ANEXO A NORMATIVA IEEE 830

ANEXO A NORMATIVA IEEE 830

Análisis de requerimientos

Ficha del documento

Fecha	Revisión	Descripción	Autor
05-05-2025	0.1	Rediseñar por completo la red	Cristian Nahuel Condori Condori

Tabla 114. Ficha del documento

Documento validado por las partes en fecha: 05/05/2025

Por el cliente	Por la empresa suministradora
Fdo. D./ Dña	Fdo. D./Dña

Tabla 115. Ficha de validación de documento

Introducción

El presente documento es la especificación de los requisitos del diseño del segmento de red de la Clínica Santísima Trinidad de la ciudad de Tarija.

Propósito

Este documento tiene como propósito definir los lineamientos y funcionalidades de la red a implementar en la Clínica Santísima Trinidad, sirviendo como base técnica para su diseño, ejecución y posterior validación por parte de la administración de la clínica.

Alcance

Este documento contempla los requerimientos de hardware y software necesarios para el rediseño y optimización de la red LAN de la Clínica Santísima Trinidad. El proyecto abarca la implementación de dispositivos de red más avanzados, segmentación mediante VLANs, mejoras en la conectividad inalámbrica y la incorporación de telefonía IP, con el objetivo de garantizar una red segura, eficiente y adaptada a las necesidades clínicas y administrativas de la institución.

Personal involucrado

Nombre	Cristian Nahuel Condori Condori
Rol	Responsable de la elaboración del

	rediseño de la red.
Categoría Profesional	Estudiante
Responsabilidades	Análisis de requerimientos, diseño de la infraestructura de la red, implementación del diseño de red
Información de contacto	crstnnhlcondori@gmail.com

Tabla 116. Personal involucrado

Nombre	Lic. Luis German Quispe Hanco
Rol	Administrador de red
Categoría Profesional	Ingeniero responsable del área de telecomunicaciones de la clínica
Responsabilidades	Vínculo y proveedor de información
Información de contacto	Luisgerman23@gmail.com

Tabla 117. Personal involucrado

Nombre	Ing. José Luis Calder
Rol	Administrador del sistema
Categoría Profesional	Ingeniero responsable del área en la clínica
Responsabilidades	Vinculo y proveedor de información
Información de contacto	Joseluiscalder65@gmail.com

Tabla 118. Personal involucrado

Definiciones, acrónimos y abreviaturas

Nombre	**Descripción**
ISP	Proveedor de servicios de internet
WAP2	Wifi Protected Access 2
VLAN	Red de Área Local Virtual
NAS	Network Attached Storage (Almacenamiento conectado en red)
Telefonía IP	Tecnología que permite hacer llamadas telefónicas usando internet.
Firewall	Protege la red controlando qué datos pueden entrar o salir.

Tabla 119. Definiciones acrónimo y abreviaturas

Referencias

Título del documento	**Referencia**

Standard IEEE 830-1998	IEEE

Tabla 120. Referencias

Resumen

El presente documento está organizado de acuerdo al formato establecido por la IEEE830. Se describe la estructura de la red y su contexto, se describe los requisitos de la red, organizados por requisitos funcionales y requisitos no funcionales, se describe los apéndices o anexos correspondientes para una mejor explicación o detalle de algunos puntos importantes.

Descripción general

La Clínica Santísima Trinidad de Tarija, es un centro de salud privado moderno y confiable, dedicado a ofrecer atención médica de calidad con un enfoque integral para la salud. Equipados con tecnología avanzada y un equipo profesional altamente capacitado, brindando servicios médicos en diversas especialidades para garantizar el bienestar de nuestros pacientes.

Perspectiva del producto

El diseño de red propuesto está orientado a garantizar el correcto funcionamiento de las comunicaciones internas dentro de la clínica, sin interferir con las redes externas, asegurando una conexión estable y eficiente entre los distintos departamentos, equipos médicos, y áreas administrativas.

El objetivo principal es implementar una red robusta y escalable que permita la interconexión entre dispositivos, como computadoras, impresoras, y dispositivos médicos, facilitando la gestión de datos, registros de pacientes y otros procesos críticos para la operación de la clínica. Además, se realizarán pruebas exhaustivas para asegurar la calidad de las conexiones y la funcionalidad de todos los sistemas internos, garantizando un rendimiento óptimo y sin interrupciones.

Funcionalidad del producto

El diseño de red tiene las siguientes funcionalidades:

El diseño de red se realizará utilizando la red actual e implementando diferentes servicios que se requieran como ser la implementación de nuevos puntos de red, segmentación de red, nuevos equipos de red entre ellos un Switch, Access point(wifi), Router así como también se realizará la implementación de un servidor DHCP en los Switch, una canalización y reestructuración del cableado de la red.

Características de los usuarios

Tipo de usuario	Responsable de dar soporte al sistema

Formación	Universitaria
Habilidades	Manejo de las actividades de los programas
Actividades	Contador y encargado de la TI

Tabla 121. Características de los usuarios

Tipo de usuario	Responsable de la red
Formación	Universitaria
Habilidades	Conocimiento en el área de redes
Actividades	Administración de la estructura de la red

Tabla 122. Características de los usuarios

Restricciones

Se realizará la simulación de la red en la herramienta Packet tracer y GNS3.

Se realizará la configuración y pruebas a la red en la herramienta VMWare.

El diseño e implementación será para las áreas de la clínica y su conexión con el Servidor y el sistema que controla los Ingresos, Contabilidad e Inventarios.

La eficacia de le conectividad a la red va ser limitada a algunos aspectos como ser el ancho de banda que se tenga y también el proveedor de internet ISP el cual este proporcionando los servicios a la institución.

Suposiciones y dependencias

Se asume que los requerimientos son estables.

Todo el hardware requerido lo proporcionará la institución.

El servicio a internet proporcionado por el ISP será estable.

El hardware requerido será el proporcionado en base al diseño.

El servidor DHCP se configurará en los Switch para no tener un gasto económico excesivo. La centralita de Telefonía IP será instalada en un servidor proporcionado por la Clínica y será configurado con máquinas virtuales VMware con el sistema operativo Issabel de Centos.

Requisitos específicos

Interfaces de usuario

El Firewall y el Servidor Issabel tendrán una ventana que se inicializará cuando se deba realizar configuraciones, ya sean implementando nuevas políticas de seguridad o implementando extensiones, también se monitoreará el servidor DHCP y a la cual solo el administrador tendrá acceso.

Interfaces de hardware

Se debe disponer de los siguientes equipos.

- Router
- Access Point
- Switch
- Patch Panel
- Equipos de Computación o Impresoras
- Mouse
- Teclado
- Monitor

Interfaces de software

- Sistema Operativo Linux Ubuntu Server
- Explorador web
- Sistema Operativo Issabel de Centos
- Acceso a Internet

Requisitos funcionales

Número de requisito	RF1
Nombre de requisito	Implementar servidor DHCP
Descripción del requisito	Se implementará un servidor DHCP para proporcionar IPs de manera dinámica
Tipo	Requisito
Fuente del requisito	Responsable evento
Prioridad del requisito	Alta

Tabla 123. Requisito funcional 1

Número de requisito	RF2
Nombre de requisito	Implementar un firewall
Descripción del requisito	Se implementará un firewall(Fortinet) para proteger la seguridad de la red y los Servidores de la Clínica.
Tipo	Requisito
Fuente del requisito	Responsable evento

Prioridad del requisito	Alta

Tabla 124. Requisito funcional 2

Número de requisito	RF3
Nombre de requisito	Implementar nuevos puntos de acceso (Access Point) a la red.
Descripción del requisito	Se implementará conectividad Wi-Fi en cada planta de la Clínica, con redes diferenciadas para el personal de salud y para los pacientes
Tipo	Requisito
Fuente del requisito	Responsable evento
Prioridad del requisito	Alta

Tabla 125. Requisito funcional 3

Número de requisito	RF4
Nombre de requisito	Elaborar direccionamiento de equipos
Descripción del requisito	Se realizará el direccionamiento del segmento de red indicando desde que rango de IP comenzará a repartir el servidor.
Tipo	Requisito
Fuente del requisito	Responsable evento
Prioridad del requisito	Alta

Tabla 126. Requisito funcional 4

Número de requisito	RF5
Nombre de requisito	Etiquetar y administrar equipos
Descripción del requisito	Colocar hostnames a los equipos y etiquetarlos por nombres
Tipo	Requisito
Fuente del requisito	Responsable evento
Prioridad del requisito	Alta

Tabla 127. Requisito funcional 5

Número de requisito	RF6
Nombre de requisito	Gestionar permisos de acceso a la red
Descripción del requisito	Se controlará, habilitará o bloqueará los permisos de acceso a la red a los

	usuarios según sean sus privilegios
Tipo	Requisito
Fuente del requisito	Responsable evento
Prioridad del requisito	Alta

Tabla 128. Requisito funcional 6

Número de requisito	RF7
Nombre de requisito	Realizar estimaciones sobre los servicios y tráfico de red
Descripción del requerimiento	Se hará un análisis de tráfico de la red de la institución, así como también un análisis del tiempo de uso de datos de los servicios con el objetivo de evitar que el servicio de red sea lento en los equipos
Tipo	Requisito
Fuente del requisito	Responsable evento
Prioridad del requisito	Media

Tabla 129. Requisito funcional 7

Número de requisito	RF8
Nombre de requisito	Realizar la segmentación de la red
Descripción del requisito	Se realizará la división de la red física en diferentes subredes lógicas implementando las VLANs
Tipo	Requisito
Fuente del requisito	Responsable evento
Prioridad del requisito	Alta

Tabla 130. Requisito funcional 8

Número de requisito	RF9
Nombre de requisito	Realizar configuración de contraseñas en los equipos
Descripción del requisito	Se debe configurar el uso de las contraseñas para el acceso a los usuarios a los equipos de computación empleando un mínimo de 8 caracteres con letras minúsculas y números Evitar los acrónimos y fechas importantes
Tipo	Requisito

Fuente del requisito	Responsable evento
Prioridad del requisito	Media

Tabla 131. Requisito funcional 9

Número de requisito	RF10
Nombre de requisito	Implementar telefonía IP
Descripción del requisito	Se implementará un servicio de telefonía IP basado en Asterisk, utilizando el sistema operativo Issabel, con el objetivo de optimizar la comunicación interna a través de la red local de la Clínica.
Tipo	Requisito
Fuente del requisito	Responsable evento
Prioridad del requisito	Media

Tabla 132. Requisito funcional 10

Requisitos no funcionales

Requisitos de rendimiento

Número de requisito	RNF1
Nombre de requisito	Rendimiento de la red
Descripción del requerimiento	La red debe poder manejar el número requerido de pacientes sin ninguna degradación del rendimiento
Tipo	Requisito
Fuente del requisito	Responsable del evento
Prioridad del requisito	Alta

Tabla 133. Requisito no funcional 1

Número de requisito	RNF2
Nombre de requisito	Capacidad de la red
Descripción del requisito	La red debe tener la capacidad de velocidad óptima y requerida por los pacientes
Tipo	Requisito
Fuente del requisito	Responsable evento
Prioridad del requisito	Media

Tabla 134. Requisito no funcional 2

Número de requisito	RNF3
Nombre de requisito	Escalabilidad de la red
Descripción del requisito	La red debe poder tener un rendimiento escalable
Tipo	Requisito
Fuente del requisito	Responsable evento
Prioridad del requisito	Alta

Tabla 135. Requisito no funcional 3

Seguridad

Número de requisito	RNF4
Nombre de requisito	Realizar cifrado de datos
Descripción de requisito	Toda la comunicación interna entre los servidores, sistema y los diferentes equipos de la clínica, deben estar cifradas(información autorizada) entre sí.
Tipo	Requisito
Fuente del requisito	Responsable evento
Prioridad del requisito	Media

Tabla 136. Requisito no funcional 4

Número de requisito	RNF5
Nombre de requisito	Realizar protección de datos
Descripción del requisito	La red debe estar protegida contra accesos no autorizados
Tipo	Requisito
Fuente del requisito	Responsable evento
Prioridad del requisito	Alta

Tabla 137. Requisito no funcional 5

Número de requisito	RNF6
Nombre de requisito	Implementación de la seguridad física
Descripción del requisito	Los servidores deben estar en condiciones óptimas de seguridad física como un sistema de refrigeración y un sistema de seguridad contra incendios.
Tipo	Requisito
Fuente del requisito	Responsable evento

Prioridad del requisito	Media

Tabla 138. Requisito no funcional 6

Fiabilidad

Número de requisito	RNF7
Nombre de requisito	Fiabilidad de la red
Descripción del requisito	La red debe ser confiable y cumplir con los requisitos de los pacientes y personal de salud.
Tipo	Requisito
Fuente del requisito	Responsable evento
Prioridad del requisito	Media

Tabla 139. Requisito no funcional 7

Disponibilidad

Número de requisito	RNF8
Nombre de requisito	Disponibilidad de la red
Descripción del requisito	La red debe estar disponible cuando sea necesario y en todo momento.
Tipo	Requisito
Fuente del requisito	Responsable evento
Prioridad del requisito	Alta

Tabla 140. Requisito no funcional 8

Mantenibilidad

Número de requisito	RNF9
Nombre de requisito	Mantenimiento de la red
Descripción del requisito	La red debe ser fácil de mantener, migrar y actualizar.
Tipo	Requisito
Fuente del requisito	Responsable evento
Prioridad del requisito	Alta

Tabla 141. Requisito no funcional 9

Portabilidad

Número de requisito	RNF10
Nombre de requisito	Portabilidad de la red
Descripción del requisito	La red debe poder funcionar en todos los dispositivos de manera eficaz.

Tipo	Requisito
Fuente del requisito	Responsable evento
Prioridad del requisito	Alta

Tabla 142. Requisito no funcional 10

Casos de uso del negocio

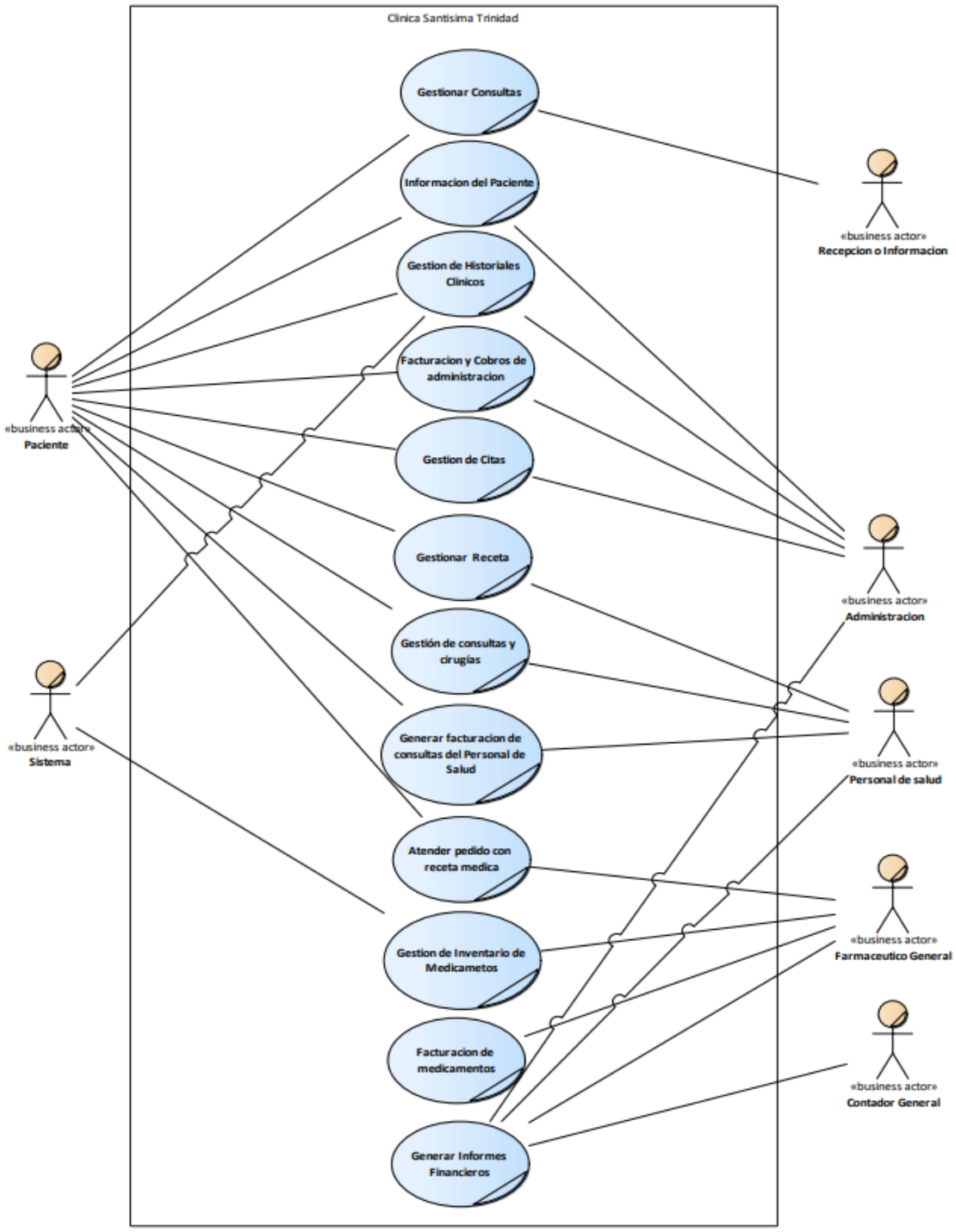

Figura 288. Casos de uso del negocio

Documentación de casos de uso del negocio

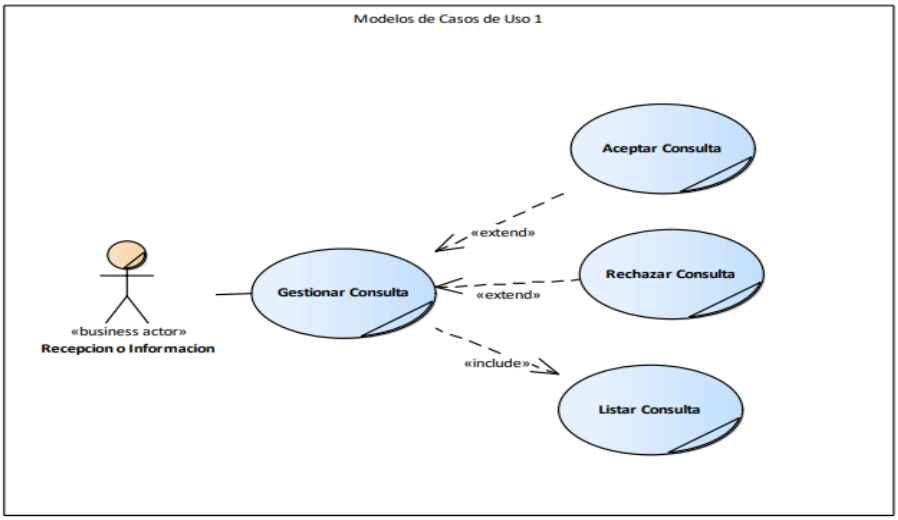

Figura 289. Modelo casos de uso 1

Proceso de negocio	Gestionar Consulta
Objetivo	Aceptar, Rechazar y Listar
Descripción	El Paciente antes de ser atendido debe consultar con Recepción
Prioridad	Media

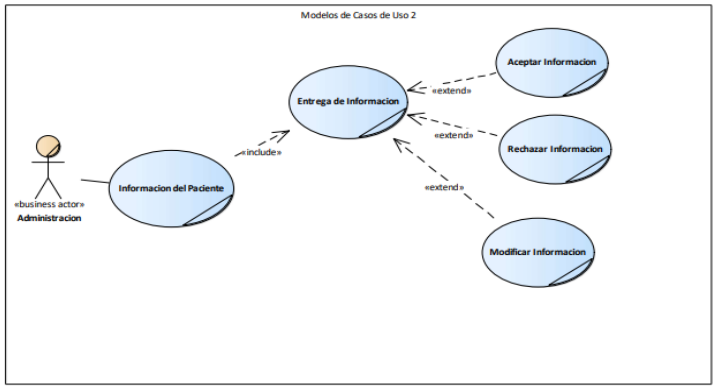

Figura 290. Modelo casos de uso 2

Proceso de negocio	Información del Paciente
Objetivo	Aceptar, Rechazar y Modificar la Información dado por el Paciente
Descripción	El Paciente debe presentar su información personal ya sea sus nombres y apellidos, cedula de identidad, número de celular para poder estar registrado en la clínica. La información se almacena de manera organizada y segura en el sistema de registros médicos electrónicos o en archivos físicos.
Prioridad	Media

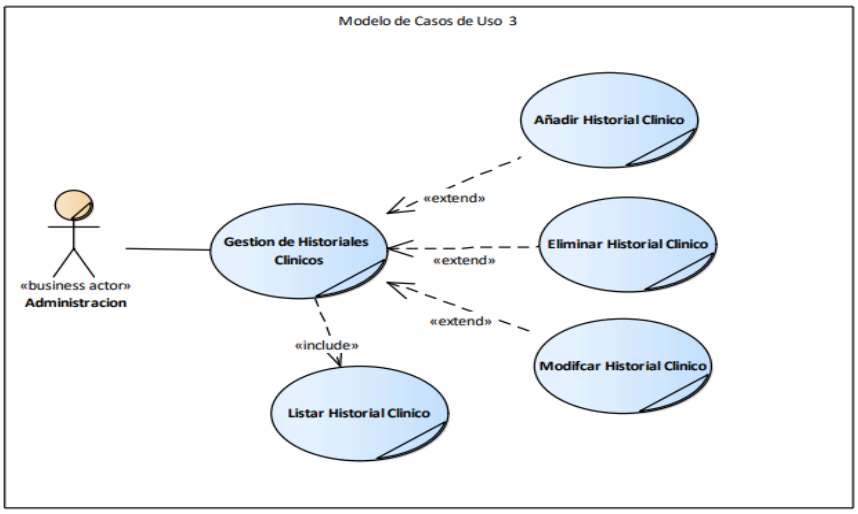

Figura 291. Modelo casos de uso 3

Proceso de negocio	Gestión de Historiales Clínicos
Objetivo	Añadir, Eliminar, Modificar y Listar los Historiales clínicos por Administración
Descripción	Implica la recopilación, almacenamiento y mantenimiento de toda la información médica relevante de los pacientes a lo largo del tiempo. Esto incluye historias clínicas, diagnósticos, tratamientos, resultados de pruebas médicas, informes de procedimientos, alergias, medicamentos actuales y cualquier otra información pertinente para la atención médica.
Prioridad	Media

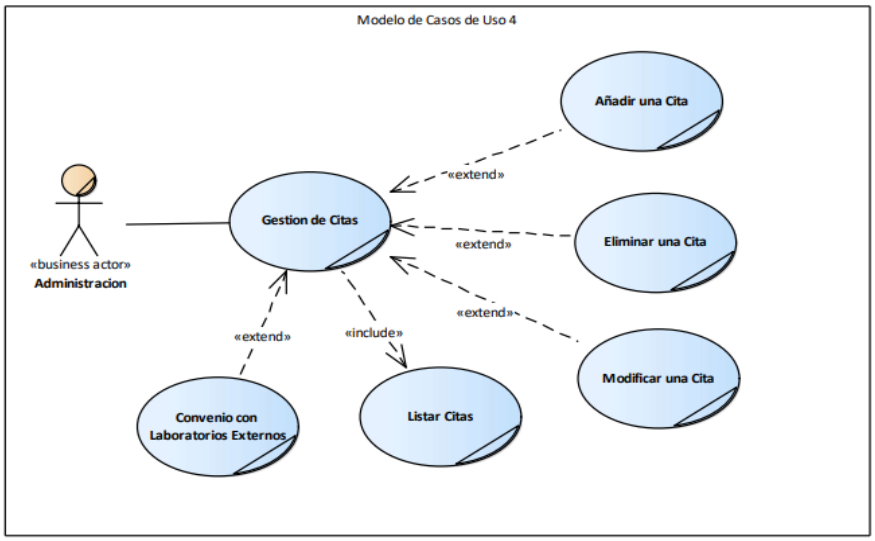

Figura 292. Modelo casos de uso 4

Proceso de negocio	Gestión de Citas
Objetivo	Añadir, Eliminar, Modificar, Listar citas y Realizar Convenios Con Laboratorios Externos.
Descripción	En este proceso, el personal administrativo coordina la programación de citas médicas para pacientes. Esto implica recibir solicitudes de citas, asignar horarios disponibles, confirmar las citas y hacer seguimiento de las mismas y también realizar convenios de laboratorios con otras clínicas u hospitales y se coordina la derivación o programación de pruebas según las necesidades de cada paciente. Además, se gestiona una lista de espera para casos de disponibilidad limitada.
Prioridad	Media.

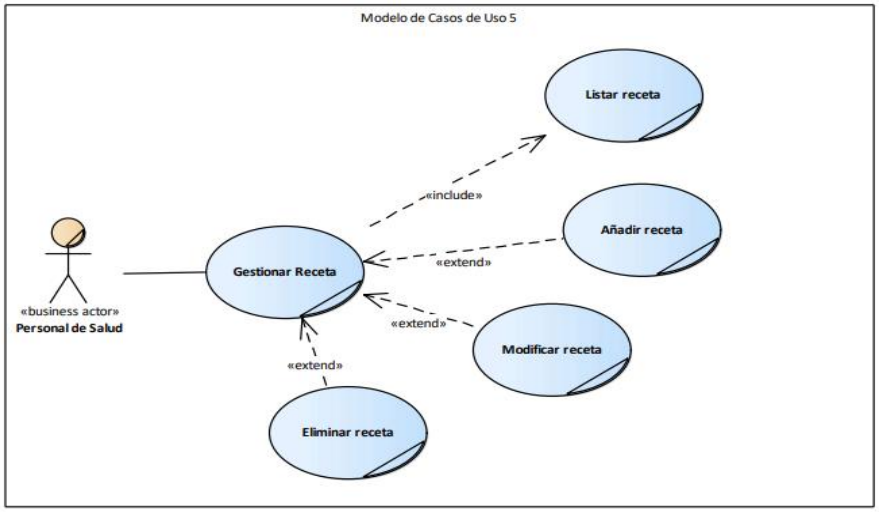

Figura 293. Modelo casos de uso 5

Proceso de negocio	Gestionar receta
Objetivo	Listar, Añadir, Modificar, Eliminar recetas medicas
Descripción	El personal de la salud redacta una prescripción detallada que incluye el nombre del medicamento, la dosis, la frecuencia de administración y la duración del tratamiento, además de cualquier instrucción especial.
Prioridad	Media

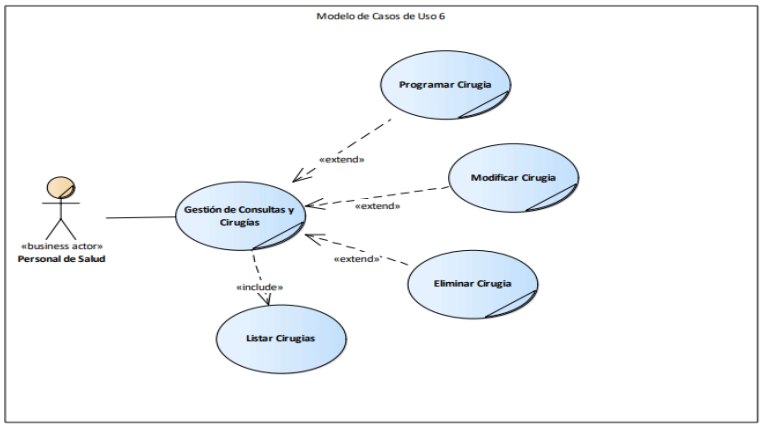

Figura 294. Modelo casos de uso 6

Proceso de negocio	Gestión de consultas y cirugías
Objetivo	Programar cirugía, Modificar cirugía, Eliminar cirugía y Listar cirugía.
Descripción	Implica la gestión integral de las citas médicas y quirúrgicas, incluye la asignación de horarios disponibles para consultas y cirugías, la coordinación entre el personal médico y quirúrgico, la preparación de la sala de operaciones, y la comunicación con los pacientes sobre los detalles de su cita.
Prioridad	Alta

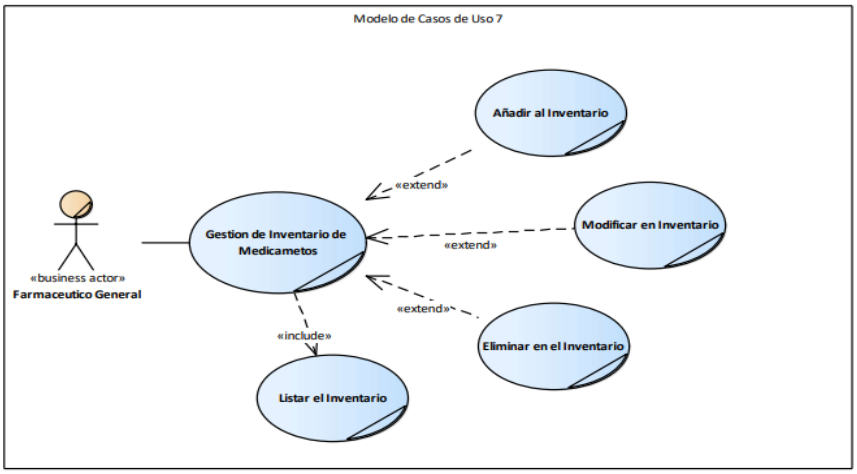

Figura 295. Modelo casos de uso 7

Proceso de negocio	Gestión de Inventario de Medicamentos
Objetivo	Añadir, Modificar, Eliminar y Listar el Inventario
Descripción	Organizar, comprar y almacenar los suministros de manera adecuada, llevar un registro actualizado de los medicamentos, monitorear los niveles de inventario y realizar pedidos de reposición de manera oportuna.
Prioridad	Alta

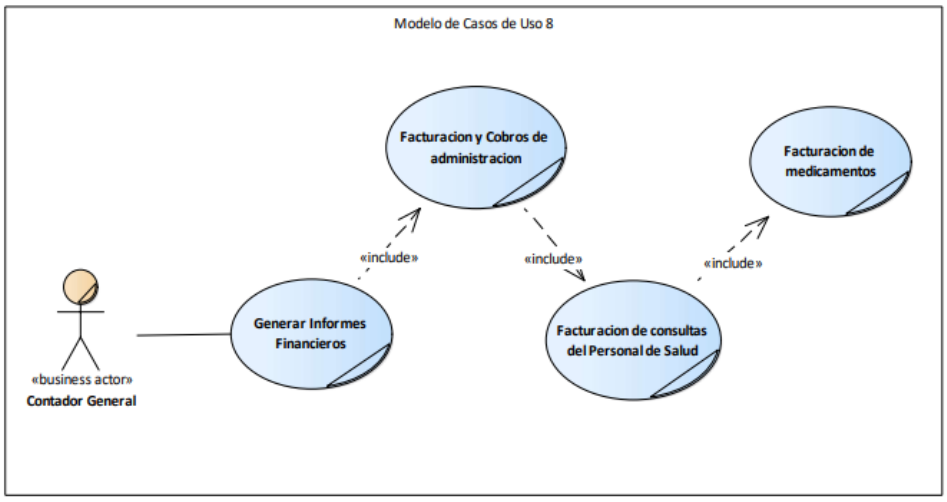

Figura 296. Modelo casos de uso 8

Proceso de negocio	Generar Informes Financieros
Objetivo	Obtener facturas de cobros de administración, facturación de consultas del Personal de Salud y de medicamentos.
Descripción	El contador general de la clínica es responsable de obtener toda la información relacionada con la facturación, incluyendo las facturas generadas por la venta de medicamentos, las consultas médicas realizadas y los cobros administrativos efectuados. Esta información es esencial para llevar a cabo un control financiero adecuado, así como para garantizar la precisión y la transparencia en el registro de ingresos y gastos de la clínica.
Prioridad	Alta

ANEXO B MANUAL DE USUARIO

ANEXO B MANUAL DE USUARIO

Índice de Manual de Usuario

1. Comandos de la configuración de los dispositivos

Configuracion de los servidores.

