOWN	JACK	SWITCH	VLAN
PC-AD24	J1	Adm 07	PD1	PD1	J1	F0/1	10
PC-AD25	J2		PD2	PD2	J2	F0/2	10
PC-AD26	J3		PD3	PD3	J3	F0/3	10
	J4		PD4	PD	J	F0/	
PC-AD27	J1	Adm 08	PD1	PD4	J4	F0/4	10
PC-AD28	J2		PD2	PD5	J5	F0/5	10
PC-AD29	J3		PD3	PD6	J6	F0/6	10
TEL-16	J4		PD4	PD23	J23	F0/23	

PC-AD30	J1	Adm 09	PD1	PD7	J7	F0/7	10
PC-AD31	J2		PD2	PD8	J8	F0/8	10
PC-AD32	J3		PD3	PD9	J9	F0/9	10
	J4		PD4	PD	J	F0/	
PC-AD33	J1	Adm 10	PD1	PD10	J10	F0/10	10
PC-AD34	J2		PD2	PD11	J11	F0/11	10
PC-AD35	J3		PD3	PD12	J12	F0/12	10
	J4		PD4	PD	J	F0/	
PC-AD21	J1	Adm 11	PD1	PD13	J13	F0/13	10
PC-AD22	J2		PD2	PD14	J14	F0/14	10
PC-AD23	J3		PD3	PD15	J15	F0/15	10
	J4		PD4	PD	J	F0/	
PC-AD36	J1	Adm 12	PD1	PD16	J16	F0/16	10
PC-AD37	J2		PD2	PD17	J17	F0/17	10
PC-AD38	J3		PD3	PD18	J18	F0/18	10
TEL-17	J4		PD4	PD24	J24	F0/24	
PISO 1							
	CONECTOR DE PARED			PATCH PANEL			
COMPONENTE	JACK		PUNCHDOWN	PUNCHDOWN	JACK	SWITCH	VLAN
PC-1ER1	J1	1er 01	PD1	PD1	J1	F0/1	40
PC-1ER2	J2		PD2	PD2	J2	F0/2	40
TEL-19	J3		PD3	PD20	J20	F0/20	
TEL-18	J4		PD4	PD21	J21	F0/21	
PC-1ER3	J1	1er 02	PD1	PD3	J3	F0/3	40
PC-1ER4	J2		PD2	PD4	J4	F0/4	40
TEL-20	J3		PD3	PD22	J22	F0/22	
	J4		PD4	PD	J	F0/	
PC-1ER6	J1	1er 03	PD1	PD5	J5	F0/5	40
PC-1ER7	J2		PD2	PD6	J6	F0/6	40
TEL-22	J3		PD3	PD23	J23	F0/23	

	J4		PD4	PD	J	F0/	
PC-1ER5	J1		PD1	PD7	J7	F0/7	40
PC-1ER8	J2	1er	PD2	PD8	J8	F0/8	40
TEL-21	J3	04	PD3	PD24	J24	F0/24	
	J4		PD4	PD	J	F0/	
PC-1ER12	J1		PD1	PD9	J9	F0/9	40
PC-1ER13	J2	1er	PD2	PD10	J10	F0/10	40
PC-1ER9	J3	05	PD3	PD11	J11	F0/11	40
	J4		PD4	PD	J	F0/	
PC-1ER10	J1		PD1	PD12	J12	F0/12	40
PC-1ER11	J2	1er	PD2	PD13	J13	F0/13	40
	J3	06	PD3	PD	J	F0/	
	J4		PD4	PD	J	F0/	
PISO 2							
	CONECTOR DE PARED			PATCH PANEL			
COMPONENTE	JACK		PUNCHDOWN	PUNCHDOWN	JACK	SWITCH	VLAN
AC-20	J1		PD1	PD15	J15	F0/15	50
PC2DO2	J2	2do	PD2	PD1	J1	F0/1	40
AC-19	J3	01	PD3	PD16	J16	F0/16	50
	J4		PD4	PD	J	F0/	
PC2DO1	J1		PD1	PD2	J2	F0/2	40
PC2DO3	J2	2do	PD2	PD3	J3	F0/3	40
AC-18	J3	02	PD3	PD17	J17	F0/17	50
PC2DO4	J4		PD4	PD4	J4	F0/4	40
AC-21	J1		PD1	PD18	J18	F0/18	50
TEL-23	J2	2do	PD2	PD20	J20	F0/20	
PC2DO6	J3	03	PD3	PD5	J5	F0/5	40
	J4		PD4	PD	J	F0/	
AC-17	J1		PD1	PD19	J19	F0/19	50
PC2DO5	J2	2do	PD2	PD6	J6	F0/6	40

	J3	04	PD3	PD	J	F0/	
	J4		PD4	PD	J	F0/	
PISO 3							
	CONECTOR DE PARED			PATCH PANEL			
COMPONENTE	JACK		PUNCHDOWN	PUNCHDOWN	JACK	SWITCH	VLAN
TEL-24	J1	3er 01	PD1	PD20	J20	F0/20	
PC3ER3	J2		PD2	PD1	J1	F0/1	40
	J3		PD3	PD	J	F0/	
	J4		PD4	PD	J	F0/	
PC3ER4	J1	3er 02	PD1	PD2	J2	F0/2	40
PC3ER5	J2		PD2	PD3	J3	F0/3	40
PC3ER6	J3		PD3	PD4	J4	F0/4	40
	J4		PD4	PD	J	F0/	
PC3ER1	J1	3er 03	PD1	PD5	J5	F0/5	40
TEL-25	J2		PD2	PD21	J21	F0/21	
PC3ER2	J3		PD3	PD6	J6	F0/6	40
	J4		PD4	PD	J	F0/	

Tabla 10

Distancia del cable UTP

Origen	Destino	Tipo de cable	Metros	Tipo
Sistemas 596mts, 45 rj45				
Switch Sistemas1 G0/1	SwitchMadre Sistemas1 G0/1	Categoría 6	1	Cruzado
Switch Sistemas2 G0/1	SwitchMadre Sistemas1 G0/2	Categoría 6	1	Cruzado
SwitchMadre Sistemas1 G0/24	Router F0/0	Categoría 6	1	Cruzado
Switch Sistemas1 F0/1	Pach Panel Sistemas J1	Categoría 6	1	Cruzado

Switch Sistemas1 F0/2	Pach Panel Sistemas J2	Categoría 6	1	Cruzado
Switch Sistemas1 F0/3	Pach Panel Sistemas J3	Categoría 6	1	Cruzado
Switch Sistemas1 F0/4	Pach Panel Sistemas J4	Categoría 6	1	Cruzado
Switch Sistemas1 F0/5	Pach Panel Sistemas J5	Categoría 6	1	Cruzado
Switch Sistemas1 F0/6	Pach Panel Sistemas J6	Categoría 6	1	Cruzado
Switch Sistemas2 F0/7	Pach Panel Sistemas J7	Categoría 6	1	Cruzado
Switch Sistemas2 F0/8	Pach Panel Sistemas J8	Categoría 6	1	Cruzado
Switch Sistemas2 F0/9	Pach Panel Sistemas J9	Categoría 6	1	Cruzado
Switch Sistemas2 F0/10	Pach Panel Sistemas J10	Categoría 6	1	Cruzado
Switch Sistemas2 F0/11	Pach Panel Sistemas J11	Categoría 6	1	Cruzado
Switch Sistemas2 F0/12	Pach Panel Sistemas J12	Categoría 6	1	Cruzado
Switch Sistemas F0/24	Pach Panel Sistemas J24	Categoría 6	1	Cruzado
Pach Panel Sistemas PD1	Switch Emergencias G0/1	Categoría 6	67	Cruzado
Pach Panel Sistemas PD2	Switch Consultorios_1 G0/1	Categoría 6	42	Cruzado
Pach Panel Sistemas PD3	Switch Consultorios_2 G0/1	Categoría 6	13	Cruzado
Pach Panel Sistemas PD4	Switch Farmacias G0/1	Categoría 6	28	Cruzado
Pach Panel Sistemas PD5	Switch Almacen G0/1	Categoría 6	59	Cruzado
Pach Panel Sistemas PD6	Switch Fichaje G0/1	Categoría 6	42	Cruzado
Pach Panel Sistemas PD7	Switch Recursos Humanos G0/1	Categoría 6	51	Cruzado
Pach Panel Sistemas PD8	Switch Administracion_1 G0/1	Categoría 6	77	Cruzado
Pach Panel Sistemas PD9	Switch Administracion_2 G0/1	Categoría 6	65	Cruzado
Pach Panel Sistemas PD10	Switch 1erPiso G0/1	Categoría 6	30	Cruzado
Pach Panel Sistemas PD11	Switch 2doPiso G0/1	Categoría 6	45	Cruzado

Pach Panel Sistemas PD12	Switch 3erPiso G0/1	Categoría 6	60	Cruzado
Pach Panel Sistemas PD24	Servidor Asterisk	Categoría 6	1	Cruzado
Emergencias 393mts, 68 rj45				
Switch Emergencias F0/1	Pach Panel Emergencias J1	Categoría 6	1	Normal
Switch Emergencias F0/2	Pach Panel Emergencias J2	Categoría 6	1	Normal
Switch Emergencias F0/3	Pach Panel Emergencias J3	Categoría 6	1	Normal
Switch Emergencias F0/4	Pach Panel Emergencias J4	Categoría 6	1	Normal
Switch Emergencias F0/5	Pach Panel Emergencias J5	Categoría 6	1	Normal
Switch Emergencias F0/6	Pach Panel Emergencias J6	Categoría 6	1	Normal
Switch Emergencias F0/7	Pach Panel Emergencias J7	Categoría 6	1	Normal
Switch Emergencias F0/8	Pach Panel Emergencias J8	Categoría 6	1	Normal
Switch Emergencias F0/9	Pach Panel Emergencias J9	Categoría 6	1	Normal
Switch Emergencias F0/10	Pach Panel Emergencias J10	Categoría 6	1	Normal
Switch Emergencias F0/11	Pach Panel Emergencias J11	Categoría 6	1	Normal
Switch Emergencias F0/12	Pach Panel Emergencias J12	Categoría 6	1	Normal
Switch Emergencias F0/18	Pach Panel Emergencias J18	Categoría 6	1	Normal
Switch Emergencias F0/19	Pach Panel Emergencias J19	Categoría 6	1	Normal
Switch Emergencias F0/20	Pach Panel Emergencias J20	Categoría 6	1	Normal
Switch Emergencias F0/21	Pach Panel Emergencias J21	Categoría 6	1	Normal
Switch Emergencias F0/22	Pach Panel Emergencias J22	Categoría 6	1	Normal

Pach Panel Emergencias PD1	Placa de pared Emer01 PD1	Categoría 6	7	Normal
Pach Panel Emergencias PD2	Placa de pared Emer01 PD2	Categoría 6	7	Normal
Pach Panel Emergencias PD3	Placa de pared Emer01 PD3	Categoría 6	7	Normal
Pach Panel Emergencias PD4	Placa de pared Emer01 PD4	Categoría 6	7	Normal
Pach Panel Emergencias PD5	Placa de pared Emer02 PD1	Categoría 6	21	Normal
Pach Panel Emergencias PD18	Placa de pared Emer02 PD2	Categoría 6	21	Normal
Pach Panel Emergencias PD21	Placa de pared Emer02 PD3	Categoría 6	21	Normal
Pach Panel Emergencias PD19	Placa de pared Emer02 PD4	Categoría 6	21	Normal
Pach Panel Emergencias PD6	Placa de pared Lab01 PD1	Categoría 6	8	Normal
Pach Panel Emergencias PD7	Placa de pared Lab01 PD2	Categoría 6	8	Normal
Pach Panel Emergencias PD8	Placa de pared Lab01 PD3	Categoría 6	8	Normal
Pach Panel Emergencias PD9	Placa de pared Lab01 PD4	Categoría 6	8	Normal
Pach Panel Emergencias PD22	Placa de pared Lab02 PD1	Categoría 6	19	Normal
Pach Panel Emergencias PD10	Placa de pared Lab02 PD2	Categoría 6	19	Normal
Pach Panel Emergencias PD20	Placa de pared Lab03 PD1	Categoría 6	17	Normal

Pach Panel Emergencias PD11	Placa de pared Lab03 PD2	Categoría 6	17	Normal
Pach Panel Emergencias PD12	Placa de pared Lab03 PD3	Categoría 6	17	Normal
Placa de pared Emer01 J1	PC-EM1	Categoría 6	8	Normal
Placa de pared Emer01 J2	PC-EM2	Categoría 6	3	Normal
Placa de pared Emer01 J3	PC-EM5	Categoría 6	12	Normal
Placa de pared Emer01 J4	PC-EM4	Categoría 6	10	Normal
Placa de pared Emer02 J1	PC-EM3	Categoría 6	9	Normal
Placa de pared Emer02 J2	AC-1	Categoría 6	13	Normal
Placa de pared Emer02 J3	TEL-1	Categoría 6	13	Normal
Placa de pared Emer02 J4	AC-2	Categoría 6	7	Normal
Placa de pared Lab01 J1	PC-LA1	Categoría 6	12	Normal
Placa de pared Lab01 J2	PC-LA2	Categoría 6	4	Normal
Placa de pared Lab01 J3	PC-LA3	Categoría 6	5	Normal
Placa de pared Lab01 J4	PC-LA4	Categoría 6	9	Normal
Placa de pared Lab02 J1	TEL-2	Categoría 6	9	Normal
Placa de pared Lab02 J2	PC-LA5	Categoría 6	2	Normal
Placa de pared Lab03 J1	AC-3	Categoría 6	3	Normal
Placa de pared Lab03 J2	PC-LA7	Categoría 6	13	Normal
Placa de pared Lab03 J3	PC-LA6	Categoría 6	11	Normal
Consultorios_1 431mts, 76 rj45				
Switch Consultorios_1 F0/1	Pach Panel Consultorios_1 J1	Categoría 6	1	Normal
Switch Consultorios_1 F0/2	Pach Panel Consultorios_1 J2	Categoría 6	1	Normal
Switch Consultorios_1 F0/3	Pach Panel Consultorios_1 J3	Categoría 6	1	Normal
Switch Consultorios_1 F0/4	Pach Panel Consultorios_1 J4	Categoría 6	1	Normal

Switch Consultorios_1 F0/5	Pach Panel Consultorios_1 J5	Categoría 6	1	Normal
Switch Consultorios_1 F0/6	Pach Panel Consultorios_1 J6	Categoría 6	1	Normal
Switch Consultorios_1 F0/7	Pach Panel Consultorios_1 J7	Categoría 6	1	Normal
Switch Consultorios_1 F0/8	Pach Panel Consultorios_1 J8	Categoría 6	1	Normal
Switch Consultorios_1 F0/9	Pach Panel Consultorios_1 J9	Categoría 6	1	Normal
Switch Consultorios_1 F0/10	Pach Panel Consultorios_1 J10	Categoría 6	1	Normal
Switch Consultorios_1 F0/11	Pach Panel Consultorios_1 J11	Categoría 6	1	Normal
Switch Consultorios_1 F0/12	Pach Panel Consultorios_1 J12	Categoría 6	1	Normal
Switch Consultorios_1 F0/13	Pach Panel Consultorios_1 J13	Categoría 6	1	Normal
Switch Consultorios_1 F0/14	Pach Panel Consultorios_1 J14	Categoría 6	1	Normal
Switch Consultorios_1 F0/15	Pach Panel Consultorios_1 J15	Categoría 6	1	Normal
Switch Consultorios_1 F0/16	Pach Panel Consultorios_1 J16	Categoría 6	1	Normal
Switch Consultorios_1 F0/19	Pach Panel Consultorios_1 J19	Categoría 6	1	Normal
Switch Consultorios_1 F0/20	Pach Panel Consultorios_1 J20	Categoría 6	1	Normal
Switch Consultorios_1 F0/22	Pach Panel Consultorios_1 J22	Categoría 6	1	Normal

Pach Panel Consultorios_1 PD19	Placa de pared Con01 PD1	Categoría 6	18	Normal
Pach Panel Consultorios_1 PD1	Placa de pared Con01 PD2	Categoría 6	18	Normal
Pach Panel Consultorios_1 PD2	Placa de pared Con01 PD3	Categoría 6	18	Normal
Pach Panel Consultorios_1 PD3	Placa de pared Con01 PD4	Categoría 6	18	Normal
Pach Panel Consultorios_1 PD4	Placa de pared Con02 PD1	Categoría 6	6	Normal
Pach Panel Consultorios_1 PD22	Placa de pared Con02 PD2	Categoría 6	6	Normal
Pach Panel Consultorios_1 PD5	Placa de pared Con02 PD3	Categoría 6	6	Normal
Pach Panel Consultorios_1 PD6	Placa de pared Con03 PD1	Categoría 6	11	Normal
Pach Panel Consultorios_1 PD7	Placa de pared Con03 PD2	Categoría 6	11	Normal
Pach Panel Consultorios_1 PD8	Placa de pared Con03 PD3	Categoría 6	11	Normal
Pach Panel Consultorios_1 PD20	Placa de pared Con03 PD4	Categoría 6	11	Normal
Pach Panel Consultorios_1 PD9	Placa de pared Con04 PD1	Categoría 6	18	Normal
Pach Panel Consultorios_1 PD10	Placa de pared Con04 PD2	Categoría 6	18	Normal
Pach Panel Consultorios_1 PD11	Placa de pared Con04 PD3	Categoría 6	18	Normal
Pach Panel Consultorios_1 PD12	Placa de pared Con04 PD4	Categoría 6	18	Normal

Pach Panel Consultorios_1 PD13	Placa de pared Con05 PD1	Categoría 6	30	Normal
Pach Panel Consultorios_1 PD14	Placa de pared Con05 PD2	Categoría 6	30	Normal
Pach Panel Consultorios_1 PD15	Placa de pared Con05 PD3	Categoría 6	30	Normal
Pach Panel Consultorios_1 PD16	Placa de pared Con05 PD4	Categoría 6	30	Normal
Placa de pared Con01 J1	AC-4	Categoría 6	7	Normal
Placa de pared Con01 J2	PC-CO1	Categoría 6	5	Normal
Placa de pared Con01 J3	PC-CO2	Categoría 6	9	Normal
Placa de pared Con01 J4	PC-CO3	Categoría 6	8	Normal
Placa de pared Con02 J1	PC-CO4	Categoría 6	6	Normal
Placa de pared Con02 J2	TEL-3	Categoría 6	5	Normal
Placa de pared Con02 J3	PC-CO5	Categoría 6	5	Normal
Placa de pared Con03 J1	PC-CO6	Categoría 6	5	Normal
Placa de pared Con03 J2	PC-CO7	Categoría 6	2	Normal
Placa de pared Con03 J3	PC-CO8	Categoría 6	2	Normal
Placa de pared Con03 J4	AC-5	Categoría 6	3	Normal
Placa de pared Con04 J1	PC-CO9	Categoría 6	2	Normal
Placa de pared Con04 J2	PC-CO10	Categoría 6	4	Normal
Placa de pared Con04 J3	PC-CO11	Categoría 6	5	Normal
Placa de pared Con04 J4	PC-CO12	Categoría 6	2	Normal
Placa de pared Con05 J1	PC-CO13	Categoría 6	7	Normal
Placa de pared Con05 J2	PC-CO14	Categoría 6	4	Normal
Placa de pared Con05 J3	PC-CO15	Categoría 6	2	Normal
Placa de pared Con05 J4	PC-CO16	Categoría 6	3	Normal
Consultorios_2 471mts, 88 rj45				
Switch Consultorios_2 F0/1	Pach Panel Consultorios_2 J1	Categoría 6	1	Normal

Switch Consultorios_2 F0/2	Pach Panel Consultorios_2 J2	Categoría 6	1	Normal
Switch Consultorios_2 F0/3	Pach Panel Consultorios_2 J3	Categoría 6	1	Normal
Switch Consultorios_2 F0/4	Pach Panel Consultorios_2 J4	Categoría 6	1	Normal
Switch Consultorios_2 F0/5	Pach Panel Consultorios_2 J5	Categoría 6	1	Normal
Switch Consultorios_2 F0/6	Pach Panel Consultorios_2 J6	Categoría 6	1	Normal
Switch Consultorios_2 F0/7	Pach Panel Consultorios_2 J7	Categoría 6	1	Normal
Switch Consultorios_2 F0/8	Pach Panel Consultorios_2 J8	Categoría 6	1	Normal
Switch Consultorios_2 F0/9	Pach Panel Consultorios_2 J9	Categoría 6	1	Normal
Switch Consultorios_2 F0/10	Pach Panel Consultorios_2 J10	Categoría 6	1	Normal
Switch Consultorios_2 F0/11	Pach Panel Consultorios_2 J11	Categoría 6	1	Normal
Switch Consultorios_2 F0/12	Pach Panel Consultorios_2 J12	Categoría 6	1	Normal
Switch Consultorios_2 F0/13	Pach Panel Consultorios_2 J13	Categoría 6	1	Normal
Switch Consultorios_2 F0/14	Pach Panel Consultorios_2 J14	Categoría 6	1	Normal
Switch Consultorios_2 F0/15	Pach Panel Consultorios_2 J15	Categoría 6	1	Normal
Switch Consultorios_2 F0/16	Pach Panel Consultorios_2 J16	Categoría 6	1	Normal

Switch Consultorios_2 F0/17	Pach Panel Consultorios_2 J17	Categoría 6	1	Normal
Switch Consultorios_2 F0/18	Pach Panel Consultorios_2 J18	Categoría 6	1	Normal
Switch Consultorios_2 F0/19	Pach Panel Consultorios_2 J19	Categoría 6	1	Normal
Switch Consultorios_2 F0/20	Pach Panel Consultorios_2 J20	Categoría 6	1	Normal
Switch Consultorios_2 F0/21	Pach Panel Consultorios_2 J21	Categoría 6	1	Normal
Switch Consultorios_2 F0/22	Pach Panel Consultorios_2 J22	Categoría 6	1	Normal
Pach Panel Consultorios_2 PD1	Placa de pared Con06 PD1	Categoría 6	20	Normal
Pach Panel Consultorios_2 PD19	Placa de pared Con06 PD2	Categoría 6	20	Normal
Pach Panel Consultorios_2 PD2	Placa de pared Con06 PD3	Categoría 6	20	Normal
Pach Panel Consultorios_2 PD3	Placa de pared Con06 PD4	Categoría 6	20	Normal
Pach Panel Consultorios_2 PD4	Placa de pared Con07 PD1	Categoría 6	12	Normal
Pach Panel Consultorios_2 PD5	Placa de pared Con07 PD2	Categoría 6	12	Normal
Pach Panel Consultorios_2 PD6	Placa de pared Con07 PD3	Categoría 6	12	Normal
Pach Panel Consultorios_2 PD7	Placa de pared Con08 PD1	Categoría 6	14	Normal
Pach Panel Consultorios_2 PD8	Placa de pared Con08 PD2	Categoría 6	14	Normal

Pach Panel Consultorios_2 PD9	Placa de pared Con08 PD3	Categoría 6	14	Normal
Pach Panel Consultorios_2 PD20	Placa de pared Con08 PD4	Categoría 6	14	Normal
Pach Panel Consultorios_2 PD10	Placa de pared Con09 PD1	Categoría 6	18	Normal
Pach Panel Consultorios_2 PD11	Placa de pared Con09 PD2	Categoría 6	18	Normal
Pach Panel Consultorios_2 PD12	Placa de pared Con09 PD3	Categoría 6	18	Normal
Pach Panel Consultorios_2 PD22	Placa de pared Con09 PD4	Categoría 6	18	Normal
Pach Panel Consultorios_2 PD13	Placa de pared Con10 PD1	Categoría 6	22	Normal
Pach Panel Consultorios_2 PD14	Placa de pared Con10 PD2	Categoría 6	22	Normal
Pach Panel Consultorios_2 PD21	Placa de pared Con10 PD3	Categoría 6	22	Normal
Pach Panel Consultorios_2 PD15	Placa de pared Con11 PD1	Categoría 6	12	Normal
Pach Panel Consultorios_2 PD16	Placa de pared Con11 PD2	Categoría 6	12	Normal
Pach Panel Consultorios_2 PD17	Placa de pared Con11 PD3	Categoría 6	12	Normal
Pach Panel Consultorios_2 PD18	Placa de pared Con11 PD4	Categoría 6	12	Normal
Placa de pared Con06 J1	PC-CO17	Categoría 6	2	Normal
Placa de pared Con06 J2	AC-6	Categoría 6	6	Normal
Placa de pared Con06 J3	PC-CO18	Categoría 6	6	Normal
Placa de pared Con06 J4	PC-CO19	Categoría 6	9	Normal
Placa de pared Con07 J1	PC-CO20	Categoría 6	3	Normal

Placa de pared Con07 J2	PC-CO21	Categoría 6	2	Normal
Placa de pared Con07 J3	PC-CO22	Categoría 6	5	Normal
Placa de pared Con08 J1	PC-CO23	Categoría 6	3	Normal
Placa de pared Con08 J2	PC-CO24	Categoría 6	5	Normal
Placa de pared Con08 J3	PC-CO25	Categoría 6	4	Normal
Placa de pared Con08 J4	AC-7	Categoría 6	1	Normal
Placa de pared Con09 J1	PC-CO26	Categoría 6	5	Normal
Placa de pared Con09 J2	PC-CO27	Categoría 6	2	Normal
Placa de pared Con09 J3	PC-CO28	Categoría 6	2	Normal
Placa de pared Con09 J4	TEL-4	Categoría 6	4	Normal
Placa de pared Con10 J1	PC-CO29	Categoría 6	3	Normal
Placa de pared Con10 J2	PC-CO30	Categoría 6	3	Normal
Placa de pared Con10 J3	AC-8	Categoría 6	7	Normal
Placa de pared Con11 J1	PC-CO31	Categoría 6	7	Normal
Placa de pared Con11 J2	PC-CO32	Categoría 6	6	Normal
Placa de pared Con11 J3	PC-CO33	Categoría 6	2	Normal
Placa de pared Con11 J4	PC-CO34	Categoría 6	4	Normal
Farmacia 416mts, 88 rj45				
Switch Farmacia F0/1	Pach Panel Farmacia J1	Categoría 6	1	Normal
Switch Farmacia F0/2	Pach Panel Farmacia J2	Categoría 6	1	Normal
Switch Farmacia F0/3	Pach Panel Farmacia J3	Categoría 6	1	Normal
Switch Farmacia F0/4	Pach Panel Farmacia J4	Categoría 6	1	Normal
Switch Farmacia F0/5	Pach Panel Farmacia J5	Categoría 6	1	Normal
Switch Farmacia F0/6	Pach Panel Farmacia J6	Categoría 6	1	Normal
Switch Farmacia F0/7	Pach Panel Farmacia J7	Categoría 6	1	Normal
Switch Farmacia F0/8	Pach Panel Farmacia J8	Categoría 6	1	Normal
Switch Farmacia F0/9	Pach Panel Farmacia J9	Categoría 6	1	Normal
Switch Farmacia F0/10	Pach Panel Farmacia J10	Categoría 6	1	Normal
Switch Farmacia F0/11	Pach Panel Farmacia J11	Categoría 6	1	Normal
Switch Farmacia F0/12	Pach Panel Farmacia J12	Categoría 6	1	Normal
Switch Farmacia F0/13	Pach Panel Farmacia J13	Categoría 6	1	Normal

Switch Farmacia F0/14	Pach Panel Farmacia J14	Categoría 6	1	Normal
Switch Farmacia F0/15	Pach Panel Farmacia J15	Categoría 6	1	Normal
Switch Farmacia F0/16	Pach Panel Farmacia J16	Categoría 6	1	Normal
Switch Farmacia F0/18	Pach Panel Farmacia J18	Categoría 6	1	Normal
Switch Farmacia F0/19	Pach Panel Farmacia J19	Categoría 6	1	Normal
Switch Farmacia F0/21	Pach Panel Farmacia J21	Categoría 6	1	Normal
Switch Farmacia F0/22	Pach Panel Farmacia J22	Categoría 6	1	Normal
Switch Farmacia F0/23	Pach Panel Farmacia J23	Categoría 6	1	Normal
Switch Farmacia F0/24	Pach Panel Farmacia J24	Categoría 6	1	Normal
Pach Panel Farmacia PD1	Placa de pared Far01 PD1	Categoría 6	6	Normal
Pach Panel Farmacia PD2	Placa de pared Far01 PD2	Categoría 6	6	Normal
Pach Panel Farmacia PD3	Placa de pared Far01 PD3	Categoría 6	6	Normal
Pach Panel Farmacia PD4	Placa de pared Far01 PD4	Categoría 6	6	Normal
Pach Panel Farmacia PD5	Placa de pared Far02 PD1	Categoría 6	10	Normal
Pach Panel Farmacia PD6	Placa de pared Far02 PD2	Categoría 6	10	Normal
Pach Panel Farmacia PD7	Placa de pared Far02 PD3	Categoría 6	10	Normal
Pach Panel Farmacia PD18	Placa de pared Far02 PD4	Categoría 6	10	Normal
Pach Panel Farmacia PD21	Placa de pared Far03 PD1	Categoría 6	5	Normal
Pach Panel Farmacia PD8	Placa de pared Far03 PD2	Categoría 6	5	Normal
Pach Panel Farmacia PD9	Placa de pared Far03 PD3	Categoría 6	5	Normal
Pach Panel Farmacia PD22	Placa de pared Far03 PD4	Categoría 6	5	Normal
Pach Panel Farmacia PD10	Placa de pared Far04 PD1	Categoría 6	26	Normal
Pach Panel Farmacia PD11	Placa de pared Far04 PD2	Categoría 6	26	Normal
Pach Panel Farmacia PD23	Placa de pared Far04 PD3	Categoría 6	26	Normal

Pach Panel Farmacia PD24	Placa de pared Far04 PD4	Categoría 6	26	Normal
Pach Panel Farmacia PD12	Placa de pared Far05 PD1	Categoría 6	15	Normal
Pach Panel Farmacia PD13	Placa de pared Far05 PD2	Categoría 6	15	Normal
Pach Panel Farmacia PD14	Placa de pared Far05 PD3	Categoría 6	15	Normal
Pach Panel Farmacia PD15	Placa de pared Far05 PD4	Categoría 6	15	Normal
Pach Panel Farmacia PD16	Placa de pared Far06 PD1	Categoría 6	10	Normal
Pach Panel Farmacia PD19	Placa de pared Far06 PD2	Categoría 6	10	Normal
Placa de pared Far01 J1	PC-FA1	Categoría 6	4	Normal
Placa de pared Far01 J2	PC-FA2	Categoría 6	4	Normal
Placa de pared Far01 J3	PC-FA3	Categoría 6	5	Normal
Placa de pared Far01 J4	PC-FA4	Categoría 6	5	Normal
Placa de pared Far02 J1	PC-FA5	Categoría 6	4	Normal
Placa de pared Far02 J2	PC-FA6	Categoría 6	5	Normal
Placa de pared Far02 J3	PC-FA7	Categoría 6	5	Normal
Placa de pared Far02 J4	AC-9	Categoría 6	8	Normal
Placa de pared Far03 J1	TEL-5	Categoría 6	11	Normal
Placa de pared Far03 J2	PC-IM8	Categoría 6	6	Normal
Placa de pared Far03 J3	PC-IM9	Categoría 6	4	Normal
Placa de pared Far03 J4	TEL-7	Categoría 6	5	Normal
Placa de pared Far04 J1	PC-IM1	Categoría 6	12	Normal
Placa de pared Far04 J2	PC-IM7	Categoría 6	4	Normal
Placa de pared Far04 J3	TEL-6	Categoría 6	3	Normal
Placa de pared Far04 J4	TEL-8	Categoría 6	13	Normal
Placa de pared Far05 J1	PC-IM2	Categoría 6	6	Normal