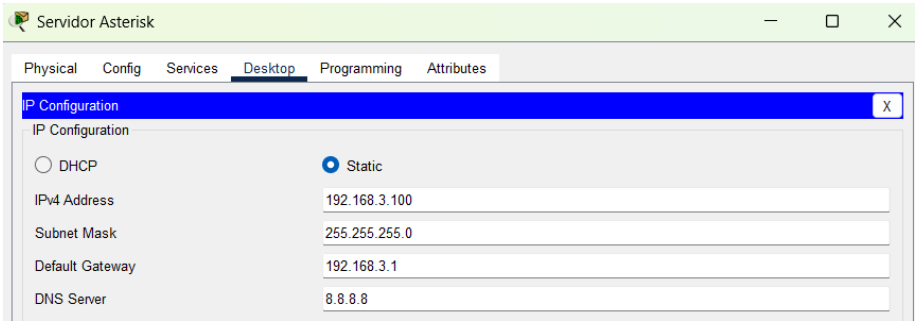

Figura 297. IP Servidor Asterisk

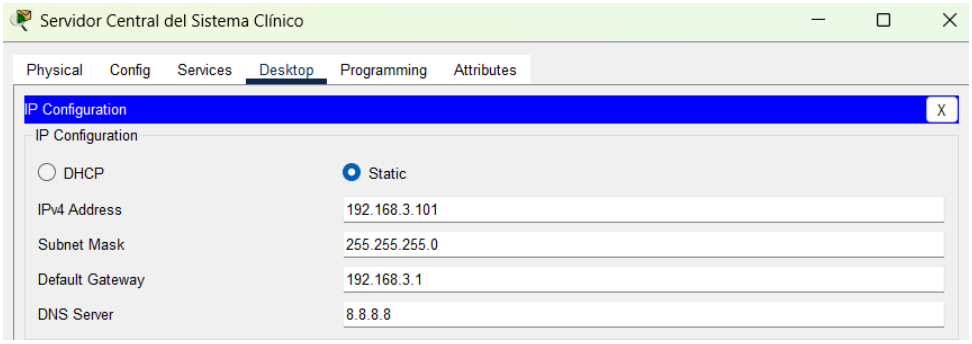

Figura 298. Servidor Central del Sistema Clínico

2. Configuración de calidad de Servicio

Crear clases para Voz, Video y Soporte:

RouterClinica>enable

RouterClinica#conf ter

RouterClinica(config)#class-map match-any VOZ

RouterClinica(config-cmap)# match protocol skinny

RouterClinica(config-cmap)# match protocol rtp

RouterClinica(config-cmap)#exit

RouterClinica(config)#class-map match-any VIDEO

RouterClinica(config-cmap)# match protocol rtp

RouterClinica(config-cmap)# match protocol udp

RouterClinica(config-cmap)#exit

RouterClinica(config)#class-map match-any SOPORTE

RouterClinica(config-cmap)# match protocol tftp

RouterClinica(config-cmap)# match protocol dhcp

RouterClinica(config-cmap)# match protocol icmp

RouterClinica(config-cmap)#exit

Creando el policy MAP con el nombre de CALIDAD

RouterClinica(config-cmap)#exitpolicy-map CALIDAD

RouterClinica(config-pmap)#class VOZ

RouterClinica(config-pmap-c)#priority percent 20

RouterClinica(config-pmap-c)#exit

RouterClinica(config-pmap)#class VIDEO

RouterClinica(config-pmap-c)#bandwidth percent 25

RouterClinica(config-pmap-c)#exit

RouterClinica(config-pmap)#class SOPORTE

RouterClinica(config-pmap-c)#bandwidth percent 10

RouterClinica(config-pmap-c)#exit

RouterClinica(config-pmap)#class class-default

RouterClinica(config-pmap-c)# fair-queue

Añadiendo hacia la Interfaz de cableado que es Gi 0/3/0 Fibra Óptica

RouterClinica(config)#interface gigabitEthernet 0/3/0

RouterClinica(config-if)#service

RouterClinica(config-if)#service-policy out

RouterClinica(config-if)#service-policy output CALIDAD

RouterClinica#show policy-map interface gigabitEthernet 0/3/0

Verificando la calidad de servicio implementado

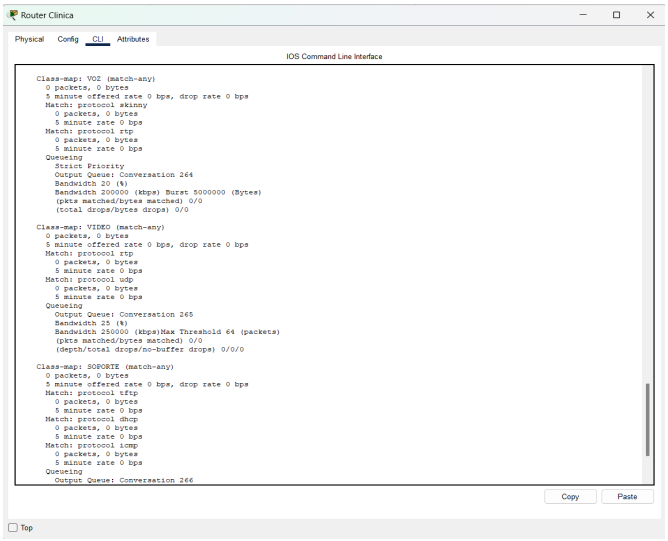

Figura 299. Calidad de Servicio

3. Configuración de subinterfaces para las VLANS

RouterClinica#conf terminal

RouterClinica(config)#interface gigabitEthernet 0/3/0.10

RouterClinica(config-subif)# encapsulation dot1Q 10

RouterClinica(config-subif)# ip address 192.168.2.1 255.255.255.224

RouterClinica(config-subif)#exit

RouterClinica(config)#interface gigabitEthernet 0/3/0.20

RouterClinica(config-subif)#encapsulation dot1Q 20

RouterClinica(config-subif)#ip address 192.168.2.33 255.255.255.240

```
RouterClinica(config-subif)#exit
RouterClinica(config)#interface gigabitEthernet 0/3/0.30
RouterClinica(config-subif)#encapsulation dot1Q 30
RouterClinica(config-subif)#ip address 192.168.2.49 255.255.255.240
RouterClinica(config-subif)#exit
RouterClinica(config)#interface gigabitEthernet 0/3/0.40
RouterClinica(config-subif)# encapsulation dot1Q 40
RouterClinica(config-subif)# ip address 192.168.2.65 255.255.255.240
RouterClinica(config-subif)#exit
RouterClinica(config)#interface gigabitEthernet 0/3/0.50
RouterClinica(config-subif)# encapsulation dot1Q 50
RouterClinica(config-subif)# ip address 192.168.2.81 255.255.255.240
RouterClinica(config-subif)#exit
RouterClinica(config)#interface gigabitEthernet 0/3/0.60
RouterClinica(config-subif)# encapsulation dot1Q 60
RouterClinica(config-subif)# ip address 192.168.2.97 255.255.255.248
RouterClinica(config-subif)#exit
RouterClinica(config)#interface gigabitEthernet 0/3/0.70
RouterClinica(config-subif)# encapsulation dot1Q 70
RouterClinica(config-subif)# ip address 192.168.2.105 255.255.255.248
RouterClinica(config-subif)#exit
RouterClinica(config)#interface gigabitEthernet 0/3/0.80
RouterClinica(config-subif)# encapsulation dot1Q 80
RouterClinica(config-subif)# ip address 192.168.2.113 255.255.255.248
RouterClinica(config-subif)#exit
RouterClinica(config)#interface gigabitEthernet 0/3/0.90
RouterClinica(config-subif)# encapsulation dot1Q 90
RouterClinica(config-subif)# ip address 192.168.2.121 255.255.255.248
RouterClinica(config-subif)#exit
RouterClinica(config)#interface gigabitEthernet 0/3/0.100
RouterClinica(config-subif)# encapsulation dot1Q 100
RouterClinica(config-subif)# ip address 192.168.2.129 255.255.255.248
RouterClinica(config-subif)#exit
RouterClinica(config)#interface gigabitEthernet 0/3/0.110
```

RouterClinica(config-subif)# encapsulation dot1Q 110

RouterClinica(config-subif)# ip address 192.168.2.137 255.255.255.248

RouterClinica(config-subif)#exit

RouterClinica(config)#interface gigabitEthernet 0/3/0.120

RouterClinica(config-subif)# encapsulation dot1Q 120

RouterClinica(config-subif)# ip address 192.168.2.145 255.255.255.248

RouterClinica(config-subif)#exit

RouterClinica(config)#interface gigabitEthernet 0/3/0.130

RouterClinica(config-subif)# encapsulation dot1Q 130

RouterClinica(config-subif)# ip address 192.168.2.153 255.255.255.248

RouterClinica(config-subif)#exit

RouterClinica(config)#interface gigabitEthernet 0/3/0.140

RouterClinica(config-subif)# encapsulation dot1Q 140

RouterClinica(config-subif)# ip address 192.168.2.161 255.255.255.248

RouterClinica(config-subif)#exit

RouterClinica(config)#interface gigabitEthernet 0/3/0.150

RouterClinica(config-subif)#encapsulation dot1Q 150

RouterClinica(config-subif)#ip address 192.168.3.1 255.255.255.0

RouterClinica(config-subif)#exit

4. Configuración en los Switch

Creando VLAN 150 y accediendo al modo Access:

SwitchP>enable

SwitchP#conf terminal

SwitchP(config)#vlan 150

SwitchP(config-vlan)#name Servidores

SwitchP(config-vlan)#exit

SwitchP(config)#interface fastEthernet 1/1

SwitchP(config-if)#switchport mode access

SwitchP(config-if)#switchport access vlan 150

SwitchP(config-if)#exit

SwitchP(config)#interface fastEthernet 0/1

SwitchP(config-if)#switchport mode access

SwitchP(config-if)#switchport access vlan 150

SwitchP(config-if)#exit

5. Configuración modo troncal con fibra a las interfaces del switch

Switch Principal:

SwitchP(config)#interface gigabitEthernet 9/1

SwitchP(config-if)#switchport mode trunk

SwitchP(config-if)#exit

SwitchP(config)#interface gigabitEthernet4/1

SwitchP(config-if)#switchport mode trunk

SwitchP(config-if)#exit

SwitchP(config)#interface gigabitEthernet 6/1

SwitchP(config-if)#switchport mode trunk

SwitchP(config-if)#exit

SwitchP(config)#interface gigabitEthernet 5/1

SwitchP(config-if)#switchport mode trunk

SwitchP(config-if)#exit

SwitchP(config)#interface gigabitEthernet 7/1

SwitchP(config-if)#switchport mode trunk

SwitchP(config-if)#exit

Switch fibra Planta Baja

SwitchFibraPB#conf terminal

SwitchFibraPB(config)#interface gigabitEthernet 4/1

SwitchFibraPB(config-if)#switchport mode trunk

SwitchFibraPB(config-if)#exit

SwitchFibraPB(config)#interface fastEthernet 0/1

SwitchFibraPB(config-if)#switchport mode trunk

SwitchFibraPB(config-if)#end

Switch Fibra Primer Piso

SwitchFibraP1#conf terminal

SwitchFibraP1(config)#interface gigabitEthernet 6/1

SwitchFibraP1(config-if)#switchport mode trunk

SwitchFibraP1(config-if)#exit

SwitchFibraP1(config)#interface fastEthernet 0/1

SwitchFibraP1(config-if)#switchport mode trunk

SwitchFibraP1(config-if)#exit

Switch Fibra Segundo Piso

SwitchFibraP2#conf terminal

SwitchFibraP2(config)#interface gigabitEthernet 4/1

SwitchFibraP2(config-if)#switchport mode trunk

SwitchFibraP2(config-if)#exit

SwitchFibraP2(config)#interface fastEthernet 0/1

SwitchFibraP2(config-if)#switchport mode trunk

SwitchFibraP2(config-if)#exit

Switch Fibra Tercer Piso

SwitchFribaP3#conf terminal

SwitchFribaP3(config)#interface gigabitEthernet 4/1

SwitchFribaP3(config-if)#switchport mode trunk

SwitchFribaP3(config-if)#exit

SwitchFribaP3(config)#interface fastEthernet 0/1

SwitchFribaP3(config-if)#switchport mode trunk

6. Configuración de switch modo troncal usando cable de cobre UTP

Switch Planta Baja

SwitchPB#conf terminal

SwitchPB(config)#interface fastEthernet 0/24

SwitchPB(config-if)#switchport mode trunk

SwitchPB(config-if)#end

Switch Primer Piso

SwitchP1#conf terminal

SwitchP1(config)#interface fastEthernet 0/24

SwitchP1(config-if)#switchport mode trunk

SwitchP1(config-if)#exit

Switch Segundo Piso

SwitchP2#conf terminal

SwitchP2(config)#interface fastEthernet 0/24

SwitchP2(config-if)#switchport mode trunk

SwitchP2(config-if)#end

Switch Tercer Piso

SwitchP3#conf terminal

SwitchP3(config)#interface fastEthernet 0/24

SwitchP3(config-if)#switchport mode trunk

SwitchP3(config-if)#exit

7. Configuración de VLAN y servidor DHCP en los switches

Vlan10:

SwitchP#conf terminal

SwitchP(config)#vlan 10

SwitchP(config-vlan)#name Internacion

SwitchP(config-vlan)#exit

SwitchP(config)#interface vlan 10

SwitchP(config-if)#ip address 192.168.2.30 255.255.255.224

SwitchP(config-if)#no shutdown

SwitchP(config-if)#exit

SwitchP(config)#ip dhcp pool vlan10

SwitchP(dhcp-config)#network 192.168.2.0 255.255.255.224

SwitchP(dhcp-config)#default-router 192.168.2.1

SwitchP(dhcp-config)# dns-server 192.168.3.100

SwitchP(dhcp-config)#exit

SwitchP(config)#ip dhcp excluded-address 192.168.2.1

SwitchP(config)#ip dhcp excluded-address 192.168.2.30

P1

SwitchFibraP1#conf terminal

SwitchFibraP1(config)#vlan 10

SwitchFibraP1(config-vlan)#name Internacion

SwitchFibraP1(config-vlan)#exit

Impresora

SwitchFibraP1(config)#interface fastEthernet 8/1

SwitchFibraP1(config-if)#switchport mode access

SwitchFibraP1(config-if)#switchport access vlan 10

SwitchFibraP1(config-if)#exit

SwitchP1#conf terminal

SwitchP1(config)#vlan 10

SwitchP1(config-vlan)#name Internacion

SwitchP1(config-vlan)#exit

SwitchP1(config)#interface range fastEthernet 0/1-7

SwitchP1(config-if-range)#switchport mode access

SwitchP1(config-if-range)#switchport access vlan 10

SwitchP1(config-if-range)#exit

P2

SwitchFibraP2#conf terminal

SwitchFibraP2(config)#vlan 10

SwitchFibraP2(config-vlan)#name Internacion

SwitchFibraP2(config-vlan)#exit

Impresora

SwitchFibraP2(config)#interface fastEthernet 9/1

SwitchFibraP2(config-if)#switchport mode access

SwitchFibraP2(config-if)#switchport access vlan 10

SwitchFibraP2(config-if)#exit

SwitchP2#conf terminal

SwitchP2(config)#vlan 10

SwitchP2(config-vlan)#name Internacion

SwitchP2(config-vlan)#exit

SwitchP2(config)#interface range fastEthernet 0/1-7

SwitchP2(config-if-range)#switchport mode access

SwitchP2(config-if-range)#switchport access vlan 10

SwitchP2(config-if-range)#exit

P3

SwitchFribaP3(config)#conf term

SwitchFribaP3(config)#vlan 10

SwitchFribaP3(config-vlan)#name Internacion

SwitchFribaP3(config-vlan)#exit

Impresora

SwitchFribaP3(config)#interface fastEthernet 6/1

SwitchFribaP3(config-if)#switchport mode access

SwitchFribaP3(config-if)#switchport access vlan 10

SwitchFribaP3(config-if)#exit

SwitchP3(config)#vlan 10

SwitchP3(config-vlan)#name Internacion

SwitchP3(config-vlan)#exit

SwitchP3(config)#interface range fastEthernet 0/6-10

SwitchP3(config-if-range)#switchport mode access

SwitchP3(config-if-range)#switchport access vlan 10

SwitchP3(config-if-range)#end

Vlan20 Wifi:

SwitchP#conf terminal

SwitchP(config)#vlan 20

SwitchP(config-vlan)#name Pacientes

SwitchP(config-vlan)#exit

SwitchP(config)#interface vlan 20

SwitchP(config-if)#ip address 192.168.2.46 255.255.255.240

SwitchP(config-if)#no shutdown

SwitchP(config-if)#exit

SwitchP(config)#ip dhcp pool vlan20

SwitchP(dhcp-config)#network 192.168.2.32 255.255.255.240

SwitchP(dhcp-config)#default-router 192.168.2.33

SwitchP(dhcp-config)#dns-server 8.8.8.8

SwitchP(dhcp-config)#exit

SwitchP(config)#ip dhcp excluded-address 192.168.2.33

SwitchP(config)#ip dhcp excluded-address 192.168.2.46

PB

SwitchFibraPB#conf terminal

SwitchFibraPB(config)#vlan 20

SwitchFibraPB(config-vlan)#name Pacientes

SwitchFibraPB(config-vlan)#exit

SwitchPB#conf terminal

SwitchPB(config)#vlan 20

SwitchPB(config-vlan)#name Pacientes

SwitchPB(config-vlan)#exit
SwitchPB(config)#interface fastEthernet 0/23
SwitchPB(config-if)#switchport mode access
SwitchPB(config-if)#switchport access vlan 20
SwitchPB(config-if)#exit
SwitchPB(config)#interface fastEthernet 0/20
SwitchPB(config-if)#switchport mode access
SwitchPB(config-if)#switchport access vlan 20
SwitchPB(config-if)#exit

P1

SwitchFibraP1#conf terminal
SwitchFibraP1(config)#vlan 20
SwitchFibraP1(config-vlan)#name Pacientes
SwitchFibraP1(config-vlan)#exit
SwitchP1#conf terminal
SwitchP1(config)#vlan 20
SwitchP1(config-vlan)#name Pacientes
SwitchP1(config-vlan)#exit
SwitchP1(config)#interface fastEthernet 0/23
SwitchP1(config-if)#switchport mode access
SwitchP1(config-if)#switchport access vlan 20
SwitchP1(config-if)#end

P2

SwitchFibraP2#conf terminal
SwitchFibraP2(config)#vlan 20
SwitchFibraP2(config-vlan)#name Pacientes
SwitchFibraP2(config-vlan)#exit
SwitchP2#conf terminal
SwitchP2(config)#vlan 20
SwitchP2(config-vlan)#name Pacientes
SwitchP2(config-vlan)#exit
SwitchP2(config)#interface fastEthernet 0/23
SwitchP2(config-if)#switchport mode access
SwitchP2(config-if)#switchport access vlan 20

SwitchP2(config-if)#end

P3

SwitchFribaP3#conf terminal

SwitchFribaP3(config)#vlan 20

SwitchFribaP3(config-vlan)#name Pacientes

SwitchFribaP3(config-vlan)#exit

SwitchP3#conf terminal

SwitchP3(config)#vlan 20

SwitchP3(config-vlan)#name Pacientes

SwitchP3(config-vlan)#exit

SwitchP3(config)#interface fastEthernet 0/23

SwitchP3(config-if)#switchport mode access

SwitchP3(config-if)#switchport access vlan 20

SwitchP3(config-if)#end

Vlan30 Wifi:

SwitchP(config)#vlan 30

SwitchP(config-vlan)#name PersonalSalud

SwitchP(config-vlan)#exit

SwitchP(config)#interface vlan 30

SwitchP(config-if)#ip address 192.168.2.62 255.255.255.240

SwitchP(config-if)#no shutdown

SwitchP(config-if)#exit

SwitchP(config)#ip dhcp pool vlan30

SwitchP(dhcp-config)#network 192.168.2.48 255.255.255.240

SwitchP(dhcp-config)#default-router 192.168.2.49

SwitchP(dhcp-config)# dns-server 192.168.3.100

SwitchP(dhcp-config)#exit

SwitchP(config)#ip dhcp excluded-address 192.168.2.49

SwitchP(config)#ip dhcp excluded-address 192.168.2.62

PB

SwitchFibraPB#conf terminal

SwitchFibraPB(config)#vlan 30

SwitchFibraPB(config-vlan)#name PersonalSalud

SwitchFibraPB(config-vlan)#exit

SwitchPB#conf terminal

SwitchPB(config)#vlan 30

SwitchPB(config-vlan)#name PersonalSalud

SwitchPB(config-vlan)#exit

SwitchPB(config)#interface range fastEthernet 0/21-22

SwitchPB(config-if)#switchport mode access

SwitchPB(config-if)#switchport access vlan 30

SwitchPB(config-if)#end

P1

SwitchFibraP1#conf terminal

SwitchFibraP1(config)#vlan 30

SwitchFibraP1(config-vlan)#name PersonalSalud

SwitchFibraP1(config-vlan)#exit

SwitchP1#conf terminal

SwitchP1(config)#vlan 30

SwitchP1(config-vlan)#name PersonalSalud

SwitchP1(config-vlan)#exit

SwitchP1(config)#interface fastEthernet 0/22

SwitchP1(config-if)#switchport mode access

SwitchP1(config-if)#switchport access vlan 30

SwitchP1(config-if)#end

P2

SwitchFibraP2#conf terminal

SwitchFibraP2(config)#vlan 30

SwitchFibraP2(config-vlan)#name PersonalSalud

SwitchFibraP2(config-vlan)#exit

SwitchP2#conf terminal

SwitchP2(config)#vlan 30

SwitchP2(config-vlan)#name PersonalSalud

SwitchP2(config-vlan)#exit

SwitchP2(config)#interface fastEthernet 0/22

SwitchP2(config-if)#switchport mode access

SwitchP2(config-if)#switchport access vlan 30

SwitchP2(config-if)#end

P3

SwitchFribaP3#conf terminal

SwitchFribaP3(config)#vlan 30

SwitchFribaP3(config-vlan)#name PersonalSalud

SwitchFribaP3(config-vlan)#exit

SwitchP3#conf terminal

SwitchP3(config)#vlan 30

SwitchP3(config-vlan)#name PersonalSalud

SwitchP3(config-vlan)#exit

SwitchP3(config)#interface fastEthernet 0/22

SwitchP3(config-if)#switchport mode access

SwitchP3(config-if)#switchport access vlan 30

SwitchP3(config-if)#end

Vlan40

SwitchP#conf terminal

SwitchP(config)#vlan 40

SwitchP(config-vlan)#name Consultoria

SwitchP(config-vlan)#exit

SwitchP(config)#interface vlan 40

SwitchP(config-if)#ip address 192.168.2.78 255.255.255.240

SwitchP(config-if)#no shutdown

SwitchP(config-if)#exit

SwitchP(config)#ip dhcp pool vlan40

SwitchP(dhcp-config)#network 192.168.2.64 255.255.255.240

SwitchP(dhcp-config)#default-router 192.168.2.65

SwitchP(dhcp-config)# dns-server 192.168.3.100

SwitchP(dhcp-config)#exit

SwitchP(config)#ip dhcp excluded-address 192.168.2.65

SwitchP(config)#ip dhcp excluded-address 192.168.2.78

PB

SwitchFibraPB#conf terminal

SwitchFibraPB(config)#vlan 40

SwitchFibraPB(config-vlan)#name Consultoria

SwitchFibraPB(config-vlan)#exit
SwitchFibraPB(config)#interface fastEthernet 3/1
SwitchFibraPB(config-if)#switchport mode access
SwitchFibraPB(config-if)#switchport access vlan 40
SwitchFibraPB(config-if)#exit
SwitchFibraPB(config)#interface range fastEthernet 5-8/1
SwitchFibraPB(config-if)#switchport mode access
SwitchFibraPB(config-if)#switchport access vlan 40
SwitchFibraPB(config-if)#exit
SwitchPB#conf terminal
SwitchPB(config)#vlan 40
SwitchPB(config-vlan)#name Consultoria
SwitchPB(config-vlan)#exit
SwitchPB(config)#interface range fastEthernet 0/4-8
SwitchPB(config-if-range)#switchport mode access
SwitchPB(config-if-range)#switchport access vlan 40
SwitchPB(config-if-range)#end

Vlan50:

SwitchP(config)#vlan 50
SwitchP(config-vlan)#name AreaTercerizada
SwitchP(config-vlan)#exit
SwitchP(config)#interface vlan 50
SwitchP(config-if)#ip address 192.168.2.94 255.255.255.240
SwitchP(config-if)#no shutdown
SwitchP(config-if)#exit
SwitchP(config)#ip dhcp pool vlan50
SwitchP(dhcp-config)#network 192.168.2.80 255.255.255.240
SwitchP(dhcp-config)#default-router 192.168.2.81
SwitchP(dhcp-config)# dns-server 192.168.3.100
SwitchP(dhcp-config)#exit
SwitchP(config)#ip dhcp excluded-address 192.168.2.81
SwitchP(config)#ip dhcp excluded-address 192.168.2.94

PB

SwitchFibraPB(config)#vlan 50

SwitchFibraPB(config-vlan)#name AreaTercerizada

SwitchFibraPB(config-vlan)#exit

SwitchFibraPB(config)#interface fastEthernet 2/1

SwitchFibraPB(config-if)#switchport mode access

SwitchFibraPB(config-if)#switchport access vlan 50

SwitchPB#conf terminal

SwitchPB(config)#vlan 50

SwitchPB(config-vlan)#name AreaTercerizada

SwitchPB(config-vlan)#exit

SwitchPB(config)#interface range fastEthernet 0/9-12

SwitchPB(config-if-range)#switchport mode access

SwitchPB(config-if-range)#switchport access vlan 50

SwitchPB(config-if-range)#exit

P3

SwitchFribaP3#conf terminal

SwitchFribaP3(config)#vlan 50

SwitchFribaP3(config-vlan)#name AreaTercerizada

SwitchFribaP3(config-vlan)#exit

SwitchP3#conf terminal

SwitchP3(config)#vlan 50

SwitchP3(config-vlan)#name AreaTercerizada

SwitchP3(config-vlan)#exit

SwitchP3(config)#interface fastEthernet 0/1

SwitchP3(config-if)#switchport mode access

SwitchP3(config-if)#switchport access vlan 50

SwitchP3(config-if)#end

Vlan60:

SwitchP(config)#vlan 60

SwitchP(config-vlan)#name Administracion

SwitchP(config-vlan)#exit

SwitchP(config)#interface vlan 60

SwitchP(config-if)#ip address 192.168.2.102 255.255.255.248

SwitchP(config-if)#no shutdown

SwitchP(config-if)#exit

SwitchP(config)#ip dhcp pool vlan60

SwitchP(dhcp-config)#network 192.168.2.96 255.255.255.248

SwitchP(dhcp-config)#default-router 192.168.2.97

SwitchP(dhcp-config)# dns-server 192.168.3.100

SwitchP(dhcp-config)#exit

SwitchP(config)#ip dhcp excluded-address 192.168.2.97

SwitchP(config)#ip dhcp excluded-address 192.168.2.102

PB

SwitchFibraPB#conf terminal

SwitchFibraPB(config)#vlan 60

SwitchFibraPB(config-vlan)#name Administracion

SwitchFibraPB(config-vlan)#exit

Impresoras

SwitchFibraPB(config)#interface fastEthernet 9/1

SwitchFibraPB(config-if)#switchport mode access

SwitchFibraPB(config-if)#switchport access vlan 60

SwitchFibraPB(config-if)#exit

SwitchPB(config)#vlan 60

SwitchPB(config-vlan)#name Administracion

SwitchPB(config-vlan)#exit

SwitchPB(config)#interface range fastEthernet 0/1-3

SwitchPB(config-if-range)#switchport mode access

SwitchPB(config-if-range)#switchport access vlan 60

SwitchPB(config-if-range)#end

Vlan70:

SwitchP(config)#vlan 70

SwitchP(config-vlan)#name Recepcion

SwitchP(config-vlan)#exit

SwitchP(config)#interface vlan 70

SwitchP(config-if)#ip address 192.168.2.110 255.255.255.248

SwitchP(config-if)#no shutdown

SwitchP(config-if)#exit

SwitchP(config)#ip dhcp pool vlan70

SwitchP(dhcp-config)#network 192.168.2.104 255.255.255.248

SwitchP(dhcp-config)#default-router 192.168.2.105

SwitchP(dhcp-config)# dns-server 192.168.3.100

SwitchP(dhcp-config)#exit

SwitchP(config)#ip dhcp excluded-address 192.168.2.105

SwitchP(config)#ip dhcp excluded-address 192.168.2.110

SwitchP(config)#end

PB

SwitchFibraPB(config)#vlan 70

SwitchFibraPB(config-vlan)#name Recepcion

SwitchFibraPB(config-vlan)#exit

SwitchPB#conf terminal

SwitchPB(config)#vlan 70

SwitchPB(config-vlan)#name Recepcion

SwitchPB(config-vlan)#exit

SwitchPB(config)#interface range fastEthernet 0/14-15

SwitchPB(config-if)#switchport mode access

SwitchPB(config-if)#switchport access vlan 70

SwitchPB(config-if)#end

Vlan80:

SwitchP#conf terminal

SwitchP(config)#vlan 80

SwitchP(config-vlan)#name Emergencias

SwitchP(config-vlan)#exit

SwitchP(config)#interface vlan 80

SwitchP(config-if)#ip address 192.168.2.118 255.255.255.248

SwitchP(config-if)#no shutdown

SwitchP(config-if)#exit

SwitchP(config)#ip dhcp pool vlan80

SwitchP(dhcp-config)#network 192.168.2.112 255.255.255.248

SwitchP(dhcp-config)#default-router 192.168.2.113

SwitchP(dhcp-config)# dns-server 192.168.3.100

SwitchP(dhcp-config)#exit

SwitchP(config)#ip dhcp excluded-address 192.168.2.113

SwitchP(config)#ip dhcp excluded-address 192.168.2.118

PB

SwitchFibraPB#conf terminal

SwitchFibraPB(config)#vlan 80

SwitchFibraPB(config-vlan)#name Emergencias

SwitchFibraPB(config-vlan)#exit

SwitchPB(config)#vlan 80

SwitchPB(config-vlan)#name Emergencias

SwitchPB(config-vlan)#exit

SwitchPB(config)#interface fastEthernet 0/13

SwitchPB(config-if)#switchport mode access

SwitchPB(config-if)#switchport access vlan 80

SwitchPB(config-if)#exit

Vlan90:

SwitchP(config)#vlan 90

SwitchP(config-vlan)#name Enfermeria

SwitchP(config-vlan)#exit

SwitchP(config)#interface vlan 90

SwitchP(config-if)#ip address 192.168.2.126 255.255.255.248

SwitchP(config-if)#no shutdown

SwitchP(config-if)#exit

SwitchP(config)#ip dhcp pool vlan90

SwitchP(dhcp-config)#network 192.168.2.120 255.255.255.248

SwitchP(dhcp-config)#default-router 192.168.2.121

SwitchP(dhcp-config)# dns-server 192.168.3.100

SwitchP(dhcp-config)#exit

SwitchP(config)#ip dhcp excluded-address 192.168.2.121

SwitchP(config)#ip dhcp excluded-address 192.168.2.126

P1

SwitchFibraP1(config)#vlan 90

SwitchFibraP1(config-vlan)#name Enfermeria

SwitchFibraP1(config-vlan)#exit

SwitchP1(config)#vlan 90

SwitchP1(config-vlan)#name Enfermeria

SwitchP1(config-vlan)#exit

SwitchP1(config)#interface fastEthernet 0/8

SwitchP1(config-if)#switchport mode access

SwitchP1(config-if)#switchport access vlan 90

SwitchP1(config-if)#end

P2

SwitchFibraP2(config)#vlan 90

SwitchFibraP2(config-vlan)#name Enfermeria

SwitchFibraP2(config-vlan)#exit

SwitchP2(config)#vlan 90

SwitchP2(config-vlan)#name Enfermeria

SwitchP2(config-vlan)#exit

P3

SwitchFribaP3(config)#vlan 90

SwitchFribaP3(config-vlan)#name Enfermeria

SwitchFribaP3(config-vlan)#exit

SwitchP3#conf terminal

SwitchP3(config)#vlan 90

SwitchP3(config-vlan)#name Enfermeria

SwitchP3(config-vlan)#exit

SwitchP3(config)#interface fastEthernet 0/12

SwitchP3(config-if)#switchport mode access

SwitchP3(config-if)#switchport access vlan 90

SwitchP3(config-if)#end

Vlan100:

SwitchP(config)#vlan 100

SwitchP(config-vlan)#name TerapiaIntensiva

SwitchP(config-vlan)#exit

SwitchP(config)#interface vlan 100

SwitchP(config-if)#ip address 192.168.2.134 255.255.255.248

SwitchP(config-if)#no shutdown

SwitchP(config-if)#exit

SwitchP(config)#ip dhcp pool vlan100

SwitchP(dhcp-config)#network 192.168.2.128 255.255.255.248

SwitchP(dhcp-config)#default-router 192.168.2.129

SwitchP(dhcp-config)# dns-server 192.168.3.100

SwitchP(dhcp-config)#exit

SwitchP(config)#ip dhcp excluded-address 192.168.2.129

SwitchP(config)#ip dhcp excluded-address 192.168.2.134

P1

SwitchFibraP1(config)#vlan 100

SwitchFibraP1(config-vlan)#name TerapiaIntensiva

SwitchFibraP1(config-vlan)#exit

SwitchFibraP1(config)#interface fastEthernet 9/1

SwitchFibraP1(config-if)#switchport mode access

SwitchFibraP1(config-if)#switchport access vlan 100

SwitchFibraP1(config-if)#exit

SwitchP1(config)#vlan 100

SwitchP1(config-vlan)#name TerapiaIntensiva

SwitchP1(config-vlan)#exit

SwitchP1(config)#interface fastEthernet 0/9

SwitchP1(config-if)#switchport mode access

SwitchP1(config-if)#switchport access vlan 100

SwitchP1(config-if)#end

P2

SwitchFibraP2(config)#vlan 100

SwitchFibraP2(config-vlan)#name TerapiaIntensiva

SwitchFibraP2(config-vlan)#exit

SwitchP2(config)#vlan 100

SwitchP2(config-vlan)#name TerapiaIntensiva

SwitchP2(config-vlan)#exit

SwitchP2(config)#interface fastEthernet 0/8

SwitchP2(config-if)#switchport mode access

SwitchP2(config-if)#switchport access vlan 100

SwitchP2(config-if)#end

P3

SwitchFribaP3(config)#vlan 100

SwitchFribaP3(config-vlan)#name TerapiaIntensiva

SwitchFribaP3(config-vlan)#exit

SwitchP3(config)#vlan 100

SwitchP3(config-vlan)#name TerapiaIntensiva

SwitchP3(config-vlan)#exit

SwitchP3(config)#interface fastEthernet 0/11

SwitchP3(config-if)#switchport mode access

SwitchP3(config-if)#switchport access vlan 100

SwitchP3(config-if)#end

Vlan110:

SwitchP(config)#vlan 110

SwitchP(config-vlan)#name Pediatria

SwitchP(config-vlan)#exit

SwitchP(config)#interface vlan 110

SwitchP(config-if)#ip address 192.168.2.142 255.255.255.248

SwitchP(config-if)#no shutdown

SwitchP(config-if)#exit

SwitchP(config)#ip dhcp pool vlan110

SwitchP(dhcp-config)#network 192.168.2.136 255.255.255.248

SwitchP(dhcp-config)#default-router 192.168.2.137

SwitchP(dhcp-config)# dns-server 192.168.3.100

SwitchP(dhcp-config)#exit

SwitchP(config)#ip dhcp excluded-address 192.168.2.137

SwitchP(config)#ip dhcp excluded-address 192.168.2.142

P3

SwitchFribaP3(config)#vlan 110

SwitchFribaP3(config-vlan)#name Pediatria

SwitchFribaP3(config-vlan)#exit

SwitchP3#conf terminal

SwitchP3(config)#vlan 110

SwitchP3(config-vlan)#name Pediatria

SwitchP3(config-vlan)#exit

SwitchP3(config)#interface range fastEthernet 0/2-5

SwitchP3(config-if-range)#switchport mode access

SwitchP3(config-if-range)#switchport access vlan 110

SwitchP3(config-if-range)#end

Vlan120:

SwitchP(config)#vlan 120

SwitchP(config-vlan)#name Farmacia

SwitchP(config-vlan)#exit

SwitchP(config)#interface vlan 120

SwitchP(config-if)#ip address 192.168.2.150 255.255.255.248

SwitchP(config-if)#no shutdown

SwitchP(config-if)#exit

SwitchP(config)#ip dhcp pool vlan120

SwitchP(dhcp-config)#network 192.168.2.144 255.255.255.248

SwitchP(dhcp-config)#default-router 192.168.2.145

SwitchP(dhcp-config)# dns-server 192.168.3.100

SwitchP(dhcp-config)#exit

SwitchP(config)#ip dhcp excluded-address 192.168.2.145

SwitchP(config)#ip dhcp excluded-address 192.168.2.150

P3

SwitchFribaP3(config)#vlan 120

SwitchFribaP3(config-vlan)#name Farmacia

SwitchFribaP3(config-vlan)#exit

SwitchFribaP3(config)#interface fastEthernet 8/1

SwitchFribaP3(config-if)#switchport mode access

SwitchFribaP3(config-if)#switchport access vlan 120

SwitchFribaP3(config-if)#exit

SwitchP3(config)#vlan 120

SwitchP3(config-vlan)#name Farmacia

SwitchP3(config-vlan)#exit

SwitchP3(config)#interface fastEthernet 0/13

SwitchP3(config-if)#switchport mode access

SwitchP3(config-if)#switchport access vlan 120

SwitchP3(config-if)#end

Vlan130:

SwitchP(config)#vlan 130

SwitchP(config-vlan)#name Esterilizacion

SwitchP(config-vlan)#exit

SwitchP(config)#interface vlan 130

SwitchP(config-if)#ip address 192.168.2.158 255.255.255.248

SwitchP(config-if)#no shutdown

SwitchP(config-if)#exit

SwitchP(config)#ip dhcp pool vlan130

SwitchP(dhcp-config)#network 192.168.2.152 255.255.255.248

SwitchP(dhcp-config)#default-router 192.168.2.153

SwitchP(dhcp-config)# dns-server 192.168.3.100

SwitchP(dhcp-config)#exit

SwitchP(config)#ip dhcp excluded-address 192.168.2.153

SwitchP(config)#ip dhcp excluded-address 192.168.2.158

P3

SwitchFribaP3(config)#vlan 130

SwitchFribaP3(config-vlan)#name Esterilizacion

SwitchFribaP3(config-vlan)#exit

Impresora

SwitchFribaP3(config)#interface fastEthernet 7/1

SwitchFribaP3(config-if)#switchport mode access

SwitchFribaP3(config-if)#switchport access vlan 130

SwitchFribaP3(config-if)#exit

SwitchP3#conf terminal

SwitchP3(config)#vlan 130

SwitchP3(config-vlan)#name Esterilizacion

SwitchP3(config-vlan)#exit

SwitchP3(config)#interface range fastEthernet 0/14-16

SwitchP3(config-if-range)#switchport mode access

SwitchP3(config-if-range)#switchport access vlan 130

SwitchP3(config-if-range)#end

Vlan140:

SwitchP(config)#vlan 140

SwitchP(config-vlan)#name Contabilidad

SwitchP(config-vlan)#exit

SwitchP(config)#interface vlan 140

SwitchP(config-if)#ip address 192.168.2.166 255.255.255.248

SwitchP(config-if)#no shutdown

SwitchP(config-if)#exit

SwitchP(config)#ip dhcp pool vlan140

SwitchP(dhcp-config)#network 192.168.2.161 255.255.255.248

SwitchP(dhcp-config)#default-router 192.168.2.161

SwitchP(dhcp-config)# dns-server 192.168.3.100

SwitchP(dhcp-config)#exit

SwitchP(config)#ip dhcp excluded-address 192.168.2.161

SwitchP(config)#ip dhcp excluded-address 192.168.2.166

P3

SwitchFribaP3(config)#vlan 140

SwitchFribaP3(config-vlan)#name Contabilidad

SwitchFribaP3(config-vlan)#exit

SwitchFribaP3(config)#interface fastEthernet 9/1

SwitchFribaP3(config-if)#switchport mode access

SwitchFribaP3(config-if)#switchport access vlan 140

SwitchFribaP3(config-if)#exit

SwitchP3(config)#vlan 140

SwitchP3(config-vlan)#name Contabilidad

SwitchP3(config-vlan)#exit

SwitchP3(config)#interface range fastEthernet 0/17-18

SwitchP3(config-if-range)#switchport mode access

SwitchP3(config-if-range)#switchport access vlan 140

SwitchP3(config-if-range)#end

8. Configuración de las contraseñas al switch

Switch por plantas	**Contraseñas**
Switch Principal	HRSJRE2025PRINC
Switch Fibra Planta Baja	HRSJDD2025FIBRPLANB
Switch Fibra Piso 1	HJRJDD2025FIBRPLAN1
Switch Fibra Piso 2	HDTRD2025FIBRPLAN2
Switch Fibra Piso 3	HSSWRT2025FIBRPLAN3
Switch Planta Baja	HRSCC2025SWITCHPB

Switch Piso 1	HRSTT2025SWITCHP1
Switch Piso 2	HRSTW2025SWITCHP2
Switch Piso 3	HRGHR2025SWITCHP3

Tabla 143. Configuracion de las contraseñas de los switch

Switch Principal

SwitchP>enable

SwitchP#conf term

SwitchP(config)#line con 0

SwitchP(config-line)#password HRSJRE2025PRINC

SwitchP(config-line)#login

SwitchP(config-line)#end

SwitchP#write memory

Switch Fibra Planta Baja

SwitchFibraPB>enable

SwitchFibraPB#conf term

SwitchFibraPB(config)#line con 0

SwitchFibraPB(config-line)#password HRSJDD2025FIBRPLANB

SwitchFibraPB(config-line)#login

SwitchFibraPB(config-line)#end

SwitchFibraPB#write memory

Switch Fibra Piso 1

SwitchFibraP1>enable

SwitchFibraP1#conf ter

SwitchFibraP1(config)#line con 0

SwitchFibraP1(config-line)#password HJRJDD2025FIBRPLAN1

SwitchFibraP1(config-line)#login

SwitchFibraP1(config-line)#end

SwitchFibraP1#write memory

Switch Fibra Piso 2

SwitchFibraP2>enable

SwitchFibraP2#conf term

SwitchFibraP2(config)#line con 0

SwitchFibraP2(config-line)#password HDTRD2025FIBRPLAN2

SwitchFibraP2(config-line)#login

SwitchFibraP2(config-line)#end

SwitchFibraP2#write memory

Switch Fibra Piso 3

SwitchFribaP3>enable

SwitchFribaP3#conf ter

SwitchFribaP3(config)#line con 0

SwitchFribaP3(config-line)#password HSSWRT2025FIBRPLAN3

SwitchFribaP3(config-line)#login

SwitchFribaP3(config-line)#end

SwitchFribaP3#write memory

Switch Planta Baja

SwitchPB>enable

SwitchPB#conf term

SwitchPB(config)#line con 0

SwitchPB(config-line)#password HRSCC2025SWITCHPB

SwitchPB(config-line)#login

SwitchPB(config-line)#end

SwitchPB#write memory

Switch Piso 1

SwitchP1>enable

SwitchP1#conf term

SwitchP1(config)#line con 0

SwitchP1(config-line)#password HRSTT2025SWITCHP1

SwitchP1(config-line)#login

SwitchP1(config-line)#end

SwitchP1#write memory

Switch Piso 2

SwitchP2>enable

SwitchP2#conf term

SwitchP2(config)#line con 0

SwitchP2(config-line)#password HRSTW2025SWITCHP2

SwitchP2(config-line)#login

SwitchP2(config-line)#end

SwitchP2#write memory

Switch Piso 3

SwitchP3>enable

SwitchP3#conf term

SwitchP3(config)#line con 0

SwitchP3(config-line)#password HRGHR2025SWITCHP3

SwitchP3(config-line)#login

SwitchP3(config-line)#end

SwitchP3#write memory

9. Conectarse a la red mediante las VLANS

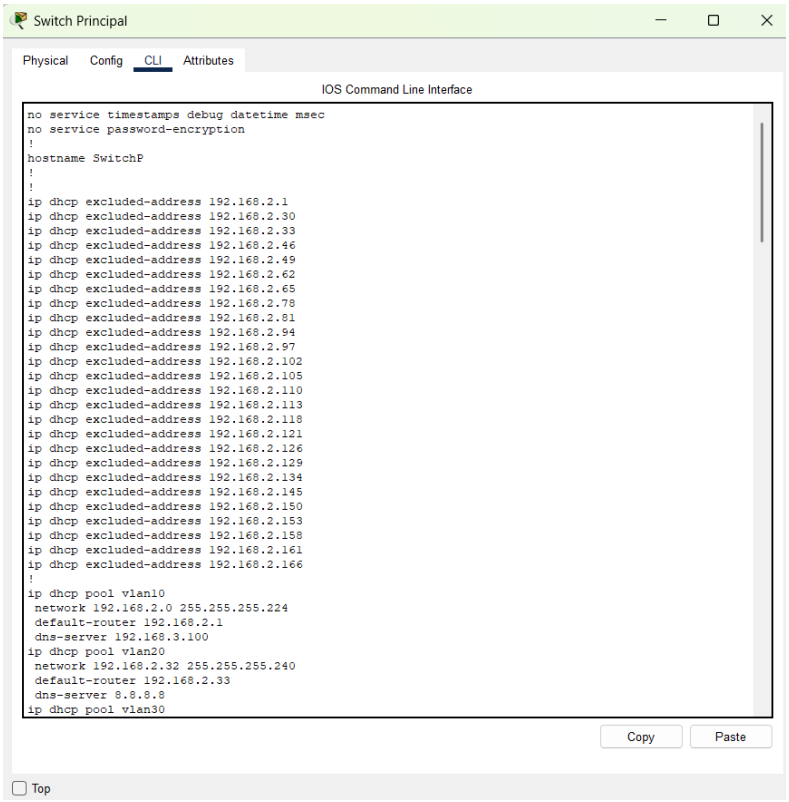

Figura 300. IP excluidas para el DHCP

En esta figura se muestra cómo en el Switch Principal se crean los pools DHCP para cada VLAN, definiendo su red, máscara y la dirección del gateway, que corresponde a la interfaz VLAN de ese segmento. Además, se configura como servidor DNS la IP 192.168.3.100, que pertenece al servidor de telefonía IP Issabel, de modo que los equipos (especialmente los teléfonos IP) reciban automáticamente esta dirección y puedan conectarse correctamente a dicho servidor para registrar sus extensiones y utilizar los servicios de voz. Con esta configuración, cualquier dispositivo que se conecte a una VLAN obtiene una IP válida, su puerta de enlace y el DNS apuntando al servidor

Issabel, asegurando la comunicación tanto dentro de la red de datos como con la plataforma de telefonía.

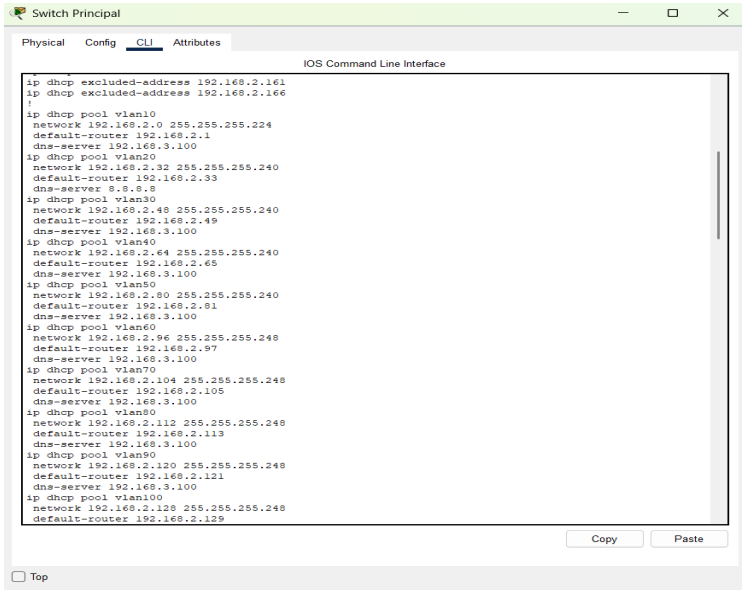

Figura 301. DHCP para cada VLAN

Se muestra la configuración del Switch Principal donde varias interfaces GigabitEthernet se establecen en modo trunk, permitiendo el transporte simultáneo de todas las VLAN entre equipos de la red. Las interfaces FastEthernet se dejan en modo access asociadas, por ejemplo, a la VLAN 150 para conectar dispositivos finales. Al final se observan las interfaces lógicas VLAN10, VLAN20 y VLAN30 con sus direcciones IP correspondientes, que funcionarán como gateway de cada segmento y permitirán el enrutamiento entre VLANs.

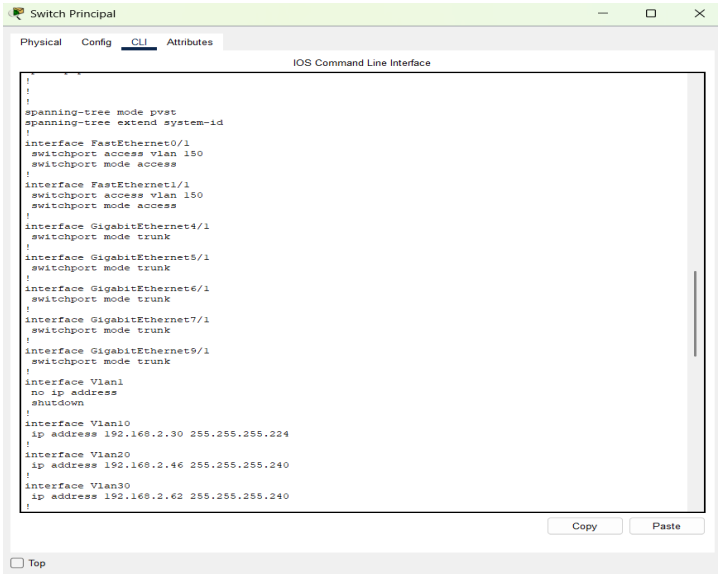

Figura 302. Modo Trunk para cada interface

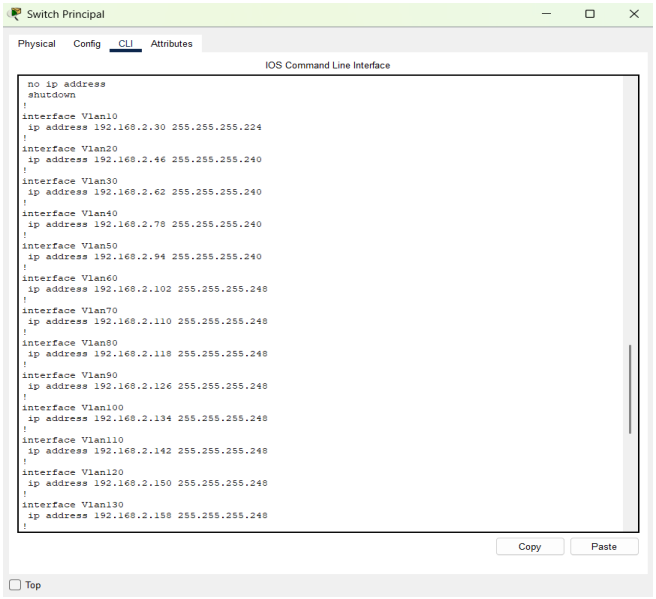

Figura 303. IP unica para cada Interface para HDCP

Se observa el resultado del comando ipconfig /renew ejecutado en el PC de la VLAN, donde el equipo solicita una nueva configuración al servidor DHCP. Como respuesta, obtiene automáticamente la dirección IP 192.168.2.11, la máscara 255.255.255.224, el gateway 192.168.2.1 correspondiente a la interfaz de su VLAN y el DNS 192.168.3.100, que es la dirección del servidor de telefonía IP Issabel. De esta manera se comprueba que el DHCP de la VLAN funciona correctamente y que el equipo queda listo para comunicarse tanto con la red de datos como con el servidor Issabel.

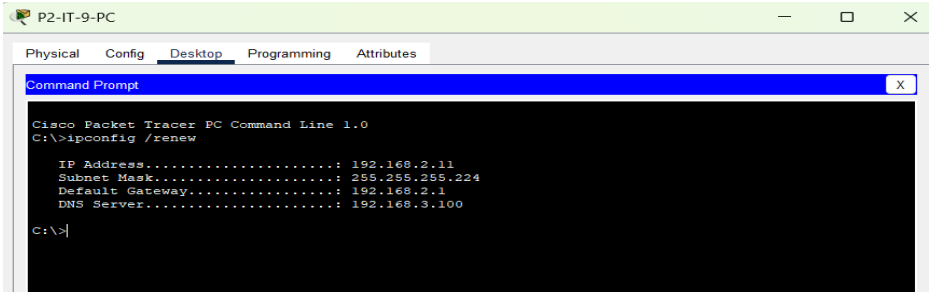

Figura 304. Obteniedo la IP de tipo DHCP para dicha VLAN

10. Configuración del ACL como políticas de seguridad

RouterClinica>enable

RouterClinica#configure terminal

RouterClinica(config)#access-list 100 deny ip 192.168.2.32 0.0.0.15 192.168.2.0 0.0.0.31

RouterClinica(config)#access-list 100 deny ip 192.168.2.32 0.0.0.15 192.168.2.64 0.0.0.15

RouterClinica(config)#access-list 100 deny ip 192.168.2.32 0.0.0.15 192.168.2.80 0.0.0.15

RouterClinica(config)#access-list 100 deny ip 192.168.2.32 0.0.0.15 192.168.2.96 0.0.0.7
RouterClinica(config)#access-list 100 deny ip 192.168.2.32 0.0.0.15 192.168.2.104 0.0.0.7
RouterClinica(config)#access-list 100 deny ip 192.168.2.32 0.0.0.15 192.168.2.112 0.0.0.7
RouterClinica(config)#access-list 100 deny ip 192.168.2.32 0.0.0.15 192.168.2.120 0.0.0.7
RouterClinica(config)#access-list 100 deny ip 192.168.2.32 0.0.0.15 192.168.2.128 0.0.0.7
RouterClinica(config)#access-list 100 deny ip 192.168.2.32 0.0.0.15 192.168.2.136 0.0.0.7
RouterClinica(config)#access-list 100 deny ip 192.168.2.32 0.0.0.15 192.168.2.144 0.0.0.7
RouterClinica(config)#access-list 100 deny ip 192.168.2.32 0.0.0.15 192.168.2.152 0.0.0.7
RouterClinica(config)#access-list 100 deny ip 192.168.2.32 0.0.0.15 192.168.2.160 0.0.0.7
RouterClinica(config)#access-list 100 deny ip 192.168.2.32 0.0.0.15 192.168.3.0 0.0.0.255
RouterClinica(config)#access-list 100 permit ip any any
RouterClinica(config)#end

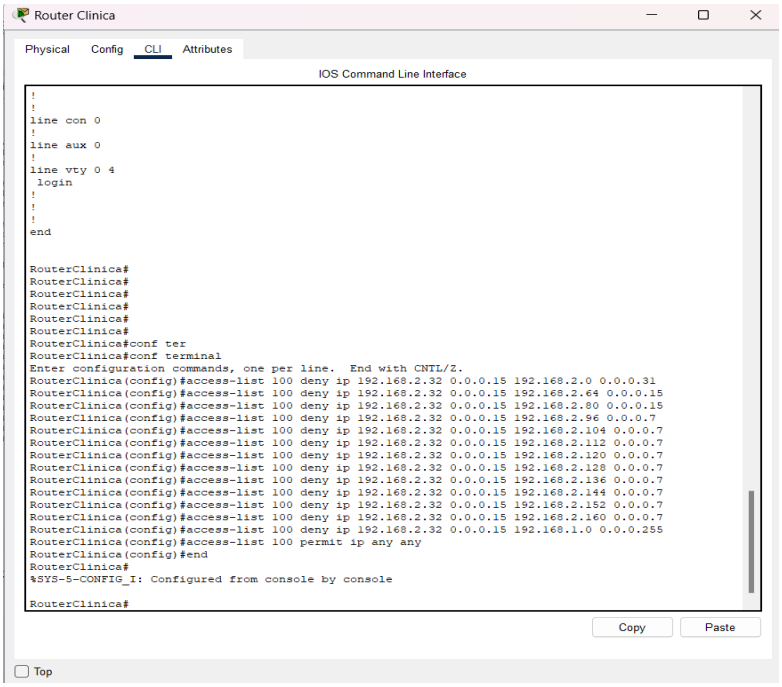

Figura 305. Configuración de ACL como política de seguridad

Se ha implementado una lista de control de acceso (ACL) que bloquea la comunicación entre la VLAN asignada a los pacientes y las demás áreas internas de la clínica. De esta forma, los dispositivos conectados al Access Point de Pacientes únicamente tendrán acceso a internet, sin posibilidad de interactuar con la red interna.