Placa de pared Far05 J2	PC-IM3	Categoría 6	4	Normal
Placa de pared Far05 J3	PC-IM4	Categoría 6	3	Normal
Placa de pared Far05 J4	PC-IM5	Categoría 6	6	Normal
Placa de pared Far06 J1	PC-IM6	Categoría 6	4	Normal
Placa de pared Far06 J2	AC-10	Categoría 6	5	Normal
Almacén 299mts, 44 rj45				
Switch Almacén F0/1	Pach Panel Almacén J1	Categoría 6	1	Normal
Switch Almacén F0/2	Pach Panel Almacén J2	Categoría 6	1	Normal
Switch Almacén F0/3	Pach Panel Almacén J3	Categoría 6	1	Normal
Switch Almacén F0/4	Pach Panel Almacén J4	Categoría 6	1	Normal
Switch Almacen F0/5	Pach Panel Almacen J5	Categoría 6	1	Normal
Switch Almacén F0/6	Pach Panel Almacén J6	Categoría 6	1	Normal
Switch Almacén F0/18	Pach Panel Almacén J18	Categoría 6	1	Normal
Switch Almacén F0/19	Pach Panel Almacén J19	Categoría 6	1	Normal
Switch Almacén F0/20	Pach Panel Almacén J20	Categoría 6	1	Normal
Switch Almacén F0/21	Pach Panel Almacén J21	Categoría 6	1	Normal
Switch Almacén F0/22	Pach Panel Almacén J22	Categoría 6	1	Normal
Pach Panel Almacén PD1	Placa de pared Alm01 PD1	Categoría 6	14	Normal
Pach Panel Almacén PD2	Placa de pared Alm01 PD2	Categoría 6	14	Normal
Pach Panel Almacén PD3	Placa de pared Alm01 PD3	Categoría 6	14	Normal
Pach Panel Almacén PD18	Placa de pared Alm01 PD4	Categoría 6	14	Normal
Pach Panel Almacén PD4	Placa de pared Alm02 PD1	Categoría 6	25	Normal
Pach Panel Almacén PD19	Placa de pared Alm02 PD2	Categoría 6	25	Normal
Pach Panel Almacén PD20	Placa de pared Alm02 PD3	Categoría 6	25	Normal
Pach Panel Almacén PD5	Placa de pared Alm03 PD1	Categoría 6	17	Normal
Pach Panel Almacén PD6	Placa de pared Alm03 PD2	Categoría 6	17	Normal
Pach Panel Almacén PD21	Placa de pared Alm03 PD3	Categoría 6	17	Normal
Pach Panel Almacén PD22	Placa de pared Alm03 PD4	Categoría 6	17	Normal
Placa de pared Alm01 J1	PC-AL1	Categoría 6	15	Normal
Placa de pared Alm01 J2	PC-AL2	Categoría 6	6	Normal
Placa de pared Alm01 J3	PC-AL3	Categoría 6	9	Normal

Placa de pared Alm01 J4	AC-11	Categoría 6	6	Normal
Placa de pared Alm02 J1	PC-AL4	Categoría 6	12	Normal
Placa de pared Alm02 J2	AC-16	Categoría 6	5	Normal
Placa de pared Alm02 J3	AC-15	Categoría 6	24	Normal
Placa de pared Alm03 J1	PC-AL5	Categoría 6	3	Normal
Placa de pared Alm03 J2	PC-AL6	Categoría 6	3	Normal
Placa de pared Alm03 J3	AC-12	Categoría 6	2	Normal
Placa de pared Alm03 J4	TEL-9	Categoría 6	4	Normal
Fichaje 193mts, 84 rj45				
Switch Fichaje F0/1	Pach Panel Fichaje J1	Categoría 6	1	Normal
Switch Fichaje F0/2	Pach Panel Fichaje J2	Categoría 6	1	Normal
Switch Fichaje F0/3	Pach Panel Fichaje J3	Categoría 6	1	Normal
Switch Fichaje F0/4	Pach Panel Fichaje J4	Categoría 6	1	Normal
Switch Fichaje F0/5	Pach Panel Fichaje J5	Categoría 6	1	Normal
Switch Fichaje F0/6	Pach Panel Fichaje J6	Categoría 6	1	Normal
Switch Fichaje F0/7	Pach Panel Fichaje J7	Categoría 6	1	Normal
Switch Fichaje F0/8	Pach Panel Fichaje J8	Categoría 6	1	Normal
Switch Fichaje F0/9	Pach Panel Fichaje J9	Categoría 6	1	Normal
Switch Fichaje F0/10	Pach Panel Fichaje J10	Categoría 6	1	Normal
Switch Fichaje F0/11	Pach Panel Fichaje J11	Categoría 6	1	Normal
Switch Fichaje F0/12	Pach Panel Fichaje J12	Categoría 6	1	Normal
Switch Fichaje F0/13	Pach Panel Fichaje J13	Categoría 6	1	Normal
Switch Fichaje F0/14	Pach Panel Fichaje J14	Categoría 6	1	Normal
Switch Fichaje F0/15	Pach Panel Fichaje J15	Categoría 6	1	Normal
Switch Fichaje F0/16	Pach Panel Fichaje J16	Categoría 6	1	Normal
Switch Fichaje F0/17	Pach Panel Fichaje J17	Categoría 6	1	Normal
Switch Fichaje F0/18	Pach Panel Fichaje J18	Categoría 6	1	Normal
Switch Fichaje F0/19	Pach Panel Fichaje J19	Categoría 6	1	Normal
Switch Fichaje F0/22	Pach Panel Fichaje J22	Categoría 6	1	Normal
Switch Fichaje F0/23	Pach Panel Fichaje J23	Categoría 6	1	Normal
Pach Panel Fichaje PD1	Placa de pared Fic01 PD1	Categoría 6	6	Normal

Pach Panel Fichaje PD2	Placa de pared Fic01 PD2	Categoría 6	6	Normal
Pach Panel Fichaje PD3	Placa de pared Fic01 PD3	Categoría 6	6	Normal
Pach Panel Fichaje PD4	Placa de pared Fic01 PD4	Categoría 6	6	Normal
Pach Panel Fichaje PD5	Placa de pared Fic02 PD1	Categoría 6	4	Normal
Pach Panel Fichaje PD6	Placa de pared Fic02 PD2	Categoría 6	4	Normal
Pach Panel Fichaje PD8	Placa de pared Fic02 PD4	Categoría 6	4	Normal
Pach Panel Fichaje PD9	Placa de pared Fic03 PD1	Categoría 6	3	Normal
Pach Panel Fichaje PD10	Placa de pared Fic03 PD2	Categoría 6	3	Normal
Pach Panel Fichaje PD11	Placa de pared Fic03 PD3	Categoría 6	3	Normal
Pach Panel Fichaje PD22	Placa de pared Fic03 PD4	Categoría 6	3	Normal
Pach Panel Fichaje PD12	Placa de pared Fic04 PD1	Categoría 6	6	Normal
Pach Panel Fichaje PD13	Placa de pared Fic04 PD2	Categoría 6	6	Normal
Pach Panel Fichaje PD14	Placa de pared Fic04 PD3	Categoría 6	6	Normal
Pach Panel Fichaje PD19	Placa de pared Fic04 PD4	Categoría 6	6	Normal
Pach Panel Fichaje PD15	Placa de pared Fic05 PD1	Categoría 6	9	Normal
Pach Panel Fichaje PD16	Placa de pared Fic05 PD2	Categoría 6	9	Normal
Pach Panel Fichaje PD17	Placa de pared Fic05 PD3	Categoría 6	9	Normal
Pach Panel Fichaje PD18	Placa de pared Fic06 PD1	Categoría 6	11	Normal
Pach Panel Fichaje PD23	Placa de pared Fic06 PD2	Categoría 6	11	Normal
Placa de pared Fic01 J1	PC-FI3	Categoría 6	3	Normal
Placa de pared Fic01 J2	PC-FI11	Categoría 6	4	Normal
Placa de pared Fic01 J3	PC-FI5	Categoría 6	3	Normal
Placa de pared Fic01 J4	PC-FI15	Categoría 6	4	Normal
Placa de pared Fic02 J1	PC-FI16	Categoría 6	2	Normal
Placa de pared Fic02 J2	PC-FI17	Categoría 6	1	Normal
Placa de pared Fic02 J4	PC-FI2	Categoría 6	7	Normal
Placa de pared Fic03 J1	PC-FI4	Categoría 6	2	Normal
Placa de pared Fic03 J2	PC-FI10	Categoría 6	1	Normal
Placa de pared Fic03 J3	PC-FI14	Categoría 6	2	Normal
Placa de pared Fic03 J4	TEL-11	Categoría 6	2	Normal
Placa de pared Fic04 J1	PC-FI7	Categoría 6	2	Normal

Placa de pared Fic04 J2	PC-FI6	Categoría 6	2	Normal
Placa de pared Fic04 J3	PC-FI8	Categoría 6	3	Normal
Placa de pared Fic04 J4	AC-13	Categoría 6	2	Normal
Placa de pared Fic05 J1	PC-FI13	Categoría 6	3	Normal
Placa de pared Fic05 J2	PC-FI9	Categoría 6	2	Normal
Placa de pared Fic05 J3	PC-FI12	Categoría 6	2	Normal
Placa de pared Fic06 J1	PC-FI1	Categoría 6	2	Normal
Placa de pared Fic06 J2	TEL-10	Categoría 6	2	Normal
Recursos Humanos 338mts, 80 rj45				
Switch RecursosHumanos F0/1	Pach Panel RecursosHumanos J1	Categoría 6	1	Normal
Switch RecursosHumanos F0/2	Pach Panel RecursosHumanos J2	Categoría 6	1	Normal
Switch RecursosHumanos F0/3	Pach Panel RecursosHumanos J3	Categoría 6	1	Normal
Switch RecursosHumanos F0/4	Pach Panel RecursosHumanos J4	Categoría 6	1	Normal
Switch RecursosHumanos F0/5	Pach Panel RecursosHumanos J5	Categoría 6	1	Normal
Switch RecursosHumanos F0/6	Pach Panel RecursosHumanos J6	Categoría 6	1	Normal
Switch RecursosHumanos F0/7	Pach Panel RecursosHumanos J7	Categoría 6	1	Normal
Switch RecursosHumanos F0/8	Pach Panel RecursosHumanos J8	Categoría 6	1	Normal
Switch RecursosHumanos F0/9	Pach Panel RecursosHumanos J9	Categoría 6	1	Normal
Switch RecursosHumanos F0/10	Pach Panel RecursosHumanos J10	Categoría 6	1	Normal
Switch RecursosHumanos F0/11	Pach Panel RecursosHumanos J11	Categoría 6	1	Normal

Switch RecursosHumanos F0/12	Pach Panel RecursosHumanos J12	Categoría 6	1	Normal
Switch RecursosHumanos F0/13	Pach Panel RecursosHumanos J13	Categoría 6	1	Normal
Switch RecursosHumanos F0/14	Pach Panel RecursosHumanos J14	Categoría 6	1	Normal
Switch RecursosHumanos F0/15	Pach Panel RecursosHumanos J15	Categoría 6	1	Normal
Switch RecursosHumanos F0/16	Pach Panel RecursosHumanos J16	Categoría 6	1	Normal
Switch RecursosHumanos F0/17	Pach Panel RecursosHumanos J17	Categoría 6	1	Normal
Switch RecursosHumanos F0/21	Pach Panel RecursosHumanos J21	Categoría 6	1	Normal
Switch RecursosHumanos F0/23	Pach Panel RecursosHumanos J23	Categoría 6	1	Normal
Switch RecursosHumanos F0/24	Pach Panel RecursosHumanos J24	Categoría 6	1	Normal
Pach Panel RecursosHumanos PD1	Placa de pared Rec01 PD1	Categoría 6	7	Normal
Pach Panel RecursosHumanos PD2	Placa de pared Rec01 PD2	Categoría 6	7	Normal
Pach Panel RecursosHumanos PD3	Placa de pared Rec01 PD3	Categoría 6	7	Normal
Pach Panel RecursosHumanos PD4	Placa de pared Rec01 PD4	Categoría 6	7	Normal
Pach Panel RecursosHumanos PD5	Placa de pared Rec02 PD1	Categoría 6	5	Normal
Pach Panel RecursosHumanos PD6	Placa de pared Rec02 PD2	Categoría 6	5	Normal

Pach Panel RecursosHumanos PD21	Placa de pared Rec02 PD3	Categoría 6	5	Normal
Pach Panel RecursosHumanos PD23	Placa de pared Rec02 PD4	Categoría 6	5	Normal
Pach Panel RecursosHumanos PD7	Placa de pared Rec03 PD1	Categoría 6	11	Normal
Pach Panel RecursosHumanos PD8	Placa de pared Rec03 PD2	Categoría 6	11	Normal
Pach Panel RecursosHumanos PD9	Placa de pared Rec04 PD1	Categoría 6	13	Normal
Pach Panel RecursosHumanos PD10	Placa de pared Rec04 PD2	Categoría 6	13	Normal
Pach Panel RecursosHumanos PD11	Placa de pared Rec04 PD3	Categoría 6	13	Normal
Pach Panel RecursosHumanos PD12	Placa de pared Rec05 PD1	Categoría 6	17	Normal
Pach Panel RecursosHumanos PD13	Placa de pared Rec05 PD2	Categoría 6	17	Normal
Pach Panel RecursosHumanos PD14	Placa de pared Rec05 PD3	Categoría 6	17	Normal
Pach Panel RecursosHumanos PD24	Placa de pared Rec05 PD4	Categoría 6	17	Normal
Pach Panel RecursosHumanos PD15	Placa de pared Rec06 PD1	Categoría 6	20	Normal
Pach Panel RecursosHumanos PD16	Placa de pared Rec06 PD2	Categoría 6	20	Normal
Pach Panel RecursosHumanos PD17	Placa de pared Rec06 PD3	Categoría 6	20	Normal
Placa de pared Rec01 J1	PC-RE1	Categoría 6	5	Normal
Placa de pared Rec01 J2	PC-RE2	Categoría 6	5	Normal
Placa de pared Rec01 J3	PC-RE3	Categoría 6	6	Normal

Placa de pared Rec01 J4	PC-RE4	Categoría 6	4	Normal
Placa de pared Rec02 J1	PC-RE10	Categoría 6	3	Normal
Placa de pared Rec02 J2	PC-RE11	Categoría 6	2	Normal
Placa de pared Rec02 J3	AC-14	Categoría 6	8	Normal
Placa de pared Rec02 J4	TEL-12	Categoría 6	8	Normal
Placa de pared Rec03 J1	PC-RE5	Categoría 6	4	Normal
Placa de pared Rec03 J2	PC-RE6	Categoría 6	5	Normal
Placa de pared Rec04 J1	PC-RE7	Categoría 6	3	Normal
Placa de pared Rec04 J2	PC-RE8	Categoría 6	4	Normal
Placa de pared Rec04 J3	PC-RE9	Categoría 6	3	Normal
Placa de pared Rec05 J1	PC-RE12	Categoría 6	3	Normal
Placa de pared Rec05 J2	PC-RE13	Categoría 6	3	Normal
Placa de pared Rec05 J3	PC-RE16	Categoría 6	4	Normal
Placa de pared Rec05 J4	TEL-13	Categoría 6	4	Normal
Placa de pared Rec06 J1	PC-RE17	Categoría 6	3	Normal
Placa de pared Rec06 J2	PC-RE15	Categoría 6	2	Normal
Placa de pared Rec06 J3	PC-RE14	Categoría 6	2	Normal
Administracion_1 247mts, 88 rj45				
Switch Administracion_1 F0/1	Pach Panel Administracion_1 J1	Categoría 6	1	Normal
Switch Administracion_1 F0/2	Pach Panel Administracion_1 J2	Categoría 6	1	Normal
Switch Administracion_1 F0/3	Pach Panel Administracion_1 J3	Categoría 6	1	Normal
Switch Administracion_1 F0/4	Pach Panel Administracion_1 J4	Categoría 6	1	Normal
Switch Administracion_1 F0/5	Pach Panel Administracion_1 J5	Categoría 6	1	Normal
Switch Administracion_1 F0/6	Pach Panel Administracion_1 J6	Categoría 6	1	Normal

Switch Administracion_1 F0/7	Pach Panel Administracion_1 J7	Categoría 6	1	Normal
Switch Administracion_1 F0/8	Pach Panel Administracion_1 J8	Categoría 6	1	Normal
Switch Administracion_1 F0/9	Pach Panel Administracion_1 J9	Categoría 6	1	Normal
Switch Administracion_1 F0/10	Pach Panel Administracion_1 J10	Categoría 6	1	Normal
Switch Administracion_1 F0/11	Pach Panel Administracion_1 J11	Categoría 6	1	Normal
Switch Administracion_1 F0/12	Pach Panel Administracion_1 J12	Categoría 6	1	Normal
Switch Administracion_1 F0/13	Pach Panel Administracion_1 J13	Categoría 6	1	Normal
Switch Administracion_1 F0/14	Pach Panel Administracion_1 J14	Categoría 6	1	Normal
Switch Administracion_1 F0/15	Pach Panel Administracion_1 J15	Categoría 6	1	Normal
Switch Administracion_1 F0/16	Pach Panel Administracion_1 J16	Categoría 6	1	Normal
Switch Administracion_1 F0/17	Pach Panel Administracion_1 J17	Categoría 6	1	Normal
Switch Administracion_1 F0/18	Pach Panel Administracion_1 J18	Categoría 6	1	Normal
Switch Administracion_1 F0/19	Pach Panel Administracion_1 J19	Categoría 6	1	Normal
Switch Administracion_1 F0/20	Pach Panel Administracion_1 J20	Categoría 6	1	Normal
Switch Administracion_1 F0/23	Pach Panel Administracion_1 J23	Categoría 6	1	Normal

Switch Administracion_1 F0/24	Pach Panel Administracion_1 J24	Categoría 6	1	Normal
Pach Panel Administracion_1 PD1	Placa de pared Adm01 PD1	Categoría 6	12	Normal
Pach Panel Administracion_1 PD2	Placa de pared Adm01 PD2	Categoría 6	12	Normal
Pach Panel Administracion_1 PD3	Placa de pared Adm01 PD3	Categoría 6	12	Normal
Pach Panel Administracion_1 PD4	Placa de pared Adm01 PD4	Categoría 6	12	Normal
Pach Panel Administracion_1 PD5	Placa de pared Adm02 PD1	Categoría 6	6	Normal
Pach Panel Administracion_1 PD6	Placa de pared Adm02 PD2	Categoría 6	6	Normal
Pach Panel Administracion_1 PD7	Placa de pared Adm02 PD3	Categoría 6	6	Normal
Pach Panel Administracion_1 PD8	Placa de pared Adm02 PD4	Categoría 6	6	Normal
Pach Panel Administracion_1 PD9	Placa de pared Adm03 PD1	Categoría 6	6	Normal
Pach Panel Administracion_1 PD10	Placa de pared Adm03 PD2	Categoría 6	6	Normal
Pach Panel Administracion_1 PD11	Placa de pared Adm03 PD3	Categoría 6	6	Normal
Pach Panel Administracion_1 PD23	Placa de pared Adm03 PD4	Categoría 6	6	Normal
Pach Panel Administracion_1 PD12	Placa de pared Adm04 PD1	Categoría 6	3	Normal
Pach Panel Administracion_1 PD13	Placa de pared Adm04 PD2	Categoría 6	3	Normal

Pach Panel Administracion_1 PD14	Placa de pared Adm04 PD3	Categoría 6	3	Normal
Pach Panel Administracion_1 PD15	Placa de pared Adm05 PD1	Categoría 6	8	Normal
Pach Panel Administracion_1 PD16	Placa de pared Adm05 PD2	Categoría 6	8	Normal
Pach Panel Administracion_1 PD17	Placa de pared Adm05 PD3	Categoría 6	8	Normal
Pach Panel Administracion_1 PD24	Placa de pared Adm05 PD4	Categoría 6	8	Normal
Pach Panel Administracion_1 PD18	Placa de pared Adm06 PD1	Categoría 6	8	Normal
Pach Panel Administracion_1 PD19	Placa de pared Adm06 PD2	Categoría 6	8	Normal
Pach Panel Administracion_1 PD20	Placa de pared Adm06 PD3	Categoría 6	8	Normal
Placa de pared Adm01 J1	PC-AD1	Categoría 6	3	Normal
Placa de pared Adm01 J2	PC-AD2	Categoría 6	2	Normal
Placa de pared Adm01 J3	PC-AD3	Categoría 6	2	Normal
Placa de pared Adm01 J4	PC-AD4	Categoría 6	1	Normal
Placa de pared Adm02 J1	PC-AD5	Categoría 6	9	Normal
Placa de pared Adm02 J2	PC-AD6	Categoría 6	3	Normal
Placa de pared Adm02 J3	PC-AD7	Categoría 6	3	Normal
Placa de pared Adm02 J4	PC-AD8	Categoría 6	2	Normal
Placa de pared Adm03 J1	PC-AD9	Categoría 6	3	Normal
Placa de pared Adm03 J2	PC-AD10	Categoría 6	3	Normal
Placa de pared Adm03 J3	PC-AD11	Categoría 6	4	Normal
Placa de pared Adm03 J4	TEL-15	Categoría 6	2	Normal
Placa de pared Adm04 J1	PC-AD12	Categoría 6	2	Normal
Placa de pared Adm04 J2	PC-AD13	Categoría 6	3	Normal
Placa de pared Adm04 J3	PC-AD14	Categoría 6	2	Normal

Placa de pared Adm05 J1	PC-AD15	Categoría 6	3	Normal
Placa de pared Adm05 J2	PC-AD19	Categoría 6	3	Normal
Placa de pared Adm05 J3	PC-AD20	Categoría 6	4	Normal
Placa de pared Adm05 J4	TEL-14	Categoría 6	2	Normal
Placa de pared Adm06 J1	PC-AD16	Categoría 6	3	Normal
Placa de pared Adm06 J2	PC-AD17	Categoría 6	2	Normal
Placa de pared Adm06 J3	PC-AD18	Categoría 6	3	Normal
Administracion_2 245mts, 80 rj45				
Switch Administracion_2 F0/1	Pach Panel Administracion_2 J1	Categoría 6	1	Normal
Switch Administracion_2 F0/2	Pach Panel Administracion_2 J2	Categoría 6	1	Normal
Switch Administracion_2 F0/3	Pach Panel Administracion_2 J3	Categoría 6	1	Normal
Switch Administracion_2 F0/4	Pach Panel Administracion_2 J4	Categoría 6	1	Normal
Switch Administracion_2 F0/5	Pach Panel Administracion_2 J5	Categoría 6	1	Normal
Switch Administracion_2 F0/6	Pach Panel Administracion_2 J6	Categoría 6	1	Normal
Switch Administracion_2 F0/7	Pach Panel Administracion_2 J7	Categoría 6	1	Normal
Switch Administracion_2 F0/8	Pach Panel Administracion_2 J8	Categoría 6	1	Normal
Switch Administracion_2 F0/9	Pach Panel Administracion_2 J9	Categoría 6	1	Normal
Switch Administracion_2 F0/10	Pach Panel Administracion_2 J10	Categoría 6	1	Normal
Switch Administracion_2 F0/11	Pach Panel Administracion_2 J11	Categoría 6	1	Normal

Switch Administracion_2 F0/12	Pach Panel Administracion_2 J12	Categoría 6	1	Normal
Switch Administracion_2 F0/13	Pach Panel Administracion_2 J13	Categoría 6	1	Normal
Switch Administracion_2 F0/14	Pach Panel Administracion_2 J14	Categoría 6	1	Normal
Switch Administracion_2 F0/15	Pach Panel Administracion_2 J15	Categoría 6	1	Normal
Switch Administracion_2 F0/16	Pach Panel Administracion_2 J16	Categoría 6	1	Normal
Switch Administracion_2 F0/17	Pach Panel Administracion_2 J17	Categoría 6	1	Normal
Switch Administracion_2 F0/18	Pach Panel Administracion_2 J18	Categoría 6	1	Normal
Switch Administracion_2 F0/23	Pach Panel Administracion_2 J23	Categoría 6	1	Normal
Switch Administracion_2 F0/24	Pach Panel Administracion_2 J24	Categoría 6	1	Normal
Pach Panel Administracion_2 PD1	Placa de pared Adm07 PD1	Categoría 6	13	Normal
Pach Panel Administracion_2 PD2	Placa de pared Adm07 PD2	Categoría 6	13	Normal
Pach Panel Administracion_2 PD3	Placa de pared Adm07 PD3	Categoría 6	13	Normal
Pach Panel Administracion_2 PD4	Placa de pared Adm08 PD1	Categoría 6	12	Normal
Pach Panel Administracion_2 PD5	Placa de pared Adm08 PD2	Categoría 6	12	Normal
Pach Panel Administracion_2 PD6	Placa de pared Adm08 PD3	Categoría 6	12	Normal

Pach Panel Administracion_2 PD23	Placa de pared Adm08 PD4	Categoría 6	12	Normal
Pach Panel Administracion_2 PD7	Placa de pared Adm09 PD1	Categoría 6	7	Normal
Pach Panel Administracion_2 PD8	Placa de pared Adm09 PD2	Categoría 6	7	Normal
Pach Panel Administracion_2 PD9	Placa de pared Adm09 PD3	Categoría 6	7	Normal
Pach Panel Administracion_2 PD10	Placa de pared Adm10 PD1	Categoría 6	3	Normal
Pach Panel Administracion_2 PD11	Placa de pared Adm10 PD2	Categoría 6	3	Normal
Pach Panel Administracion_2 PD12	Placa de pared Adm10 PD3	Categoría 6	3	Normal
Pach Panel Administracion_2 PD13	Placa de pared Adm11 PD1	Categoría 6	5	Normal
Pach Panel Administracion_2 PD14	Placa de pared Adm11 PD2	Categoría 6	5	Normal
Pach Panel Administracion_2 PD15	Placa de pared Adm11 PD3	Categoría 6	5	Normal
Pach Panel Administracion_2 PD16	Placa de pared Adm12 PD1	Categoría 6	8	Normal
Pach Panel Administracion_2 PD17	Placa de pared Adm12 PD2	Categoría 6	8	Normal
Pach Panel Administracion_2 PD18	Placa de pared Adm12 PD3	Categoría 6	8	Normal
Pach Panel Administracion_2 PD24	Placa de pared Adm12 PD4	Categoría 6	8	Normal
Placa de pared Adm07 J1	PC-AD24	Categoría 6	3	Normal
Placa de pared Adm07 J2	PC-AD25	Categoría 6	3	Normal
Placa de pared Adm07 J3	PC-AD26	Categoría 6	2	Normal

Placa de pared Adm08 J1	PC-AD27	Categoría 6	3	Normal
Placa de pared Adm08 J2	PC-AD28	Categoría 6	3	Normal
Placa de pared Adm08 J3	PC-AD29	Categoría 6	2	Normal
Placa de pared Adm08 J4	TEL-16	Categoría 6	3	Normal
Placa de pared Adm09 J1	PC-AD30	Categoría 6	3	Normal
Placa de pared Adm09 J2	PC-AD31	Categoría 6	2	Normal
Placa de pared Adm09 J3	PC-AD32	Categoría 6	2	Normal
Placa de pared Adm10 J1	PC-AD33	Categoría 6	2	Normal
Placa de pared Adm10 J2	PC-AD34	Categoría 6	3	Normal
Placa de pared Adm10 J3	PC-AD35	Categoría 6	2	Normal
Placa de pared Adm11 J1	PC-AD21	Categoría 6	4	Normal
Placa de pared Adm11 J2	PC-AD22	Categoría 6	4	Normal
Placa de pared Adm11 J3	PC-AD23	Categoría 6	3	Normal
Placa de pared Adm12 J1	PC-AD36	Categoría 6	4	Normal
Placa de pared Adm12 J2	PC-AD37	Categoría 6	3	Normal
Placa de pared Adm12 J3	PC-AD38	Categoría 6	5	Normal
Placa de pared Adm12 J4	TEL-17	Categoría 6	5	Normal
1er Piso 721mts, 72 rj45				
Switch 1erPiso F0/1	Pach Panel 1erPiso J1	Categoría 6	1	Normal
Switch 1erPiso F0/2	Pach Panel 1erPiso J2	Categoría 6	1	Normal
Switch 1erPiso F0/3	Pach Panel 1erPiso J3	Categoría 6	1	Normal
Switch 1erPiso F0/4	Pach Panel 1erPiso J4	Categoría 6	1	Normal
Switch 1erPiso F0/5	Pach Panel 1erPiso J5	Categoría 6	1	Normal
Switch 1erPiso F0/6	Pach Panel 1erPiso J6	Categoría 6	1	Normal
Switch 1erPiso F0/7	Pach Panel 1erPiso J7	Categoría 6	1	Normal
Switch 1erPiso F0/8	Pach Panel 1erPiso J8	Categoría 6	1	Normal
Switch 1erPiso F0/9	Pach Panel 1erPiso J9	Categoría 6	1	Normal
Switch 1erPiso F0/10	Pach Panel 1erPiso J10	Categoría 6	1	Normal
Switch 1erPiso F0/11	Pach Panel 1erPiso J11	Categoría 6	1	Normal
Switch 1erPiso F0/12	Pach Panel 1erPiso J12	Categoría 6	1	Normal
Switch 1erPiso F0/13	Pach Panel 1erPiso J13	Categoría 6	1	Normal