11. Configuración del Firewall Fortinet

Se muestra la configuración de la interfaz port1 en el firewall Fortinet, donde se activa el modo

DHCP y se permiten accesos para ping, http, https, y ssh. Esto asegura que la interfaz pueda obtener una IP dinámica y manejar tráfico básico.

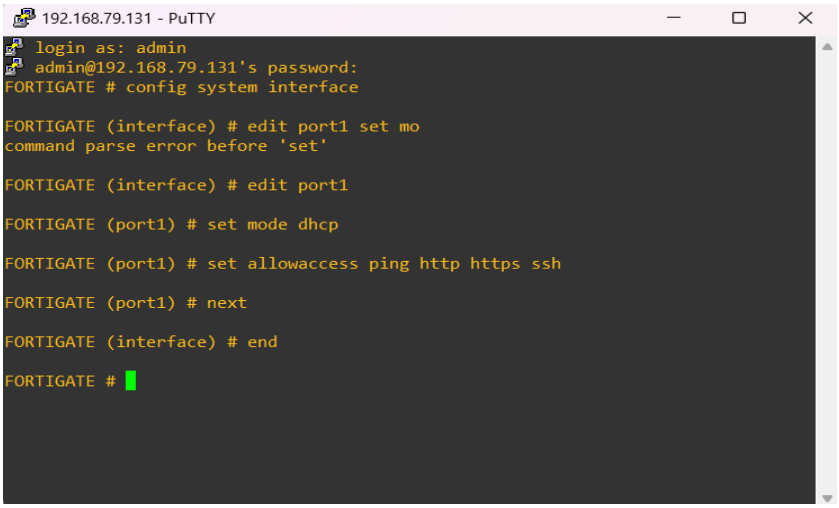

Figura 306. Configuracion port1 DHCP

Aquí se verifica la configuración de la interfaz port1, donde se confirma que ha recibido una dirección IP de 192.168.1.143 con máscara 255.255.255.0 y con conexión “up”. También se muestra el estado de la interfaz y su velocidad de conexión.

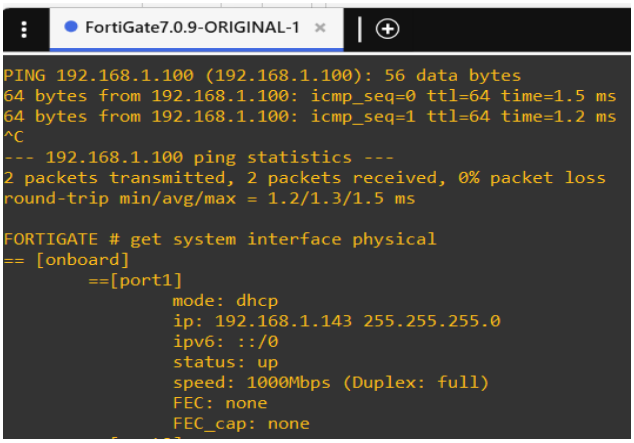

Figura 307. Verificacion de Ips

Se muestra la pantalla de inicio de sesión del firewall Fortinet. El usuario ingresa su nombre de usuario y contraseña para acceder a la interfaz de administración del dispositivo y realizar configuraciones.

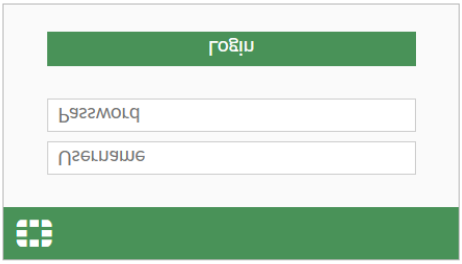

Figura 308. Inicio de sesion Fortinet

En esta captura, se verifica la configuración de la interfaz port1 en el Fortinet, mostrando que está configurada en modo DHCP. Se observa que el dispositivo ha adquirido una dirección IP dinámica (192.168.1.143) con una máscara de subred de 255.255.255.0 y un puerto WAN activo, confirmando la correcta obtención de la configuración de red.

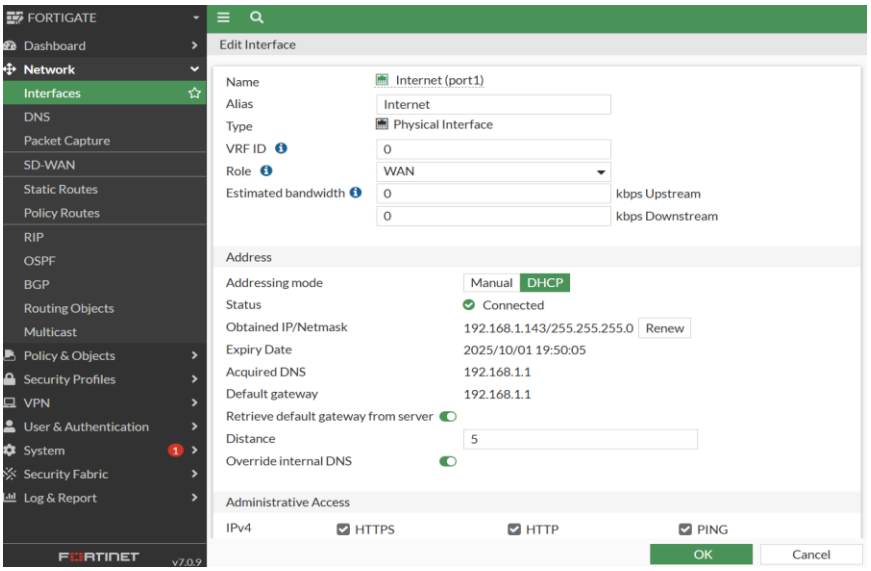

Figura 309. Verificación de tipo DHCP puerto1

Se está configurando la interfaz Red Interna (port10) en el Fortinet. Se le asigna un nombre (Red Interna) y se configura como una interfaz de tipo LAN, en modo manual para la dirección IP, y otras configuraciones de acceso administrativo habilitadas como HTTPS, PING.

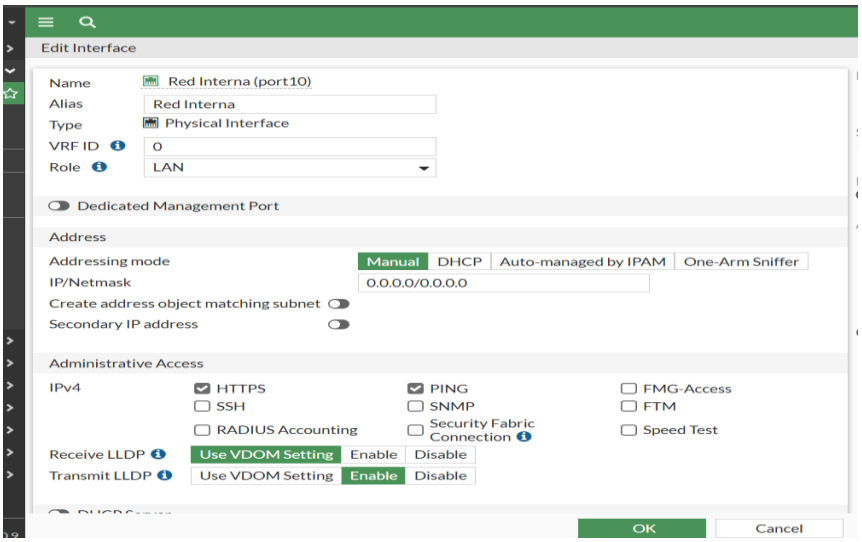

Figura 310. Ingresar nombre puerto10

12. Asignación de VLANs en el puerto 10

Se muestra la configuración de la VLAN 70 llamada Recepción, asignada a la interfaz Red Interna (port10). Se especifica el protocolo 802.1Q, el ID de VLAN 70, y se asigna la dirección IP 192.168.2.105 con la máscara 255.255.255.248. Esta configuración permite segmentar la red en diferentes VLANs para una mejor gestión del tráfico.

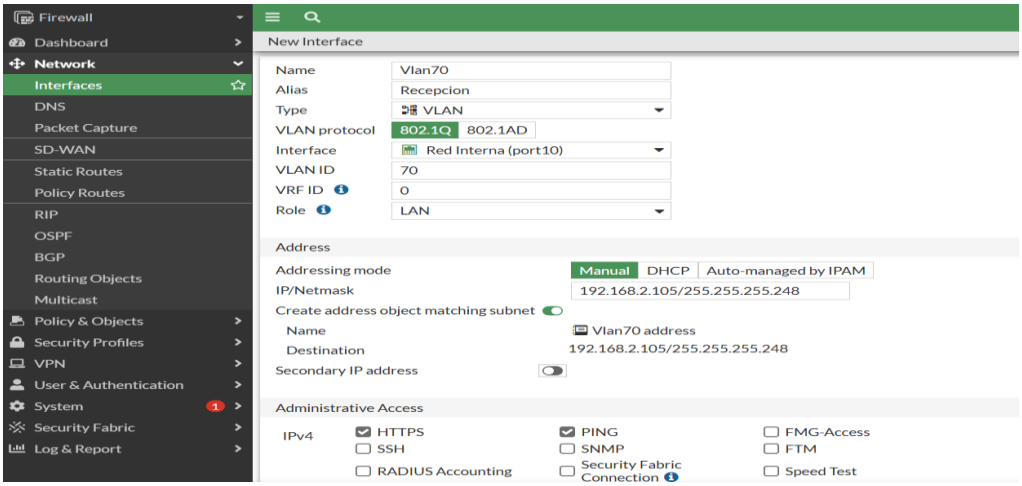

Figura 311. Crear VLAN 70 Tipo Interface

Se muestra la configuración de la VLAN 10 llamada Internación, asignada a la interfaz Red Interna (port10). Se configura el protocolo 802.1Q para la VLAN, con el ID de VLAN 10 y la dirección IP 192.168.2.1/255.255.255.224. Esta configuración segmenta la red para un área específica, permitiendo un control de tráfico eficiente.

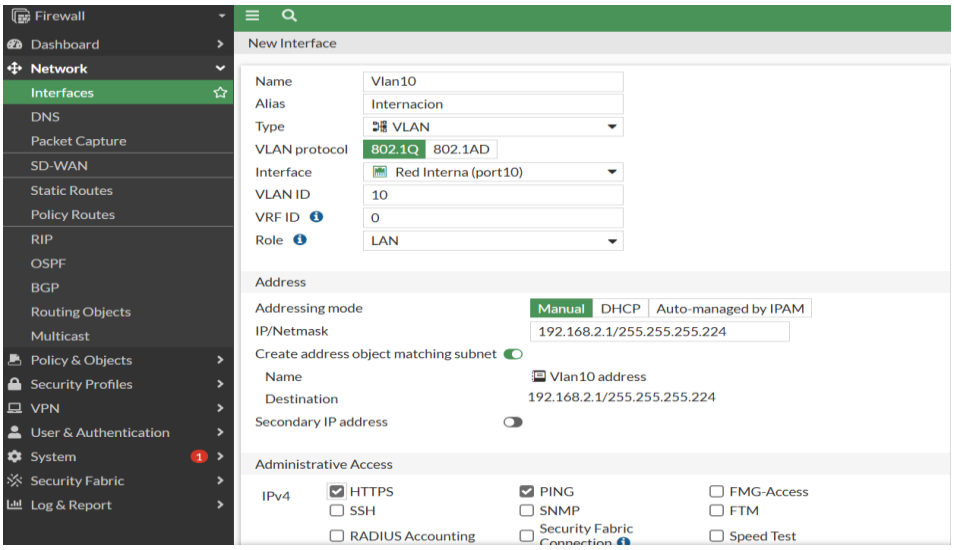

Figura 312. Crear VLAN 10 tipo Interface

Se configura la VLAN 100 llamada Terapia Intensiva, también asignada a la interfaz Red Interna (port10). La VLAN tiene el ID 100, se utiliza el protocolo 802.1Q, y se asigna la dirección IP 192.168.2.129/255.255.255.248, lo que también crea una red separada para gestionar el tráfico de la zona correspondiente.

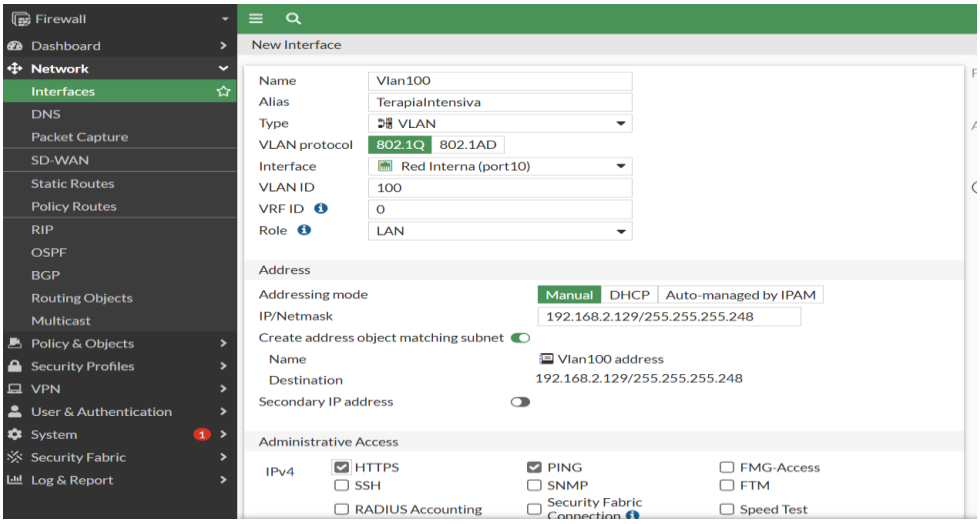

Figura 313. Crear VLAN 100 tipo Interface

Se muestra la configuración de la VLAN 150 llamada Servidores, asignada a la interfaz Red Interna (port10). Se configura el protocolo 802.1Q para esta VLAN y se asigna la dirección IP 192.168.3.1/255.255.255.0, lo que crea una subred específica para los servidores de la red, segmentando el tráfico para optimizar el rendimiento y la seguridad.

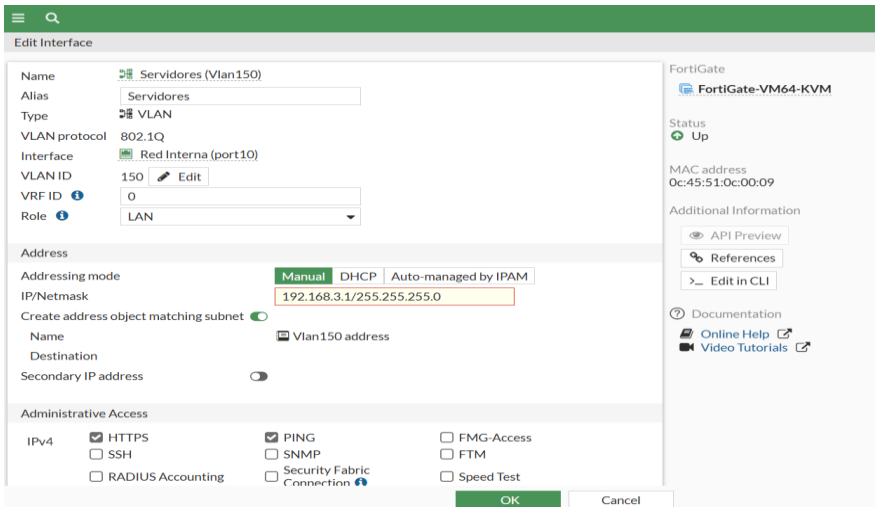

Figura 314. Crear VLAN 150 tipo Interface

13. Configuración de Objetos de Dirección (Address)

Se configurarán los Address Objects en Fortinet para controlar los rangos de IPs en diferentes VLANs. Se crearán los objetos para Vlan70, Vlan10 y Vlan100, asignando rangos de IPs específicos a cada uno, lo que permite gestionar y segmentar el tráfico dentro de cada subred asociada a las VLANs correspondientes. Esto facilita el control y la organización del tráfico en la red.

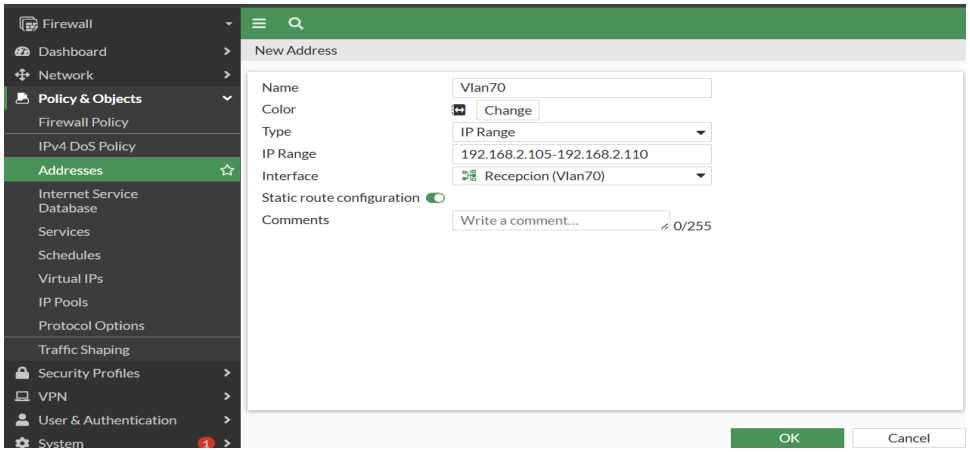

Figura 315. Crear Address para controlar el rango de la subred VLAN70

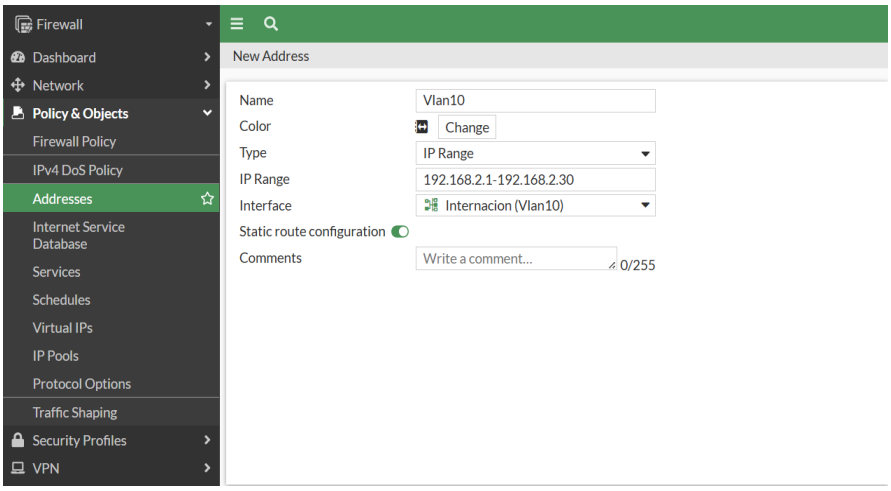

Figura 316. Crear Address para controlar el rango de la subred VLAN10

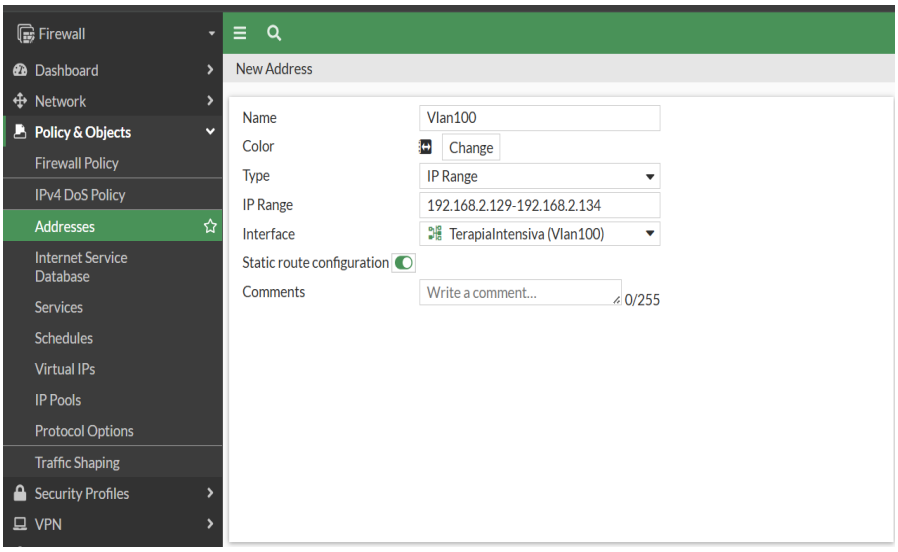

Figura 317. Crear Address para controlar el rango de la subred VLAN100

14. Configuración de las Políticas de seguridad perimetral

Se configura una política de seguridad para la VLAN 10, que permite la comunicación entre la VLAN 10 y el Internet. La política define las interfaces de entrada y salida, el tipo de tráfico permitido y la acción que se debe tomar (permitir o denegar).

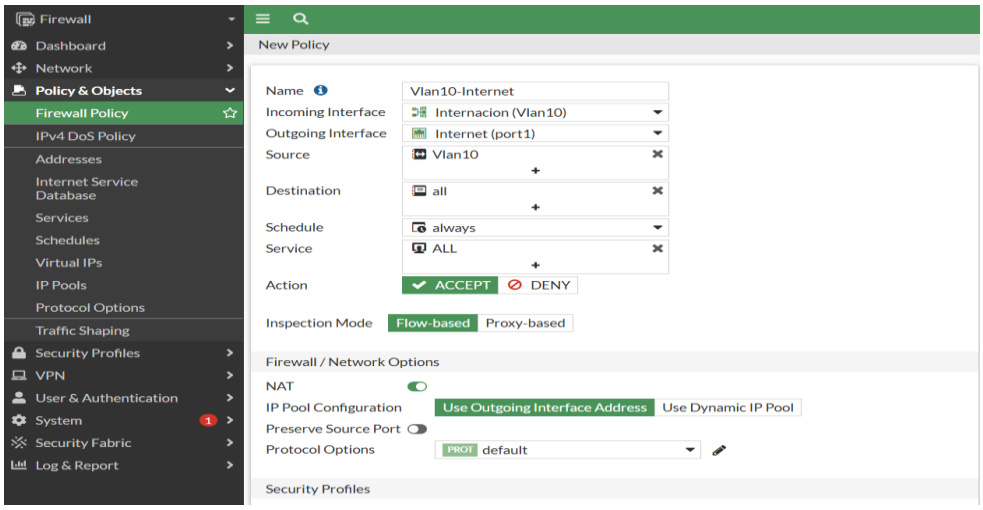

Figura 318. Política de Seguridad Vlan10-Internet

Esta es otra política de seguridad, pero en este caso para la VLAN 70, permitiendo la comunicación entre VLAN 70 y Internet. La configuración sigue la misma lógica que la política de la VLAN 10, asegurando que el tráfico deseado se permita.

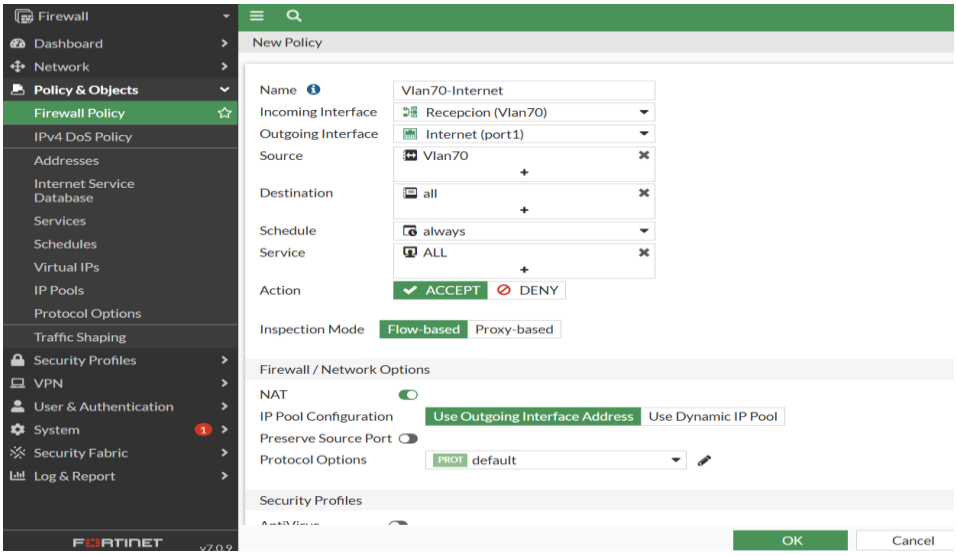

Figura 319. Política de Seguridad Vlan70-Internet

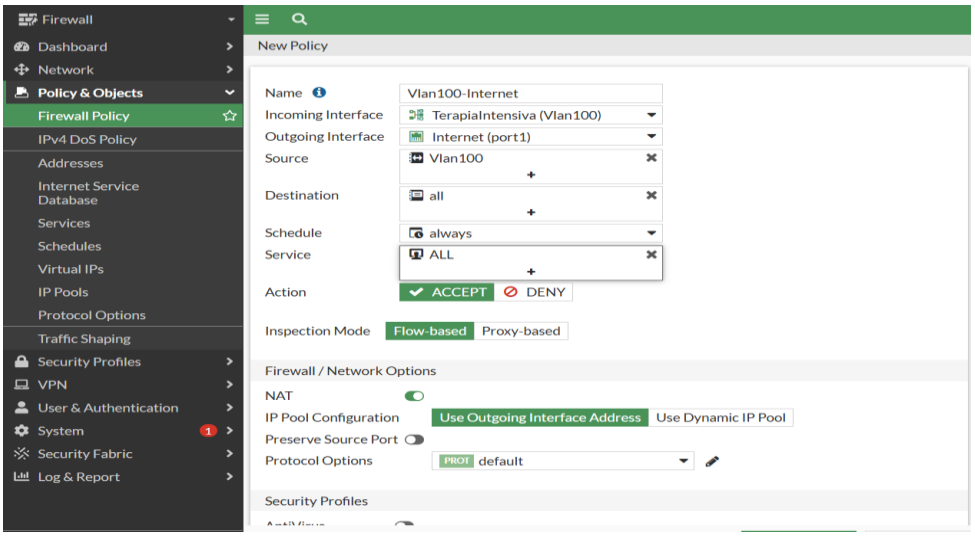

Figura 320. Política de Seguridad Vlan100-Internet

Aquí se configura una política que permite el tráfico entre la VLAN 70 y un sistema específico llamado Issabel. Esta política se utiliza para controlar el acceso entre una VLAN 150 Servidor.

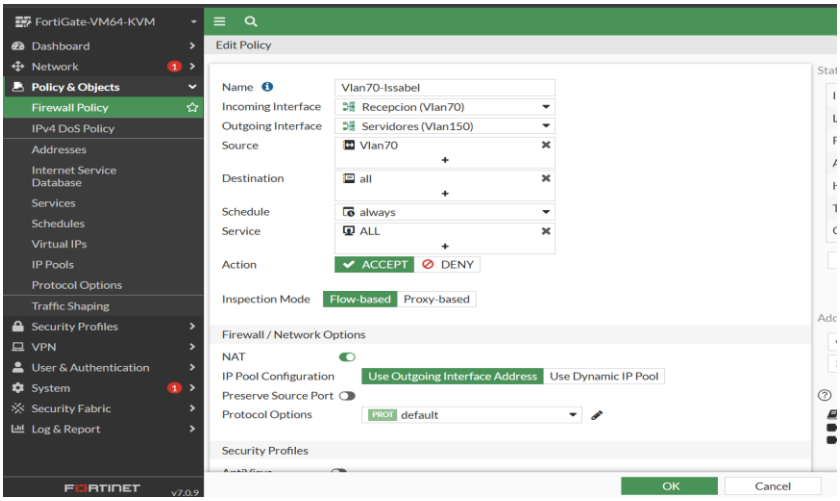

Figura 321. Politica de Seguridad Vlan70 a Issabel

Se muestra la configuración de un filtro web para bloquear el acceso a redes sociales como Facebook, YouTube y TikTok. Este filtro se aplica a una política de seguridad que controla el acceso a Internet y asegura que los usuarios no puedan acceder a estas plataformas.