Switch 1erPiso F0/20	Pach Panel 1erPiso J20	Categoría 6	1	Normal
Switch 1erPiso F0/21	Pach Panel 1erPiso J21	Categoría 6	1	Normal
Switch 1erPiso F0/22	Pach Panel 1erPiso J22	Categoría 6	1	Normal
Switch 1erPiso F0/23	Pach Panel 1erPiso J23	Categoría 6	1	Normal
Switch 1erPiso F0/24	Pach Panel 1erPiso J24	Categoría 6	1	Normal
Pach Panel 1erPiso PD1	Placa de pared 1er01 PD1	Categoría 6	49	Normal
Pach Panel 1erPiso PD2	Placa de pared 1er01 PD2	Categoría 6	49	Normal
Pach Panel 1erPiso PD20	Placa de pared 1er01 PD3	Categoría 6	49	Normal
Pach Panel 1erPiso PD21	Placa de pared 1er01 PD4	Categoría 6	49	Normal
Pach Panel 1erPiso PD2	Placa de pared 1er02 PD1	Categoría 6	29	Normal
Pach Panel 1erPiso PD4	Placa de pared 1er02 PD2	Categoría 6	29	Normal
Pach Panel 1erPiso PD22	Placa de pared 1er02 PD3	Categoría 6	29	Normal
Pach Panel 1erPiso PD5	Placa de pared 1er03 PD1	Categoría 6	44	Normal
Pach Panel 1erPiso PD6	Placa de pared 1er03 PD2	Categoría 6	44	Normal
Pach Panel 1erPiso PD23	Placa de pared 1er03 PD3	Categoría 6	44	Normal
Pach Panel 1erPiso PD7	Placa de pared 1er04 PD1	Categoría 6	18	Normal
Pach Panel 1erPiso PD8	Placa de pared 1er04 PD2	Categoría 6	18	Normal
Pach Panel 1erPiso PD24	Placa de pared 1er04 PD3	Categoría 6	18	Normal
Pach Panel 1erPiso PD9	Placa de pared 1er05 PD1	Categoría 6	14	Normal
Pach Panel 1erPiso PD10	Placa de pared 1er05 PD2	Categoría 6	14	Normal
Pach Panel 1erPiso PD11	Placa de pared 1er05 PD3	Categoría 6	14	Normal
Pach Panel 1erPiso PD12	Placa de pared 1er06 PD1	Categoría 6	38	Normal
Pach Panel 1erPiso PD13	Placa de pared 1er06 PD2	Categoría 6	38	Normal
Placa de pared 1er01 J1	PC-1ER1	Categoría 6	4	Normal
Placa de pared 1er01 J2	PC-1ER2	Categoría 6	9	Normal
Placa de pared 1er01 J3	TEL-19	Categoría 6	5	Normal
Placa de pared 1er01 J4	TEL-18	Categoría 6	15	Normal
Placa de pared 1er02 J1	PC-1ER3	Categoría 6	12	Normal
Placa de pared 1er02 J2	PC-1ER4	Categoría 6	7	Normal
Placa de pared 1er02 J3	TEL-20	Categoría 6	11	Normal
Placa de pared 1er03 J1	PC-1ER6	Categoría 6	4	Normal

Placa de pared 1er03 J2	PC-1ER7	Categoría 6	3	Normal
Placa de pared 1er03 J3	TEL-22	Categoría 6	7	Normal
Placa de pared 1er04 J1	PC-1ER5	Categoría 6	2	Normal
Placa de pared 1er04 J2	PC-1ER8	Categoría 6	5	Normal
Placa de pared 1er04 J3	TEL-21	Categoría 6	8	Normal
Placa de pared 1er05 J1	PC-1ER12	Categoría 6	6	Normal
Placa de pared 1er05 J2	PC-1ER13	Categoría 6	3	Normal
Placa de pared 1er05 J3	PC-1ER9	Categoría 6	7	Normal
Placa de pared 1er06 J1	PC-1ER10	Categoría 6	7	Normal
Placa de pared 1er06 J2	PC-1ER11	Categoría 6	1	Normal
2do Piso 431mts, 48 rj45				
Switch 2doPiso F0/1	Pach Panel 2doPiso J1	Categoría 6	1	Normal
Switch 2doPiso F0/2	Pach Panel 2doPiso J2	Categoría 6	1	Normal
Switch 2doPiso F0/3	Pach Panel 2doPiso J3	Categoría 6	1	Normal
Switch 2doPiso F0/4	Pach Panel 2doPiso J4	Categoría 6	1	Normal
Switch 2doPiso F0/5	Pach Panel 2doPiso J5	Categoría 6	1	Normal
Switch 2doPiso F0/6	Pach Panel 2doPiso J6	Categoría 6	1	Normal
Switch 2doPiso F0/15	Pach Panel 2doPiso J15	Categoría 6	1	Normal
Switch 2doPiso F0/16	Pach Panel 2doPiso J16	Categoría 6	1	Normal
Switch 2doPiso F0/17	Pach Panel 2doPiso J17	Categoría 6	1	Normal
Switch 2doPiso F0/18	Pach Panel 2doPiso J18	Categoría 6	1	Normal
Switch 2doPiso F0/19	Pach Panel 2doPiso J19	Categoría 6	1	Normal
Switch 2doPiso F0/20	Pach Panel 2doPiso J20	Categoría 6	1	Normal
Pach Panel 2doPiso PD15	Placa de pared 2do01 PD1	Categoría 6	37	Normal
Pach Panel 2doPiso PD1	Placa de pared 2do01 PD2	Categoría 6	37	Normal
Pach Panel 2doPiso PD16	Placa de pared 2do01 PD3	Categoría 6	37	Normal
Pach Panel 2doPiso PD2	Placa de pared 2do02 PD1	Categoría 6	10	Normal
Pach Panel 2doPiso PD3	Placa de pared 2do02 PD2	Categoría 6	10	Normal
Pach Panel 2doPiso PD17	Placa de pared 2do02 PD3	Categoría 6	10	Normal
Pach Panel 2doPiso PD4	Placa de pared 2do02 PD4	Categoría 6	10	Normal
Pach Panel 2doPiso PD18	Placa de pared 2do03 PD1	Categoría 6	41	Normal

Pach Panel 2doPiso PD20	Placa de pared 2do03 PD2	Categoría 6	41	Normal
Pach Panel 2doPiso PD5	Placa de pared 2do03 PD3	Categoría 6	41	Normal
Pach Panel 2doPiso PD19	Placa de pared 2do04 PD1	Categoría 6	29	Normal
Pach Panel 2doPiso PD6	Placa de pared 2do04 PD2	Categoría 6	29	Normal
Placa de pared 2do01 J1	AC-20	Categoría 6	17	Normal
Placa de pared 2do01 J2	PC-2DO2	Categoría 6	7	Normal
Placa de pared 2do01 J3	AC-19	Categoría 6	5	Normal
Placa de pared 2do02 J1	PC-2DO1	Categoría 6	11	Normal
Placa de pared 2do02 J2	PC-2DO3	Categoría 6	1	Normal
Placa de pared 2do02 J3	AC-18	Categoría 6	5	Normal
Placa de pared 2do02 J4	PC-2DO4	Categoría 6	10	Normal
Placa de pared 2do03 J1	AC-21	Categoría 6	13	Normal
Placa de pared 2do03 J2	TEL-23	Categoría 6	2	Normal
Placa de pared 2do03 J3	PC-2DO6	Categoría 6	3	Normal
Placa de pared 2do04 J1	AC-17	Categoría 6	11	Normal
Placa de pared 2do04 J2	PC-2DO5	Categoría 6	2	Normal
3er Piso 326mts, 32 rj45				
Switch 3erPiso F0/1	Pach Panel 3erPiso J1	Categoría 6	1	Normal
Switch 3erPiso F0/2	Pach Panel 3erPiso J2	Categoría 6	1	Normal
Switch 3erPiso F0/3	Pach Panel 3erPiso J3	Categoría 6	1	Normal
Switch 3erPiso F0/4	Pach Panel 3erPiso J4	Categoría 6	1	Normal
Switch 3erPiso F0/5	Pach Panel 3erPiso J5	Categoría 6	1	Normal
Switch 3erPiso F0/6	Pach Panel 3erPiso J6	Categoría 6	1	Normal
Switch 3erPiso F0/20	Pach Panel 3erPiso J20	Categoría 6	1	Normal
Switch 3erPiso F0/21	Pach Panel 3erPiso J21	Categoría 6	1	Normal
Pach Panel 3erPiso PD15	Placa de pared 3er01 PD1	Categoría 6	37	Normal
Pach Panel 3erPiso PD1	Placa de pared 3er01 PD2	Categoría 6	37	Normal
Pach Panel 3erPiso PD2	Placa de pared 3er02 PD1	Categoría 6	17	Normal
Pach Panel 3erPiso PD3	Placa de pared 3er02 PD2	Categoría 6	17	Normal
Pach Panel 3erPiso PD4	Placa de pared 3er02 PD3	Categoría 6	17	Normal
Pach Panel 3erPiso PD5	Placa de pared 3er03 PD1	Categoría 6	48	Normal

Pach Panel 3erPiso PD21	Placa de pared 3er03 PD2	Categoría 6	48	Normal
Pach Panel 3erPiso PD6	Placa de pared 3er03 PD3	Categoría 6	48	Normal
Placa de pared 3er01 J1	TEL-24	Categoría 6	3	Normal
Placa de pared 3er01 J2	PC-3ER3	Categoría 6	2	Normal
Placa de pared 3er02 J1	PC-3ER4	Categoría 6	4	Normal
Placa de pared 3er02 J2	PC-3ER5	Categoría 6	2	Normal
Placa de pared 3er02 J3	PC-3ER6	Categoría 6	23	Normal
Placa de pared 3er03 J1	PC-3ER1	Categoría 6	6	Normal
Placa de pared 3er03 J2	TEL-25	Categoría 6	2	Normal
Placa de pared 3er03 J3	PC-3ER2	Categoría 6	7	Normal

Configuración de los switch para las VLAN para el hospital san juan de Dios

Switch Madre

Creación de las vlans en el switch

Switch>enable

Switch#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#vlan 10

Switch(config-vlan)#name Administrativos

Switch(config-vlan)#exit

Switch(config)#vlan 20

Switch(config-vlan)#name Consultas

Switch(config-vlan)#exit

Switch(config)#vlan 30

Switch(config-vlan)#name Emergencias

Switch(config-vlan)#exit

Switch(config)#vlan 40

Switch(config-vlan)#name Internacion

Switch(config-vlan)#exit

Switch(config)#vlan 50

Switch(config-vlan)#name Wifi

Enlaces en modo troncal

Switch(config-if)#interface gigabitEthernet 1/0/1

Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport trunk allowed vlan 10,20,30,40,50

Switch(config-if)#interface gigabitEthernet 1/0/2

Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport trunk allowed vlan 10,20,30,40,50

Switch(config)#interface gigabitEthernet 1/0/24

Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport trunk allowed vlan 10,20,30,40,50

Switch de Sistemas 1 y 2

Creación de las vlans en el switch

Switch>enable

Switch#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#vlan 10

Switch(config-vlan)#name Administrativos

Switch(config-vlan)#exit

Switch(config)#vlan 20

Switch(config-vlan)#name Consultas

Switch(config-vlan)#exit

Switch(config)#vlan 30

Switch(config-vlan)#name Emergencias

Switch(config-vlan)#exit

Switch(config)#vlan 40

Switch(config-vlan)#name Internacion

Switch(config-vlan)#exit

Switch(config)#vlan 50

Switch(config-vlan)#name Wifi

Enlaces en modo troncal

Vlan 30 y 50

Switch>enable

Switch# configure terminal

Switch(config)# interface range f0/1, f0/4, f0/5

Switch(config-if-range)# switchport mode trunk

Switch(config-if-range)# switchport trunk allowed vlan 30,50

Switch(config-if-range)# no shutdown

Switch(config-if-range)# exit

Switch(config)# exit

Switch# wr

Vlan 20 y 50

Switch# configure terminal

Switch(config)# interface range f0/2, f0/3, f0/6

Switch(config-if-range)# switchport mode trunk

Switch(config-if-range)# switchport trunk allowed vlan 20,50

Switch(config-if-range)# no shutdown

Switch(config-if-range)# exit

Switch(config)# exit

Switch# wr

Vlan 10 y 50

Switch# configure terminal

Switch(config)# interface range f0/7, f0/8, f0/9

Switch(config-if-range)# switchport mode trunk

Switch(config-if-range)# switchport trunk allowed vlan 10,50

Switch(config-if-range)# no shutdown

Switch(config-if-range)# exit

Switch(config)# exit

Switch# wr

Vlan 40 y 50

Switch# configure terminal

Switch(config)# interface range f0/10, f0/11, f0/12

Switch(config-if-range)# switchport mode trunk

Switch(config-if-range)# switchport trunk allowed vlan 40,50

Switch(config-if-range)# no shutdown

Switch(config-if-range)# exit

Switch# wr

Switch de Emergencia-Laboratorio

DHCP Principal Vlan 30 (comando para ver el dhcp Switch>show ip dhcp binding)

Modo trunk para conexión de switch

Switch>enable

Switch(config)#interface Gi0/1

Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport trunk allowed vlan 30,50

Switch(config-if)#no shutdown

Switch(config-if)#exit

Switch(config)#exit

Switch#wr

VLAN 30 Emergencias

CREACION DE LA VLAN

Switch> enable

Switch# configure terminal

Switch(config)# vlan 30 (numero de vlan)

Switch(config-vlan)# name Emergencias (nombre de vlan)

Switch(config-vlan)# exit

ASIGNAR PUERTOS ALA VLAN 30

Switch(config)# interface range fa0/1-17 (puertos del switch)

Switch(config-if-range)# switchport mode Access

Switch(config-if-range)# switchport Access vlan 30 (numero de vlan)

Switch(config-if-range)# no shutdown

Switch(config-if-range)# end

Switch# wr

ACTIVAR EL SERVICIO DHCP

Switch# configure terminal

Switch(config)# interface vlan 30 (numero de vlan)

Switch(config-if)# ip address 192.168.30.1 255.255.255.0 (puerta de enlace con mascara) Switch(config-if)# exit

Switch(config)# exit

Switch# wr

Crearemos un pool de DHCP para el direccionamiento 192.168.30.0

Switch# configure terminal

Switch(config)# ip dhcp pool vlan30 (numero de vlan)

Switch(dhcp-config)# network 192.168.30.0 255.255.255.0 (segmento de red 192.168.30.0)

Switch(dhcp-config)# default-router 192.168.30.1 (puerta de enlace)

Switch(dhcp-config)# dns-server 1.1.1.3 8.8.8.8 (si existe dns)

Switch(dhcp-config)# exit

Switch(config)# ip dhcp excluded-address 192.168.30.1 192.168.30.5 (opcional restriccion de ip)

Switch(config)# exit

Switch# wr

VLAN 50 Wifi

CREACION DE LA VLAN

Switch> enable

Switch# configure terminal

Switch(config)# vlan 50 (numero de vlan)

Switch(config-vlan)# name Wifi (nombre de vlan)

Switch(config-vlan)# exit

ASIGNAR PUERTOS ALA VLAN 50

Switch(config)# interface range fa0/18-20 (puertos del switch)

Switch(config-if-range)# switchport mode Access

Switch(config-if-range)# switchport Access vlan 50 (numero de vlan)

Switch(config-if-range)# no shutdown

Switch(config-if-range)# end

Switch# wr

ACTIVAR EL SERVICIO DHCP

Switch# configure terminal

Switch(config)# interface vlan 50 (numero de vlan)

Switch(config-if)# ip address 192.168.50.1 255.255.255.0 (puerta de enlace con mascara) Switch(config-if)# exit

Switch(config)# exit

Switch# wr

Crearemos un pool de DHCP para el direccionamiento 192.168.50.0

Switch# configure terminal

Switch(config)# ip dhcp pool vlan50 (numero de vlan)

Switch(dhcp-config)# network 192.168.50.0 255.255.255.0 (segmento de red 192.168.50.0)

Switch(dhcp-config)# default-router 192.168.50.1 (puerta de enlace)

Switch(dhcp-config)# dns-server 1.1.1.3 8.8.8.8 (si existe dns)

Switch(dhcp-config)# exit

Switch(config)# ip dhcp excluded-address 192.168.50.1 192.168.50.15 (opcional restriccion de ip)

Switch(config)# exit

Switch# wr

Switch de Consultorios_1

DHCP Principal Vlan 20 (comando para ver el dhcp Switch>show ip dhcp binding)

Modo trunk para conexión de switch

Switch>enable

Switch(config)#interface Gi0/1

Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport trunk allowed vlan 20,50

Switch(config-if)#no shutdown

Switch(config-if)#exit

Switch(config)#exit

Switch#wr

VLAN 20 Consultas

CREACION DE LA VLAN

Switch> enable

Switch# configure terminal

Switch(config)# vlan 20 (numero de vlan)

Switch(config-vlan)# name Consultas (nombre de vlan)

Switch(config-vlan)# exit

ASIGNAR PUERTOS ALA VLAN 20

Switch(config)# interface range fa0/1-18 (puertos del switch)

Switch(config-if-range)# switchport mode Access

Switch(config-if-range)# switchport Access vlan 20 (numero de vlan)

Switch(config-if-range)# no shutdown

Switch(config-if-range)# end

Switch# wr

ACTIVAR EL SERVICIO DHCP

Switch# configure terminal

Switch(config)# interface vlan 20 (numero de vlan)

Switch(config-if)# ip address 192.168.20.1 255.255.255.0 (puerta de enlace con mascara) Switch(config-if)# exit

Switch(config)# exit

Switch# wr

Crearemos un pool de DHCP para el direccionamiento 192.168.20.0

Switch# configure terminal

Switch(config)# ip dhcp pool vlan20 (numero de vlan)

Switch(dhcp-config)# network 192.168.20.0 255.255.255.0 (segmento de red 192.168.20.0)

Switch(dhcp-config)# default-router 192.168.20.1 (puerta de enlace)

Switch(dhcp-config)# dns-server 1.1.1.3 8.8.8.8 (si existe dns)

Switch(dhcp-config)# exit

Switch(config)# ip dhcp excluded-address 192.168.20.1 192.168.20.5 (opcional restriccion de ip)

Switch(config)# exit

Switch# wr

VLAN 50 Wifi

CREACION DE LA VLAN

Switch> enable

Switch# configure terminal

Switch(config)# vlan 50 (numero de vlan)

Switch(config-vlan)# name Wifi (nombre de vlan)

Switch(config-vlan)# exit

ASIGNAR PUERTOS ALA VLAN 50

Switch(config)# interface range fa0/19-21 (puertos del switch)

Switch(config-if-range)# switchport mode Access

Switch(config-if-range)# switchport Access vlan 50 (numero de vlan)

Switch(config-if-range)# no shutdown

Switch(config-if-range)# end

Switch# wr

HABILITAR LA INTERFAZ VLAN 50

Switch# configure terminal

Switch(config)# interface vlan 50

Switch(config-if)# ip address 192.168.50.2 255.255.255.0

Switch(config-if)# no shutdown

Switch(config-if)# exit

CONFIGURAR EL DHCP RELAY

Switch(config)# interface vlan 50

Switch(config-if)# ip helper-address 192.168.50.1

Switch(config-if)# exit

Switch(config)# exit

Switch# ping 192.168.50.1 (verificamos conexión con el dhcp)

Switch de Consultorios_2

modo trunk para conexión de switch

Switch>enable

Switch# configure terminal

Switch(config)# interface Gi0/1

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk allowed vlan 20,50

Switch(config-if)# no shutdown

Switch(config-if)# exit

Switch(config)# exit

Switch# wr

VLAN 20 Consultas

CREACION DE LA VLAN

Switch> enable

Switch# configure terminal

Switch(config)# vlan 20 (numero de vlan)

Switch(config-vlan)# name Consultas (nombre de vlan)

Switch(config-vlan)# exit

ASIGNAR PUERTOS ALA VLAN 20

Switch(config)# interface range fa0/1-18 (puertos del switch)

Switch(config-if-range)# switchport mode Access

Switch(config-if-range)# switchport Access vlan 20 (numero de vlan)

Switch(config-if-range)# no shutdown

Switch(config-if-range)# end

Switch# wr

HABILITAR LA INTERFAZ VLAN 20

Switch# configure terminal

Switch(config)# interface vlan 20

Switch(config-if)# ip address 192.168.20.2 255.255.255.0

Switch(config-if)# no shutdown

Switch(config-if)# exit

CONFIGURAR EL DHCP RELAY

Switch(config)# interface vlan 20

Switch(config-if)# ip helper-address 192.168.20.1

Switch(config-if)# exit

Switch(config)# exit

Switch# ping 192.168.20.1 (verificamos conexión con el dhcp)

VLAN 50 Wifi

CREACION DE LA VLAN

Switch> enable

Switch# configure terminal

Switch(config)# vlan 50 (numero de vlan)

Switch(config-vlan)# name Wifi (nombre de vlan)

Switch(config-vlan)# exit

ASIGNAR PUERTOS ALA VLAN 50

Switch(config)# interface range fa0/19-21 (puertos del switch)

Switch(config-if-range)# switchport mode Access

Switch(config-if-range)# switchport Access vlan 50 (numero de vlan)

Switch(config-if-range)# no shutdown

Switch(config-if-range)# end

Switch# wr

HABILITAR LA INTERFAZ VLAN 50

Switch# configure terminal

Switch(config)# interface vlan 50

Switch(config-if)# ip address 192.168.50.3 255.255.255.0

Switch(config-if)# no shutdown

Switch(config-if)# exit

CONFIGURAR EL DHCP RELAY

Switch(config)# interface vlan 50

Switch(config-if)# ip helper-address 192.168.50.1

Switch(config-if)# exit

Switch(config)# exit

Switch# ping 192.168.50.1 (verificamos conexión con el dhcp)

Switch de Farmacia-Imagenes

modo trunk para conexión de switch

Switch>enable

Switch# configure terminal

Switch(config)# interface Gi0/1

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk allowed vlan 30,50

Switch(config-if)# no shutdown

Switch(config-if)# exit

Switch(config)# exit

Switch# wr

VLAN 30 Consultas

CREACION DE LA VLAN

Switch# configure terminal

Switch(config)# vlan 30 (numero de vlan)

Switch(config-vlan)# name Emergencias (nombre de vlan)

Switch(config-vlan)# exit

ASIGNAR PUERTOS ALA VLAN 30

Switch(config)# interface range fa0/1-17 (puertos del switch)

Switch(config-if-range)# switchport mode Access

Switch(config-if-range)# switchport Access vlan 30 (numero de vlan)

Switch(config-if-range)# no shutdown

Switch(config-if-range)# end

Switch# wr

HABILITAR LA INTERFAZ VLAN 30

Switch# configure terminal

Switch(config)# interface vlan 30

Switch(config-if)# ip address 192.168.30.2 255.255.255.0

Switch(config-if)# no shutdown

Switch(config-if)# exit

CONFIGURAR EL DHCP RELAY

Switch(config)# interface vlan 30

Switch(config-if)# ip helper-address 192.168.30.1

Switch(config-if)# exit

Switch(config)# exit

Switch# ping 192.168.30.1 (verificamos conexión con el dhcp)

VLAN 50 Wifi

CREACION DE LA VLAN

Switch> enable

Switch# configure terminal

Switch(config)# vlan 50 (numero de vlan)

Switch(config-vlan)# name Wifi (nombre de vlan)

Switch(config-vlan)# exit

ASIGNAR PUERTOS ALA VLAN 50

Switch(config)# interface range fa0/18-20 (puertos del switch)

Switch(config-if-range)# switchport mode Access

Switch(config-if-range)# switchport Access vlan 50 (numero de vlan)

Switch(config-if-range)# no shutdown

Switch(config-if-range)# end

Switch# wr

HABILITAR LA INTERFAZ VLAN 50

Switch# configure terminal

Switch(config)# interface vlan 50

Switch(config-if)# ip address 192.168.50.4 255.255.255.0

Switch(config-if)# no shutdown

Switch(config-if)# exit

CONFIGURAR EL DHCP RELAY

Switch(config)# interface vlan 50

Switch(config-if)# ip helper-address 192.168.50.1

Switch(config-if)# exit

Switch(config)# exit

Switch# ping 192.168.50.1 (verificamos conexión con el dhcp)

Switch de Almacen

modo trunk para conexión de switch

Switch>enable

Switch# configure terminal

Switch(config)# interface Gi0/1

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk allowed vlan 30,50

Switch(config-if)# no shutdown

Switch(config-if)# exit

Switch(config)# exit

Switch# wr

VLAN 30 Consultas

CREACION DE LA VLAN

Switch> enable

Switch# configure terminal

Switch(config)# vlan 30 (numero de vlan)

Switch(config-vlan)# name Emergencias (nombre de vlan)

Switch(config-vlan)# exit

ASIGNAR PUERTOS ALA VLAN 30

Switch(config)# interface range fa0/1-17 (puertos del switch)

Switch(config-if-range)# switchport mode Access

Switch(config-if-range)# switchport Access vlan 30 (numero de vlan)

Switch(config-if-range)# no shutdown

Switch(config-if-range)# end

Switch# wr

HABILITAR LA INTERFAZ VLAN 30

Switch# configure terminal

Switch(config)# interface vlan 30

Switch(config-if)# ip address 192.168.30.3 255.255.255.0

Switch(config-if)# no shutdown

Switch(config-if)# exit

CONFIGURAR EL DHCP RELAY

Switch(config)# interface vlan 30

Switch(config-if)# ip helper-address 192.168.30.1

Switch(config-if)# exit

Switch(config)# exit

Switch# ping 192.168.30.1 (verificamos conexión con el dhcp)

VLAN 50 Wifi

CREACION DE LA VLAN

Switch> enable

Switch# configure terminal

Switch(config)# vlan 50 (numero de vlan)

Switch(config-vlan)# name Wifi (nombre de vlan)

Switch(config-vlan)# exit

ASIGNAR PUERTOS ALA VLAN 50

Switch(config)# interface range fa0/18-21 (puertos del switch)

Switch(config-if-range)# switchport mode Access

Switch(config-if-range)# switchport Access vlan 50 (numero de vlan)

Switch(config-if-range)# no shutdown

Switch(config-if-range)# end

Switch# wr

HABILITAR LA INTERFAZ VLAN 50

Switch# configure terminal

Switch(config)# interface vlan 50

Switch(config-if)# ip address 192.168.50.5 255.255.255.0

Switch(config-if)# no shutdown

Switch(config-if)# exit

CONFIGURAR EL DHCP RELAY

Switch(config)# interface vlan 50

Switch(config-if)# ip helper-address 192.168.50.1

Switch(config-if)# exit

Switch(config)# exit

Switch# ping 192.168.50.1 (verificamos conexión con el dhcp)

Switch de Fichaje

modo trunk para conexión de switch

Switch>enable

Switch# configure terminal

Switch(config)# interface Gi0/1

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk allowed vlan 20,50

Switch(config-if)# no shutdown

Switch(config-if)# exit

Switch(config)# exit

Switch# wr

VLAN 20 Consultas

CREACION DE LA VLAN

Switch> enable

Switch# configure terminal

Switch(config)# vlan 20 (numero de vlan)

Switch(config-vlan)# name Consultas (nombre de vlan)

Switch(config-vlan)# exit

ASIGNAR PUERTOS ALA VLAN 20

Switch(config)# interface range fa0/1-18 (puertos del switch)

Switch(config-if-range)# switchport mode Access

Switch(config-if-range)# switchport Access vlan 20 (numero de vlan)

Switch(config-if-range)# no shutdown

Switch(config-if-range)# end

Switch# wr

HABILITAR LA INTERFAZ VLAN 20

Switch# configure terminal

Switch(config)# interface vlan 20

Switch(config-if)# ip address 192.168.20.3 255.255.255.0

Switch(config-if)# no shutdown

Switch(config-if)# exit

CONFIGURAR EL DHCP RELAY

Switch(config)# interface vlan 20

Switch(config-if)# ip helper-address 192.168.20.1

Switch(config-if)# exit

Switch(config)# exit

Switch# ping 192.168.20.1 (verificamos conexión con el dhcp)

VLAN 50 Wifi

CREACION DE LA VLAN

Switch> enable

Switch# configure terminal

Switch(config)# vlan 50 (numero de vlan)

Switch(config-vlan)# name Wifi (nombre de vlan)

Switch(config-vlan)# exit

ASIGNAR PUERTOS ALA VLAN 50

Switch(config)# interface range fa0/19-21 (puertos del switch)

Switch(config-if-range)# switchport mode Access

Switch(config-if-range)# switchport Access vlan 50 (numero de vlan)

Switch(config-if-range)# no shutdown

Switch(config-if-range)# end

Switch# wr

HABILITAR LA INTERFAZ VLAN 50

Switch# configure terminal

Switch(config)# interface vlan 50

Switch(config-if)# ip address 192.168.50.6 255.255.255.0

Switch(config-if)# no shutdown

Switch(config-if)# exit

CONFIGURAR EL DHCP RELAY

Switch(config)# interface vlan 50

Switch(config-if)# ip helper-address 192.168.50.1

Switch(config-if)# exit

Switch(config)# exit

Switch# ping 192.168.50.1 (verificamos conexión con el dhcp)

Switch de Recursos Humanos

modo trunk para conexión de switch

Switch>enable

Switch# configure terminal

Switch(config)# interface Gi0/1

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk allowed vlan 10,50

Switch(config-if)# no shutdown

Switch(config-if)# exit

Switch(config)# exit

Switch# wr

VLAN 10 Administrativos

CREACION DE LA VLAN

Switch> enable

Switch# configure terminal

Switch(config)# vlan 10 (numero de vlan)

Switch(config-vlan)# name Administrativos (nombre de vlan)

Switch(config-vlan)# exit

ASIGNAR PUERTOS ALA VLAN 10

Switch(config)# interface range fa0/1-20 (puertos del switch)

Switch(config-if-range)# switchport mode Access

Switch(config-if-range)# switchport Access vlan 10 (numero de vlan)

Switch(config-if-range)# no shutdown

Switch(config-if-range)# end

Switch# wr

ACTIVAR EL SERVICIO DHCP

Switch# configure terminal

Switch(config)# interface vlan 10 (numero de vlan)

Switch(config-if)# ip address 192.168.10.1 255.255.255.0 (puerta de enlace con mascara) Switch(config-if)# exit

Switch(config)# exit

Switch# wr

Crearemos un pool de DHCP para el direccionamiento 192.168.10.0

Switch# configure terminal

Switch(config)# ip dhcp pool vlan10 (numero de vlan)

Switch(dhcp-config)# network 192.168.10.0 255.255.255.0 (segmento de red 192.168.10.0)

Switch(dhcp-config)# default-router 192.168.10.1 (puerta de enlace)

Switch(dhcp-config)# dns-server 1.1.1.3 8.8.8.8 (si existe dns)

Switch(dhcp-config)# exit

Switch(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.5 (opcional restriccion de ip)

Switch(config)# exit

Switch# wr

VLAN 50 Wifi

CREACION DE LA VLAN

Switch> enable

Switch# configure terminal

Switch(config)# vlan 50 (numero de vlan)

Switch(config-vlan)# name Wifi (nombre de vlan)

Switch(config-vlan)# exit

ASIGNAR PUERTOS ALA VLAN 50

Switch(config)# interface range fa0/21-22 (puertos del switch)

Switch(config-if-range)# switchport mode Access

Switch(config-if-range)# switchport Access vlan 50 (numero de vlan)

Switch(config-if-range)# no shutdown

Switch(config-if-range)# end

Switch# wr

HABILITAR LA INTERFAZ VLAN 50

Switch# configure terminal

Switch(config)# interface vlan 50

Switch(config-if)# ip address 192.168.50.7 255.255.255.0

Switch(config-if)# no shutdown

Switch(config-if)# exit

CONFIGURAR EL DHCP RELAY

Switch(config)# interface vlan 50

Switch(config-if)# ip helper-address 192.168.50.1

Switch(config-if)# exit

Switch(config)# exit

Switch# ping 192.168.50.1 (verificamos conexión con el dhcp)

Switch de Administracion_1

modo trunk para conexión de switch

Switch>enable

Switch# configure terminal

Switch(config)# interface Gi0/1

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk allowed vlan 10,50

Switch(config-if)# no shutdown

Switch(config-if)# exit

Switch(config)# exit

Switch# wr

VLAN 10 Administrativos

CREACION DE LA VLAN

Switch> enable

Switch# configure terminal

Switch(config)# vlan 10 (numero de vlan)

Switch(config-vlan)# name Administrativos (nombre de vlan)

Switch(config-vlan)# exit

ASIGNAR PUERTOS ALA VLAN 10

Switch(config)# interface range fa0/1-20 (puertos del switch)

Switch(config-if-range)# switchport mode Access

Switch(config-if-range)# switchport Access vlan 10 (numero de vlan)

Switch(config-if-range)# no shutdown

Switch(config-if-range)# end

Switch# wr

HABILITAR LA INTERFAZ VLAN 10

Switch# configure terminal

Switch(config)# interface vlan 10

Switch(config-if)# ip address 192.168.10.2 255.255.255.0

Switch(config-if)# no shutdown

Switch(config-if)# exit

CONFIGURAR EL DHCP RELAY

Switch(config)# interface vlan 10

Switch(config-if)# ip helper-address 192.168.10.1

Switch(config-if)# exit

Switch(config)# exit

Switch# ping 192.168.10.1 (verificamos conexión con el dhcp)

VLAN 50 Wifi

CREACION DE LA VLAN

Switch> enable

Switch# configure terminal

Switch(config)# vlan 50 (numero de vlan)

Switch(config-vlan)# name Wifi (nombre de vlan)

Switch(config-vlan)# exit

ASIGNAR PUERTOS ALA VLAN 50

Switch(config)# interface range fa0/21-22 (puertos del switch)

Switch(config-if-range)# switchport mode Access

Switch(config-if-range)# switchport Access vlan 50 (numero de vlan)

Switch(config-if-range)# no shutdown

Switch(config-if-range)# end

Switch# wr

HABILITAR LA INTERFAZ VLAN 50

Switch# configure terminal

Switch(config)# interface vlan 50

Switch(config-if)# ip address 192.168.50.8 255.255.255.0

Switch(config-if)# no shutdown

Switch(config-if)# exit

CONFIGURAR EL DHCP RELAY

Switch(config)# interface vlan 50

Switch(config-if)# ip helper-address 192.168.50.1

Switch(config-if)# exit

Switch(config)# exit

Switch# ping 192.168.50.1 (verificamos conexión con el dhcp)

Switch de Administracion_2

modo trunk para conexión de switch

Switch>enable

Switch# configure terminal

Switch(config)# interface Gi0/1

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk allowed vlan 10,50

Switch(config-if)# no shutdown

Switch(config-if)# exit

Switch(config)# exit

Switch# wr

VLAN 10 Administrativos

CREACION DE LA VLAN

Switch> enable

Switch# configure terminal

Switch(config)# vlan 10 (numero de vlan)

Switch(config-vlan)# name Administrativos (nombre de vlan)

Switch(config-vlan)# exit

ASIGNAR PUERTOS ALA VLAN 10

Switch(config)# interface range fa0/1-20 (puertos del switch)

Switch(config-if-range)# switchport mode Access

Switch(config-if-range)# switchport Access vlan 10 (numero de vlan)

Switch(config-if-range)# no shutdown

Switch(config-if-range)# end

Switch# wr

HABILITAR LA INTERFAZ VLAN 10

Switch# configure terminal

Switch(config)# interface vlan 10

Switch(config-if)# ip address 192.168.10.3 255.255.255.0

Switch(config-if)# no shutdown

Switch(config-if)# exit

CONFIGURAR EL DHCP RELAY

Switch(config)# interface vlan 10

Switch(config-if)# ip helper-address 192.168.10.1

Switch(config-if)# exit

Switch(config)# exit

Switch# ping 192.168.10.1 (verificamos conexión con el dhcp)

VLAN 50 Wifi

CREACION DE LA VLAN

Switch> enable

Switch# configure terminal

Switch(config)# vlan 50 (numero de vlan)

Switch(config-vlan)# name Wifi (nombre de vlan)

Switch(config-vlan)# exit

ASIGNAR PUERTOS ALA VLAN 50

Switch(config)# interface range fa0/21-22 (puertos del switch)

Switch(config-if-range)# switchport mode Access

Switch(config-if-range)# switchport Access vlan 50 (numero de vlan)

Switch(config-if-range)# no shutdown

Switch(config-if-range)# end

Switch# wr

HABILITAR LA INTERFAZ VLAN 50

Switch# configure terminal

Switch(config)# interface vlan 50

Switch(config-if)# ip address 192.168.50.9 255.255.255.0

Switch(config-if)# no shutdown

Switch(config-if)# exit

CONFIGURAR EL DHCP RELAY

Switch(config)# interface vlan 50

Switch(config-if)# ip helper-address 192.168.50.1

Switch(config-if)# exit

Switch(config)# exit

Switch# ping 192.168.50.1 (verificamos conexión con el dhcp)

Switch de 1er Piso

DHCP Principal Vlan 40 (comando para ver el dhcp Switch>show ip dhcp binding)

Modo trunk para conexión de switch

Switch>enable

Switch(config)#interface Gi0/1

Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport trunk allowed vlan 40,50

Switch(config-if)#no shutdown

Switch(config-if)#exit

Switch(config)#exit

Switch#wr

VLAN 40 Internacion

CREACION DE LA VLAN

Switch> enable

Switch# configure terminal

Switch(config)# vlan 40 (numero de vlan)

Switch(config-vlan)# name Internacion (nombre de vlan)

Switch(config-vlan)# exit

ASIGNAR PUERTOS ALA VLAN 40

Switch(config)# interface range fa0/1-14 (puertos del switch)

Switch(config-if-range)# switchport mode Access

Switch(config-if-range)# switchport Access vlan 40 (numero de vlan)

Switch(config-if-range)# no shutdown

Switch(config-if-range)# end

Switch# wr

ACTIVAR EL SERVICIO DHCP

Switch# configure terminal

Switch(config)# interface vlan 40 (numero de vlan)

Switch(config-if)# ip address 192.168.40.1 255.255.255.0 (puerta de enlace con mascara) Switch(config-if)# exit

Switch(config)# exit

Switch# wr

Crearemos un pool de DHCP para el direccionamiento 192.168.40.0

Switch# configure terminal

Switch(config)# ip dhcp pool vlan40 (numero de vlan)

Switch(dhcp-config)# network 192.168.40.0 255.255.255.0 (segmento de red 192.168.40.0)

Switch(dhcp-config)# default-router 192.168.40.1 (puerta de enlace)

Switch(dhcp-config)# dns-server 8.8.8.8 (si existe dns)

Switch(dhcp-config)# exit

Switch(config)# ip dhcp excluded-address 192.168.40.1 192.168.40.2 (opcional restriccion de ip)

Switch(config)# exit

Switch# wr

VLAN 50 Wifi

CREACION DE LA VLAN

Switch> enable

Switch# configure terminal

Switch(config)# vlan 50 (numero de vlan)

Switch(config-vlan)# name Wifi (nombre de vlan)

Switch(config-vlan)# exit

ASIGNAR PUERTOS ALA VLAN 50

Switch(config)# interface range fa0/15-19 (puertos del switch)

Switch(config-if-range)# switchport mode Access

Switch(config-if-range)# switchport Access vlan 50 (numero de vlan)

Switch(config-if-range)# no shutdown

Switch(config-if-range)# end

Switch# wr

HABILITAR LA INTERFAZ VLAN 50

Switch# configure terminal

Switch(config)# interface vlan 50

Switch(config-if)# ip address 192.168.50.10 255.255.255.0

Switch(config-if)# no shutdown

Switch(config-if)# exit

CONFIGURAR EL DHCP RELAY

Switch(config)# interface vlan 50

Switch(config-if)# ip helper-address 192.168.50.1

Switch(config-if)# exit

Switch(config)# exit

Switch# ping 192.168.50.1 (verificamos conexión con el dhcp)

Switch de 2do Piso

modo trunk para conexión de switch

Switch>enable

Switch# configure terminal

Switch(config)# interface Gi0/1

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk allowed vlan 40,50

Switch(config-if)# no shutdown

Switch(config-if)# exit

Switch(config)# exit

Switch# wr

VLAN 40 Internacion

CREACION DE LA VLAN

Switch# configure terminal

Switch(config)# vlan 40 (numero de vlan)

Switch(config-vlan)# name Internacion (nombre de vlan)

Switch(config-vlan)# exit

ASIGNAR PUERTOS ALA VLAN 40

Switch(config)# interface range fa0/1-14 (puertos del switch)

Switch(config-if-range)# switchport mode Access

Switch(config-if-range)# switchport Access vlan 40 (numero de vlan)

Switch(config-if-range)# no shutdown

Switch(config-if-range)# end

Switch# wr

HABILITAR LA INTERFAZ VLAN 40

Switch1(config)# interface vlan 40

Switch1(config-if)# ip address 192.168.40.2 255.255.255.0

Switch1(config-if)# no shutdown

Switch1(config-if)# exit

CONFIGURAR EL DHCP RELAY

Switch1# configure terminal

Switch1(config)# interface vlan 40

Switch1(config-if)# ip helper-address 192.168.40.1

Switch1(config-if)# exit

Switch1# ping 192.168.40.1 (verificamos conexión con el dhcp)

VLAN 50 Wifi

CREACION DE LA VLAN

Switch> enable

Switch# configure terminal

Switch(config)# vlan 50 (numero de vlan)

Switch(config-vlan)# name Wifi (nombre de vlan)

Switch(config-vlan)# exit

ASIGNAR PUERTOS ALA VLAN 50

Switch(config)# interface range fa0/15-19 (puertos del switch)

Switch(config-if-range)# switchport mode Access

Switch(config-if-range)# switchport Access vlan 50 (numero de vlan)

Switch(config-if-range)# no shutdown

Switch(config-if-range)# end

Switch# wr

HABILITAR LA INTERFAZ VLAN 50

Switch# configure terminal

Switch(config)# interface vlan 50

Switch(config-if)# ip address 192.168.50.11 255.255.255.0

Switch(config-if)# no shutdown

Switch(config-if)# exit

CONFIGURAR EL DHCP RELAY

Switch(config)# interface vlan 50

Switch(config-if)# ip helper-address 192.168.50.1

Switch(config-if)# exit

Switch(config)# exit

Switch# ping 192.168.50.1 (verificamos conexión con el dhcp)

Switch de 3er Piso

modo trunk para conexión de switch

Switch>enable

Switch# configure terminal

Switch(config)# interface Gi0/1

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk allowed vlan 40,50

Switch(config-if)# no shutdown

Switch(config-if)# exit

Switch(config)# exit

Switch# wr

VLAN 40 Internacion

CREACION DE LA VLAN

Switch# configure terminal

Switch(config)# vlan 40 (numero de vlan)

Switch(config-vlan)# name Internacion (nombre de vlan)

Switch(config-vlan)# exit

ASIGNAR PUERTOS ALA VLAN 40

Switch(config)# interface range fa0/1-14 (puertos del switch)

Switch(config-if-range)# switchport mode Access

Switch(config-if-range)# switchport Access vlan 40 (numero de vlan)

Switch(config-if-range)# no shutdown

Switch(config-if-range)# end

Switch# wr

HABILITAR LA INTERFAZ VLAN 40

Switch# configure terminal

Switch1(config)# interface vlan 40

Switch1(config-if)# ip address 192.168.40.3 255.255.255.0

Switch1(config-if)# no shutdown

Switch1(config-if)# exit

Switch1(config)# exit

CONFIGURAR EL DHCP RELAY

Switch1# configure terminal

Switch1(config)# interface vlan 40

Switch1(config-if)# ip helper-address 192.168.40.1

Switch1(config-if)# exit

Switch1(config)# exit

Switch1# ping 192.168.40.1 (verificamos conexión con el dhcp)

VLAN 50 Wifi

CREACION DE LA VLAN

Switch> enable

Switch# configure terminal

Switch(config)# vlan 50 (numero de vlan)

Switch(config-vlan)# name Wifi (nombre de vlan)

Switch(config-vlan)# exit

ASIGNAR PUERTOS ALA VLAN 50

Switch(config)# interface range fa0/15-19 (puertos del switch)

Switch(config-if-range)# switchport mode Access

Switch(config-if-range)# switchport Access vlan 50 (numero de vlan)

Switch(config-if-range)# no shutdown

Switch(config-if-range)# end

Switch# wr

HABILITAR LA INTERFAZ VLAN 50

Switch# configure terminal

Switch(config)# interface vlan 50

Switch(config-if)# ip address 192.168.50.12 255.255.255.0

Switch(config-if)# no shutdown

Switch(config-if)# exit

CONFIGURAR EL DHCP RELAY

Switch(config)# interface vlan 50

Switch(config-if)# ip helper-address 192.168.50.1

Switch(config-if)# exit

Switch(config)# exit

Switch# ping 192.168.50.1 (verificamos conexión con el dhcp)

Configuración del Router

Tabla 11

Segmentación de la Puerta de Enlace del Router

Puerto del router	VLAN	Puerta de enlace
FA0/0	1	192.168.231.1
FA0/0.10	VLAN10 ADMINISTRATIVOS	192.168.10.1
FA0/0.20	VLAN20 CONSULTAS	192.168.20.1

FA0/0.30	VLAN30 EMERGENCIAS	192.168.30.1
FA0/0.40	VLAN40 INTERNACION	192.168.40.1
FA0/0.50	VLAN50 ACCESS POINTS	192.168.50.1

Configuración de los segmentos del router aplicando el estándar de VLAN IEEE 802.1Q

Router(config)#interface FastEthernet0/0

Router(config-if)#ip address 192.168.231.1 255.255.255.0

Router(config)# interface fastEthernet 0/0.10

Router(config-subif)# encapsulation dot1Q 10

Router(config-subif)# ip address 192.168.10.1 255.255.255.0

Router(config)# interface fastEthernet 0/0.20

Router(config-subif)# encapsulation dot1Q 20

Router(config-subif)# ip address 192.168.20.1 255.255.255.0

Router(config)# interface fastEthernet 0/0.30

Router(config-subif)# encapsulation dot1Q 30

Router(config-subif)# ip address 192.168.30.1 255.255.255.0

Router(config)# interface fastEthernet 0/0.40

Router(config-subif)# encapsulation dot1Q 40

Router(config-subif)# ip address 192.168.40.1 255.255.255.0

Router(config)# interface fastEthernet 0/0.50

Router(config-subif)# encapsulation dot1Q 50

Router(config-subif)# ip address 192.168.50.1 255.255.255.0

Tabla 12

Contraseñas de Acceso a los Switch por Áreas

Rack por áreas	Contraseñas
Madre	HRSJDD2024MADR
Sistemas1	HRSJDD2024SIST
Sistemas2	HRSJDD2024SIST
Emergencias-Laboratorios	HRSJDD2024EMER
Consultorios_1	HRSJDD2024CON1
Consultorios_2	HRSJDD2024CON2
Farmacia-Imágenes	HRSJDD2024FARM
Almacén (Área Restringida)	HRSJDD2024ALMA
Fichaje	HRSJDD2024FICH
Recursos Humanos	HRSJDD2024RECU
Administracion_1	HRSJDD2024ADM1
Administracion_2	HRSJDD2024ADM2
PISO 1	HRSJDD2024PIS1
PISO 2	HRSJDD2024PIS2
PISO 3	HRSJDD2024PIS3

Configuración de las contraseñas al switch

Switch de Madre

Switch>en

Switch#conf t

Switch(config)#line con 0

Switch(config-line)#password HRSJDD2024MADR

Switch(config-line)#login

Switch(config-line)#end

Switch#

Switch#write memory

Switch de Sistemas1

Switch>en

Switch#conf t

Switch(config)#line con 0

Switch(config-line)#password HRSJDD2024SIST

Switch(config-line)#login

Switch(config-line)#end

Switch#

Switch#write memory

Switch#

Switch de Sistemas2

Switch>en

Switch#conf t

Switch(config)#line con 0

Switch(config-line)#password HRSJDD2024SIST

Switch(config-line)#login

Switch(config-line)#end

Switch#

Switch#write memory

Switch#

Switch de Emergencia-Laboratorio

Switch>en

Switch#conf t

Switch(config)#line con 0

Switch(config-line)#password HRSJDD2024EMER

Switch(config-line)#login

Switch(config-line)#end

Switch#

Switch#write memory

Switch de Consultorios_1

Switch>en

Switch#conf t

Switch(config)#line con 0

Switch(config-line)#password HRSJDD2024CON1

Switch(config-line)#login

Switch(config-line)#end

Switch#

Switch#write memory

Switch de Consultorios_2

Switch>en

Switch#conf t

Switch(config)#line con 0

Switch(config-line)#password HRSJDD2024CON2

Switch(config-line)#login

Switch(config-line)#end

Switch#

Switch#write memory

Switch de Farmacia-Imágenes

Switch>en

Switch#conf t

Switch(config)#line con 0

Switch(config-line)#password HRSJDD2024FARM

Switch(config-line)#login

Switch(config-line)#end

Switch#

Switch#write memory

Switch de Alacen

Switch>en

Switch#conf t

Switch(config)#line con 0

Switch(config-line)#password HRSJDD2024ALMA

Switch(config-line)#login

Switch(config-line)#end

Switch#

Switch#write memory

Switch de Fichaje

Switch>en

Switch#conf t

Switch(config)#line con 0

Switch(config-line)#password HRSJDD2024FICH

Switch(config-line)#login

Switch(config-line)#end

Switch#

Switch#write memory

Switch de Recursos Humanos

Switch>en

Switch#conf t

Switch(config)#line con 0

Switch(config-line)#password HRSJDD2024RECU

Switch(config-line)#login

Switch(config-line)#end

Switch#

Switch#write memory

Switch de Administracion_1

Switch>en

Switch#conf t

Switch(config)#line con 0

Switch(config-line)#password HRSJDD2024ADM1

Switch(config-line)#login

Switch(config-line)#end

Switch#

Switch#write memory

Switch de Administracion_2

Switch>en

Switch#conf t

Switch(config)#line con 0

Switch(config-line)#password HRSJDD2024ADM2

Switch(config-line)#login

Switch(config-line)#end

Switch#

Switch#write memory

Switch de Piso1

Switch>en

Switch#conf t

Switch(config)#line con 0

Switch(config-line)#password HRSJDD2024PIS1

Switch(config-line)#login

Switch(config-line)#end

Switch#

Switch#write memory

Switch de Piso2

```
Switch>en
Switch#conf t
Switch(config)#line con 0
Switch(config-line)#password HRSJDD2024PIS2
Switch(config-line)#login
Switch(config-line)#end
Switch#
Switch#write memory
```

Switch de Piso3

```
Switch>en
Switch#conf t
Switch(config)#line con 0
Switch(config-line)#password HRSJDD2024PIS3
Switch(config-line)#login
Switch(config-line)#end
Switch#
Switch#write memory
```

Tabla 13

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	Aisla 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 necesidad de aumentar la infraestructura.	Limitada: Las subredes están limitadas por la cantidad de direcciones IP disponibles en la red, lo que puede hacer que una red crezca más lentamente.
Seguridad	Alta: El tráfico entre VLANs está aislado, por lo que se	Baja: Aunque las subredes pueden ayudar a aislar el

	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.).	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	Las subredes no optimizan el rendimiento de la red de

	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.	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, mejorando la calidad del servicio en redes de alto tráfico.	Las subredes no proporcionan un control tan específico de QoS, ya que la segmentación es menos precisa y no se puede aplicar la misma granularidad que con las VLANs.

3.3.2. Wi-Fi

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, 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 hospitales 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.

Configuración de la red Wifi

Figura 43

Configuramos la Conexión DHCP de la VLAN para la Red Wifi

Figura 44

Verificamos que nos esté Accediendo Dinámicamente a la Red VLAN 50 de Wifi

Figura 45

Configuramos la Red del DHCP que Repartiremos a los Usuarios

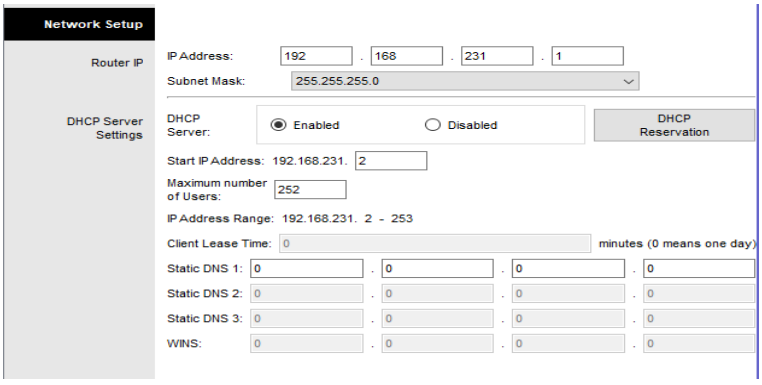


Figura 46

Verificamos la Configuración LAN

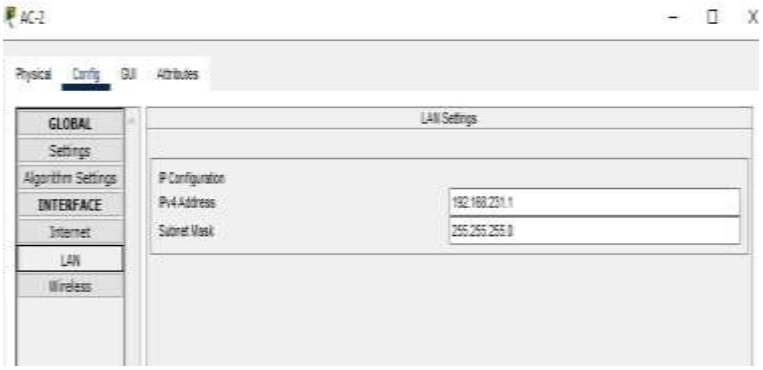


Figura 47

Configuramos el Nombre al Wifi (SSID) en este caso HRSJDD

Figura 48

La configuración Network Mode la Mantenemos en Mixed

Figura 49

La configuración Radio Band la Mantenemos en Auto

Figura 50

La Configuración Wide Channel la Mantenemos en Auto

Figura 51

La configuración Standard Chanel la Mantenemos en el 1 - 2.412 GHz

Figura 52

La configuración SSID Broadcast la Mantenemos en Enabled

Figura 53

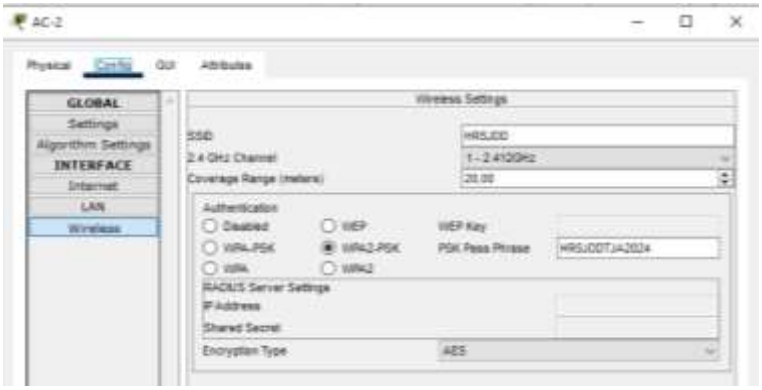
Configuramos una Contraseña con la seguridad de WPA3 Personal en este caso HRSJDDTJA2024 (en este caso el simulador cuenta hasta WPA2)

Figura 54

Configuramos la encriptación en AES

Figura 55

Verificamos la configuración asignada



Consideraciones para No Utilizar Filtrado MAC en una Red Wi-Fi Pública del Hospital

No utilizar el filtrado MAC en una red Wi-Fi pública puede ser una decisión estratégica, especialmente si el objetivo es ofrecer acceso libre y sin restricciones a los usuarios. El filtrado MAC, aunque útil para restringir el acceso a dispositivos específicos, no es una solución ideal en redes abiertas, ya que requiere una gestión constante y la inclusión de nuevas direcciones MAC cada vez que un usuario desee conectarse. En un entorno donde el acceso debe ser libre y accesible para cualquier persona, implementar un sistema de filtrado MAC podría generar una carga administrativa innecesaria, además de que no ofrece una protección real contra usuarios malintencionados, ya que las direcciones MAC pueden ser fácilmente falsificadas. Por lo tanto, en una red Wi-Fi pública donde la accesibilidad y la facilidad de uso son prioridades, es más eficiente centrarse en otros métodos de seguridad, como la autenticación y la encriptación, en lugar de complicar el acceso mediante el filtrado MAC.

Seguridad de la red Wifi

Para implementar mejoras en la seguridad de la red Wi-Fi del hospital, vamos a utilizar WPA3, que es la tercera versión del protocolo de acceso protegido para redes Wi-Fi, introducida 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.

Figura 56

Seguridad de la red Wifi

	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

Aproximado de cuantas personas acceden al hospital por turnos

Se evaluó cuantas personas ingresan al Hospital 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 del hospital y los pacientes para ver la capacidad de cuantas personas accederán a la red inalámbrica que tiene un aproximado de 1250 personas.

Tabla 14

Aproximado de Personas dentro del Hospital por Turnos

Turno	Personal Administrativo y Médicos	Pacientes, Pasantes, Internos, Residentes	Total
Mañana	350	250	600
Tarde	250	200	450
Noche	150	50	200
			1250

Ancho de banda

Para evitar la congestión y asegurar una experiencia más estable para 600 personas, lo ideal es contar con un ancho de aproximadamente 800 Mbps.

Servicios del Access Point

El TP-Link Omada EAP620 HD es un punto de acceso de clase empresarial de doble banda (2,4 y 5GHz) montado en la pared que soporta WI-FI 6 y ofrece velocidades de conexión de hasta 1775MB/s. Equipado con MU-MIMO 2x2:2, OFDMA, WPA3, AirTime Fairness, QoS, el dispositivo puede utilizarse en entornos de alto tráfico con el estándar 802.11ax.

Wi-Fi ultrarrápido 6 velocidades: 574 Mbps simultáneos en 2.4 GHz y 1201 Mbps en 5 GHz sumando velocidades Wi-Fi de 1775 Mbps.

Conectividad de alta densidad: 4 veces mayor capacidad para conectar más dispositivos simultáneamente.

Integrado en Omada SDN: Provisionmiento sin intervención (ZTP) , Administración centralizada en la nube y Monitorización inteligente.

Administración centralizada: acceso vía nube y aplicación Omada para una comodidad y administración fáciles.

Roaming sin interrupciones: incluso las transmisiones de video y las llamadas de voz no se ven afectadas a medida que los usuarios se mueven entre ubicaciones.

Soporte PoE: Admite alimentación por Ethernet (802.3at) para una implementación e instalación conveniente.

Red de invitados segura: Junto con múltiples opciones de autenticación (SMS / Facebook Wi-Fi / Voucher, etc.) y abundantes tecnologías de seguridad inalámbrica.

Características relevantes del TP-Link Omada EAP620 HD:

Compatibilidad con Omada SDN:

Puede ser gestionado por el controlador Omada (hardware, software o en la nube), lo que permite configurar una red Wi-Fi unificada y con roaming.

Esto permite crear una red inalámbrica eficiente con roaming rápido, similar a una red Mesh.

Roaming rápido (Fast Roaming):

Compatible con 802.11k/v, lo que permite a los clientes moverse entre puntos de acceso sin interrupciones.

Ideal para usuarios que se desplazan en el área de cobertura.

Dual-Band Wi-Fi 6 (AX1800):

Soporta 2.4 GHz y 5 GHz con tecnología Wi-Fi 6, ofreciendo mayor velocidad y capacidad para múltiples dispositivos.

Modo Mesh (con Omada):

Aunque el EAP620 HD no es un dispositivo Mesh independiente, puedes usarlo como parte de una red Mesh dentro de un sistema Omada SDN.

Esto requiere configurar los puntos de acceso para conectarse entre sí (si no están cableados) usando su capacidad Mesh.

Figura 57

Estándares de Wi-Fi

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[2]
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

3.3.3. Servidor Telefonía IP

Tabla 15

Teléfonos Internos del Hospital

N.º	Nombre de Área	Número de teléfono
1	Administración	122
2	Almacén General	139
3	Cirugía Mujeres	242
4	Cirugía Varones	256
5	Compras y Ventas	119
6	Contabilidad	120
7	Docencia	273
8	Endoscopia	240
9	Farmacia	175
10	Fichaje	126
11	Laboratorio Clínico	220
12	Mantenimiento	115
13	Maternidad	313

14	Medicina Mujeres	333
15	Medicina Varones	408
16	Policía	210
17	Quemado	136
18	Rayos X – Ecografía	251
19	Recursos Humanos	127
20	Seguros	169
21	Sistemas	402
22	Terapia Intensiva	257
23	Tesorería	124
24	Tomografía	168
25	Trabajo Social	174
26	Traumatología	264
27	Asesoría Legal	112
28	Banco de Sangre	176
29	Soat	121
30	Estadística	126
31	Fisioterapia	165
32	Pediatría	283

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.

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.