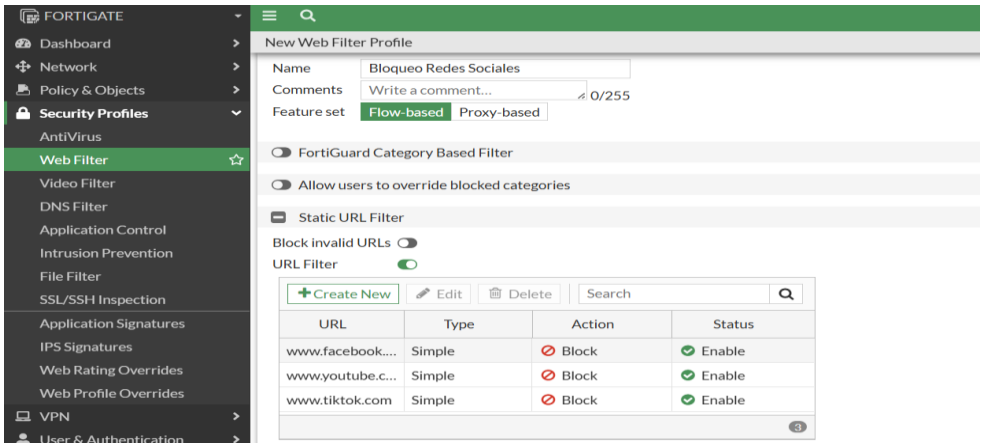

Figura 322. Bloqueo de redes sociales

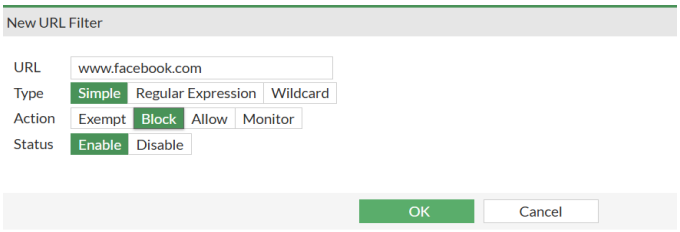

Figura 323. Bloqueo por URL

Aquí se configura el sensor de aplicaciones para bloquear ciertas aplicaciones en la red, como Redes Sociales, Juegos, y P2P. Esto se aplica a través de una política de seguridad que permite controlar el acceso a aplicaciones específicas.

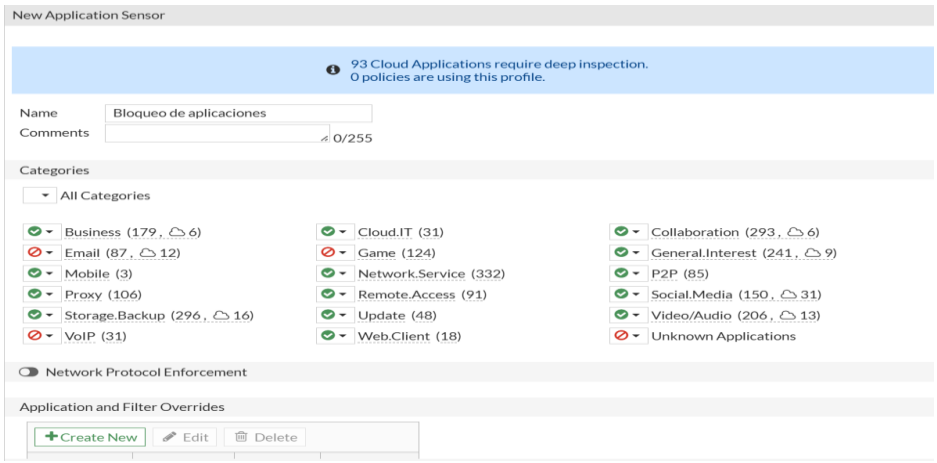

Figura 324. Bloqueo de Aplicaciones por el Fortinet

Finalmente, se muestra cómo añadir un filtro web a una política de seguridad. Este filtro permite bloquear el acceso a categorías específicas de sitios web (como redes sociales o aplicaciones de entretenimiento), proporcionando una capa adicional de control sobre el tráfico web.

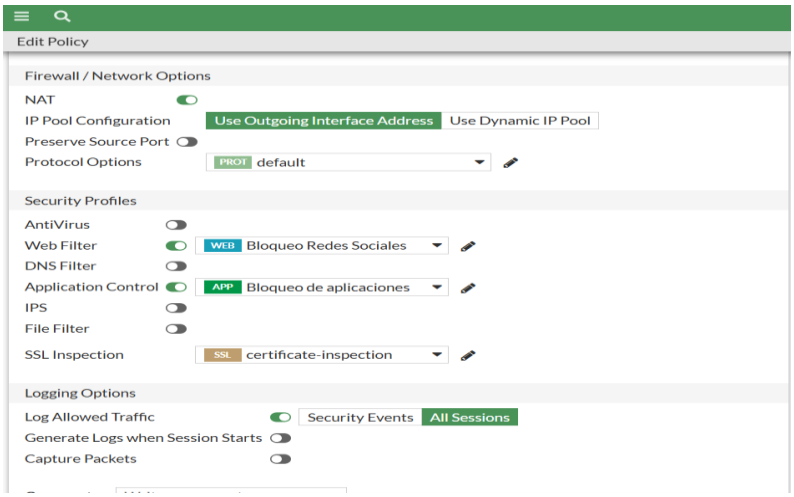

Figura 325. Añadir el filtro web

15. Configuración del Wifi

Se muestra la configuración del router donde la conexión a Internet está ajustada en modo DHCP automático, permitiendo que el dispositivo obtenga su dirección IP de forma dinámica. Esto garantiza que la red WiFi reciba parámetros de red sin configuración manual.

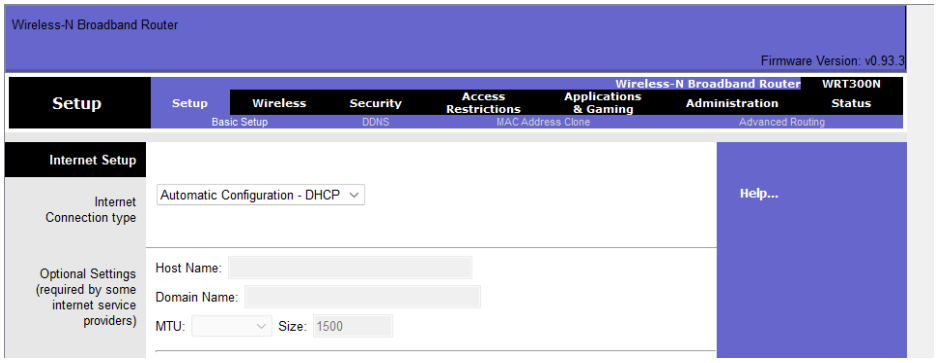

Figura 326. Configuramos la Conexión DHCP de la VLAN para la Red Wifi

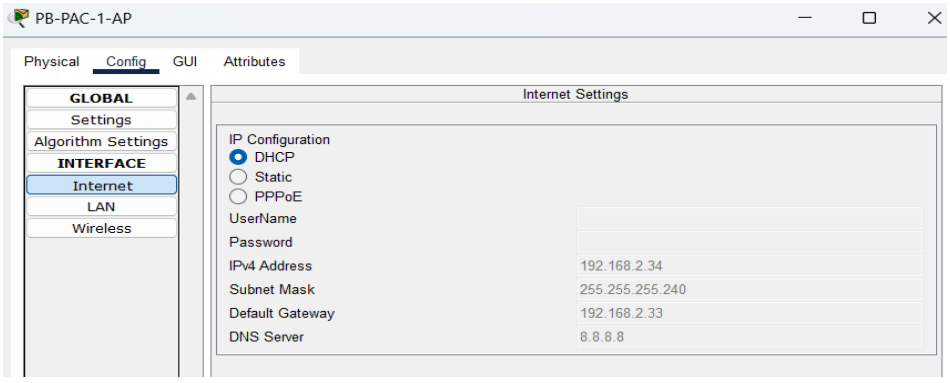

Figura 327. Verificamos que nos esté Accediendo Dinámicamente a la Red VLAN 20 de Wifi

Se configura el servidor DHCP que asignará direcciones IP automáticamente a los usuarios de la

red WiFi. Se define el rango de direcciones 10.10.0.1 - 10.10.0.50, así como la máscara y la cantidad máxima de clientes que podrán recibir servicio.

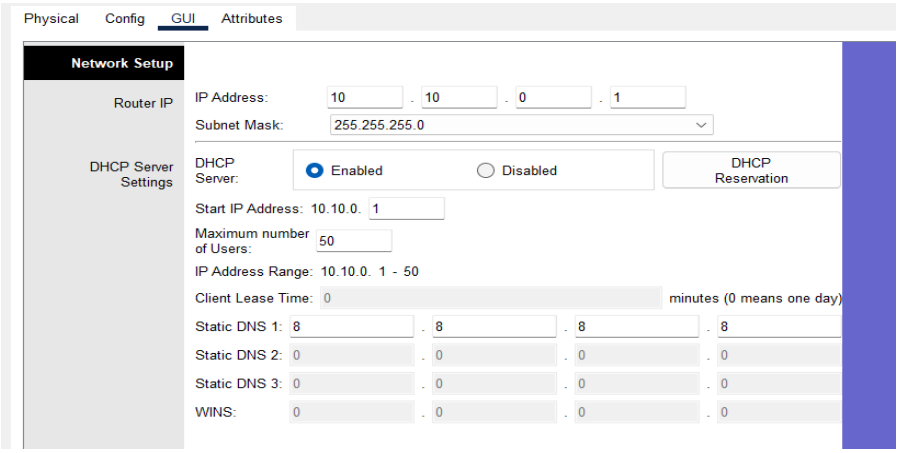

Figura 328. Configuramos la Red del DHCP que Repartiremos a los Usuarios

Se confirma que la interfaz LAN del punto de acceso está configurada correctamente con la dirección 10.10.0.1 y su respectiva máscara de subred. Esto asegura que el AP pueda administrar la red local y repartir DHCP según lo establecido.

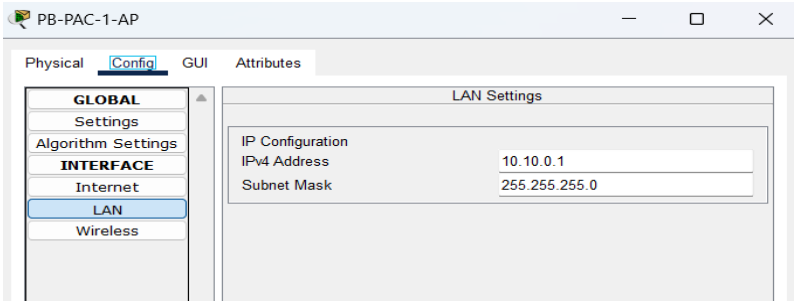

Figura 329. Verificamos la Configuración LAN

Se asigna el nombre **PacientesPB** a la red inalámbrica, permitiendo que los usuarios identifiquen el SSID al momento de conectarse. También se mantiene la emisión del SSID habilitada para que la red sea visible.

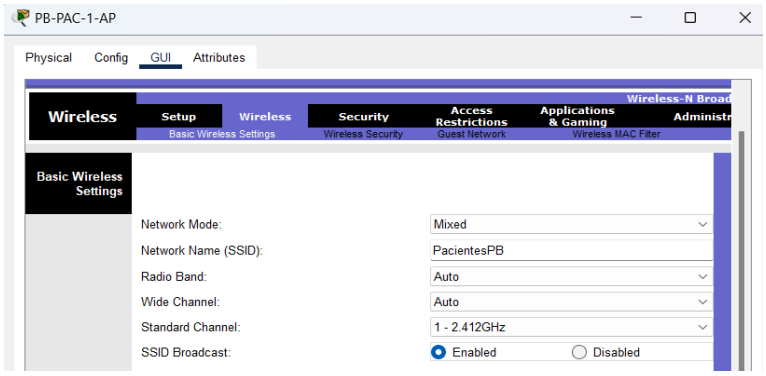

Figura 330. Configuramos el Nombre al Wifi (SSID) en este caso PacientesPB

Se establece el modo de operación en **Mixed**, permitiendo compatibilidad con diferentes estándares WiFi (b/g/n). Esto garantiza que dispositivos antiguos y nuevos puedan conectarse sin problemas a la red.

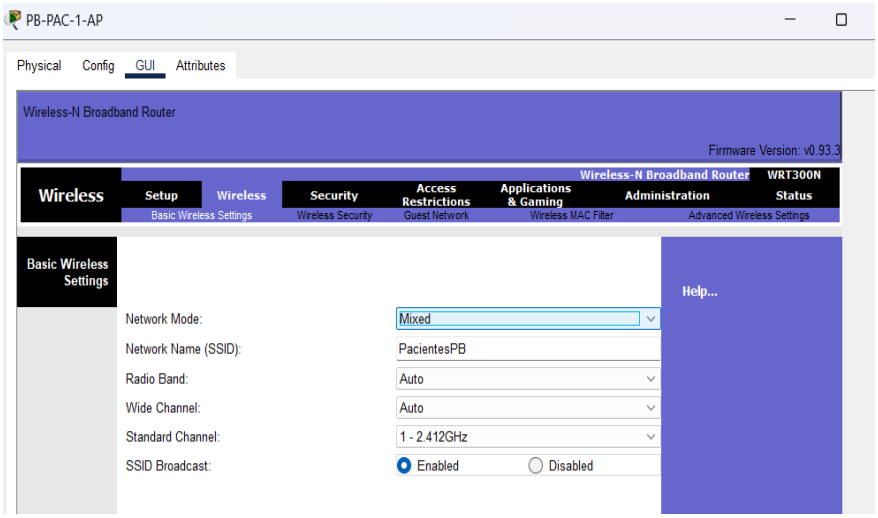

Figura 331. La configuración Network Mode la Mantenemos en Mixed

Se mantiene la opción **Radio Band** en Auto, permitiendo que el punto de acceso seleccione automáticamente la banda adecuada (2.4 GHz o 5 GHz) según el entorno y los dispositivos conectados, optimizando así el rendimiento inalámbrico.

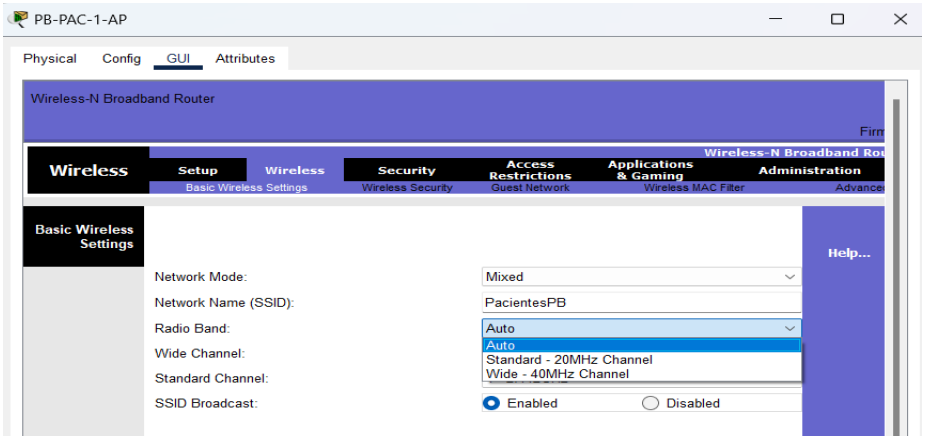

Figura 332. La configuración Radio Band la Mantenemos en Auto

La opción **Wide Channel** también se deja en Auto, permitiendo que el AP elija automáticamente el ancho de canal más eficiente (20 MHz o 40 MHz). Esto mejora la estabilidad y evita interferencias con otras redes cercanas.

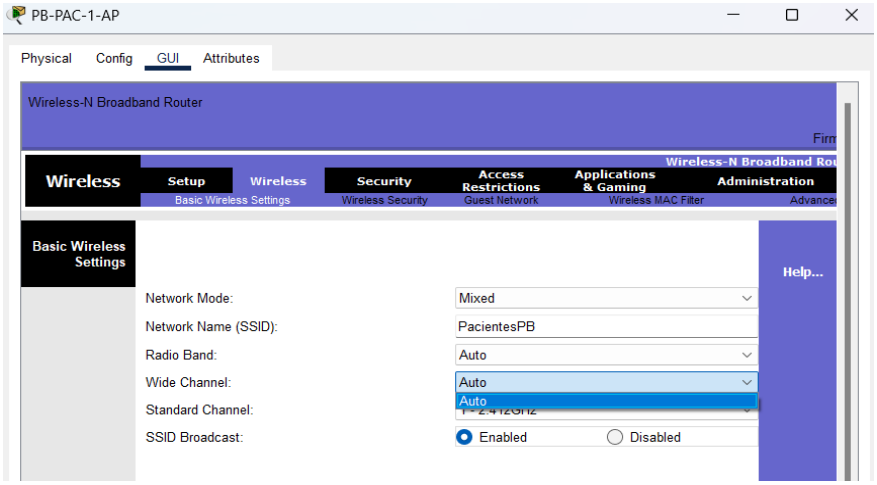

Figura 333. La Configuración Wide Channel la Mantenemos en Auto

Se selecciona el canal **1 (2.412 GHz)** para la red WiFi, una opción común que reduce interferencias y mejora la estabilidad, especialmente en entornos con múltiples redes inalámbricas.

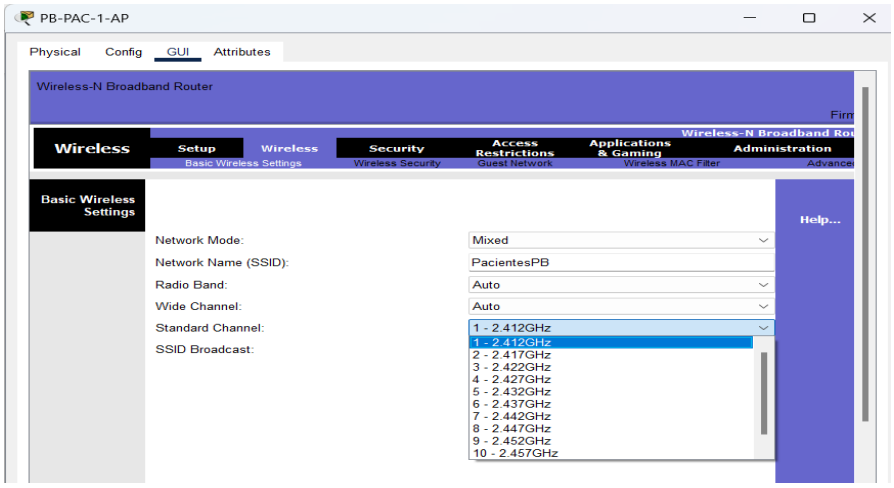

Figura 334. La configuración Standard Chanel la Mantenemos en el 1 - 2.412 GHz

El parámetro **SSID Broadcast** se mantiene en Enabled, lo que permite que el nombre de la red (SSID) sea visible para los usuarios y pueda ser detectado fácilmente por sus dispositivos.

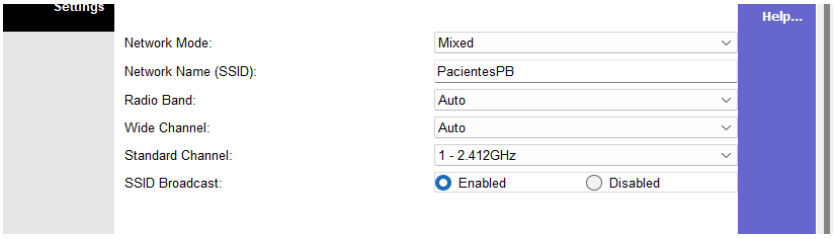

Figura 335. La configuración SSID Broadcast la Mantenemos en Enabled

Se establece una contraseña para la red WiFi utilizando el modo de seguridad **WPA2 Personal** (el simulador solo soporta hasta WPA2). Esto garantiza una conexión protegida mediante autenticación

segura para los usuarios.

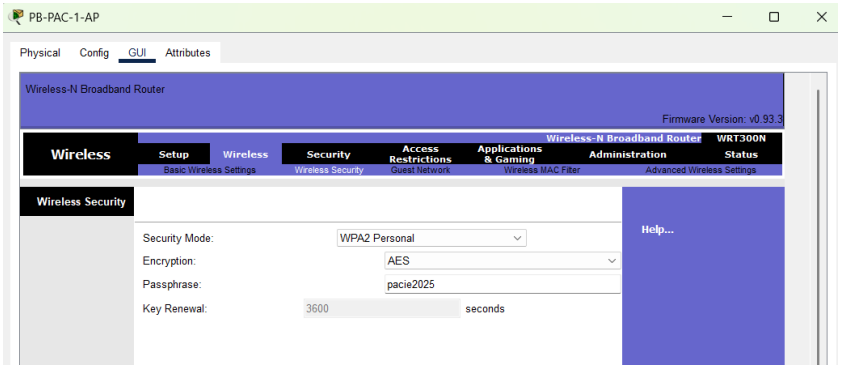

Figura 336. Configuramos una Contraseña con la seguridad de WPA3 Personal en este caso pacie123 (en este caso el simulador cuenta hasta WPA2)

La encriptación se configura en **AES**, el estándar más seguro y recomendado para redes inalámbricas. Esto ofrece mayor protección frente a ataques y asegura que los datos transmitidos por WiFi viajen cifrados correctamente.

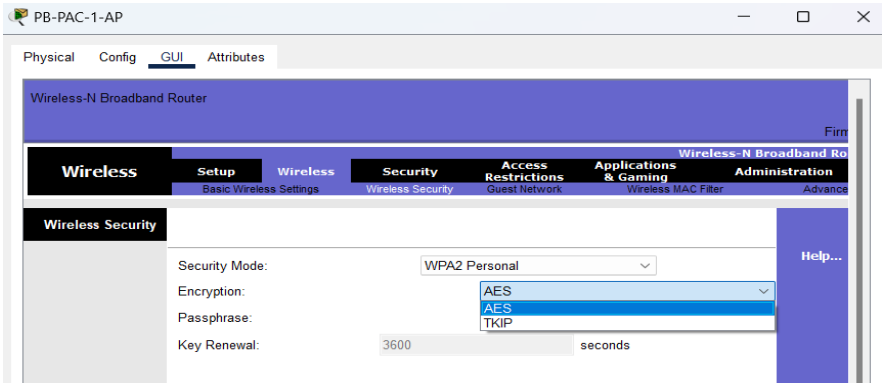

Figura 337. Configuramos la encriptación en AES

Se verifica la configuración inalámbrica aplicada, confirmando que el SSID, canal, autenticación y cifrado coinciden con los parámetros definidos. Esto asegura que la red WiFi esté funcionando correctamente según las especificaciones del diseño de red.

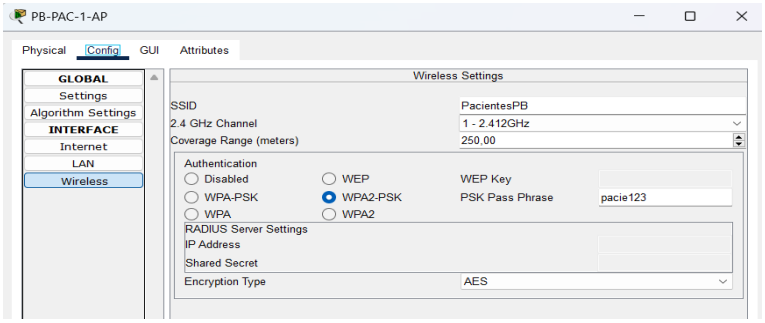

Figura 338. Verificamos la configuración asignada

Se muestra las contraseñas asignadas a cada punto de acceso (AP) según la planta y el tipo de

usuario Médicos o Pacientes. Cada planta cuenta con una clave distinta para mejorar la seguridad, evitar accesos no autorizados y facilitar la gestión por segmentos, permitiendo controlar quién se conecta y desde dónde. Esta separación también ayuda a identificar y administrar mejor el tráfico de cada área dentro de la clínica.

Switch por plantas	**Contraseñas**
MédicosPB	medic2025
MédicosP1	medicP12025
MédicosP2	medicP22025
MédicosP3	medicP32025
PacientesPB	pacie2025
PacientesP1	pacieP12025
PacientesP2	pacieP22025
PacientesP3	pacieP32025

Tabla 144. Configuración de las contraseñas de los Access Point de la Clinica

16. Autentificación de la red wifi

Se observa el proceso de autenticación del dispositivo inalámbrico para ingresar a la red WiFi. El usuario selecciona el SSID correspondiente e introduce la contraseña configurada bajo el método de seguridad WPA2-PSK (WPA3 limitado por packet tracer). Las credenciales utilizadas están autorizadas únicamente para el personal de salud, ya que pertenecen a la VLAN 30, la cual es una red privada destinada exclusivamente a personal autorizado. De esta manera, solo dispositivos validados pueden acceder a los recursos internos definidos para esta VLAN.

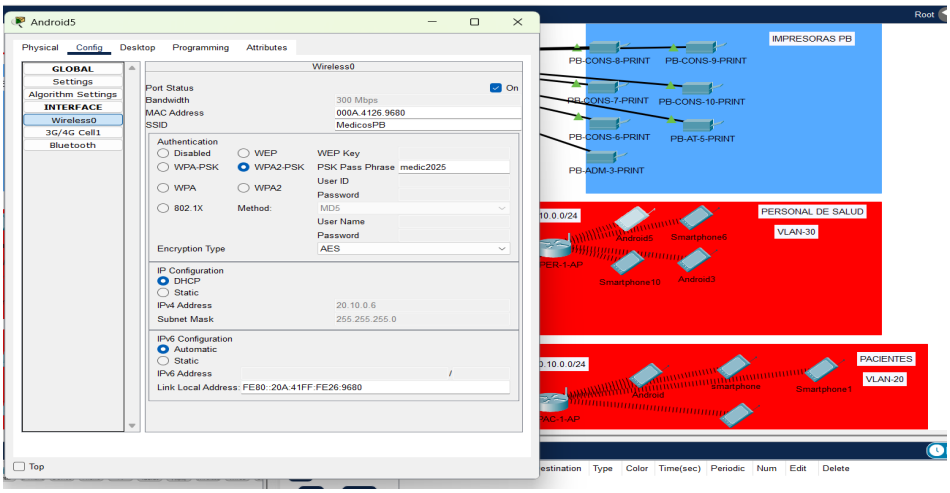

Figura 339. Autentificar dispositivo

Aquí se configura el Access Point donde se definen los parámetros de autenticación de la red WiFi, como el SSID, el tipo de seguridad (WPA2/WPA2-PSK), el cifrado AES y la clave de acceso. La contraseña asignada está limitada únicamente al personal de salud, perteneciente a la VLAN 30, que es una red privada y restringida. Por otro lado, la VLAN 20 es configurada como una red pública, destinada a los pacientes, con credenciales distintas y acceso limitado para mayor seguridad.