Instalación de Issabel

Figura 58

Una vez Cargada la Imagen ISO Colocamos Test this media & install

Figura 59

Esperamos la instalación

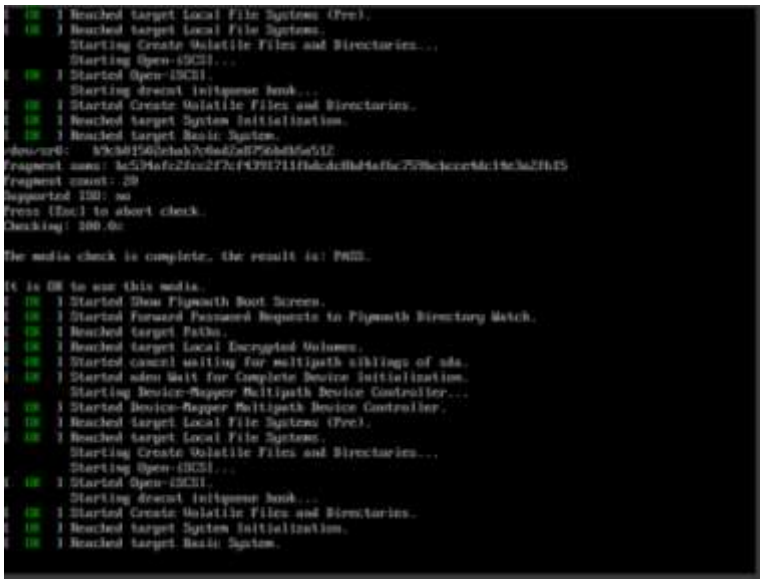


Figura 60

Seleccionamos el Idioma Español

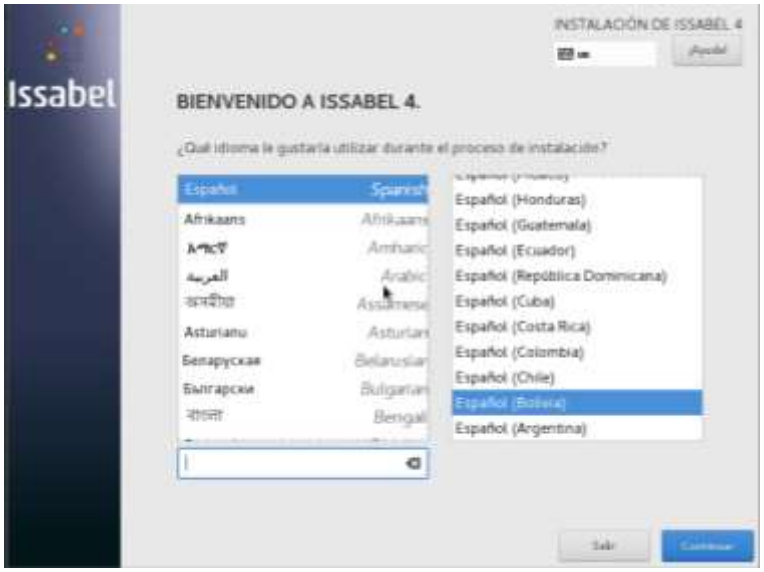


Figura 61

Seleccionamos el Software de Asterisk 11

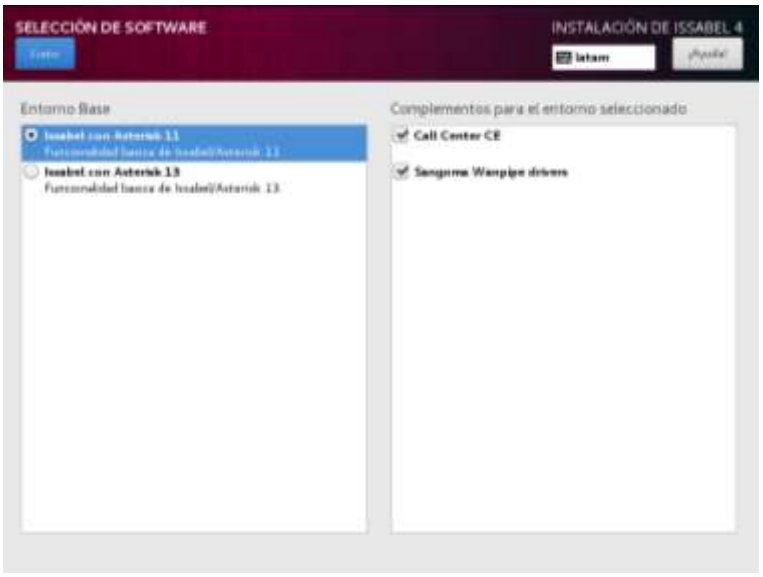


Figura 62

Colocamos una Contraseña Root

Figura 63

Colocamos una Contraseña Administrativa Root HRSJDD2024

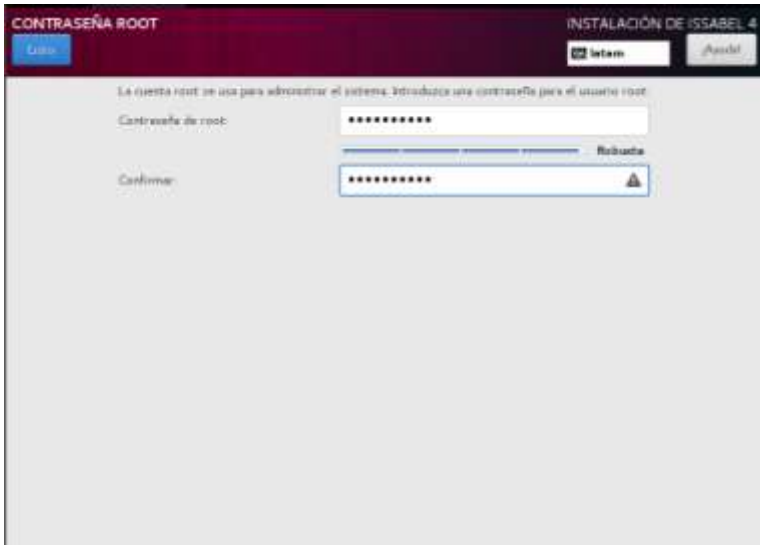


Figura 64

Creamos un Usuario y Contraseña

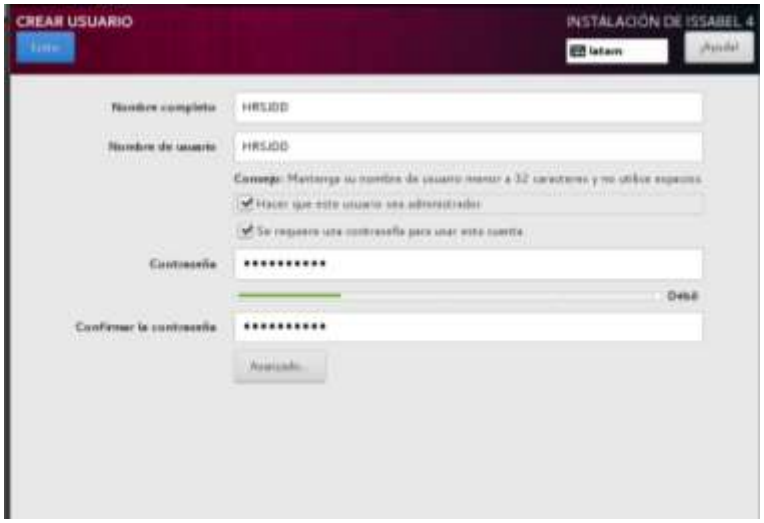


Figura 65

Continua la Instalación

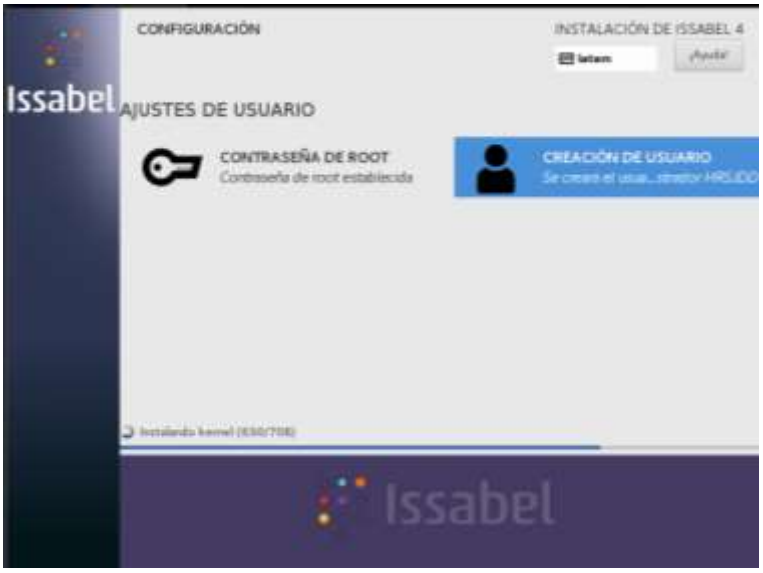


Figura 66

Luego de Instalar Pedirá que Coloquen la Contraseña de Root de la base de datos HRSJDD2024

Figura 67

Seleccionamos el Idioma Español

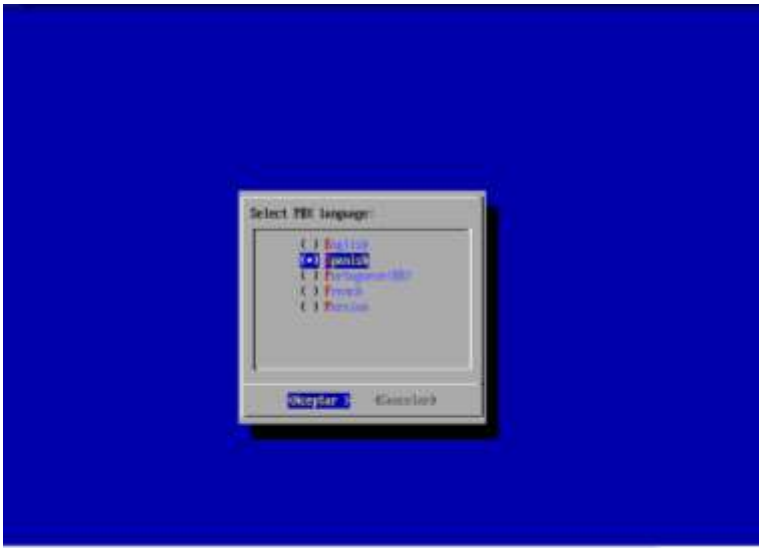


Figura 68

Selecciona el tipo de SIP Chanel chan_pjsip

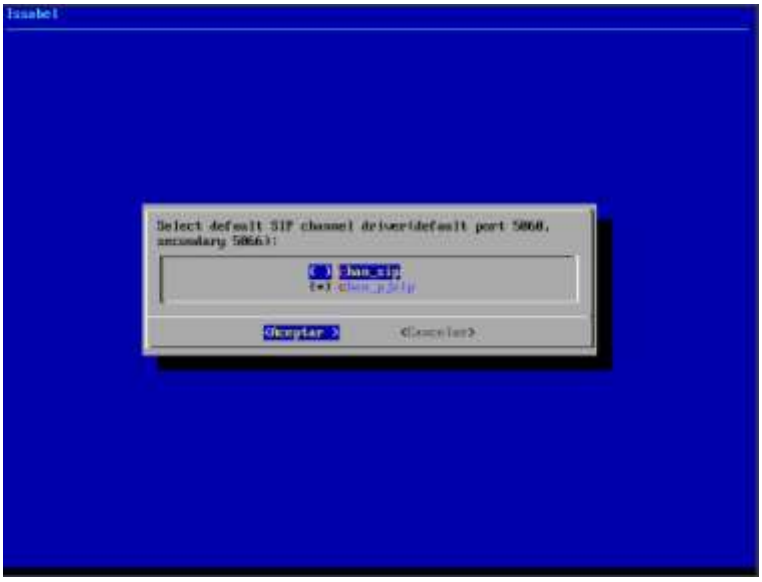


Figura 69

Desea Acceder a su Página Oficial

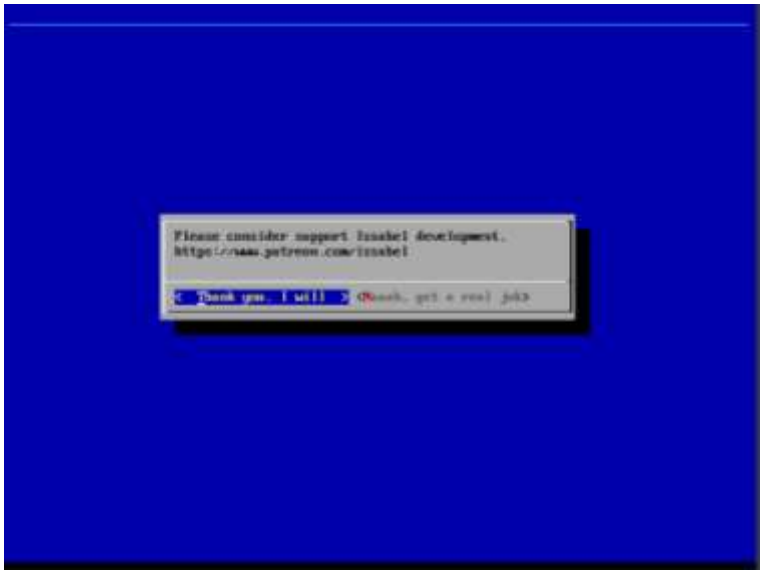


Figura 70

Iniciamos Sesión login: HRSJDD password: HRSJDD2024

Figura 71

Issabel se Inicia Entramos a su Interfaz con https://192.168.86.128/ en el navegador

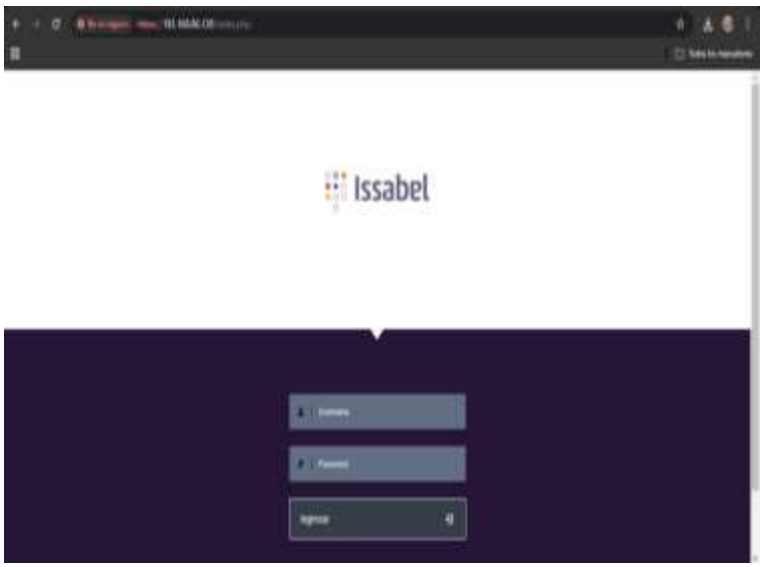
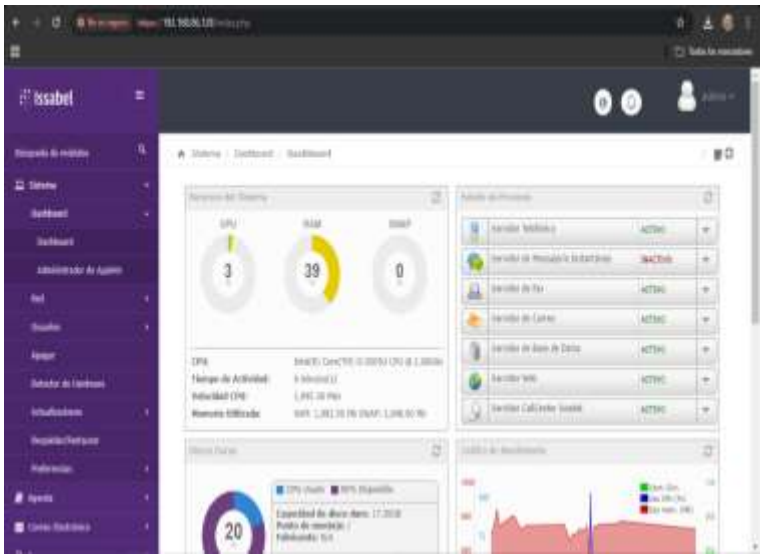


Figura 72

Iniciamos Sesión con Nombre de Usuario: admin contraseña: HRSJDD2024



Añadir una extensión(numero) al servidor

Figura 73

Entramos a PBX -> Configuración PBX, Dejamos por Defecto SIP y Damos Enviar

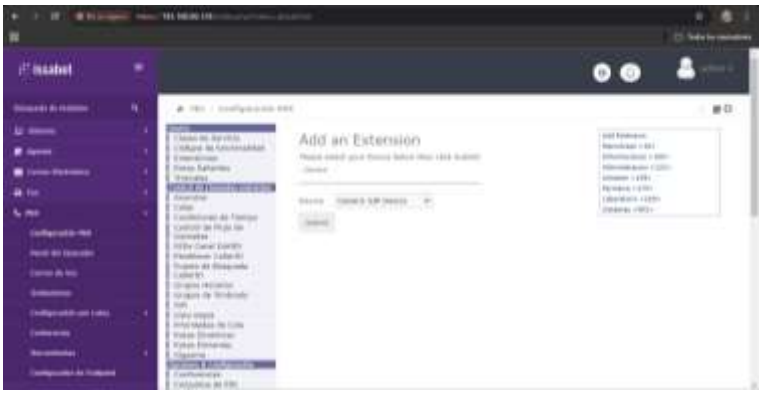


Figura 74

Llenamos los datos Extensión de Usuario: 122 Nombre para mostrar: Administración

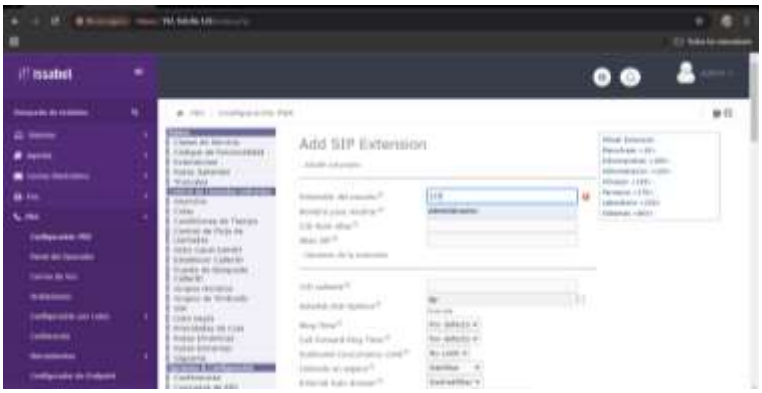


Figura 75

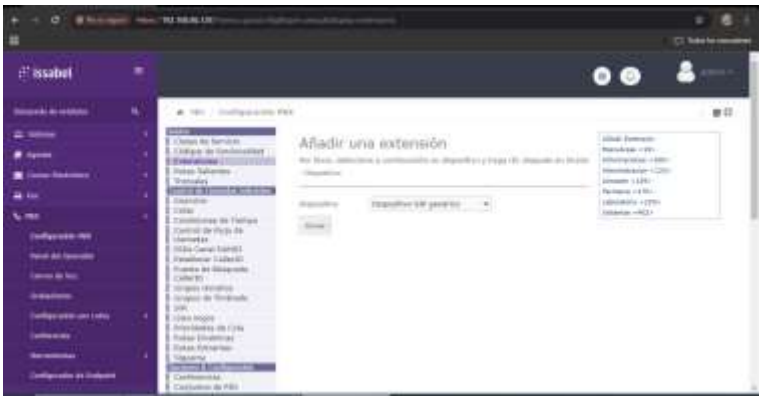
Colocamos una Contraseña ala Extensión: HRSJDD122

Figura 76

Colocamos Enviar al Final

Figura 77

Verificamos la Extensión Creada



Instalación de video llamadas

Figura 78

Entramos a Seguridad y Después Configuraciones Avanzadas

Figura 79

Activamos el Acceso Directo no Integrado y Colocamos la Contraseña: HRSJDD2024 para Guardar Cambios

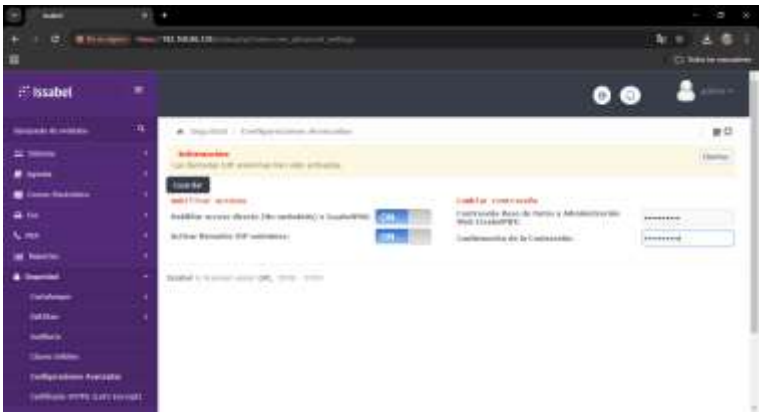


Figura 80

Después Entramos a PBX y Configuración de PBX

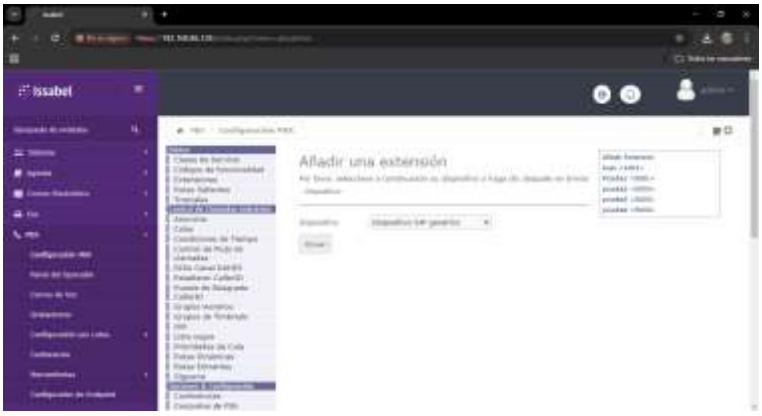


Figura 81

Bajamos Hasta IssabelPBX Si Embeber

Figura 82

Nos Redireccionara a Otra Página de Administrador

Figura 83

Buscamos en Settings y Asterisk SIP Settings

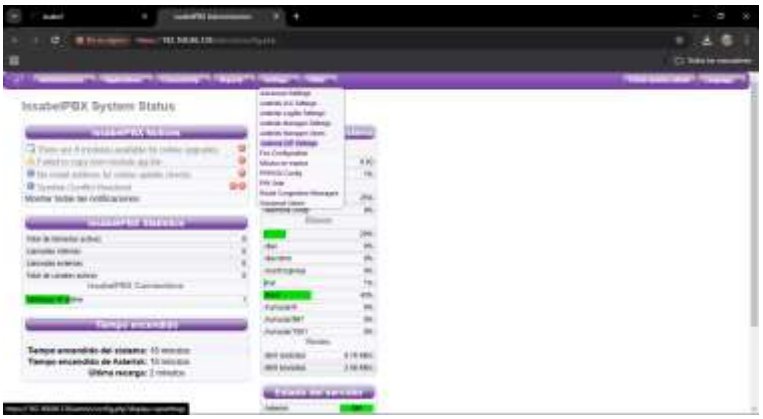


Figura 84

Después Colocamos Nuestra IP del Servidor 192.168.86.128

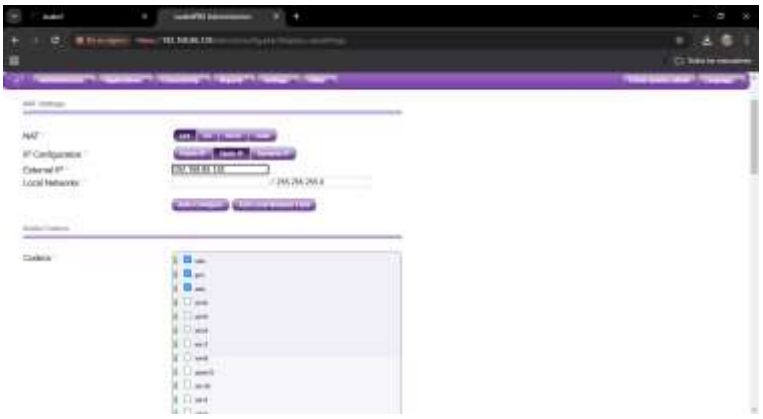


Figura 85

Video Suport lo Activamos y Seleccionamos Todos los Formatos de Video

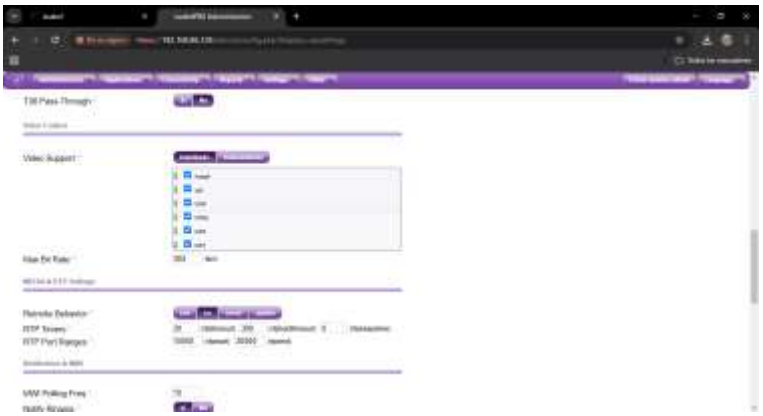


Figura 86

Y le Damos en Enviar Cambios

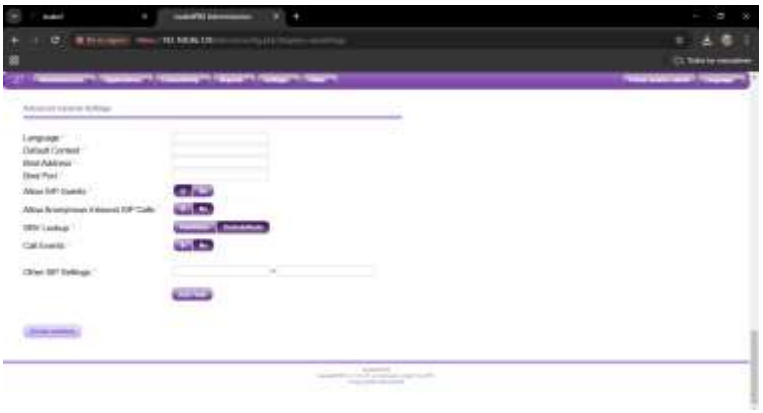
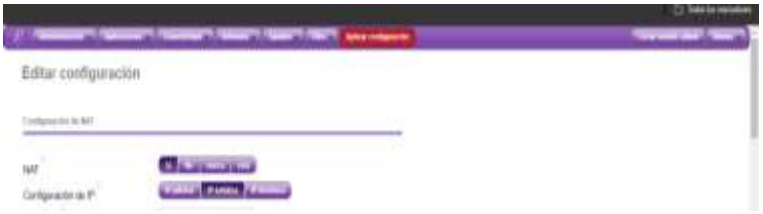


Figura 87

Aplicar Cambios



Grupos de llamadas

Figura 88

Entramos a PBX -> Configuración PBX

Figura 89

Entramos a Colas

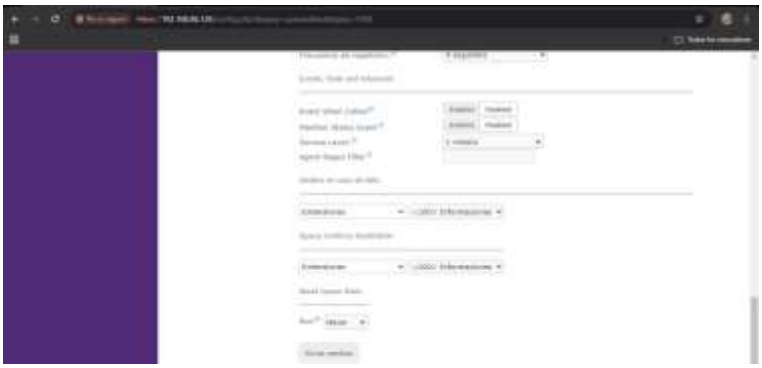
Figura 90

Colocamos los Datos de la Cola

Número de cola: 1000 -Nombre de la cola: Grupo 1 -Agentes fijos: 122 , 139 -Ring Strategy: Sonar todos

Figura 91

Momento de no Contestar Derivamos la Llamada a la Extensión 100 que Sería Informaciones y Damos Enviar Cambios



Menú de llamadas

Figura 92

Entramos a PBX -> Configuración PBX

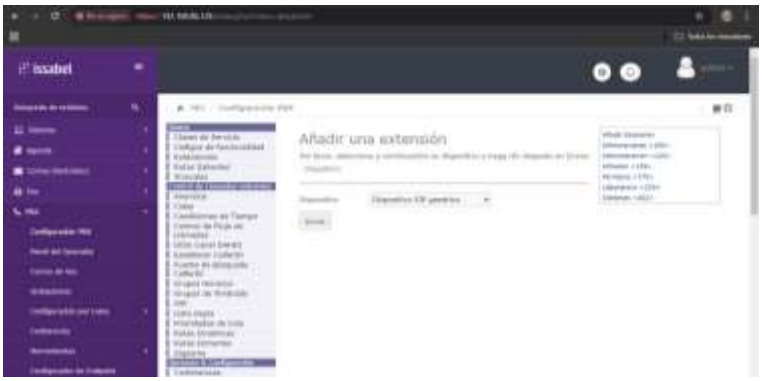


Figura 93

Entramos a Grabaciones de Sistema

Figura 94

Colocamos una Extensión para Comprobar Grabaciones le Colocamos 139

Figura 95

Guardar un Mensaje de Voz Marcar *77 Desde la Extensión 139

Figura 96

Colocamos el Nombre del Menú y Guardamos

Figura 97

Continuación Creamos el IVR (menú)

Figura 98

Colocamos Datos del IVR

-IVR Name: Menu_HRSJDD -Anuncio: Menú -Direct Dial: Extensions -Tiempo de espera: 5

Si el Número Marcado es Incorrecto Colocamos Terminar la Llamada

Figura 99

Terminando el Tiempo de Espera

Timeout Destination: Terminar la Llamada y Añadimos el Menú y las Extensiones y Damos Guardar

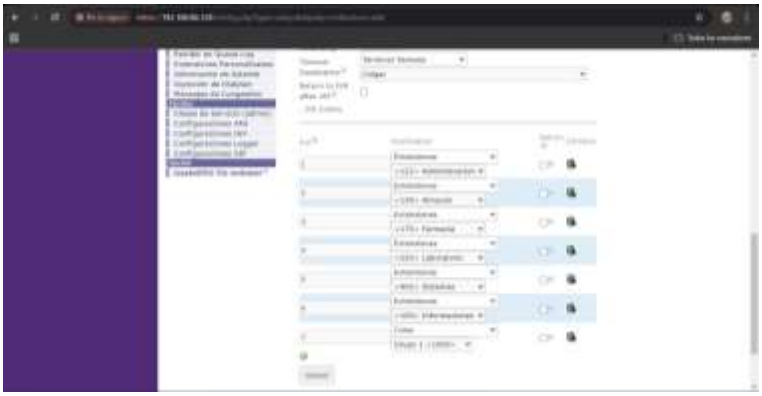


Figura 100

Creamos la Extensión del Menú

-Extensión del Usuario: 10 -Nombre Para Mostrar: MenuAreas

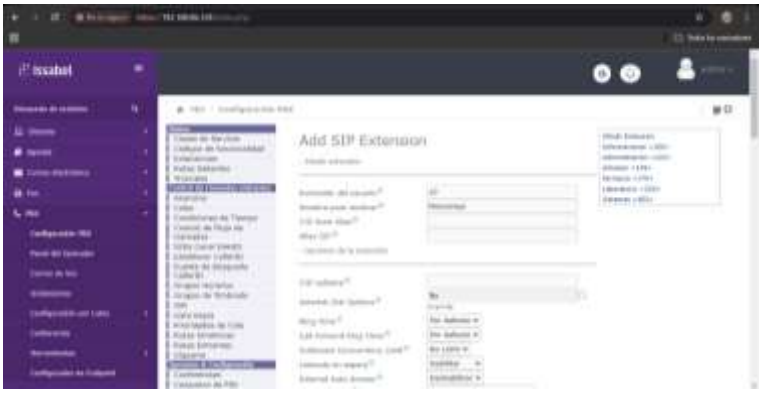


Figura 101

Seguido Entramos a la Extensión y le Damos a add follow me settings

Figura 102

Bajamos Hasta Destination if no Answer le Damos IVR y el Menu_HRSJDD y Guardamos Cambios

Configuración de Audio en Español

Figura 103

Entramos a PBX-> Herramientas-> Editor Archivos Asterisk

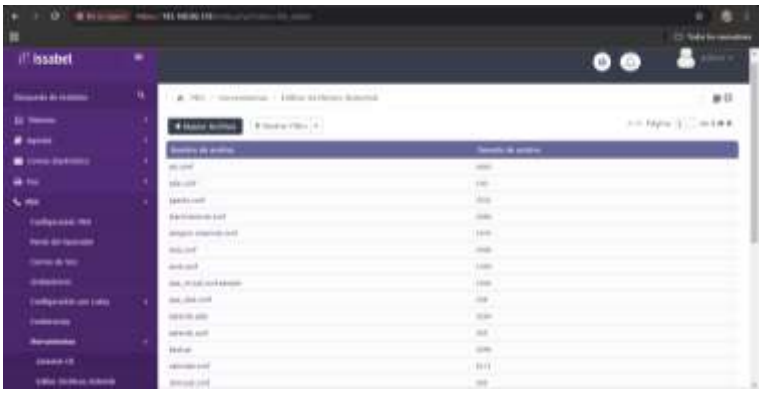


Figura 104

En el Buscador Buscamos sip

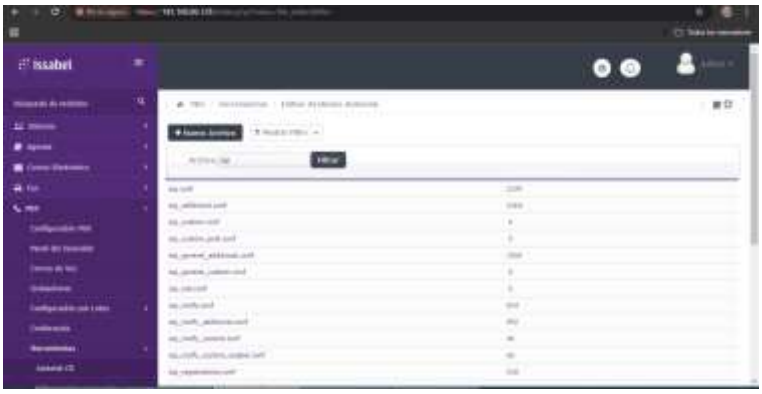


Figura 105

Buscamos sip_general_custom.conf

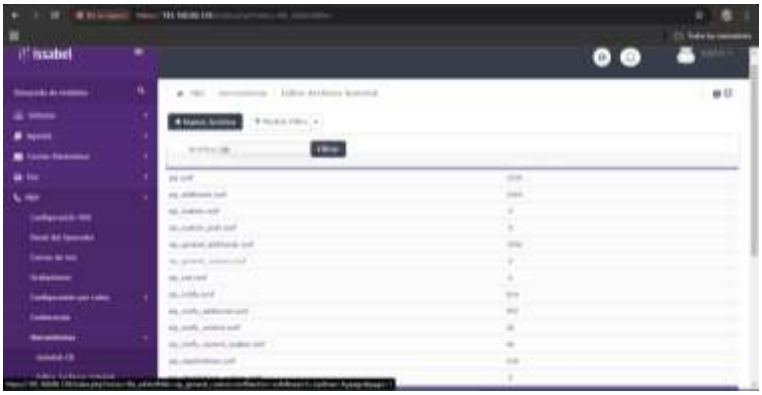


Figura 106

Editamos y Colocamos

allowguest=no

language=es

Guardar y Recargar Asterisk

Buzón de Voz

Figura 107

Entramos a Correo Electrónico-> Dominios

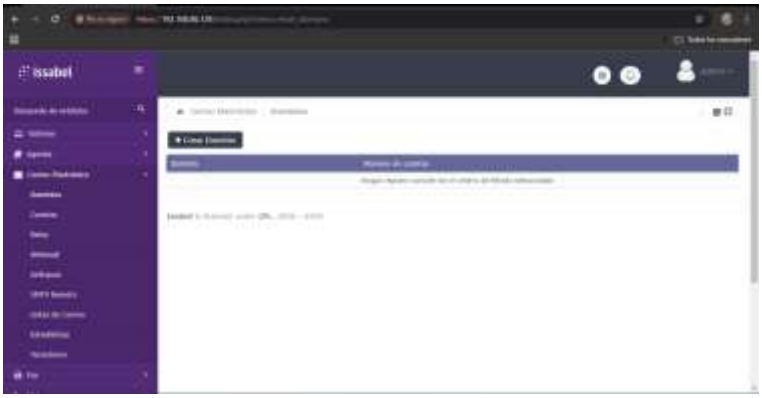


Figura 108

Creamos el Dominio hrsjdd.com

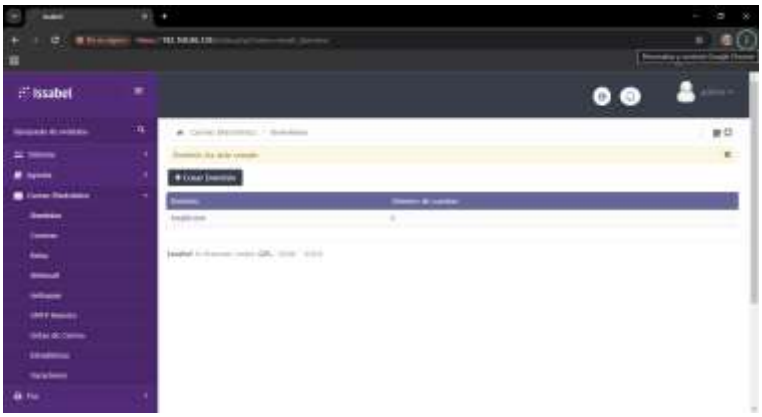


Figura 109

Ahora Vamos a Cuentas

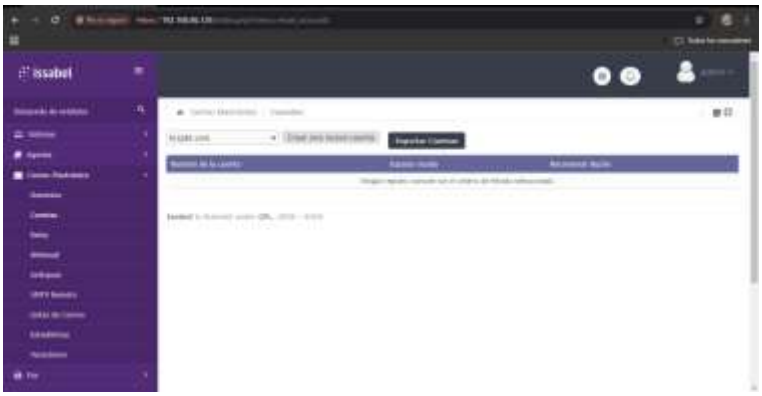


Figura 110

Seleccionamos el Dominio y Creamos una Cuenta

administración@hrsjdd.com

Contraseña: 1234

Cuota (KB): * 2000

Guardamos

Figura 111

Continuamos Creamos Para Todas las Extensiones

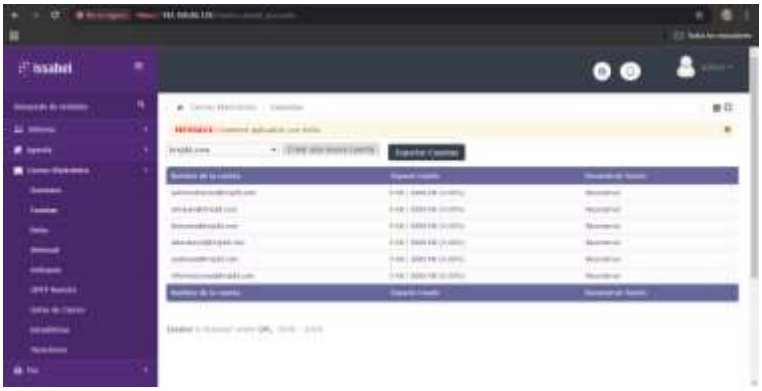


Figura 112

Entramos a la Extensión Creada para Administración

Cambiamos Ring Time a 7seg (si no hay respuesta de llamada)

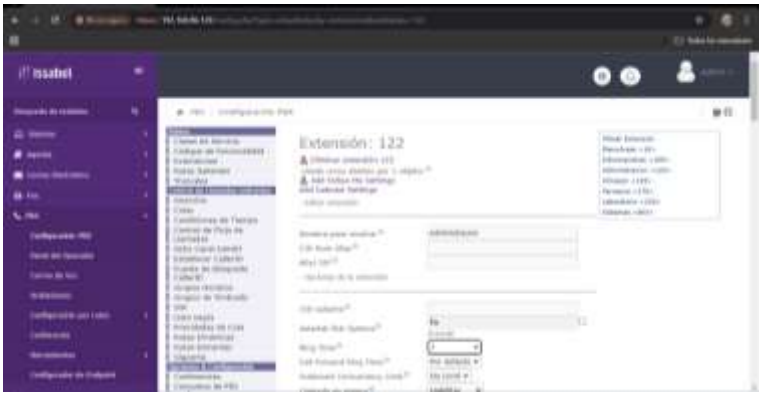


Figura 113

Bajamos Hasta Buzón de Voz y lo Habilitamos

Colocamos la Contraseña 1234

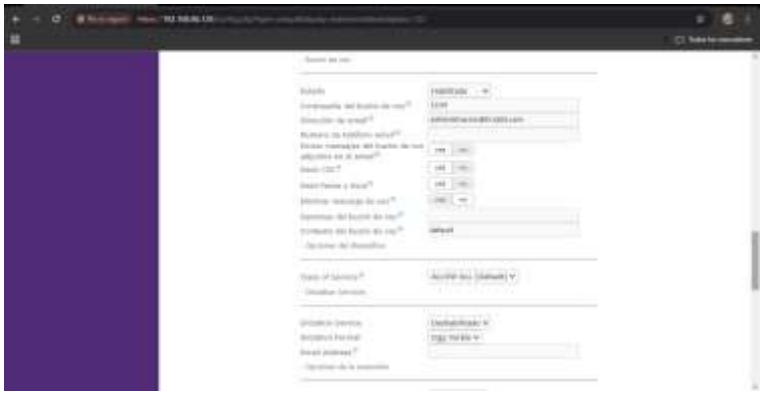
Dirección de Email administracion@hrsjdd.com

Enviar Mensajes del Buzón de Voz Adjuntos en el Email: yes

Decir CID: yes

Decir Fecha y Hora: yes

Aceptamos los Cambios



Configuración dispositivo móvil con el servidor

Figura 114

Tenemos que estar Conectados a la red Wifi del Hospital HRSJDD

Figura 115

Descargamos la Aplicación Zoiper del Google Play

Figura 116

Dentro de la Aplicación Necesitamos Colocar la Extensión Creada Seguido de @ y la Dirección del Servidor de Telefonía IP y la Contraseña Creada en el Servidor

Username

139@192.168.231.128

Password

HRSJDD139

Figura 117

En Hostname Dejamos la IP del Servidor de Telefonía IP

Figura 118

Mantenemos por defecto la Configuración del Proxy

Figura 119

Esperamos la Conexión SIP UDP (si marco verde) la Configuración fue Todo un Éxito

Figura 120

Verificamos que la Cuenta Este Activada

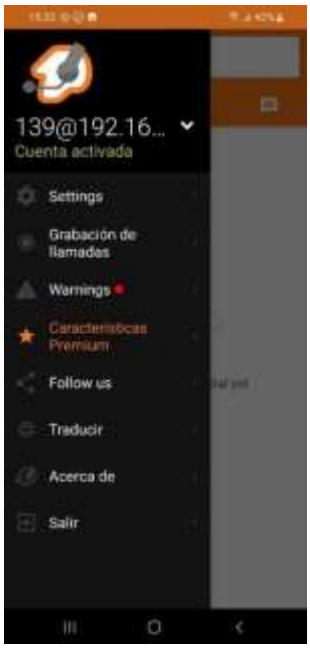


Figura 121

Podemos Comenzar a Usar los Teléfonos Mediante la Telefonía IP

Figura 122

Podemos ver el Historial de Llamadas

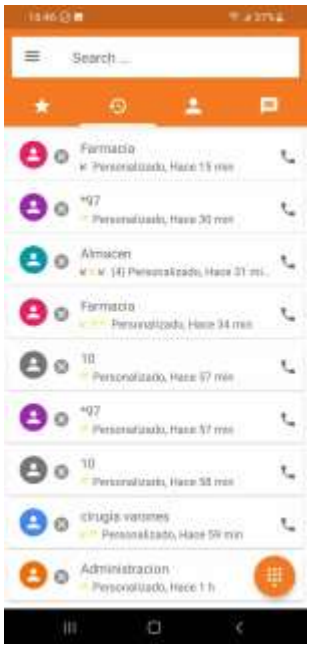


Figura 123

Podemos Vincular Nuestros Contactos

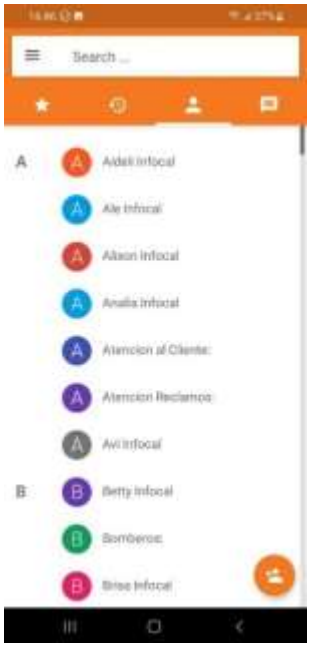


Figura 124

Prueba de Llamada Entramos al Teléfono

Figura 125

Marcamos *60 Para Escuchar la Hora

Figura 126

Interfaz de Llamada Entrante

Figura 127

Interfaz de Llamada en Espera a Contestar

Beneficios y comparativa al usar el servidor de telefonia IP Issabel

Tabla 16

Comparativa de una central de telefonía IP externa a 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 y configuraciones están alojados en los servidores del proveedor, lo que puede ser un riesgo para la privacidad.	Totalmente local, los datos 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	Muy alta en redes locales, ya que no depende de factores externos. Además, puedes configurar redundancia

	embargo, puede ser vulnerable a fallas de internet o problemas con el proveedor.	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 sistema.	No necesarios. Puedes usar Zoiper o cualquier softphone.
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 17

Comparativa con la central de telefonía fija Cossett

Característica	Issabel (Telefonía IP)	Telefonía Tradicional
Costo de llamadas internas	Gratis entre usuarios de la	Pago por cada llamada

	misma red (si están en la misma central)	interna si está fuera de tu red local
Requiere infraestructura de red	Sí, una red local o acceso a internet es necesario	No, solo necesitas línea telefónica fija
Escalabilidad	Alta: Puedes agregar extensiones sin instalar más cables	Baja: Necesitas contratar nuevas líneas telefónicas físicas
Movilidad	Alta: Funciona en cualquier lugar con acceso a internet	Baja: Solo funciona en la ubicación de la línea telefónica fija
Funciones avanzadas	Alta: IVR, conferencias, grabación de llamadas, etc.	Baja: Limitado a llamadas, mensajes de voz y poco más
Tarifas mensuales	No cuenta con tarifas mesuales	Pagos mensuales por la utilizacion de cada linea de telefonia fija
Precio de compra de Teléfono Panasonic KX-TS500	Sin gasto ya que no requiere comprar teléfonos fijos	32 teléfonos para cada área precio unitario Bs. 194,70 precio total Bs 6230,4

3.4. Diseño Físico

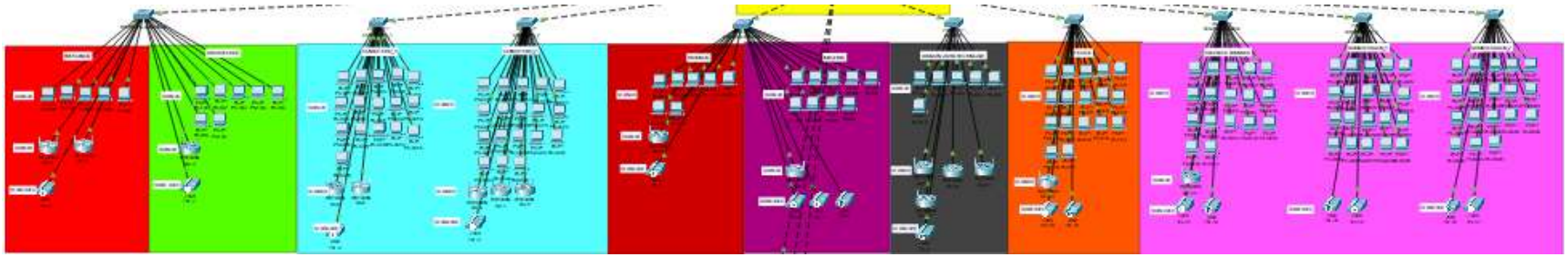
3.4.1 VLAN

Separación de la red por áreas y vlans

	Emergencias	(vlan 30)
	Laboratorios	(vlan 30)
	Consultorios	(vlan 20)
	Farmacia	(vlan 30)
	Imágenes	(vlan 30)
	Almacén (Área Restringida)	(vlan 30)
	Fichaje	(vlan 20)
	Administración	(vlan 10)

Figura 128

Prototipo de Red por Áreas y VLAN Planta Baja



	1er Piso	(vlan 40)
	2do Piso	(vlan 40)
	3er Piso	(vlan 40)