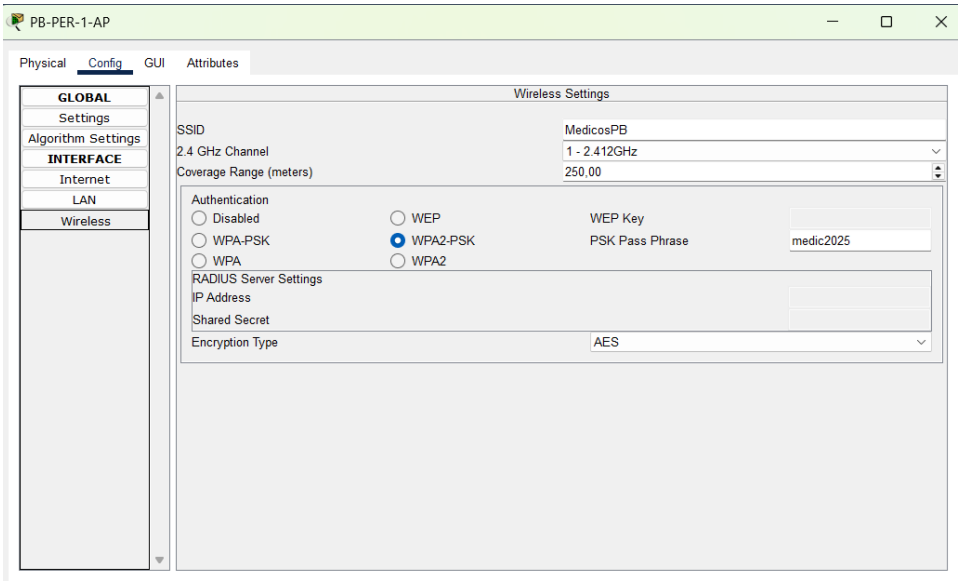

Figura 340. Access Poit a cual conectarse

17. Instalación de Issabel

Figura 341. Una vez Cargada la Imagen ISO Colocamos Test this media & install

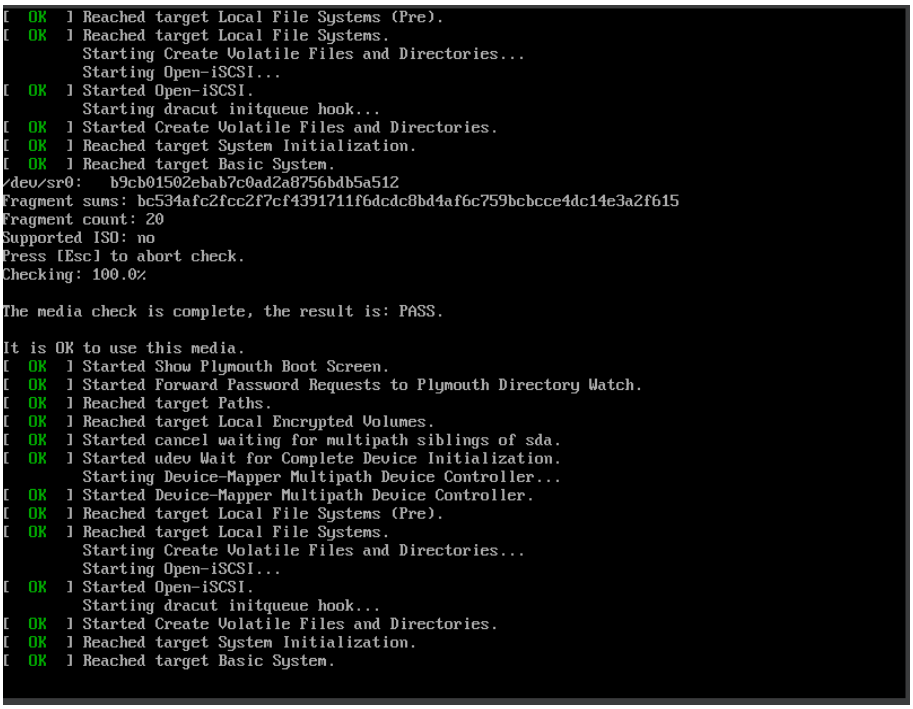

Figura 342. Esperamos la instalación

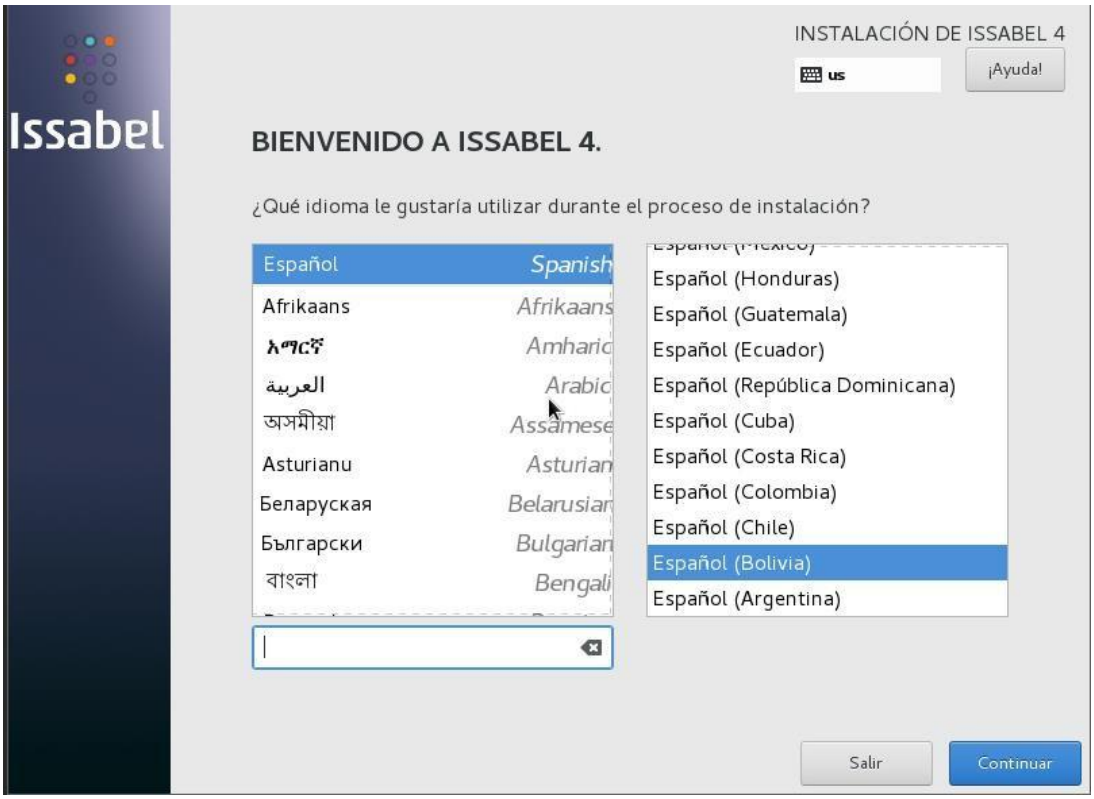

Figura 343. Seleccionamos el Idioma Español

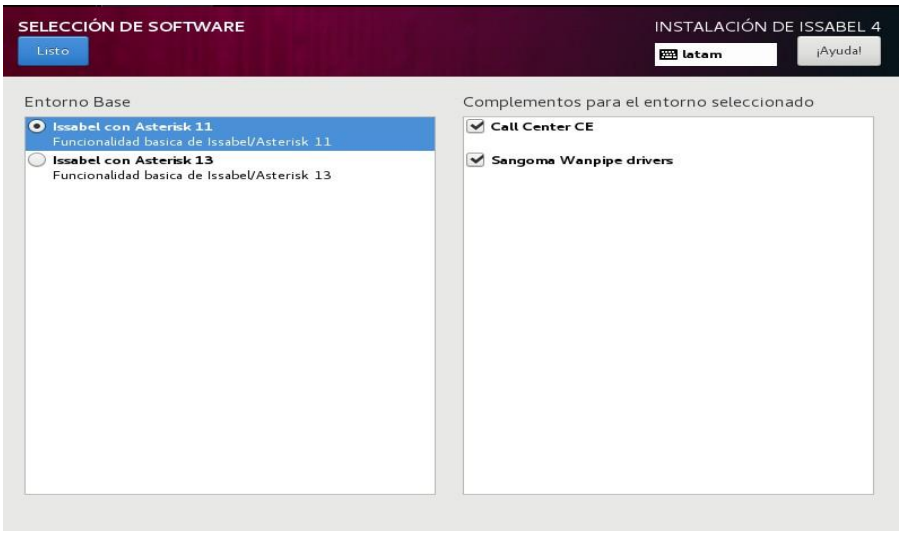

Figura 344. Seleccionamos el Software de Asterisk 11

Figura 345. Colocamos una Contraseña Root

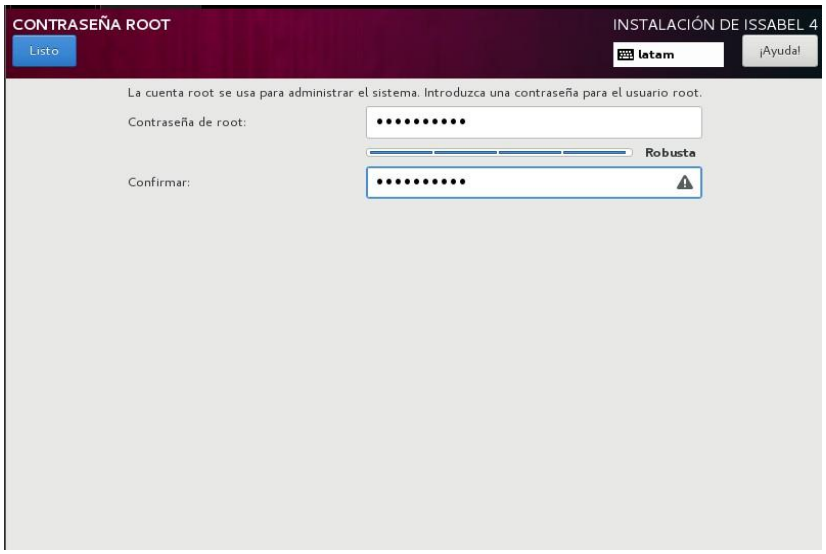

Figura 346. Colocamos una Contraseña Administrativa Root 12623385c

Figura 347. Continua la Instalación

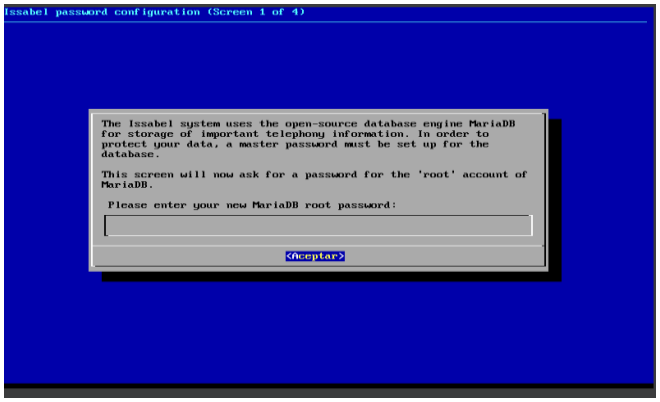

Figura 348. Luego de Instalar Pedirá que Coloquen la Contraseña de Root de la base de datos 12623385c

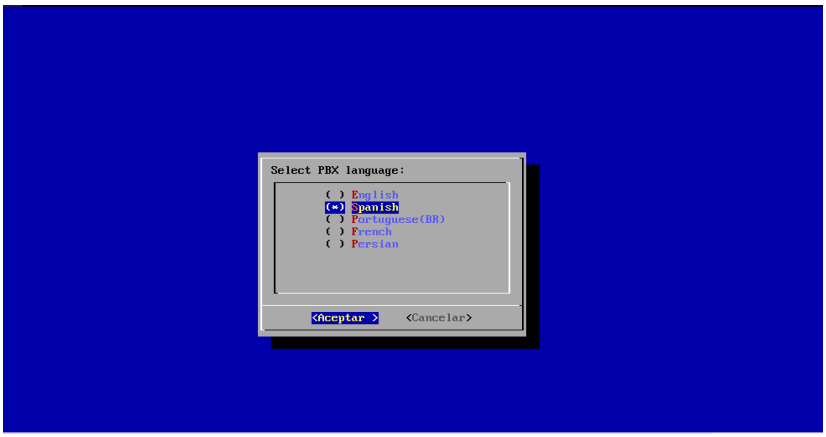

Figura 349. Seleccionamos el Idioma Español

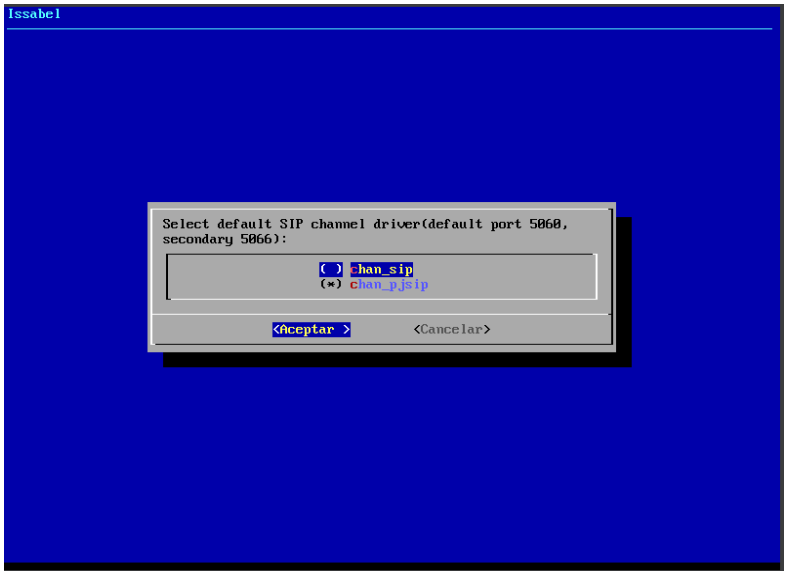

Figura 350. Selecciona el tipo de SIP Chanel chan_pjsip

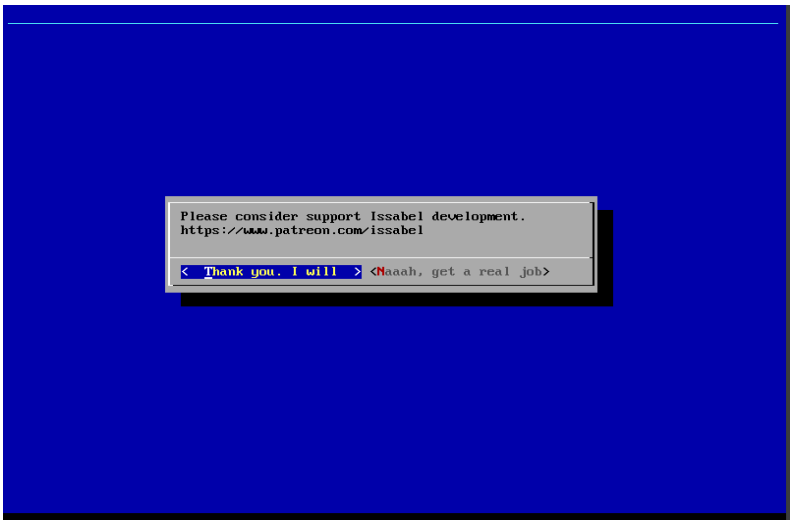

Figura 351. Desea Acceder a su Página Oficial

Figura 352. Iniciamos Sesión login: root password: 12623385c

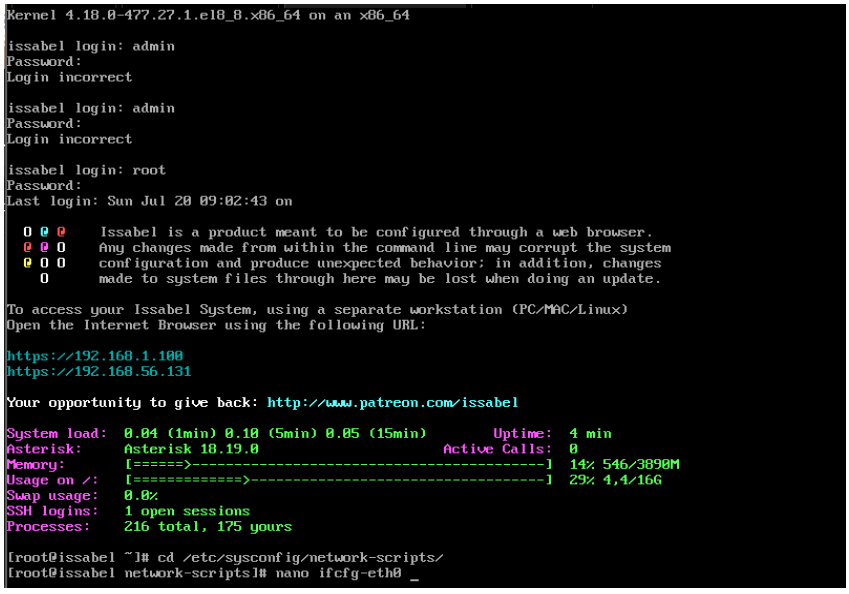

Figura 353. Dirección IP tipo Estático

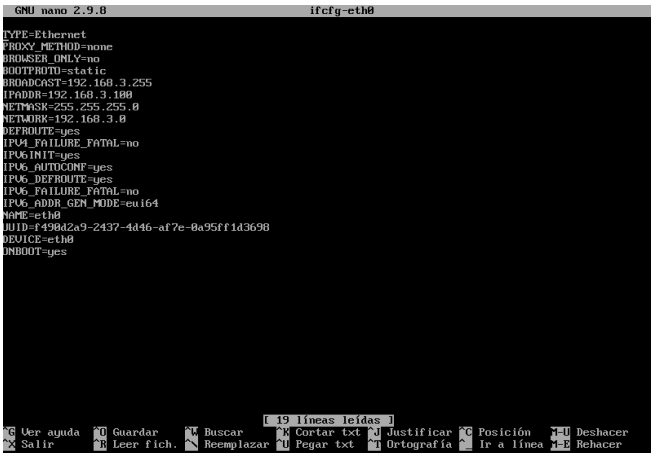

Figura 354. Configuramos la IP 192.168.3.100 para el servidor Asterisk

```
[root@issabel network-scripts]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.3.100  netmask 255.255.255.0  broadcast 192.168.3.255
        inet6 fe80::20c:29ff:fe7c:37e3  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:7c:37:e3  txqueuelen 1000  (Ethernet)
        RX packets 102  bytes 35110 (34.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 117  bytes 47406 (46.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 6210  bytes 475707 (464.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6210  bytes 475707 (464.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@issabel network-scripts]# _
```

Figura 355. Verificar el cambio de IP

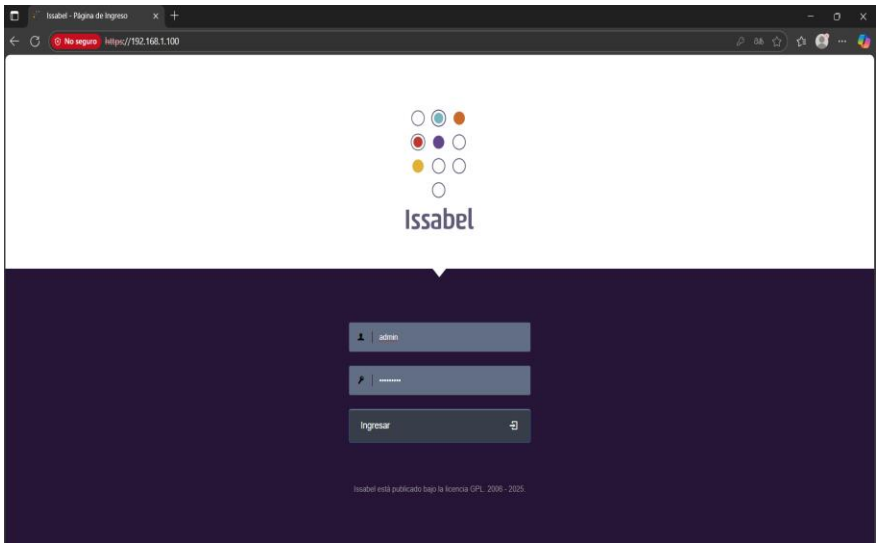

Figura 356. Inicio de Sesión por Interfaz ingresando la IP 192.168.3.100

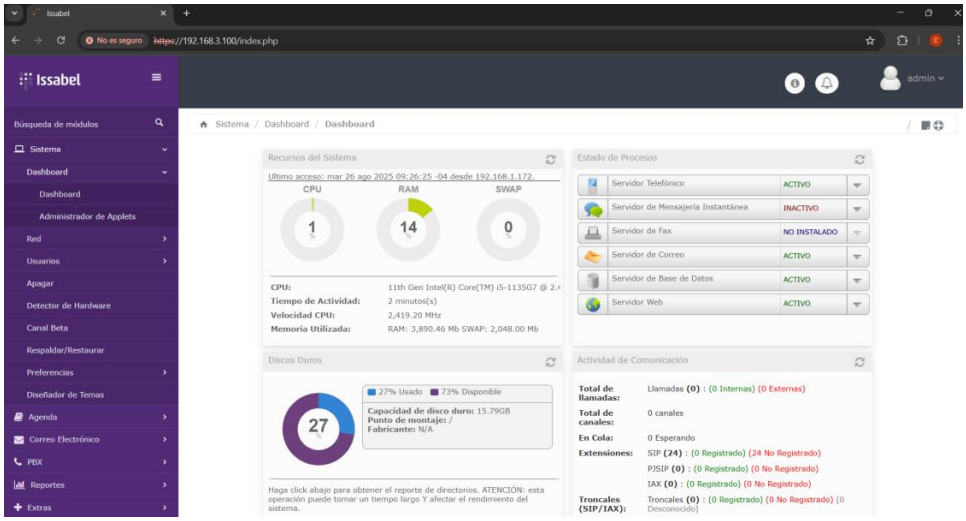

Figura 357. Iniciamos Sesión con Nombre de Usuario: admin contraseña: 12623385c

18. Añadir una extensión(numero) al servidor

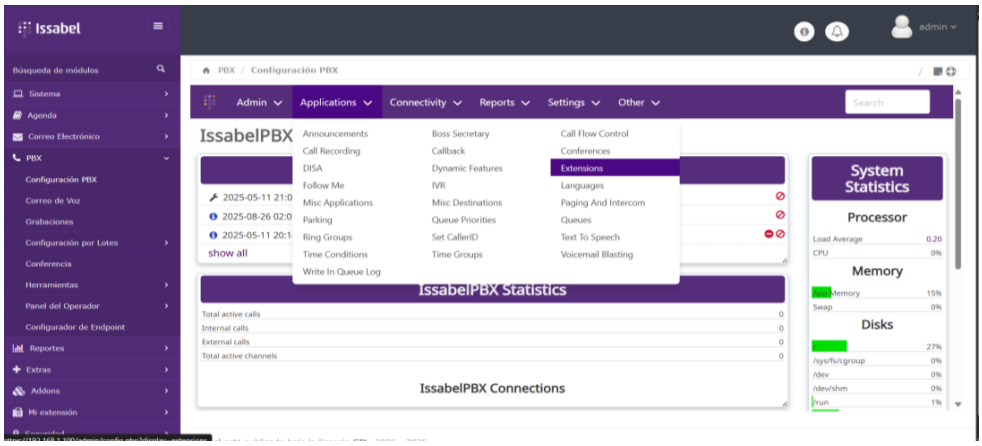

Figura 358. Entramos a PBX -> Configuración PBX, Dejamos por Defecto SIP y Damos Enviar

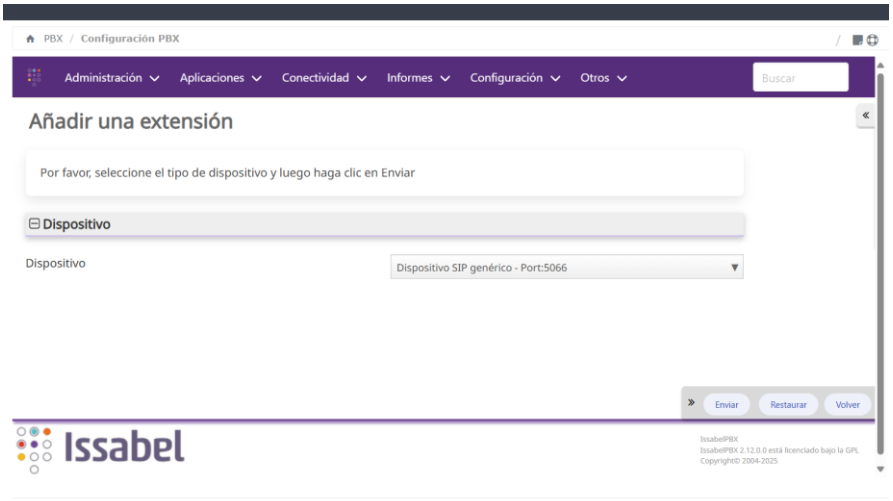

Figura 359. Protocolo de inicio de sesión SIP

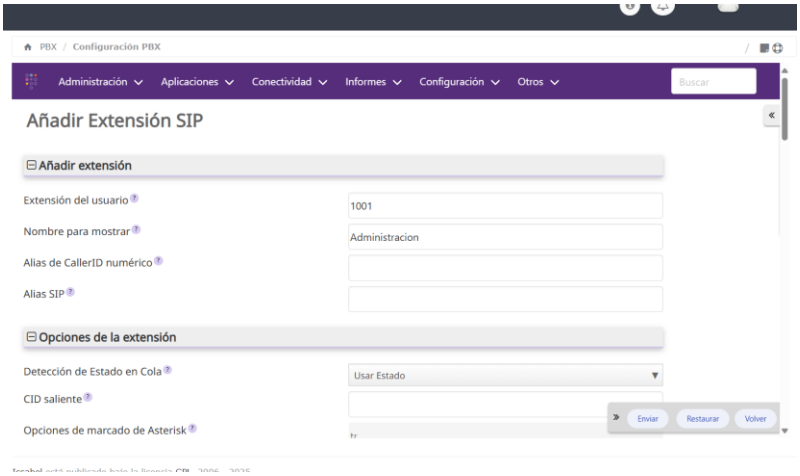

Figura 360. Llenamos los datos Extensión de Usuario: 1001 Nombre para mostrar: Administración

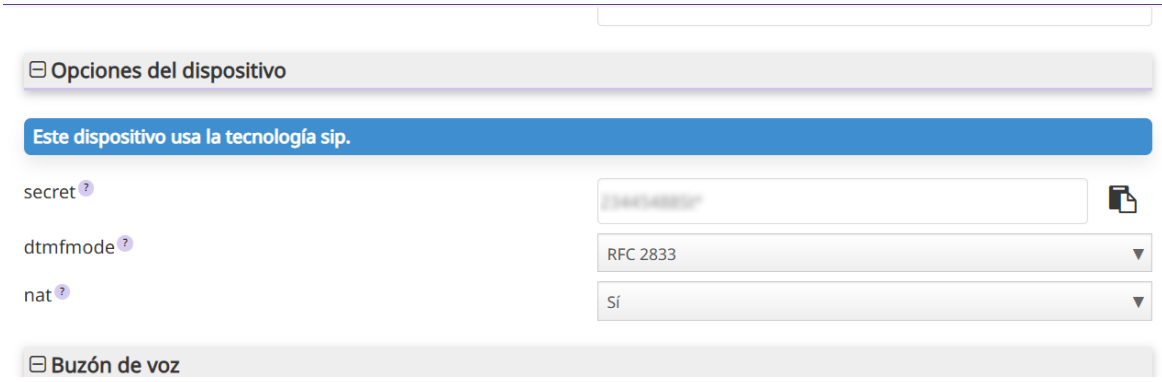

Figura 361. Contraseña con la cual iniciará sesión para los dispositivos

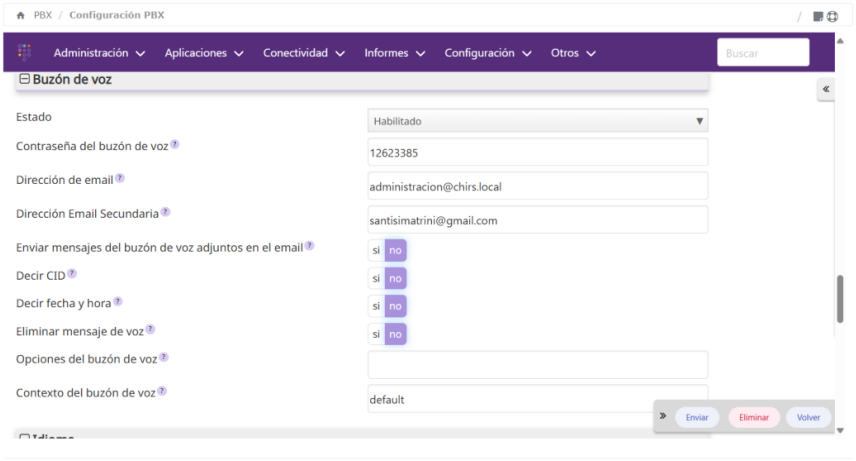

Figura 362. Habilitamos el Buzón de Voz para poder escuchar los mensajes de voz guardados

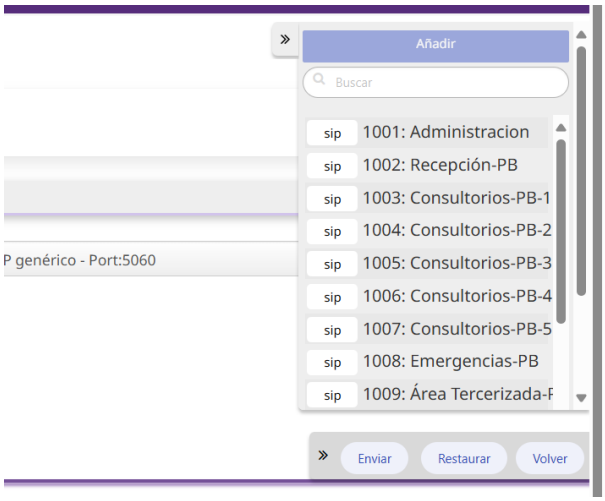

Figura 363. Verificamos las Extensiones Creadas

19. Instalación de video llamadas

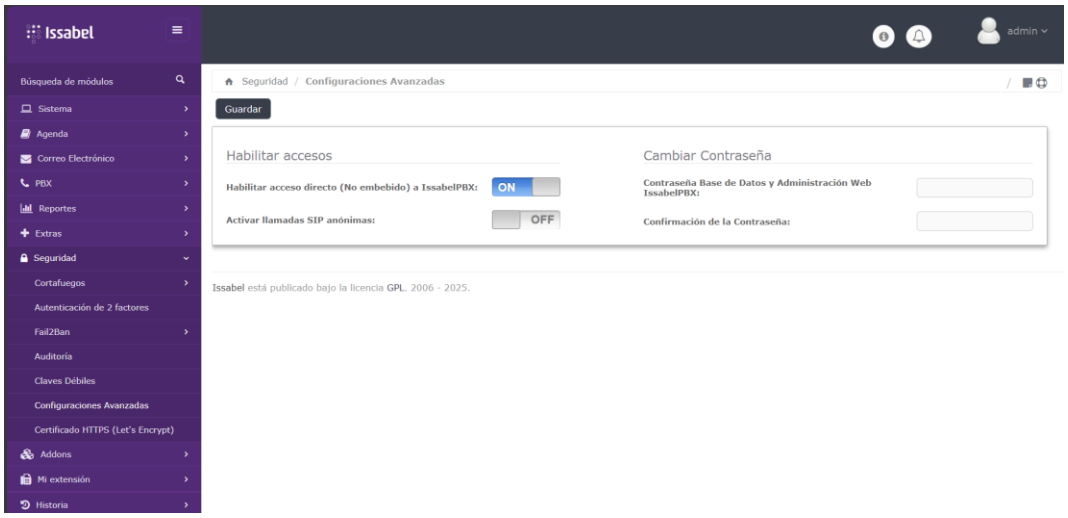

Figura 364. Entramos a Seguridad y Después Configuraciones Avanzadas

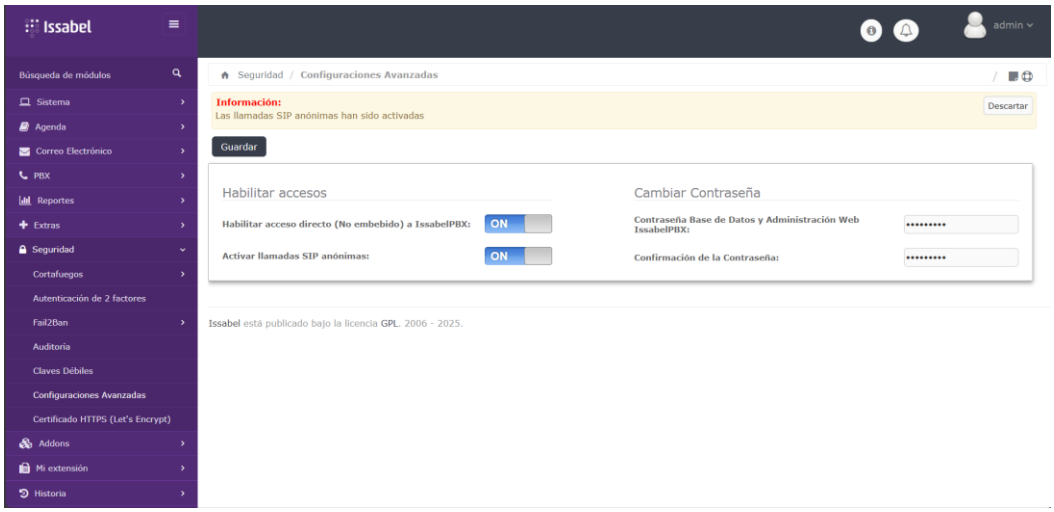

Figura 365. Activamos el Acceso Directo no Integrado e Insertamos la Contraseña: HRSJDD2024 para Guardar Cambios

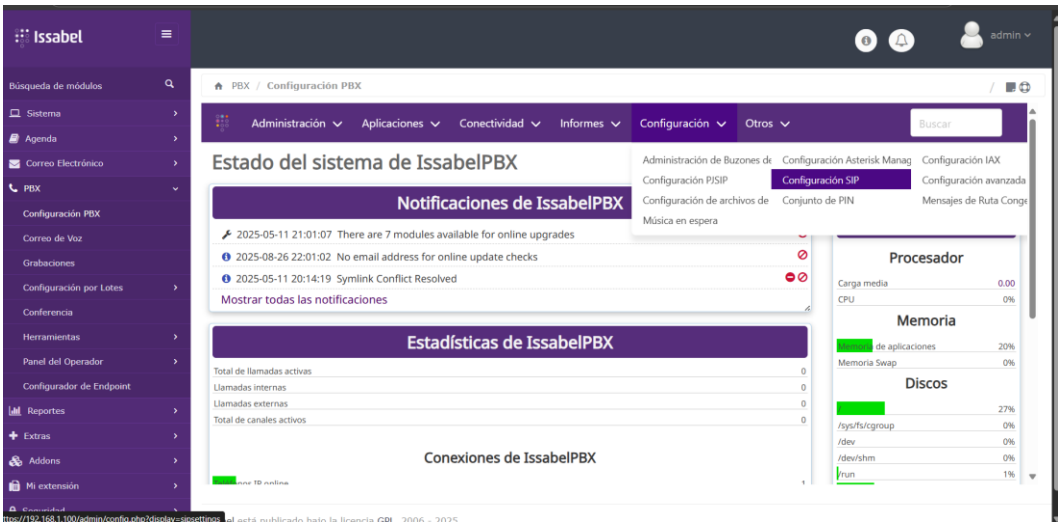

Figura 366. Volvemos a PBX>Configuración PBX>Configuración SIP

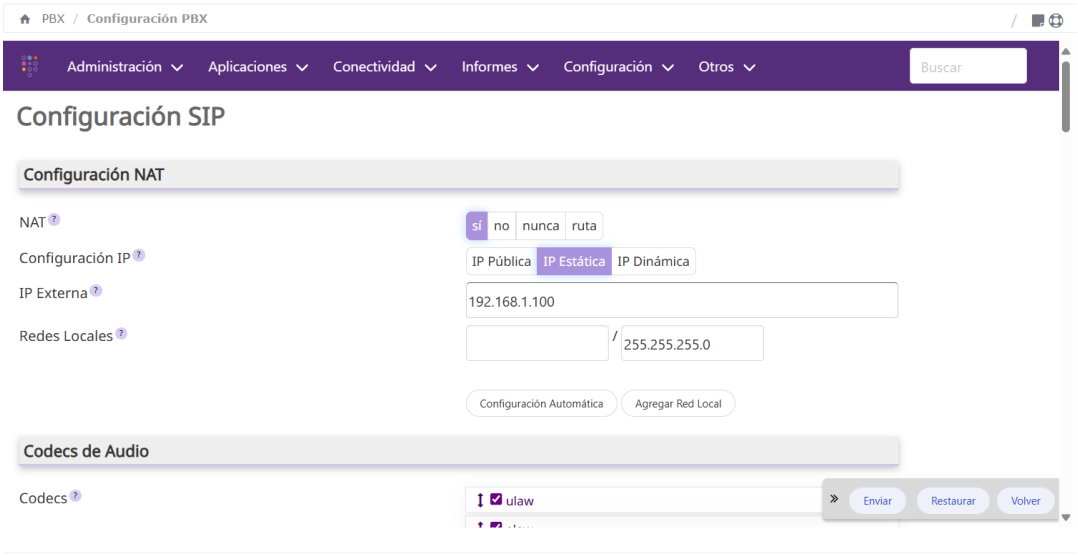

Figura 367. En este apartado añadimos la IP del servidor 192.168.3.100

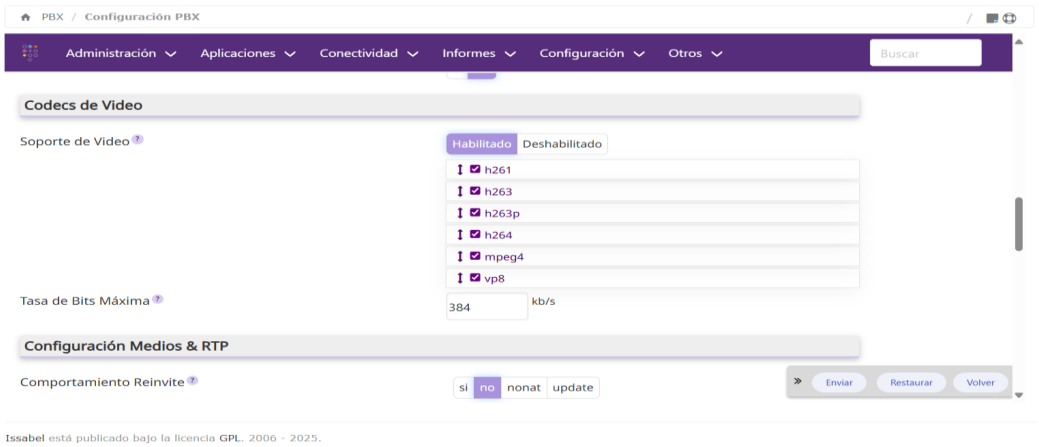

Figura 368. Video Suport lo Activamos y Seleccionamos Todos los Formatos de Video

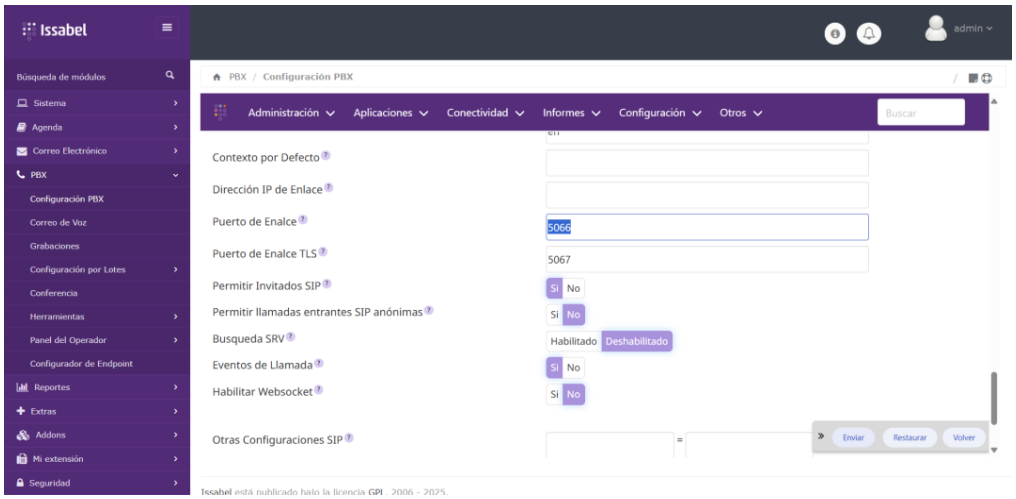

Figura 369. Verificamos el puerto 5066 y presionamos Enviar

20. Colas de llamadas

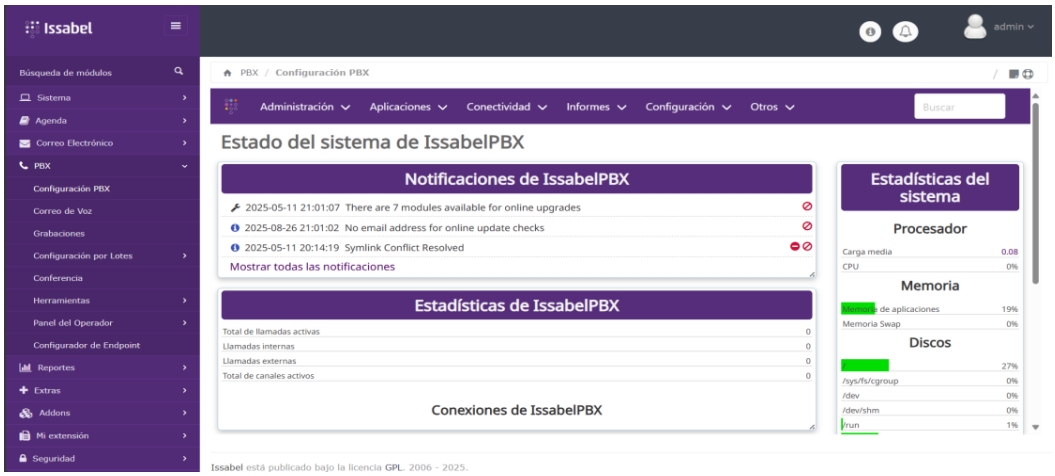

Figura 370. Entramos a PBX -> Configuración PBX

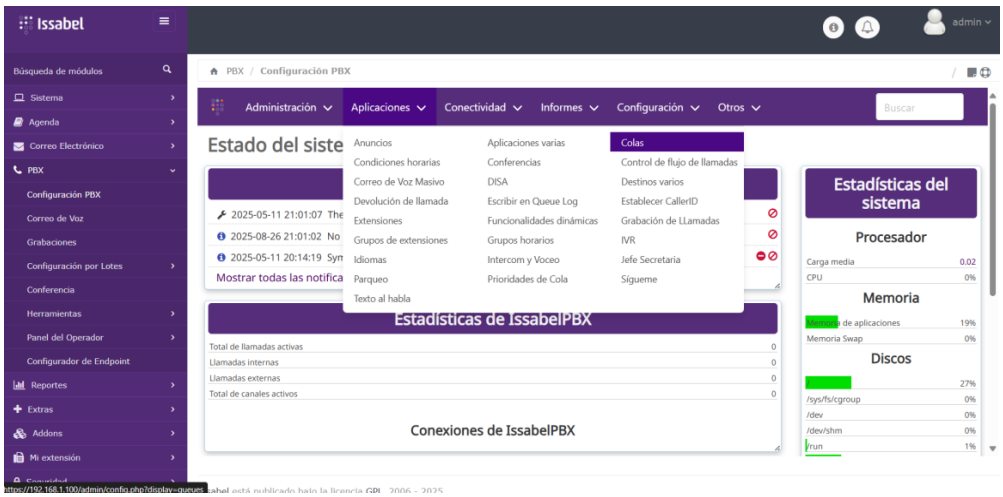

Figura 371. Entramos a Colas

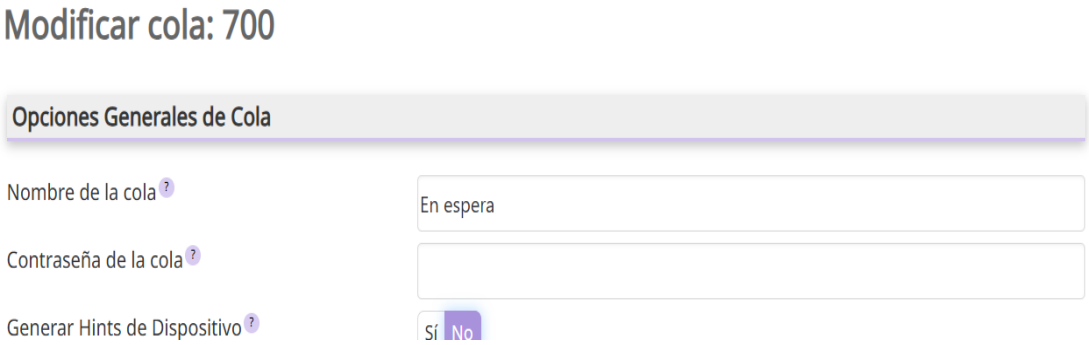

Figura 372. Creamos el grupo y el número de cola

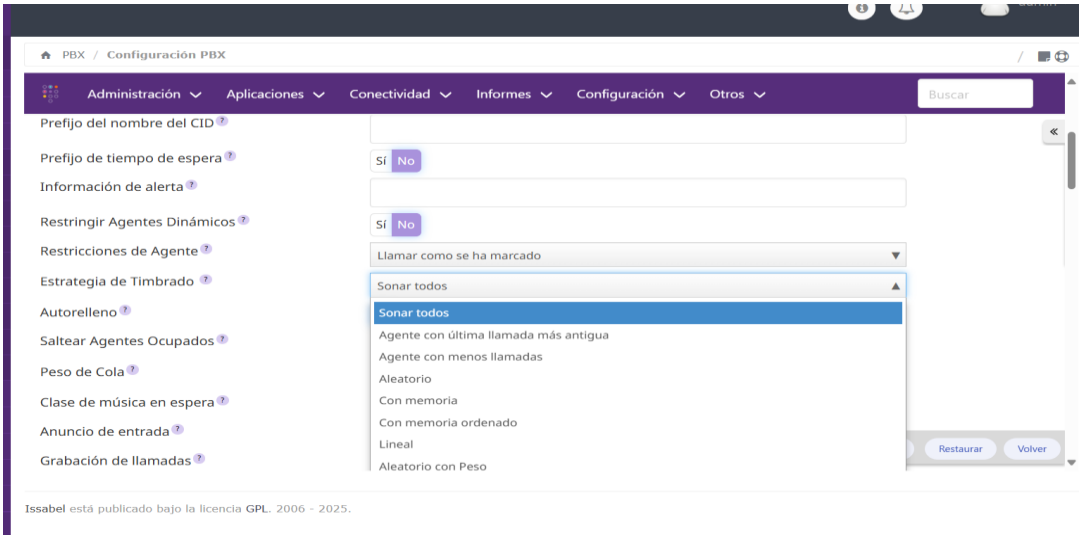

Figura 373. En estrategia de timbrado sonar todos

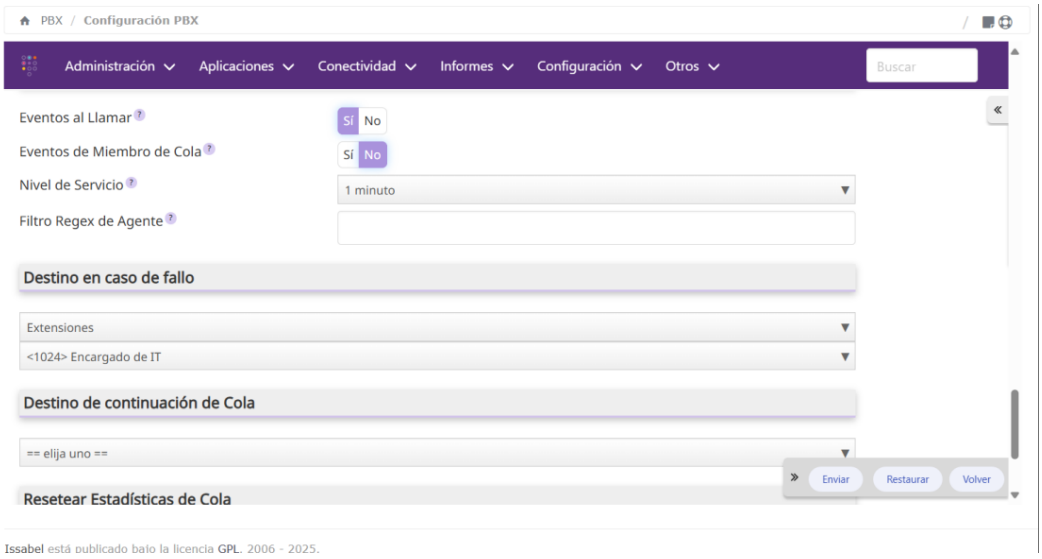

Figura 374. En caso de fallos

21. Grabacion de llamadas

Figura 375. Entramos a Grabaciones

Figura 376. Se encuentra registrado todas las grabaciones de llamadas a las diferentes extensions

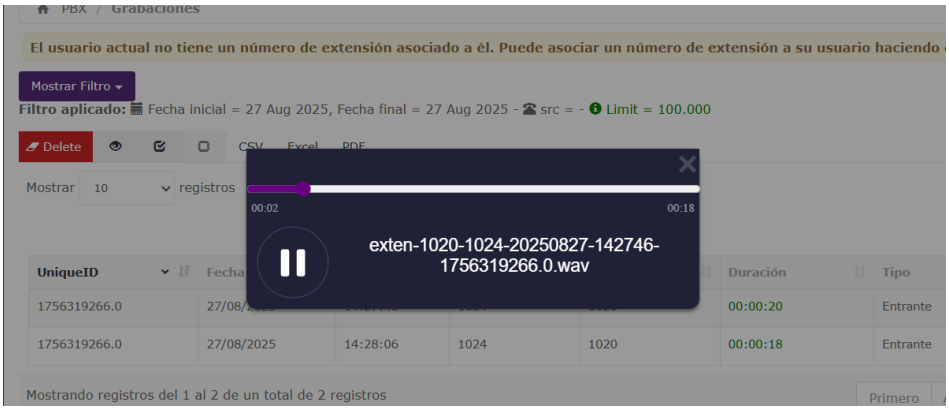

Figura 377. Escuchando la grabación

22. Buzón de voz

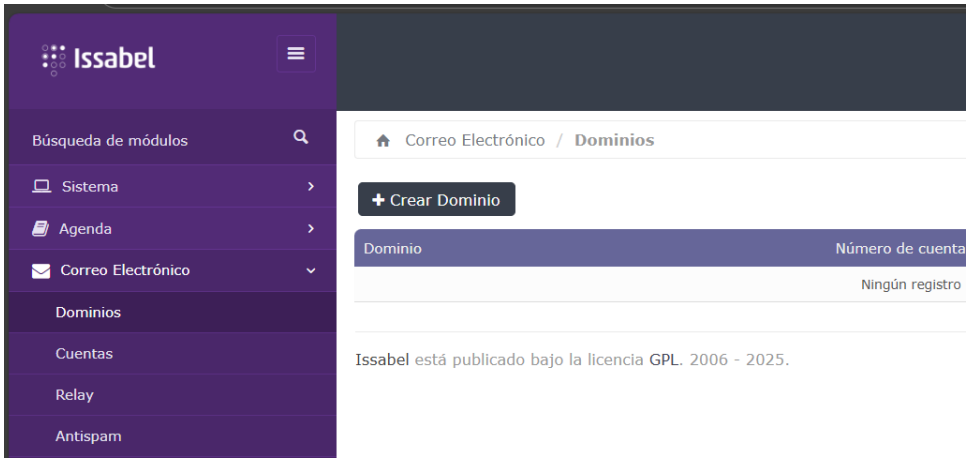

Figura 378. Nos dirigimos hacia Correo Electronico -> Dominios

Figura 379. Creamos el Dominio como "santisimatrinidad.local"

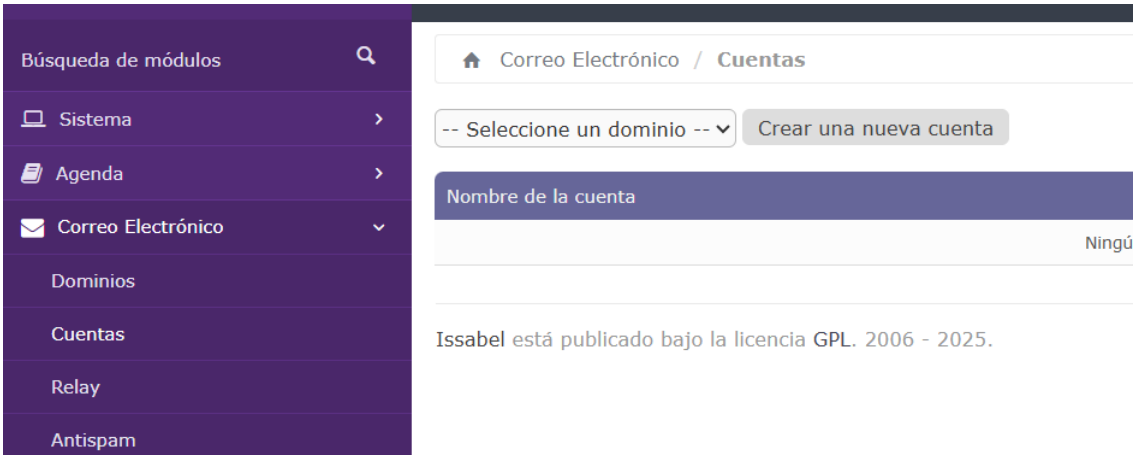

Figura 380. Nos dirigimos a cuentas

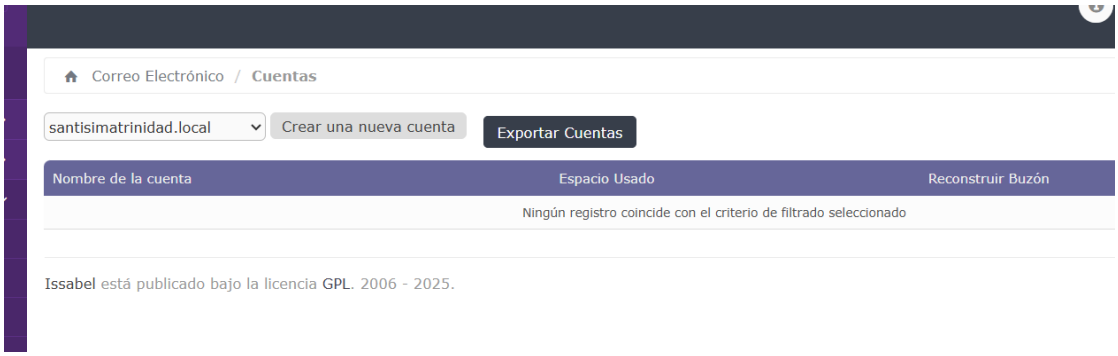

Figura 381. Seleccionamos el Dominio y creamos una nueva cuenta

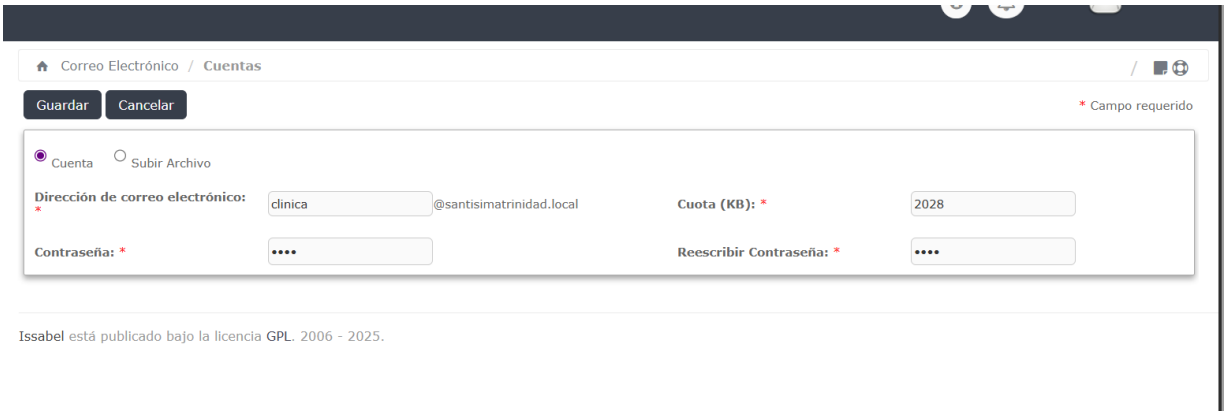

Figura 382. Seleccionamos el Dominio y Creamos una Cuenta

clinica@santisimatrinidad.local Contraseña: 6545

Cuota (KB): * 2028 Guardamos

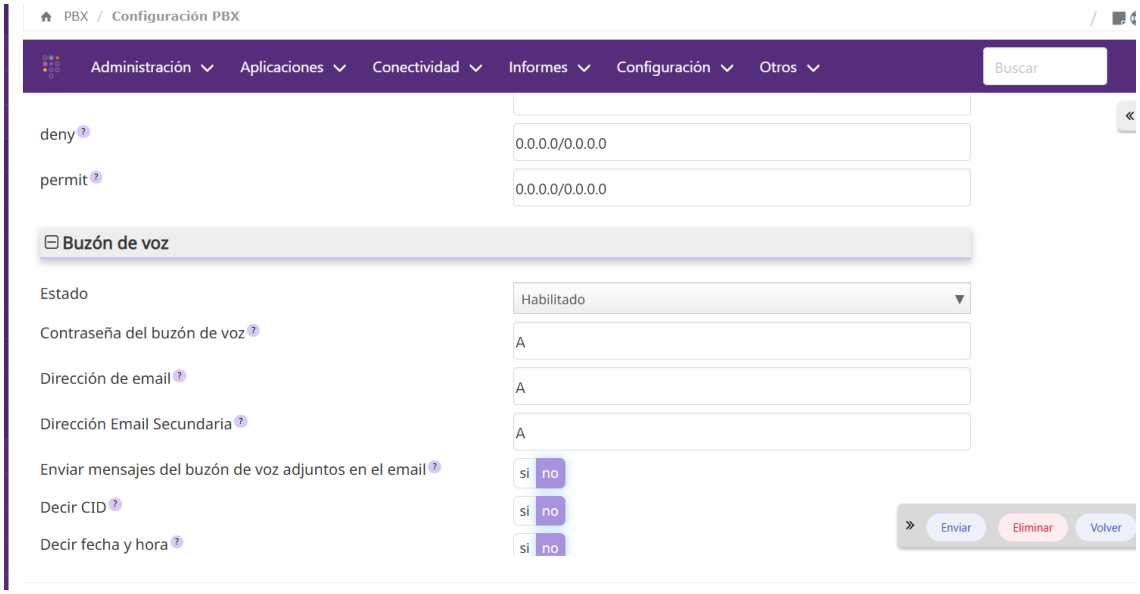

Figura 383. Volvemos al apartado de buzón de voz en dichas extensiones

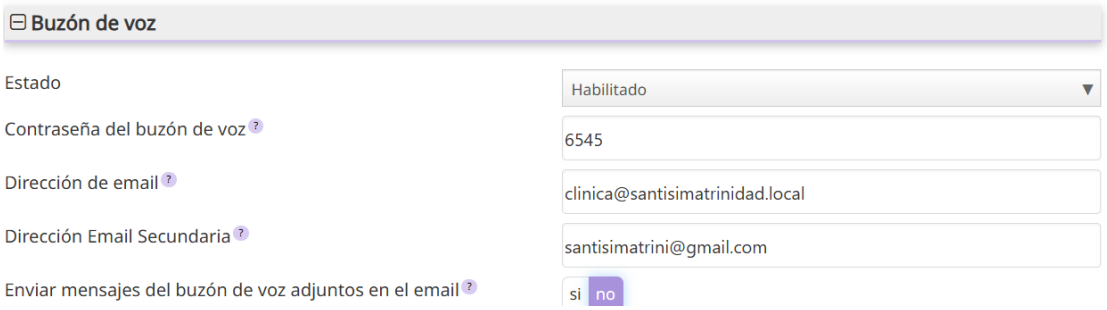

Figura 384. Habilitamos y empezamos a añadir dichas direcciones

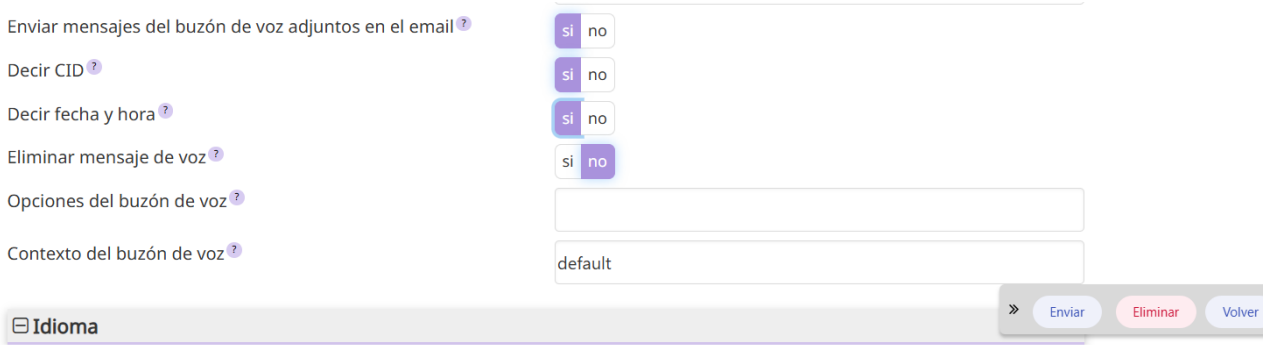

Figura 385. Enviar Mensajes del Buzón de Voz Adjuntos en el Email: yes, Decir CID: yes, Decir Fecha y Hora: yes y Enviar