Figura 129

Prototipo de Red por Áreas y VLAN 1er 2do y 3er Piso

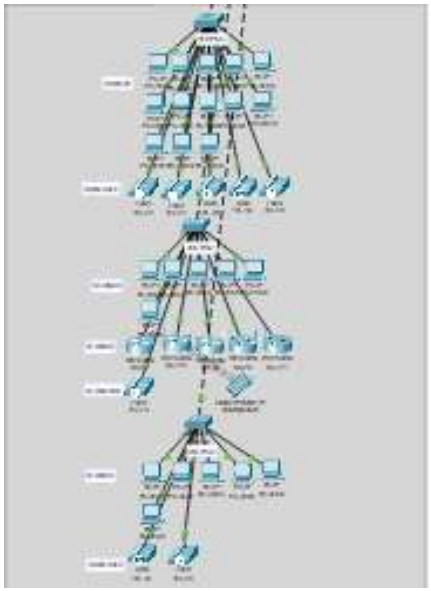


Figura 130

Plano de la Planta Baja por Áreas

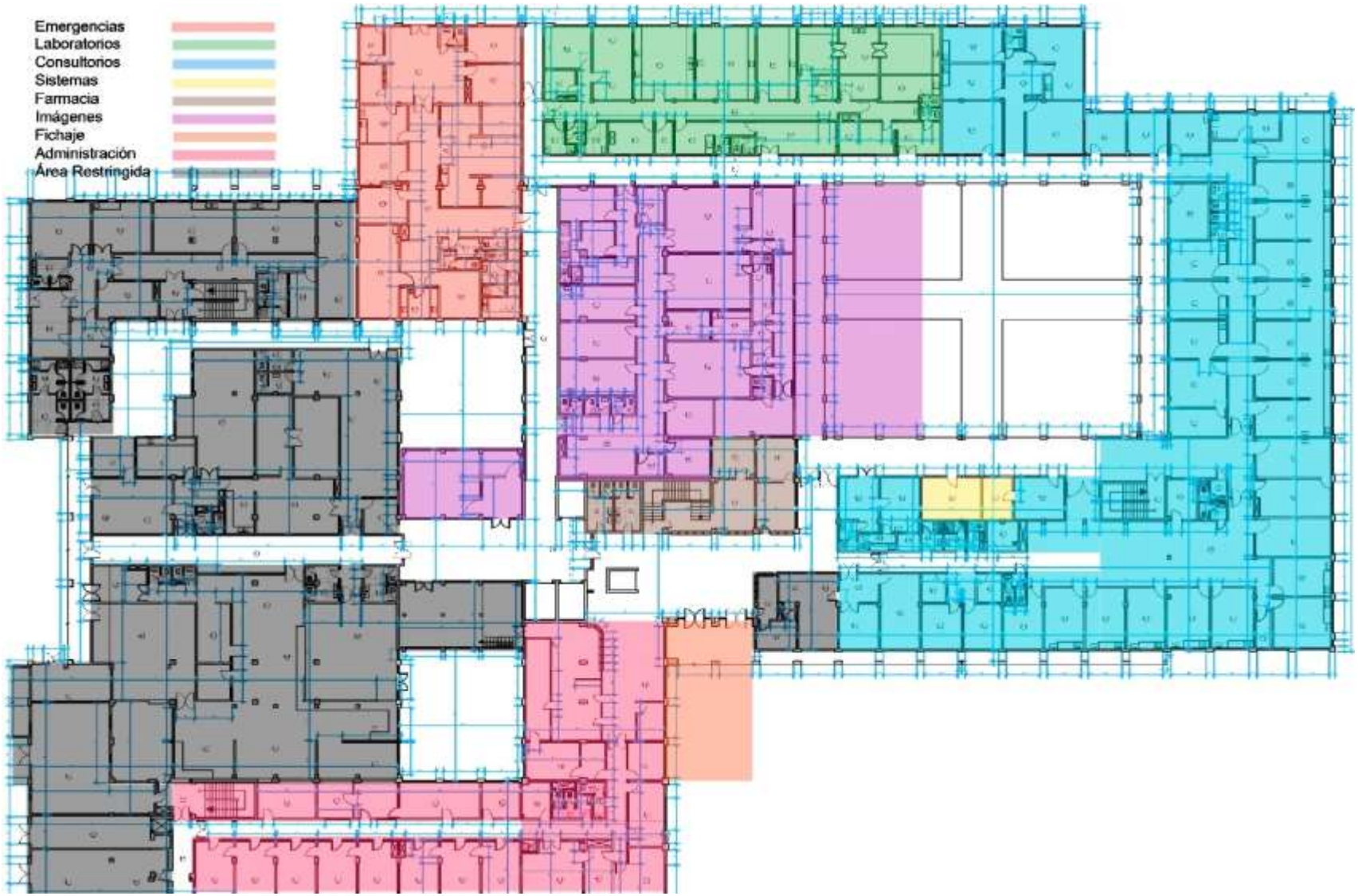


Figura 131

Simulación de la Ubicación del Área de Emergencias en el Hospital

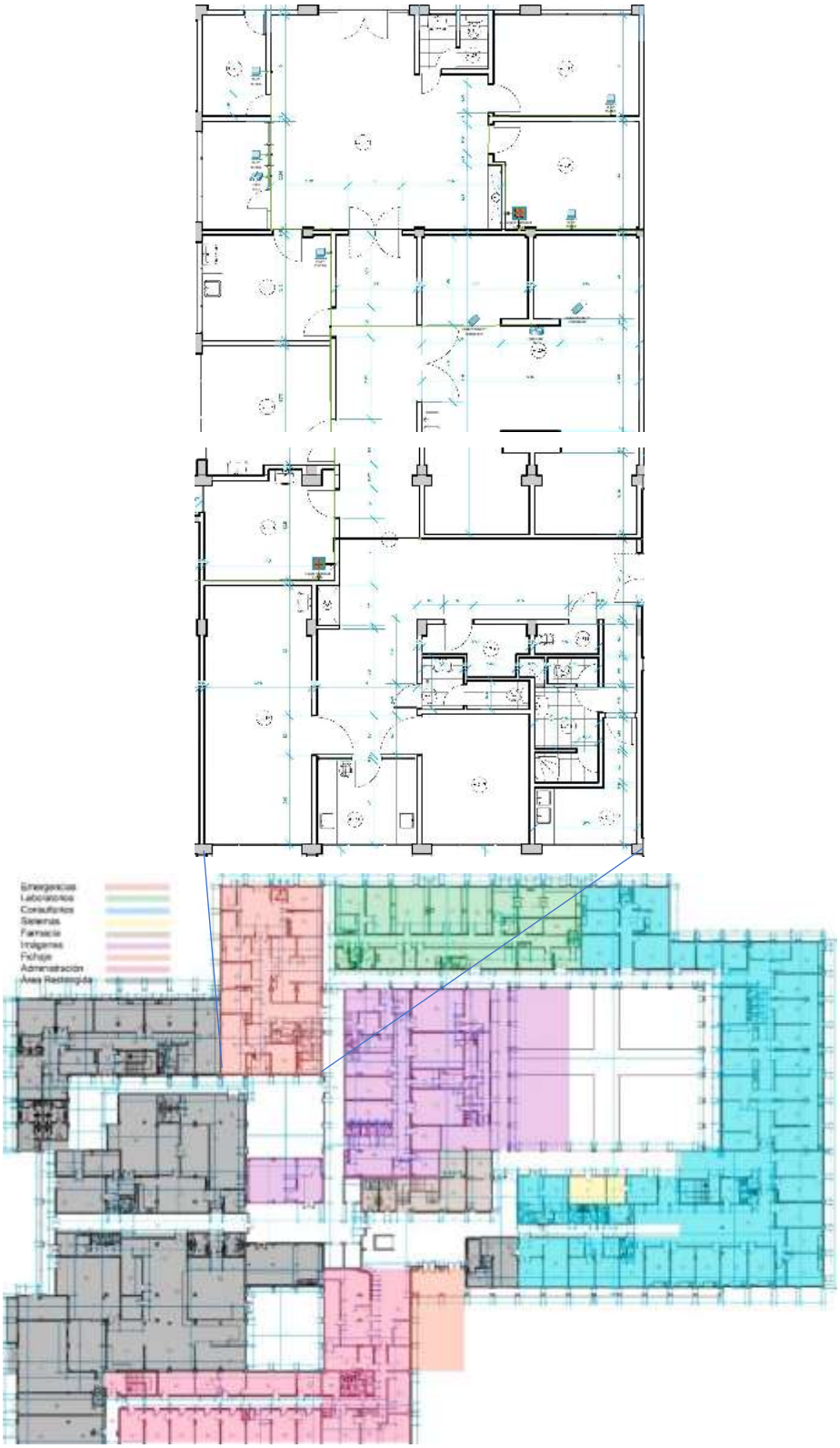


Figura 132

Simulación de la Ubicación del Área de Laboratorios en el Hospital

Figura 133

Simulación de la Ubicación del Área de Consultorios en el Hospital

Figura 134

Simulación de la Ubicación del Área de Sistemas en el Hospital

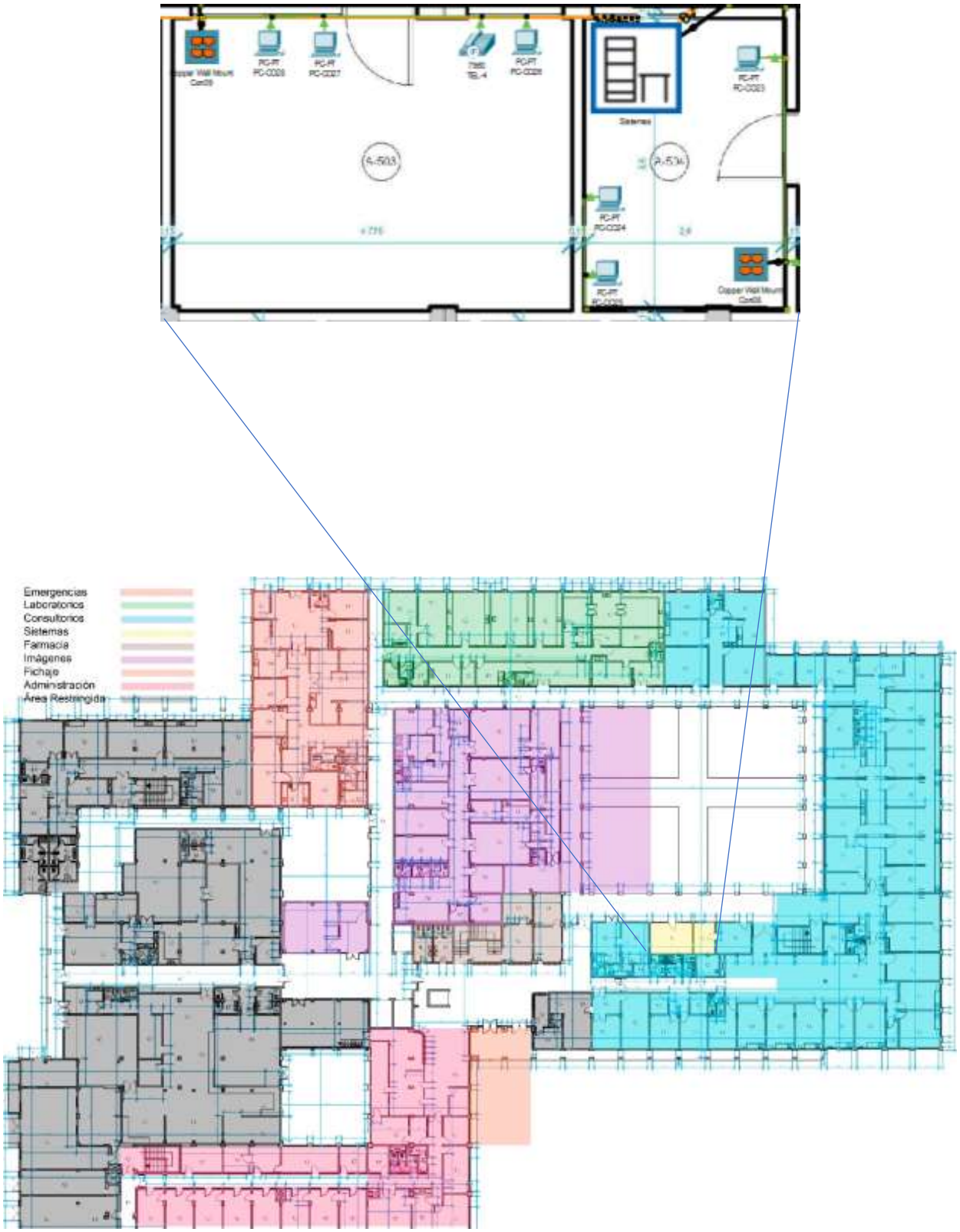


Figura 135

Simulación de la Ubicación del Área de Farmacia en el Hospital

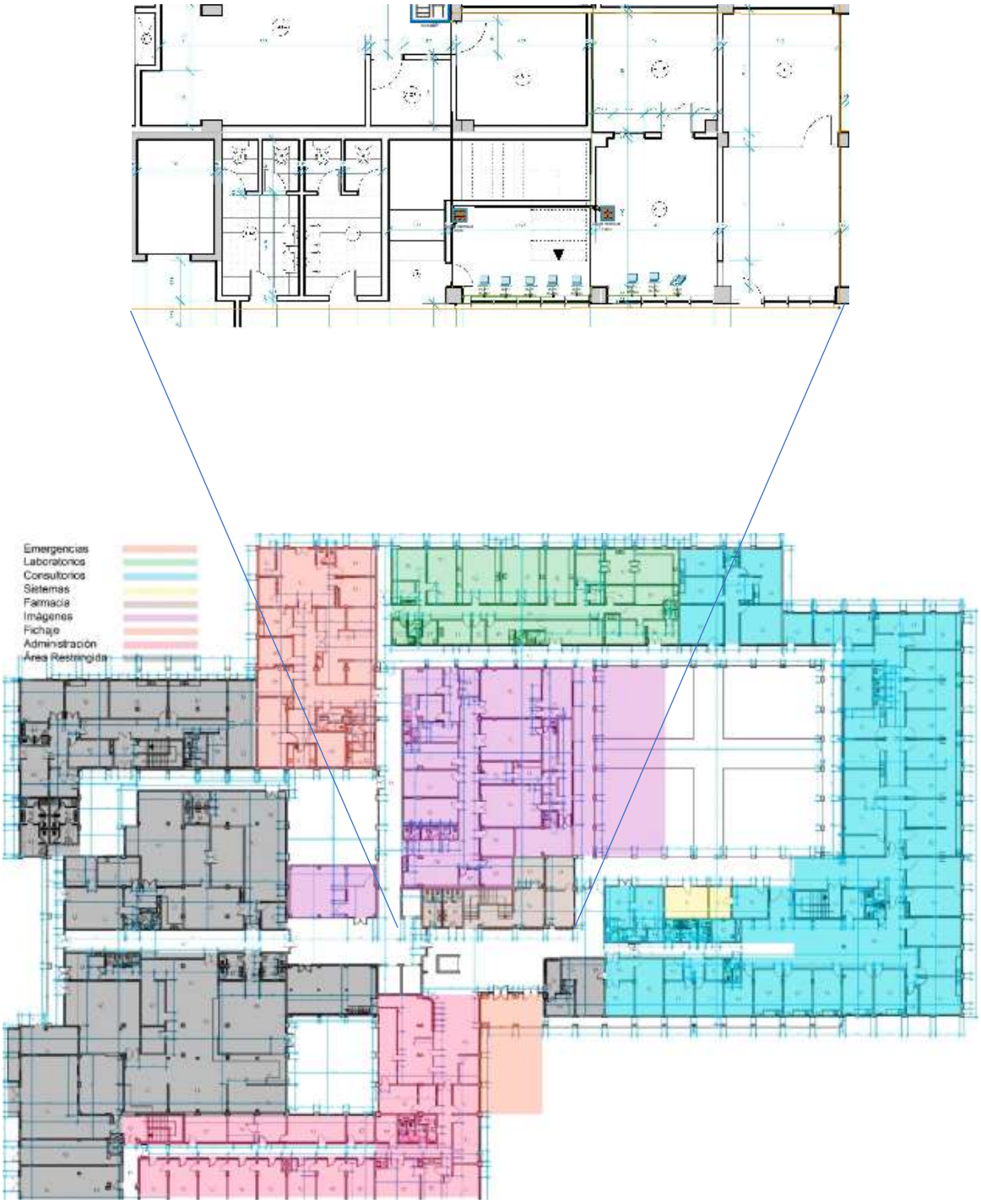


Figura 136

Simulación de la Ubicación del Área de Imágenes en el Hospital

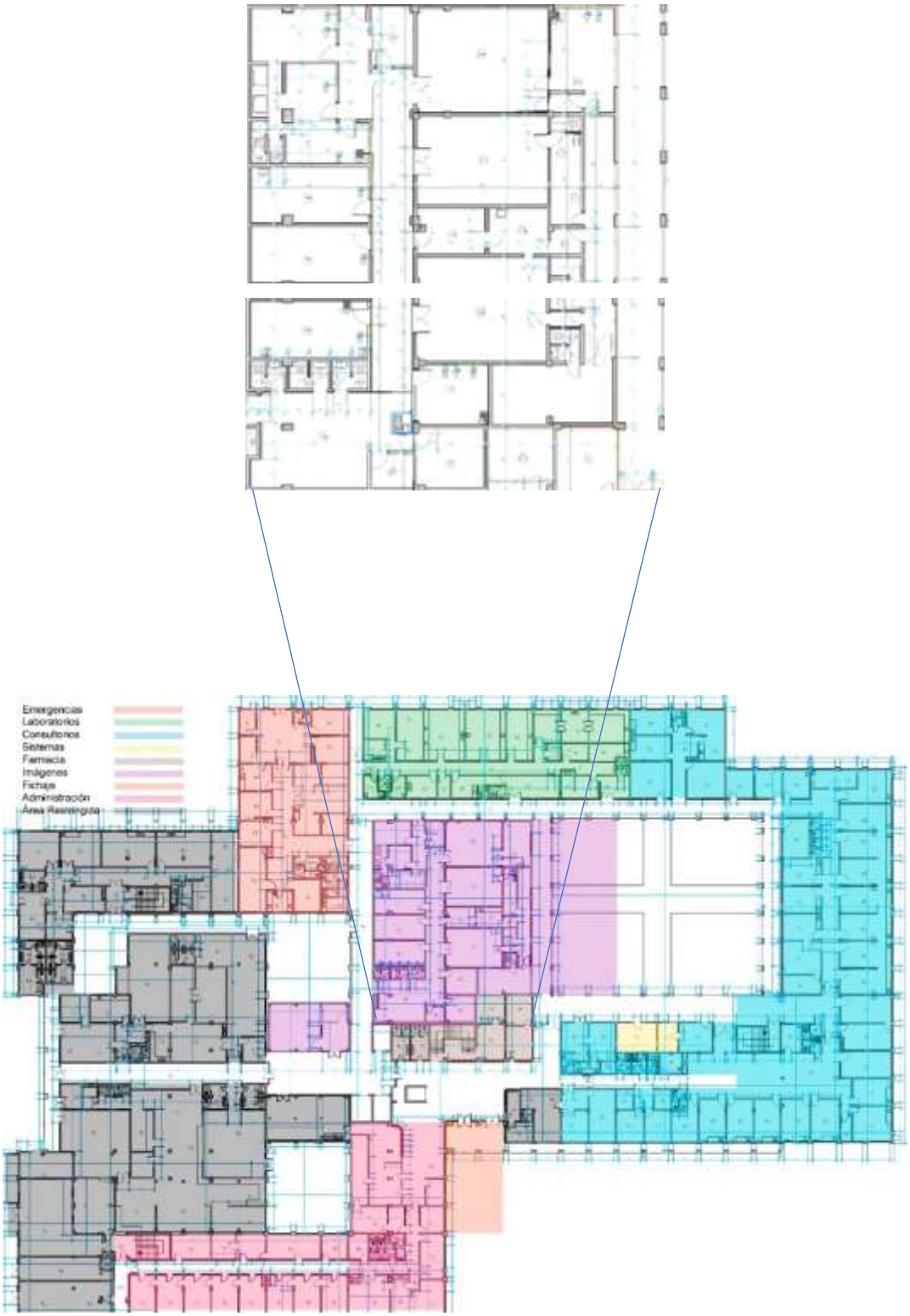


Figura 137

Simulación de la Ubicación del Área de Fichaje en el Hospital

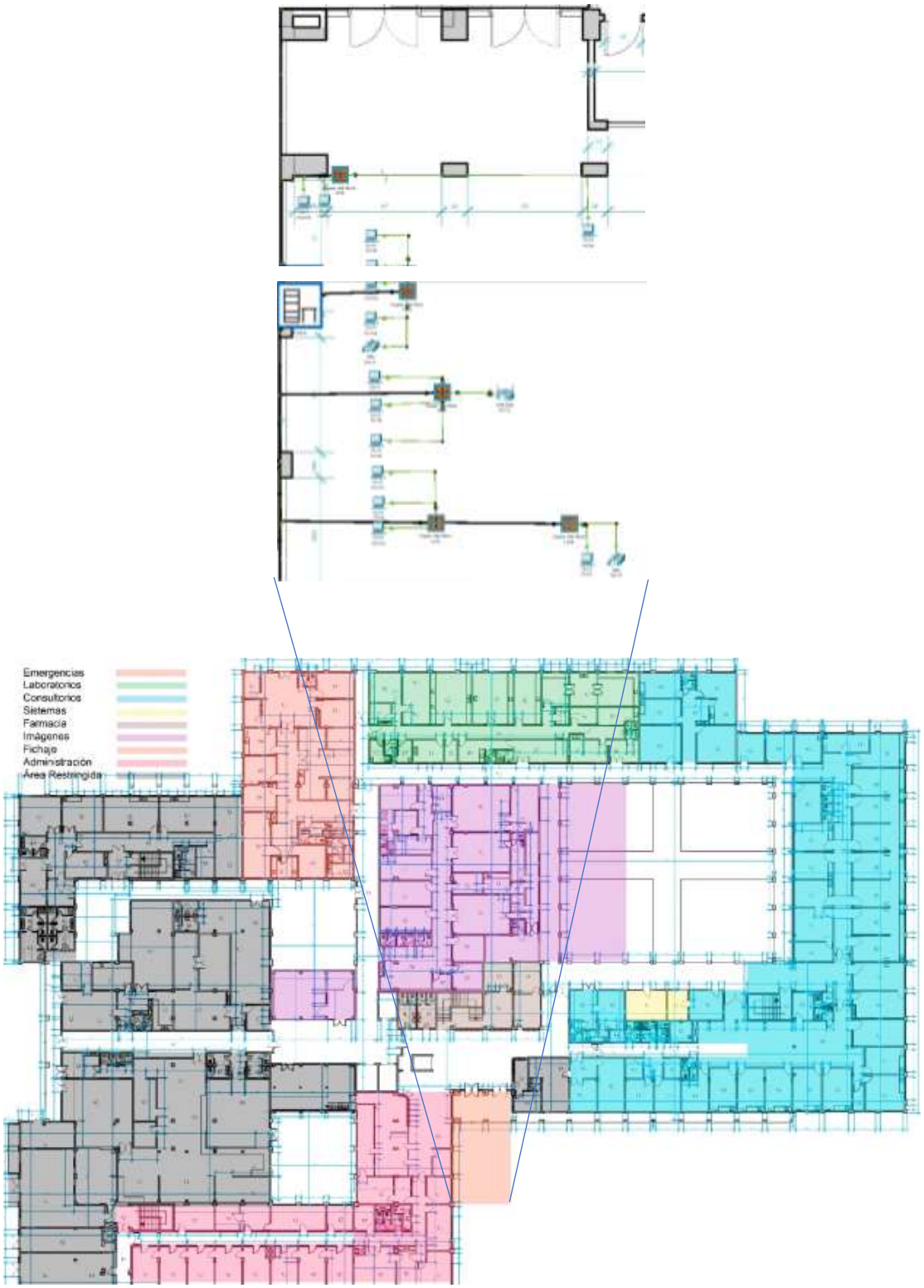


Figura 138

Simulación de la Ubicación del Área de Administración en el Hospital

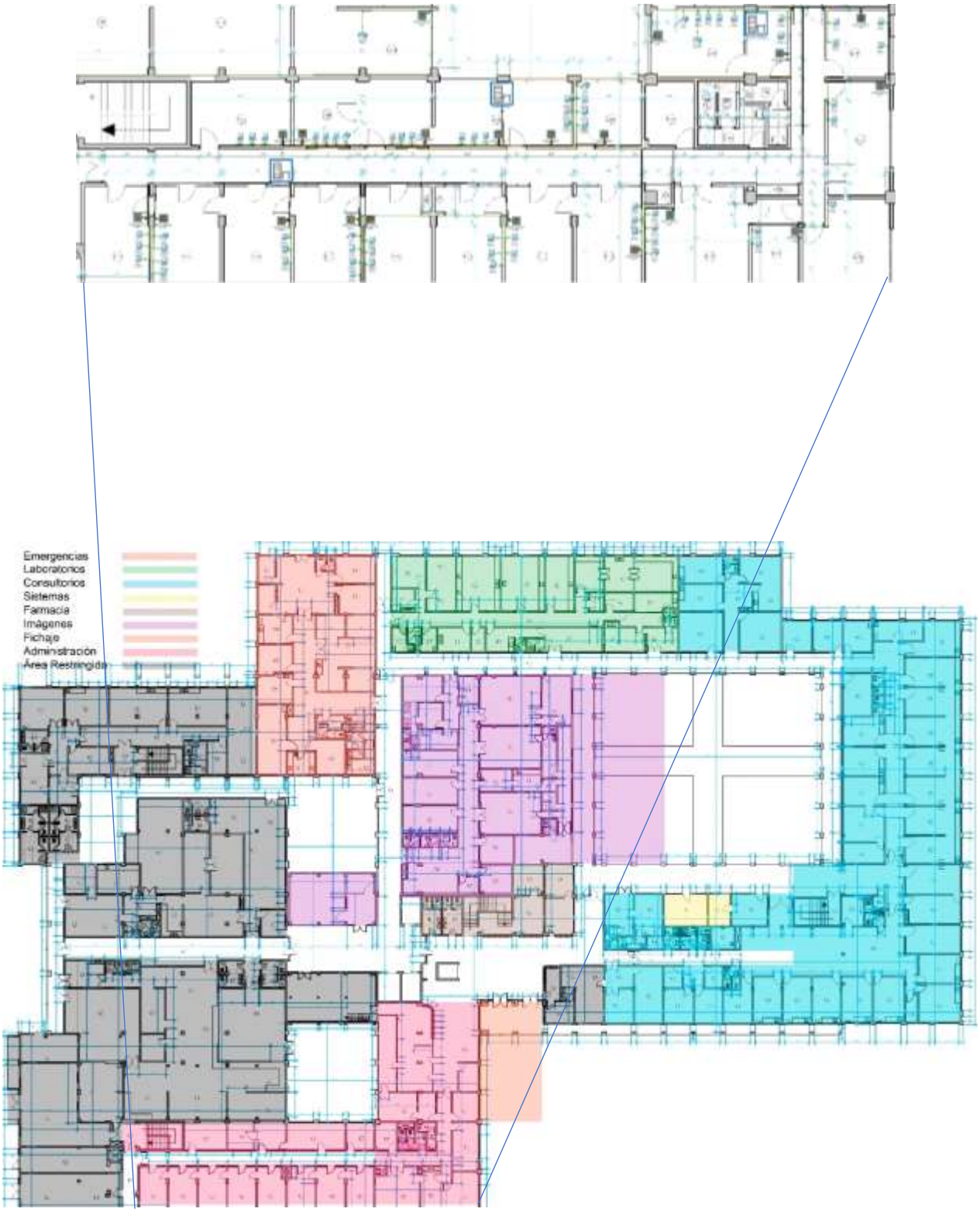
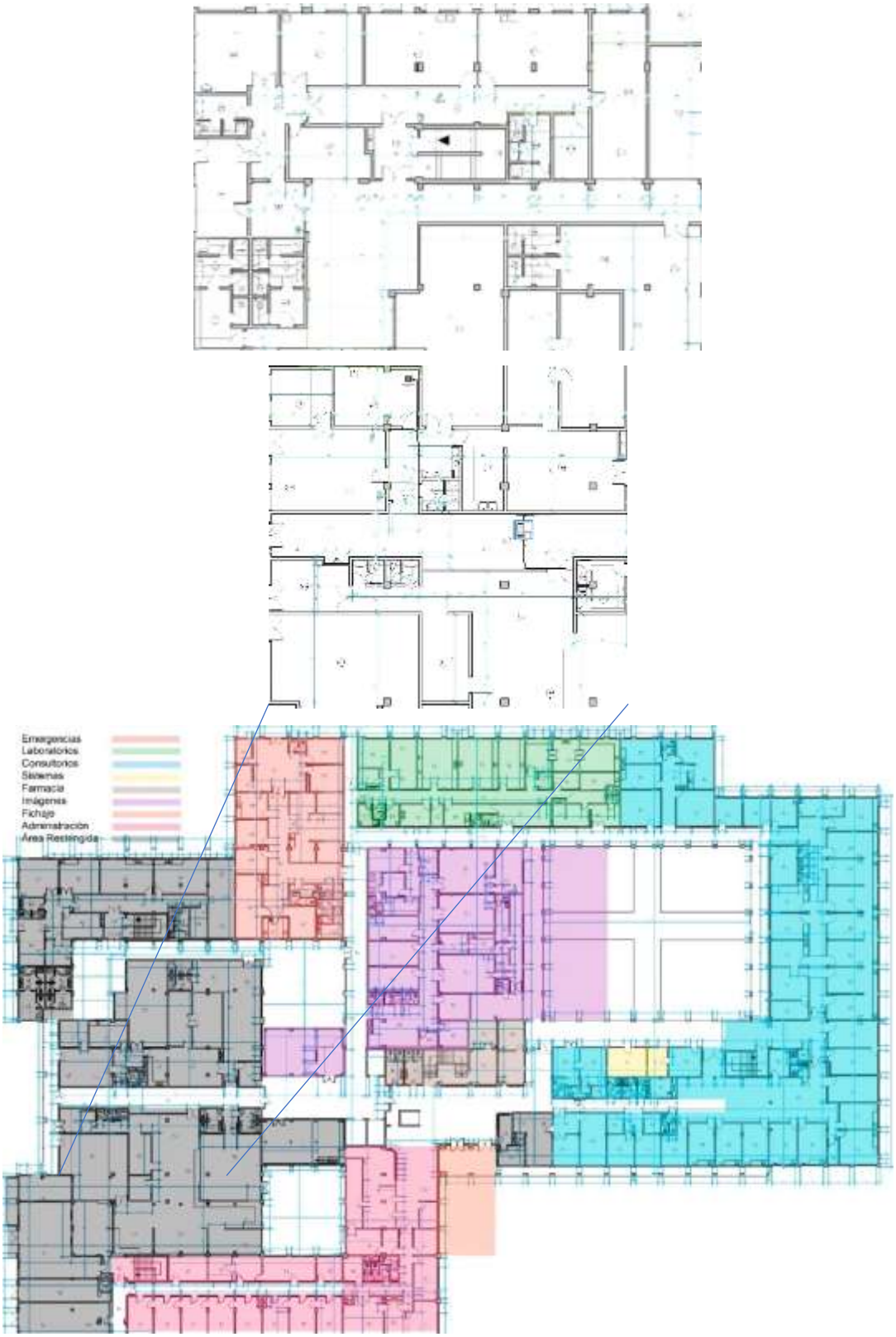


Figura 139

Simulación de la Ubicación del Área Restringida en el Hospital



3.4.2 Wi-Fi

Ubicación de los Access Points en toda la empresa

Figura 140

Access Points Ubicados por Toda la Planta Baja y que Brinda También Conexión Inalámbrica al 1er Piso

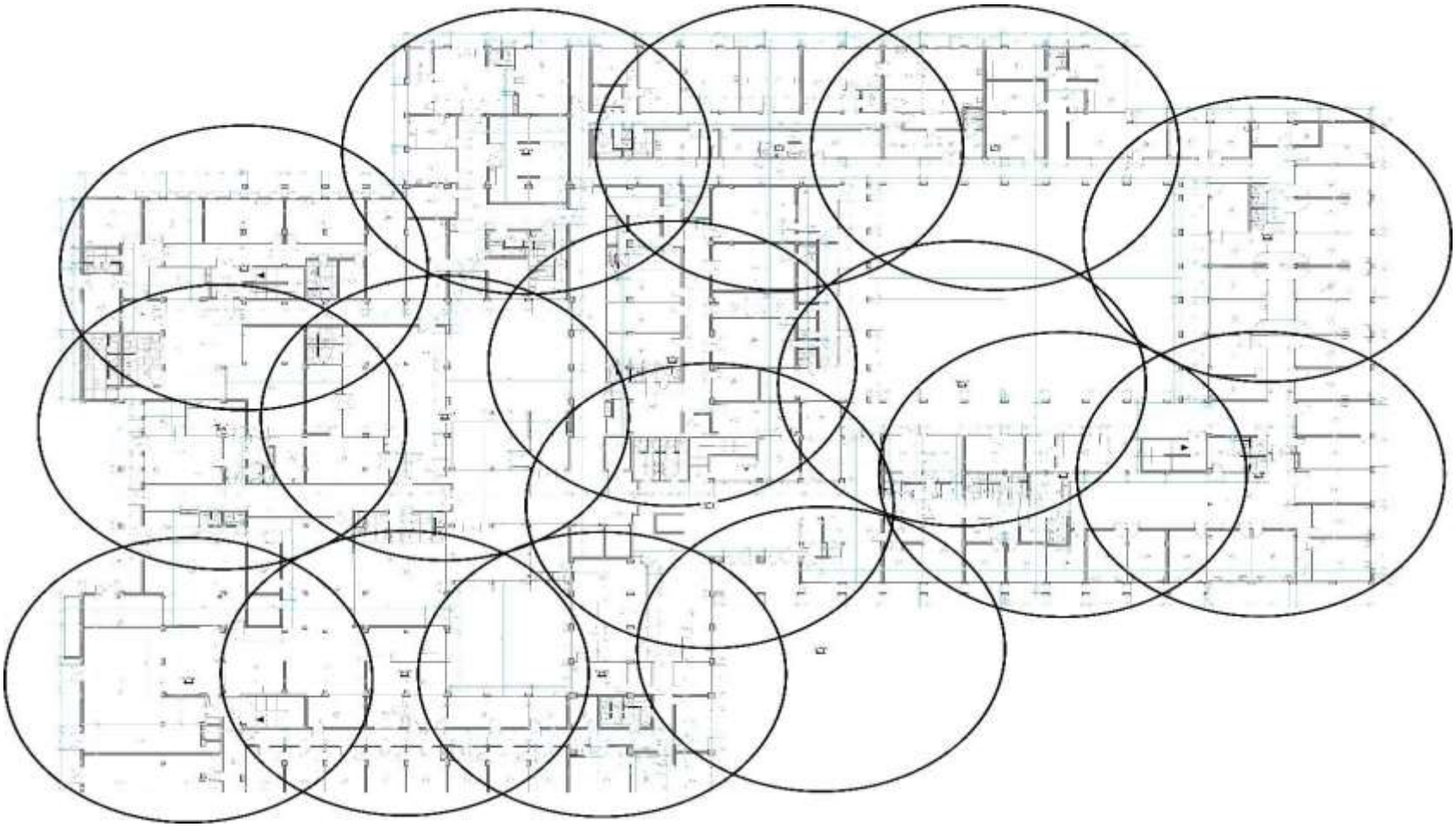


Figura 141

Access Points Ubicados en el 2do Piso del Hospital que Brinda También Conexión Inalámbrica al 3er Piso

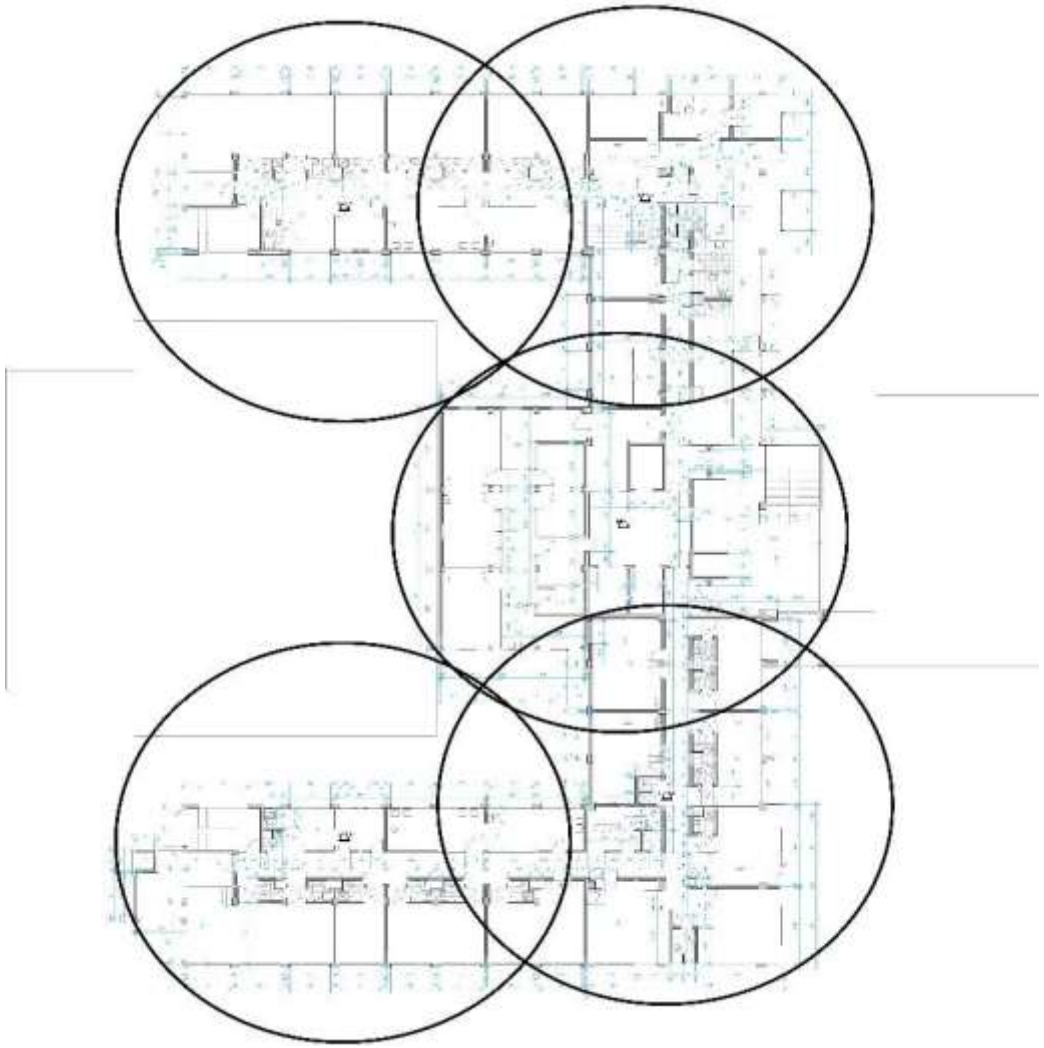


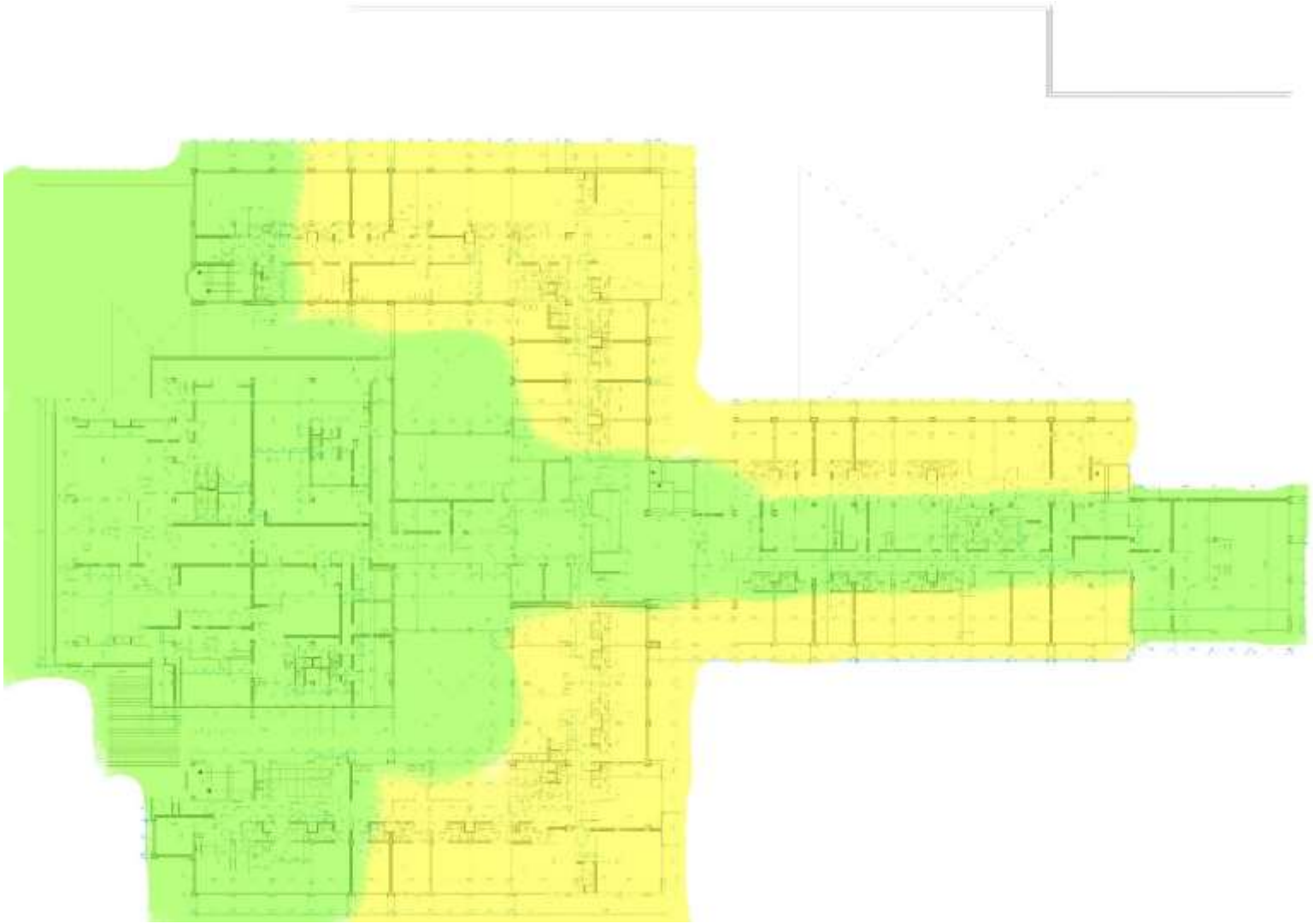
Figura 142

Simulación del Mapa de Calor del Wifi de la Planta Baja del Hospital

Mapa de calor de la planta baja indicando el mayor número de personas en la zona roja, regular en zona amarilla y baja en zona verde

Figura 143

Simulación del Mapa de Calor del Wifi del 1er Piso del Hospital



Mapa de calor del primer piso indicando que el promedio de personas es regular en zona amarilla y baja en zona verde

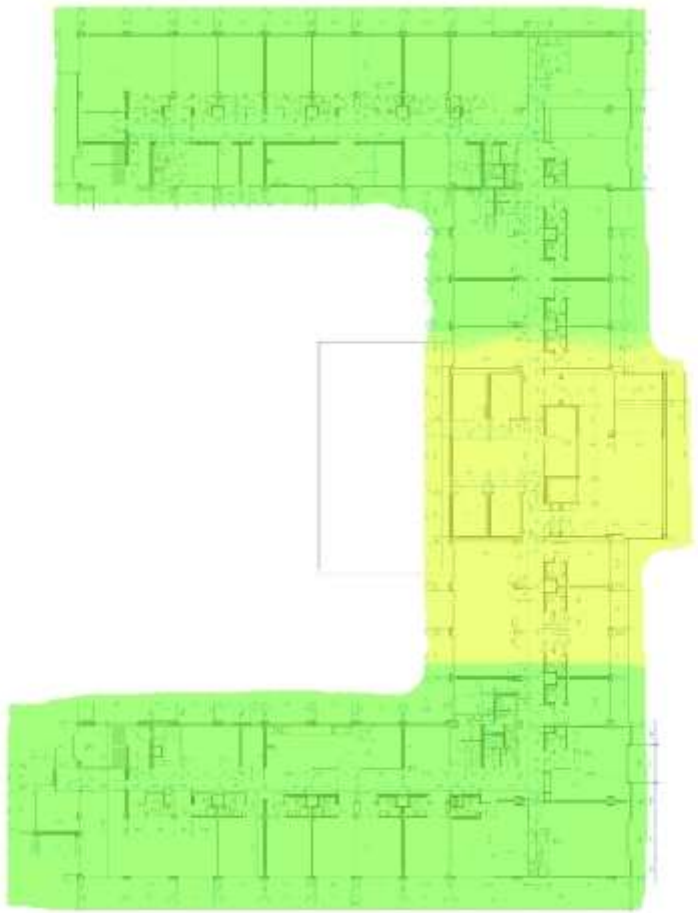
Figura 144

Simulación del Mapa de Calor del Wifi del 2do Piso del Hospital

Mapa de calor del segundo piso indicando que el promedio de personas es regular en zona amarilla y baja en zona verde

Figura 145

Simulación del Mapa de Calor del Wifi del 3er Piso del Hospital



Mapa de calor del tercer piso indicando que el promedio de personas es regular en zona amarilla y baja en zona verde

3.5. Gestión de costos del proyecto

Tabla 18

Costos del Proyecto

Accesorio	Modelo	Cantidad	Precio Unitario	Precio Total
Cable de red	Categoría 6	5107mts	1.5bs el metro	7660.5bs
Conectores	Rj45	889	1bs	889bs
Router	CISCO2811	1	75$	522bs
Switch	WS-C2960-24TT-L	14	749$	72982,56bs
Switch	WS-C3650-24PS-E	1	5390$	37111,96bs
Pach panel	Cat6 24P	13	54$	4885,92bs
Placa de pared	Cat6-4port	62	13$	5609,76bs
Access Points	Tp-Link EAP620 HD	21	170$	24847.2bs
Servidor	PowerEdge R620	1	210$	1461,6bs
Rack de pared	4 RU	3	59$	1231,92bs
Internet Entel	800 Mbps	1año	869bs	10428bs
Instalación	De todo el proyecto	1	3275$	22794bs
Total				190.424,42bs

Tabla 19

Desglose de costos de instalación de red

Componente	Descripción	Precio
Cables	Tendido de cable desde el punto de conexión hasta los puntos de acceso a la red	$2,000
Placas de pared	Tomas de corriente para puntos de acceso a la red	$200
Conmutadores de red	Conecta varios dispositivos al mismo enrutador	$50
Puerto Ethernet	Conecta dispositivos a la red de malla local	$70
Router	Permite que los dispositivos	$80

	accedan a la conexión a Internet	
Uniones de cable	Organice los cables para facilitar el mantenimiento y las modificaciones	$5
Wi-Fi Extender	Ampliar la cobertura de la red inalámbrica	$60
Divisor de Ethernet	Conecte varios dispositivos a una red de área local	$10
Reemplazos de hardware	Reemplazos de hardware	$300
Servidor	Instalación y configuración de servidores	$500
Total		$3275

3.6. Implementación, prototipo o simulación

En esta sección se describe la implementación de la infraestructura de red del Hospital Regional San Juan de Dios de Tarija. Para ilustrar la efectividad de las mejoras realizadas, se realizará una demostración en tiempo real de la red optimizada. Esta demostración incluirá la visualización de la configuración de VLAN, Wifi y la configuración del Servidor de Telefonía IP la conectividad de los dispositivos, permitiendo observar el funcionamiento y la eficiencia de la red.