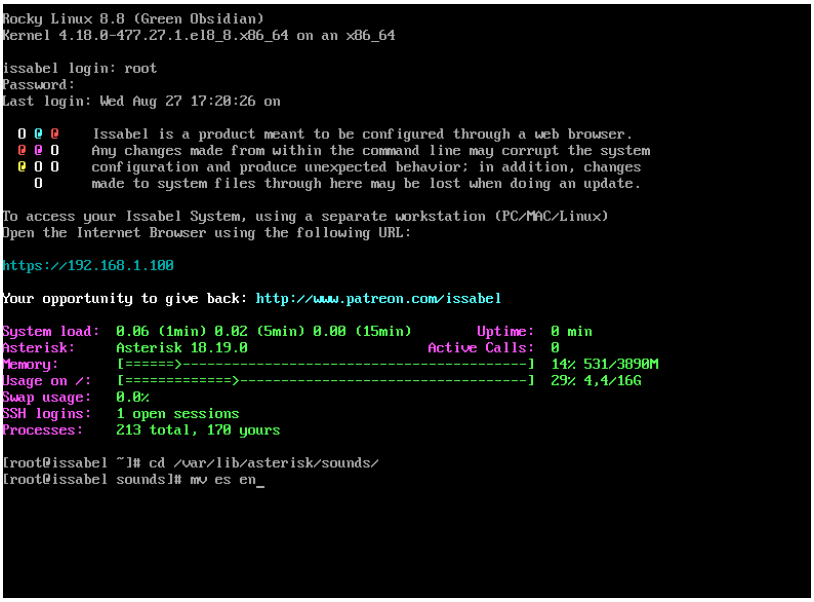

Figura 386. Configuramos para cambiar al operador a español

23. Configuración dispositivo móvil con el servidor

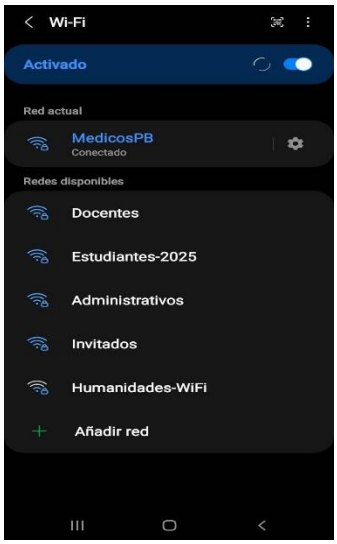

Figura 387. Tenemos que estar Conectados a la red Wifi de la clínica en el área de Personal de salud

Figura 388. Descargamos la Aplicación Zoiper del Google Play

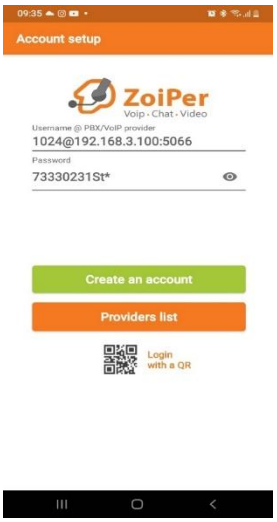

Figura 389. Dentro de la Aplicación Necesitamos Colocar la Extensión Creada Seguido de @ y la Dirección del Servidor de Telefonía IP agregando: el puerto que se está utilizando y la Contraseña Creada en el Servidor

Figura 390. En Hostname Dejamos la IP del Servidor de Telefonía IP

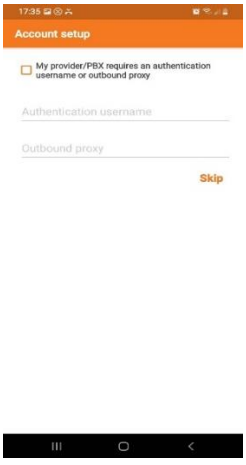

Figura 391. Mantenemos por defecto la Configuración del Proxy

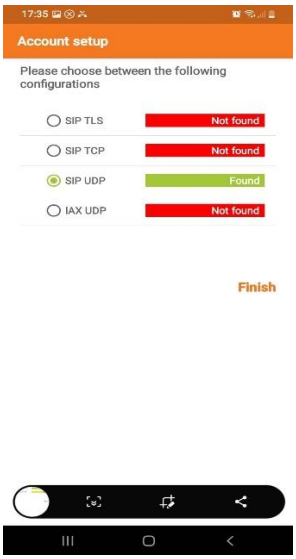

Figura 392. Esperamos la Conexión SIP UDP (si marco verde) la Configuración fue Todo un Éxito

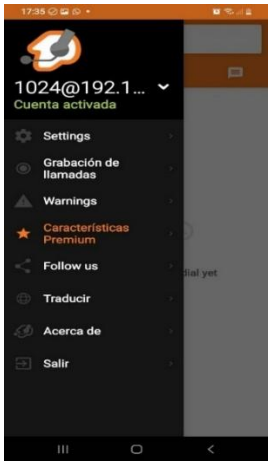

Figura 393. Verificamos que la Cuenta Este Activada

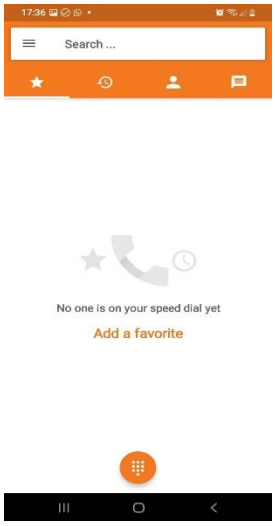

Figura 394. Podemos Comenzar a Usar los Teléfonos Mediante la Telefonía IP

Figura 395. Podemos ver el Historial de Llamadas

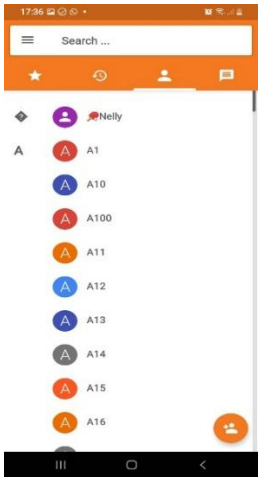

Figura 396. Podemos Vincular Nuestros Contactos

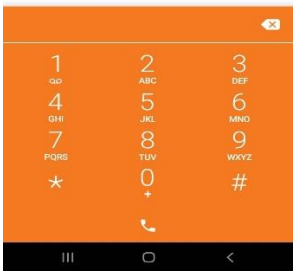

Figura 397. Prueba de Llamada Entramos al Teléfono

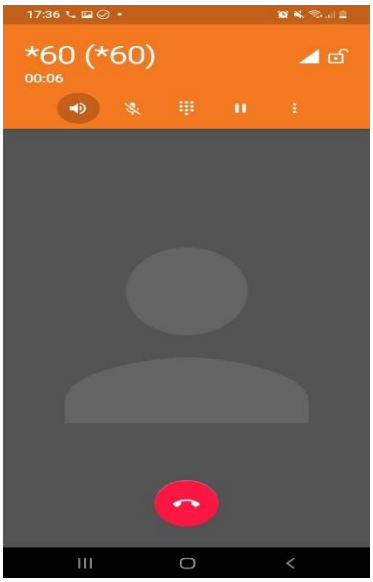

Figura 398. Marcamos *60 Para Escuchar la Hora

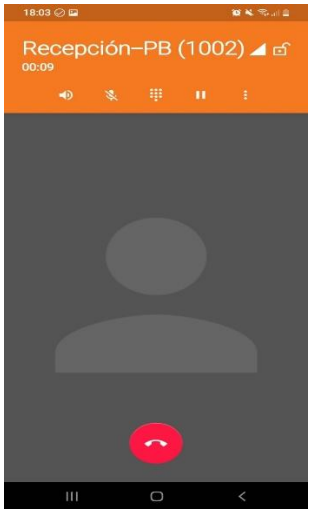

Figura 399. Interfaz de Llamada Entrante

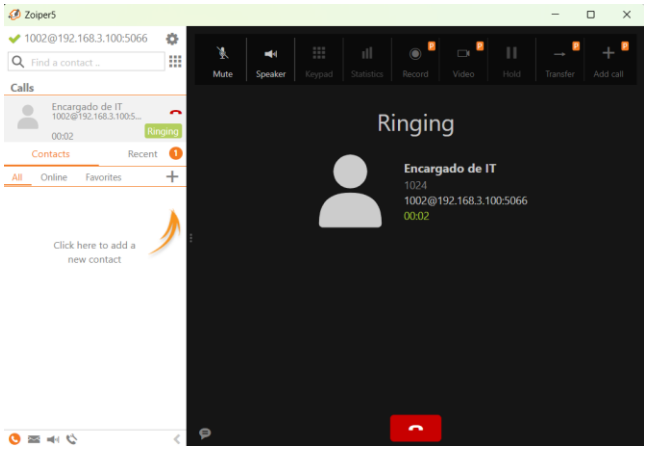

Figura 400. Interfaz de Llamada en Espera a Contestar

24. Pruebas de comunicación

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

Configuramos el archivo que se va a compartir en la red, IT-2 192.168.2.4

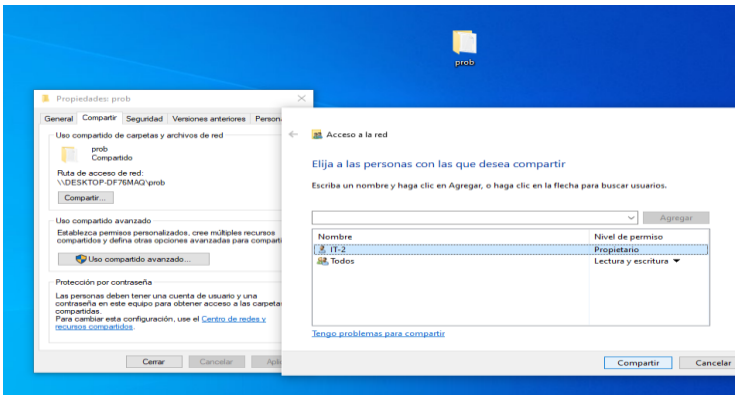

Figura 401. Compartir archivos en la red

Ya que se verificó que hay ping entre maquina entonces entonces procedemos a presiona Windows+R

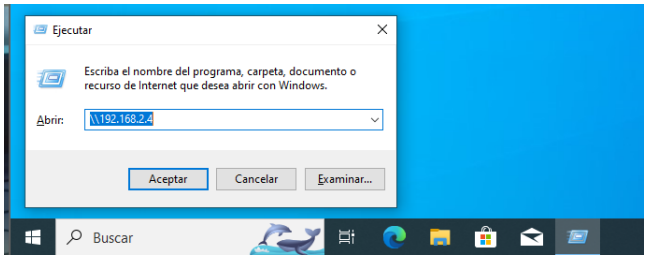

Figura 402. Acceso a la IP de la máquina que comparte los archivos

Iniciamos sesión con el Usuario y Contraseña de la máquina que está compartiendo el archivo por métodos de seguridad

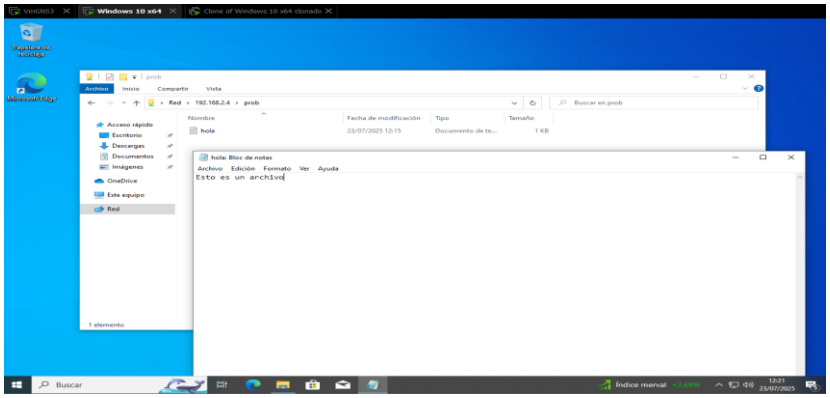

Figura 403. Resultado de prueba compartida

Y como se puede ver se compartió con éxito el Block de Notas, esto será necesario para que los funcionarios de la Clínica puedan compartir sus archivos importantes en toda la red, así de forma rápida y segura.

Realizar pruebas

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

Se utilizarán los siguientes métodos de prueba para la red:

Probar la conectividad de la red

En primer lugar, se realizará ping a los servicios web que utiliza la clínica, así como también a sus respectivas páginas.

Ping a los servicios utilizados

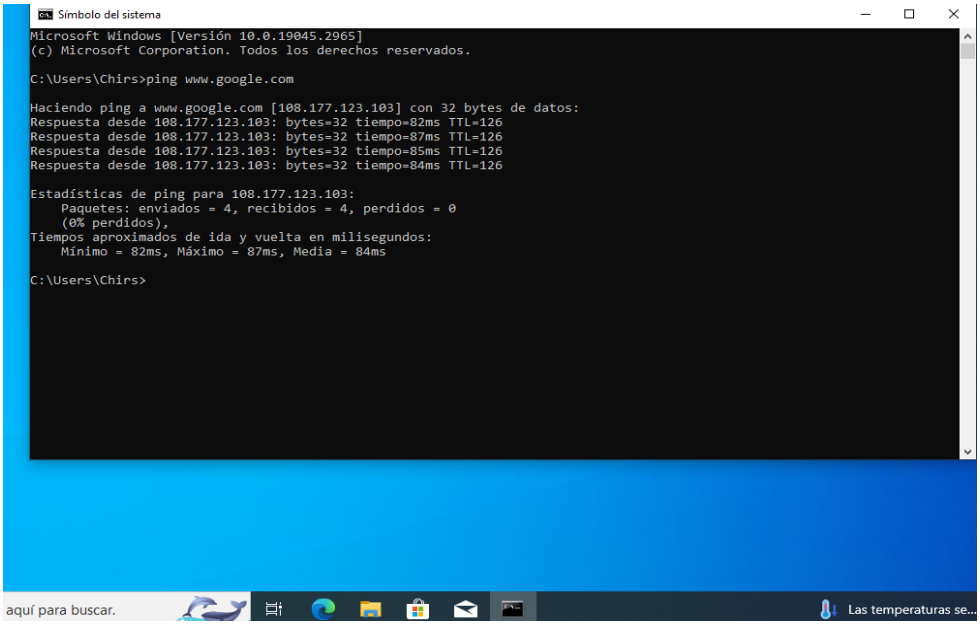

Figura 404. Probar la conectividad de la red

Pruebas de los equipos

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

El servidor DHCP asigno a los equipos de su respectiva VLAN una IP de manera dinámica por lo que probaremos la conectividad entre uno de los equipos de escritorio de la VLAN Recepción y una de las máquinas de Internación.

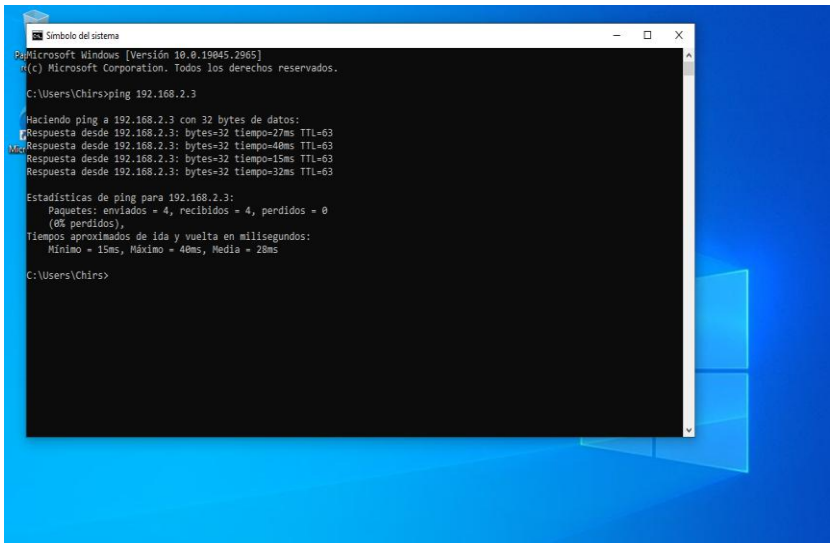

Figura 405. Ping entre Recepcion e Internacion

Probaremos la conectividad entre uno de los equipos de escritorio de la VLAN Terapia Intensiva con el equipo de Internación.

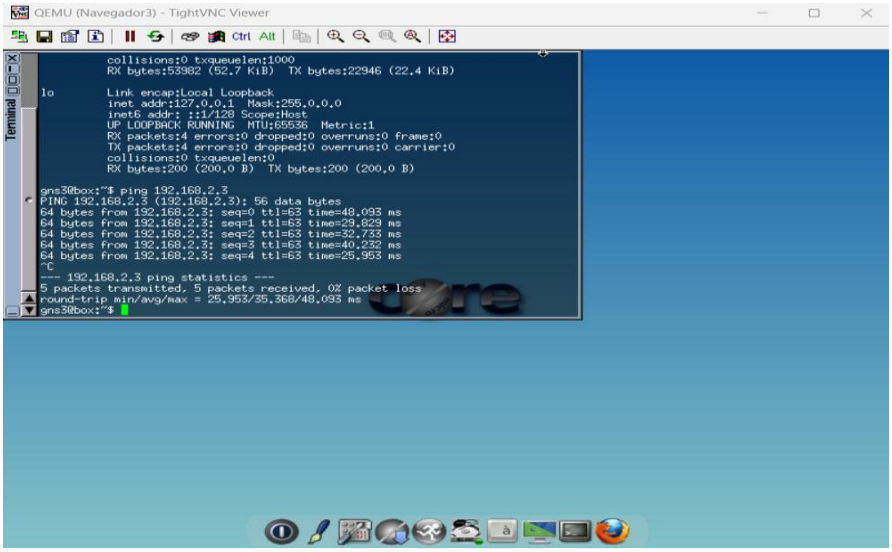

Figura 406. Ping entre Terapia Intensiva e Internación

Resultados esperados del Testeo

Figura 407. Resultados esperados del Testeo

Pruebas de funcionalidad

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

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

- Sitio web de Impuestos Nacionales
- Sitio web de la Caja Nacional de Tarija
- Sitio web de Sedem (Subsidios)
- Google Maps
- Sitio web Seprec (Servicio Plurinacional de Registro de Comercio)

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

Sitio web de Impuestos Nacionales

La Clínica Santísima Trinidad utilizará el sistema de facturación en línea para gestionar sus pagos y obligaciones tributarias de manera más rápida y segura. Este método le permite emitir y recibir facturas electrónicas, reduciendo el uso de documentos físicos. Además, facilitará el control interno y el cumplimiento con Impuestos Nacionales. En general, mejorará la eficiencia administrativa y agilizará sus procesos de pago.

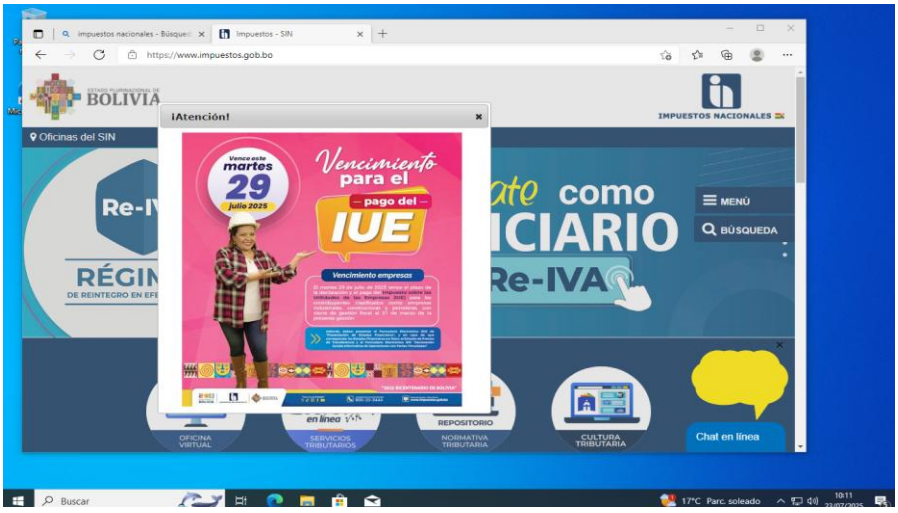

Figura 408. Sitio web de Impuestos Nacionales

Sitio web de la Caja Nacional de Tarija

Para la clínica, este portal servirá para consultar información de afiliaciones, prestaciones y comunicados de la CAJA NACIONAL DE SALUD, facilitando así la coordinación con pacientes

asegurados. También permitirá acceder rápidamente a datos institucionales y procedimientos necesarios para su atención.

Figura 409. Sitio web de la Caja Nacional de Tarija

Sitio web de Sedem

El sitio web de SEDEM sirve para informar al público sobre las actividades y productos que esta institución elabora y distribuye, especialmente relacionados con el subsidio alimentario. En la página se pueden ver noticias, comunicados, datos de sus empresas y formas de contacto. También muestra información actualizada sobre la calidad y entrega de los productos.

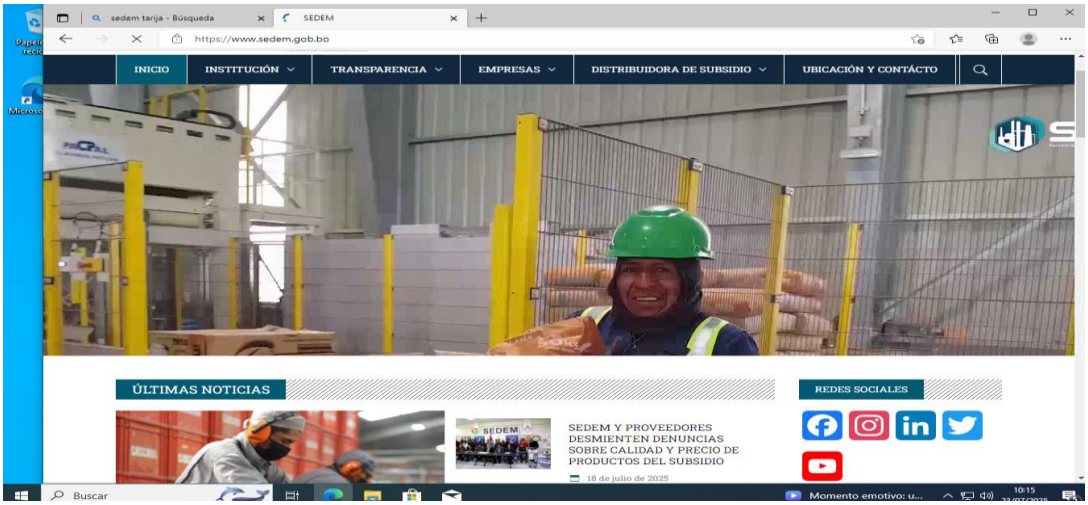

Figura 410. Sitio web de Sedem

Google Maps

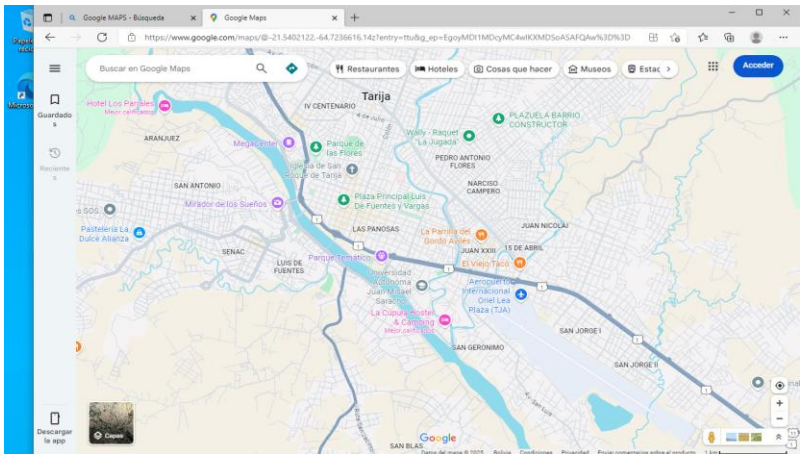

Figura 411. Google Maps

Sitio web Seprec

El sitio web de SEPREC sirve para realizar y consultar trámites del Registro de Comercio en Bolivia. Desde allí se puede buscar información de empresas, revisar requisitos y ver la normativa que regula las actividades comerciales. También permite hacer consultas y llevar el seguimiento de trámites en línea. En resumen, es la página donde se gestionan todos los registros y datos oficiales de las empresas.

Figura 412. Sitio web Seprec

Resultado de pruebas y problemas

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

ANEXO C MEDIOS DE VERIFICACIÓN

ANEXO C MEDIOS DE VERIFICACIÓN

UNIVERSIDAD AUTÓNOMA
"JUAN MISAEL SARACHO"
FACULTAD DE CIENCIAS Y TECNOLOGÍA
CARRERA DE INGENIERIA INFORMATICA
"Con Ética y Responsabilidad Social"

ingeniería informática

Tarija, 24 de abril de 2025
FAC. CS.Y TEC, CARR. ING. INF, OF. Nº 133 /2025

Señora
Lic. Laura Martínez Acosta
ADMINISTRADORA "CLINICA SANTISIMA TRINIDAD"
Presente.-

Clínica Santísima Trinidad S.R.L.
Direc. Calle Alejandro del Carpio Nº 850
Teléfono: 66-72006
T-13-10-25

De mi mayor consideración:

A tiempo de saludarle y desearle éxitos en las delicadas funciones que desempeña diariamente, me dirijo a su autoridad a objeto de informarle que el estudiante **CRISTIAN NAHUEL CONDORI CONDORI** con C.I. 12623385Pt., cursa la materia de Profesionalización **DIS 501 TALLER III** del Plan de Estudios de la carrera de Ingeniería Informática; actualmente solicita realizar un proyecto titulado: "REDISEÑO Y OPTIMIZACIÓN DE LA INFRAESTRUCTURA DE RED DE LA CLINICA SANTISIMA TRINIDAD". A tal efecto, agradeceré a usted prestar su colaboración al mencionado estudiante y solicitamos a usted pueda autorizar a los funcionarios de su repartición proporcionar la información requerida para el desarrollo de su proyecto.

Agradeciendo de antemano su gentil deferencia, aprovecho la oportunidad para saludarle.

Atentamente,

M.Sc. Lic. Deysi Beatriz Arancibia Marquez
DIRECTORA a.i. CARRERA DE INGENIERÍA INFORMÁTICA
FACULTAD DE CIENCIAS Y TECNOLOGIA

UNIVERSIDAD AUTÓNOMA "JUAN MISAEL SARACHO" FACULTAD CIENCIAS Y TECNOLOGÍA CARRERA DE INGENIERIA INFORMATICA Tarija - Bolivia

cc/Arch

Figura 413. Carta de Aval de Autorización

Tarija 11 de marzo de 2025

Ing. Erick Cortez Michel.

Docente de la carrera de Ingeniería Informática de la universidad Juan Misael Saracho

REF.: SOLICITUD DE TUTORIA EN PROYECTO DE GRADO DE LA MATERIA DE TALLER III

Estimado ingeniero Erick:

Me dirijo a usted con el propósito de solicitar su apoyo y orientación como tutor de mi Proyecto de Grado en el marco de la carrera de ingeniería Informática en la universidad autónoma Juan Misael Saracho.

Mi proyecto tiene como objetivo principal la implementación de un rediseño en red en la Clínica Santísima Trinidad en Tarija.

Considero que su experiencia y conocimientos en nuestra carrera serian de gran valor para la correcta ejecución y desarrollo de esta investigación.

Agradecería mucho su orientación en cada etapa del proyecto, desde la definición metodológica hasta la implementación de los resultados. Estoy dispuesto a coordinar reuniones periódicas según su disponibilidad y requerimientos.

Quedo atento a su pronta respuesta y agradezco de antemano su tiempo y consideración. Adjunto un resumen de mi propuesta de investigación para su evaluación

Atentamente,

Univ. Cristian Nahuel Condori Condori

Recibí
Fernando Cortes
12/03/2025

Figura 414. Carta de solicitud de Tutoría

TARIJA, 20 de octubre de 2025

Señor(a):

Cristian Nahuel Condori Condori

Estudiante de la Universidad Autónoma Juan Misael Saracho

Presente. -

REF.: CARTA DE GRADO DE SATISFACCIÓN

De mi consideración:

Por medio de la presente, se hace constar que el proyecto titulado ***"Rediseño y Optimización de la Infraestructura de Red de la Clínica Santísima Trinidad"***, presentado y desarrollado por su persona, alcanza un grado de satisfacción del 87%, de acuerdo con la evaluación realizada sobre los servicios implementados en relación con los requerimientos establecidos en la etapa de planificación.

Este resultado refleja un alto nivel de cumplimiento de los objetivos técnicos y funcionales propuestos, garantizando la eficiencia, escalabilidad y seguridad en el funcionamiento de la infraestructura de red implementada en la Clínica Santísima Trinidad.

Sin otro particular, extiendo la presente en constancia del grado de conformidad alcanzado con el trabajo desarrollado.

Atentamente,

Lic. Luis Germán Quispe Hanco

Jefe de División – Telecomunicaciones

Clínica Santísima Trinidad – Tarija

Figura 415. Carta de grado de satisfacción