Figura 146

Estándares de cableado estructurado implementados en la parte física de la simulación

Figura 147

Estándares de etiquetado en el área de sistemas

Figura 148

Implementación de la topología jerárquica en la parte lógica de la simulación

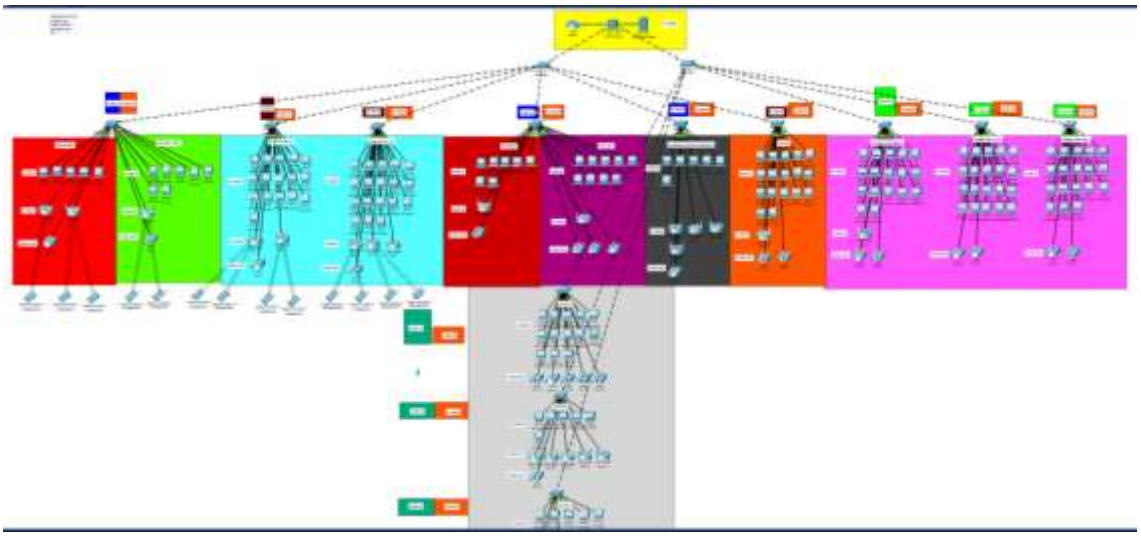


Figura 149

Simulación de la tabla de ruteo del router y sus caminos

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

Gateway of last resort is not set

     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, FastEthernet0/0.10
L       192.168.10.1/32 is directly connected, FastEthernet0/0.10
     192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.20.0/24 is directly connected, FastEthernet0/0.20
L       192.168.20.1/32 is directly connected, FastEthernet0/0.20
     192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.30.0/24 is directly connected, FastEthernet0/0.30
L       192.168.30.1/32 is directly connected, FastEthernet0/0.30
     192.168.40.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.40.0/24 is directly connected, FastEthernet0/0.40
L       192.168.40.1/32 is directly connected, FastEthernet0/0.40
     192.168.50.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.50.0/24 is directly connected, FastEthernet0/0.50
L       192.168.50.1/32 is directly connected, FastEthernet0/0.50
     192.168.231.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.231.0/24 is directly connected, FastEthernet0/0
L       192.168.231.1/32 is directly connected, FastEthernet0/0

Router#
```

Figura 150

Mapa de cobertura del wifi en la simulación de packet tracer planta baja

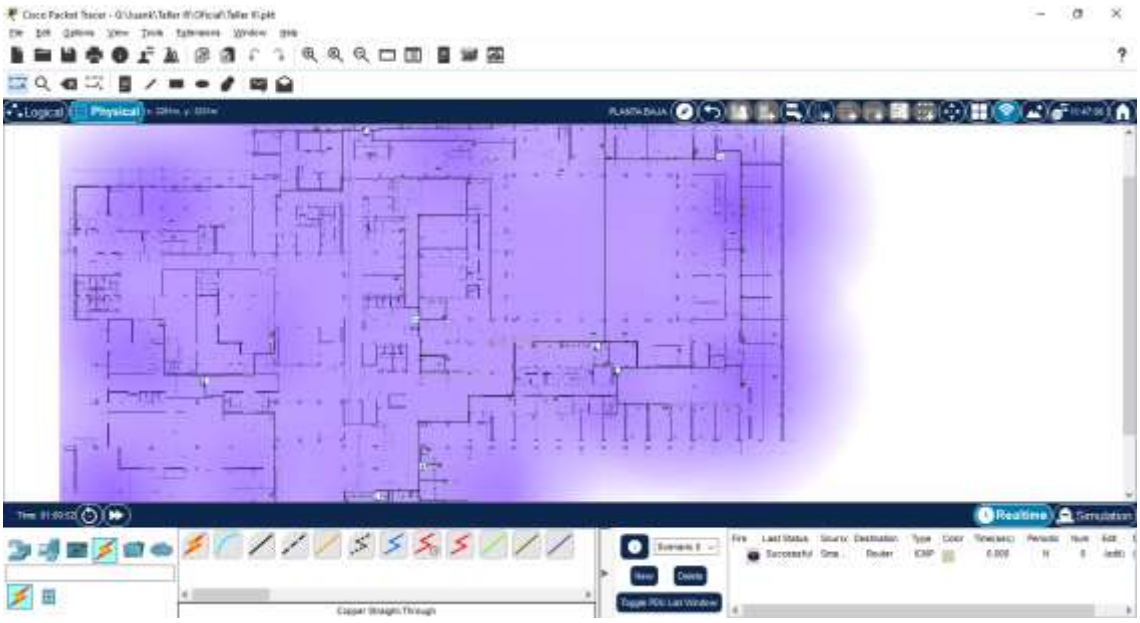


Figura 151

Simulación de la Conexión inalámbrica a los dispositivos móviles

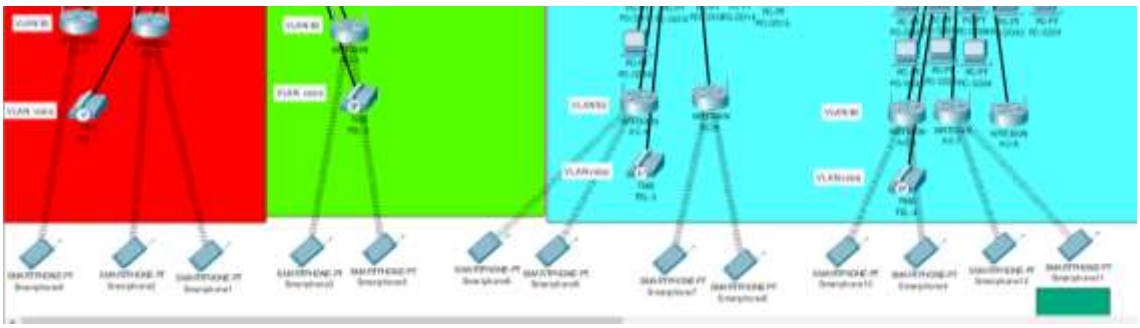
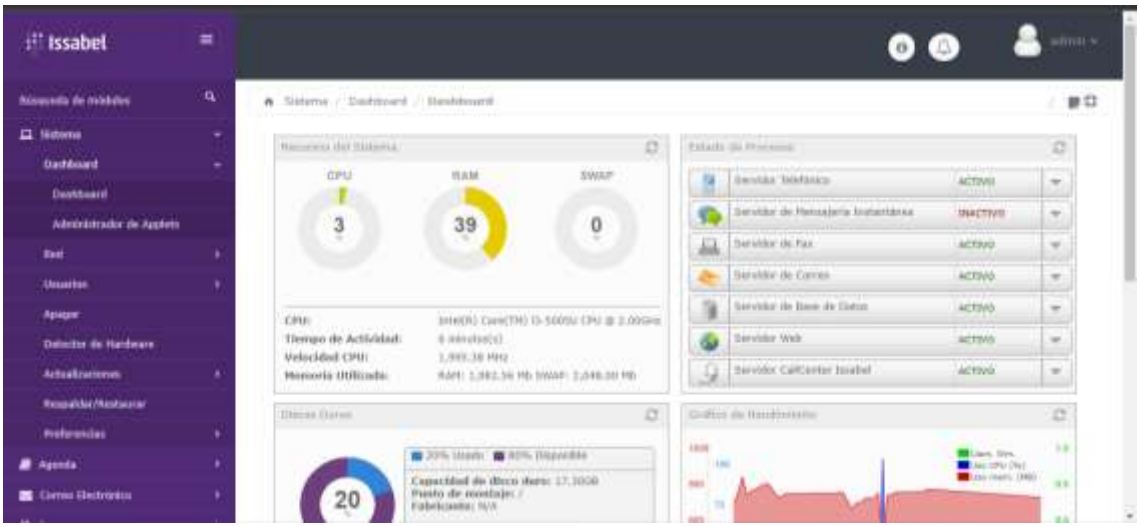


Figura 152

Diagnóstico del estado del servidor de telefonía IP



3.7. Pruebas y validación

Figura 153

Tiempos de Respuesta Esperados en el Trafico de Red con un Testeo de Red

Tabla 20

Dispositivos Necesarios para la Implementación

Dispositivos	Modelo	Cantidad	Observación
Router	TP-Link ER605	Obsoleto	Desactualizado
Switch	Tp-link TL-SG1024	Obsoleto	No soporta VLAN
Racks de Pared	6RU	Necesario	Aun útil para la implementación
Rack de Piso	18U	Necesario	Aun útil para la implementación
Computadoras	Delux	Necesario	Aun útil para la

			implementación
Cable UTP	Categoria 6	Nuevo	Necesario para la implementación
Conector de cable	Rj45	Nuevo	Necesario para la implementación
Router	Cisco2811	Nuevo	Necesario para la implementación
Switch	WS-C2960-24TT-L	Nuevo	Necesario para la implementación
Switch	WS-C3650-24PS-E	Nuevo	Necesario para la implementación
Pach panel	Cat6 24P	Nuevo	Necesario para la implementación
Access Points	Tp-Link EAP620 HD	Nuevo	Necesario para la implementación
Servidor	PowerEdge R620	Nuevo	Necesario para la implementación

Figura 154

Diagrama de Red Propuesto Para la Implementación

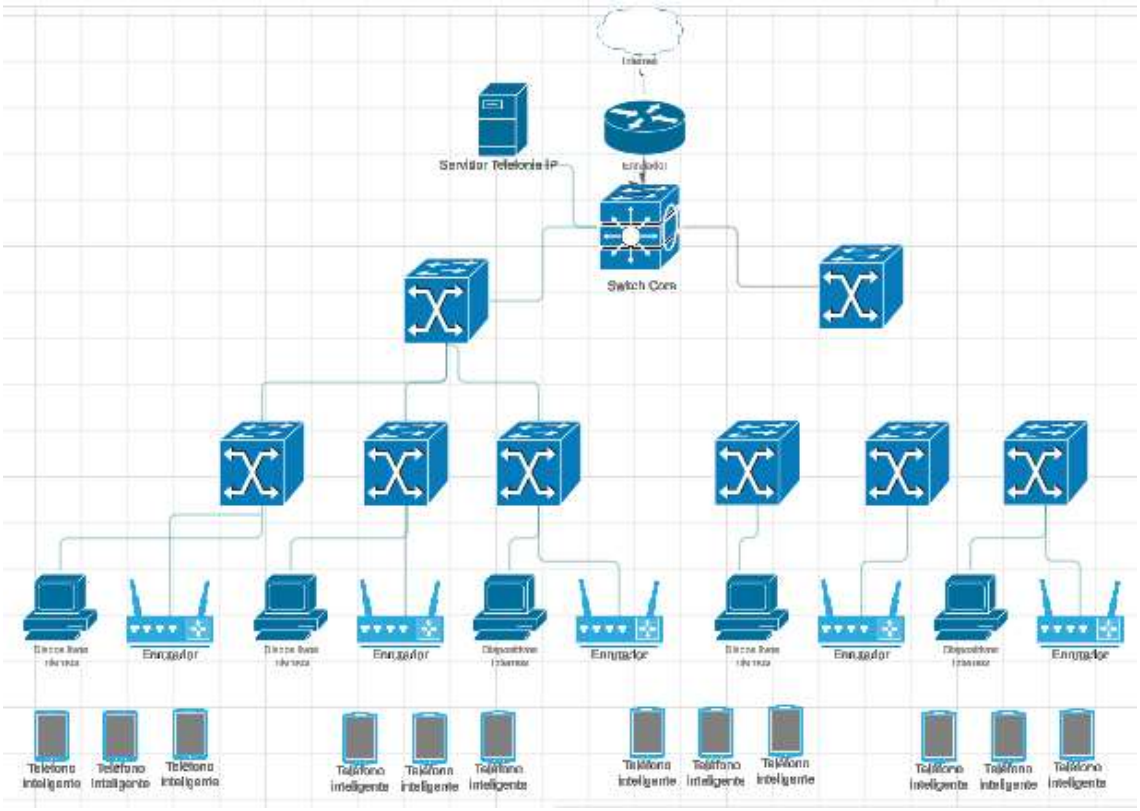


Figura 155

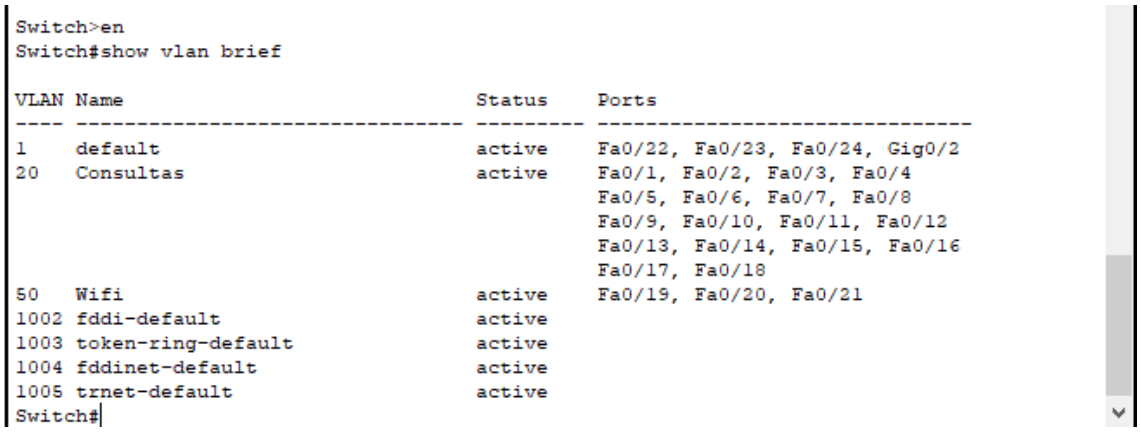
Simulación de las VLAN 10,50 Creadas en los Switch

```
Switch>en
Switch#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/23, Fa0/24, Gig0/2
10   Administrativos                   active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
50   Wifi                              active    Fa0/21, Fa0/22
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#
```

Figura 156

Simulación de las VLAN 20,50 Creadas en los Switch

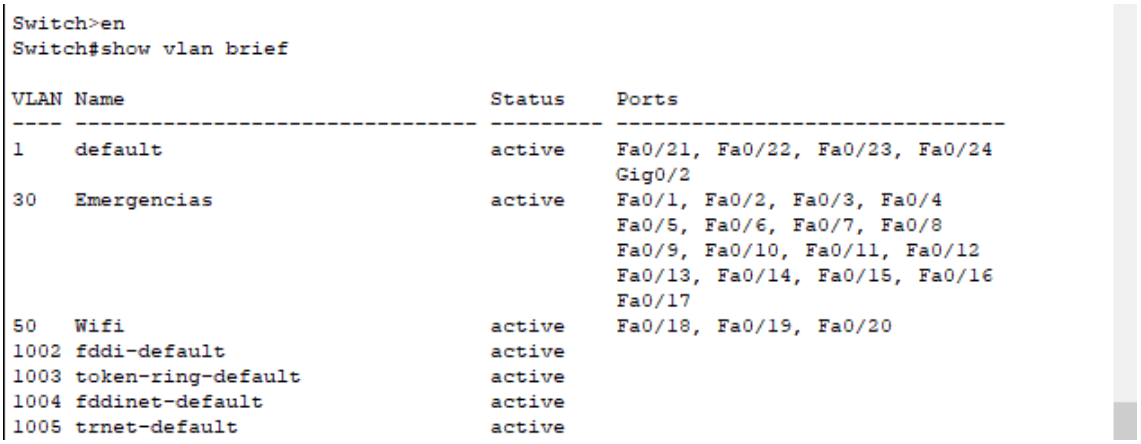


```
Switch>en
Switch#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/22, Fa0/23, Fa0/24, Gig0/2
20   Consultas                         active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18
50   Wifi                              active    Fa0/19, Fa0/20, Fa0/21
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#
```

Figura 157

Simulación de las VLAN 30,50 Creadas en los Switch



```
Switch>en
Switch#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/2
30   Emergencias                       active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17
50   Wifi                              active    Fa0/18, Fa0/19, Fa0/20
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Figura 158

Simulación de las VLAN 40,50 Creadas en los Switch

```
Switch>en
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gig0/2
40   Internacion                      active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14
50   Wifi                             active    Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#
```

Figura 159

Interfaz de la Configuración del Wifi con su DHCP

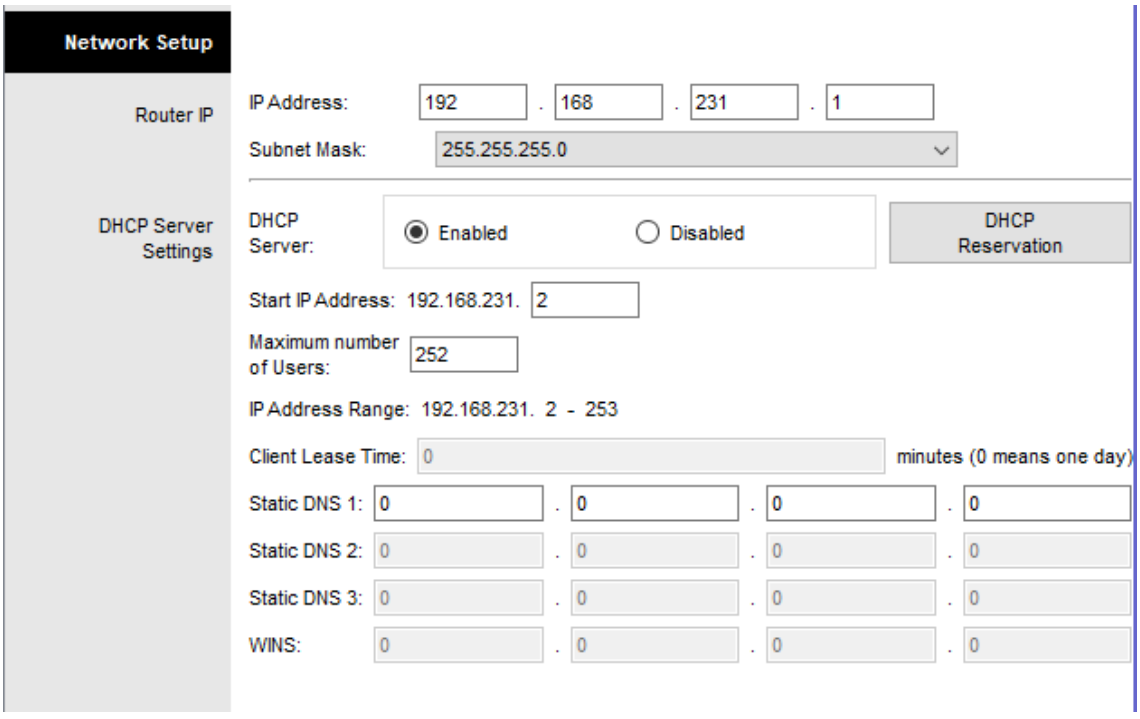
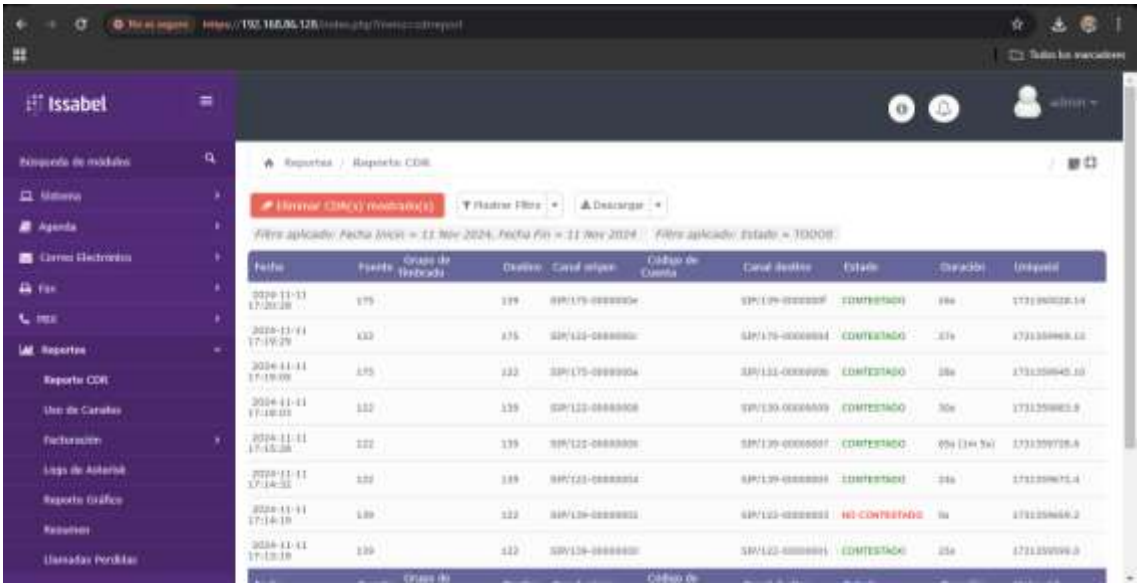


Figura 160

Registro de Llamadas del Hospital con el Servido de Telefonía IP



Soporte a futuras expansiones

Segmentación de red mediante VLANs

Diseño Modular y Escalable:

- Cada VLAN está asignada a un área tácticas del hospital (por ejemplo, administración, emergencias, fichaje). Este enfoque permite agregar nuevas áreas sin afectar las VLAN existentes.
- Switches gestionables con capacidad de crecimiento, permitiendo la creación de más VLANs cuando se incorporen nuevas alas o departamentos.
- Separación lógica del tráfico para mitigar colisiones de red y permitir un mejor rendimiento, incluso al aumentar la cantidad de dispositivos conectados.

Ejemplo de Expansión: Si en el futuro se inaugura un nuevo edificio, se pueden agregar switches y asignar nuevas VLANs sin alterar la configuración de los segmentos existentes.

Red Wi-Fi con conectividad avanzada

Cobertura Escalable:

- Los puntos de acceso (APs) serán ubicados estratégicamente para garantizar cobertura inicial, pero el diseño incluirá espacio para integrar APs adicionales según crezca el número de usuarios y dispositivos.

- Implementación de estándares modernos como Wi-Fi 6 para garantizar un rendimiento óptimo con alta densidad de dispositivos.

Ejemplo de Expansión: Si el hospital decide ofrecer servicios inalámbricos a visitantes o pacientes, se podrá implementar una VLAN específica para esta función sin impactar la red interna.

Servidor de comunicaciones unificadas basado en Asterisk

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 el hospital desea incluir extensiones para un nuevo departamento, se pueden añadir fácilmente con configuraciones en el software.

CAPITULO 4

CONCLUSIONES Y RECOMENDACIONES

4. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

- **Mejora en la Eficiencia de la Red:** La implementación de la tecnología VLAN y la configuración de una topología jerárquica han permitido optimizar el rendimiento de la red del hospital. La segmentación del tráfico no solo reduce la congestión, sino que también mejora la velocidad de acceso a la información crítica para la atención de los pacientes, lo que se traduce en un servicio más ágil y eficiente.

- **Aumento de la Seguridad:** Con la implementación de contraseñas para acceder a cada switch y la creación de una red Wi-Fi 6 encriptada, se han fortalecido las medidas de seguridad de la infraestructura de red. Estas acciones minimizan el riesgo de accesos no autorizados y protegen los datos sensibles, garantizando así la confidencialidad y la integridad de la información de los pacientes y del personal.

- **Facilitación de la Comunicación Interna:** La integración de un servidor de comunicaciones unificadas basado en Asterisk permitirá al personal del hospital comunicarse de manera más efectiva y directa. Esta mejora en la comunicación interna resulta esencial para la coordinación de actividades, especialmente en situaciones de emergencia, donde cada segundo cuenta.

- **Impacto Positivo en la Atención al Paciente:** Las mejoras en la infraestructura de red no solo benefician al personal del hospital, sino que también se traducen en una experiencia más satisfactoria para los pacientes. Con un acceso más rápido y seguro a la información médica, se logra una atención más eficiente y oportuna, lo que es fundamental para el éxito en el ámbito de la salud.

- **Preparación para el Futuro:** Este proyecto establece las bases para futuras mejoras y expansiones de la infraestructura tecnológica del hospital. La adopción de soluciones modernas y escalables permite que el hospital esté mejor preparado para adaptarse a las innovaciones tecnológicas y a las demandas cambiantes del sector de la salud.

4.2. Recomendaciones

- **Monitoreo Continuo de la Red:** Es recomendable implementar herramientas de monitoreo que permitan supervisar el rendimiento de la red en tiempo real. Esto ayudará a detectar y resolver problemas de conectividad o seguridad de manera proactiva, garantizando un funcionamiento óptimo de la infraestructura.

- **Documentación de la Topología de Red**: Es crucial mantener una documentación actualizada de la topología de la red, incluyendo la configuración de VLAN, direcciones IP asignadas y contraseñas de acceso a switches. Esta documentación facilitará la resolución de problemas y permitirá una gestión más eficiente de la red.

- **Evaluaciones de Seguridad Periódicas:** Realizar auditorías de seguridad periódicas para evaluar la efectividad de las contraseñas, el cifrado de datos y otras medidas de seguridad implementadas en la red. Estas auditorías deben incluir pruebas de penetración para identificar posibles vulnerabilidades.

- **Actualización Regular de la Infraestructura:** Se sugiere establecer un plan de mantenimiento y actualización regular de los equipos y software utilizados en la red. Esto incluye la revisión periódica de contraseñas, firmware de los switches y protocolos de seguridad para adaptarse a las nuevas amenazas cibernéticas.

- **Planificación para Futuras Expansiones:** Es recomendable diseñar la infraestructura de red de manera escalable, anticipándose a futuras necesidades. Esto incluye considerar la incorporación de nuevos dispositivos, la ampliación de la cobertura Wi-Fi y la implementación de tecnologías emergentes.

- **Implementar Redundancia con Dos Proveedores de Internet:** Una conexión a Internet confiable es esencial para el Hospital Regional San Juan de Dios de Tarija, dado que muchas de sus operaciones críticas, como sistemas de telefonía IP, facturación virtual, comunicación externa con él SUS, SIAT y al sistema de la gobernación, dependen de estar siempre conectados. Por ello, se recomienda contar con dos proveedores de servicios de Internet (ISPs) para garantizar continuidad y disponibilidad.