CAPÍTULO I
INTRODUCCIÓN

CAPÍTULO I: INTRODUCCIÓN

Las instituciones públicas o privadas suelen a implementar redes de área local (LAN) para conectar sus equipos informáticos. Estas redes pueden ser de tipo cableado o inalámbricas. De acuerdo a las necesidades de la empresa, es necesario diseñar una arquitectura de red que permita la transferencia de datos que conectarán las estaciones de trabajo que son la constante frustración y reclamo de los usuarios internos de la misma institución, que se encuentren operativas y/o o administrativo, busca otras alternativas tecnológicas para realizar las tareas diarias que le son asignadas; La ausencia de soporte técnico, actualizaciones y mantenimiento preventivo de los equipos de cómputo puede generar insatisfacción en los usuarios y un uso inadecuado de la infraestructura tecnológica.

En la Subgobernación de Villa Montes desde las gestiones pasadas y actuales no se realizaron adquisiciones nuevas de equipos tecnológicos, softwares actualizados y mucho menos de equipos de comunicación, situación que llevó a continuar usando tecnologías obsoletas encareciendo las habilidades y herramientas de los profesionales, generando deterioro de sus componentes y acortando la vida útil de tan importante activo en este caso dentro de la Institución pública. Es por expuesto, que en el presente proyecto se buscara analizar y diseñar la red de comunicación con los recursos físicos que se encuentre al alcance del Departamento de Informática, para lo que se iniciaría inmediatamente con un análisis tecnológico de la situación actual de las áreas de trabajo de la Subgobernación de Villa Montes tomando en cuenta la metodología y normas que más adelante serán mencionadas.

Para cumplir con los objetivos propuestos se usara la metodología Top-Down con sus componentes esenciales para gestionar la elaboración de proyecto, esta metodología ayudara a implementar diferentes marcos de trabajo, que nos guiara para avanzar hacia una nueva organización de los equipos de manera efectiva en cuanto a la disponibilidad de servicios y consumo de recursos físicos, Se especificará las necesidades de la institución bajo el marco de elaboración propia denominado (Especificación de requerimientos de configuración); siguiendo estas guías se pretende garantizar de manera efectiva y eficiente cada una de las tareas de los equipos de computación y servicios.

Nos enfocaremos en la gestión estratégicas que brinda la comunicación de red y establecer los requerimientos en la infraestructura tecnológica de las áreas de trabajo de la Subgobernación.

I.1. Descripción del Proyecto

Título del Proyecto: Mejorar la red de comunicación administrativa de las áreas de trabajo en la Subgobernación de Villa Montes

Apellidos y Nombres: Nuñez Barba Katherine Romina

Carrera/Facultad: Ing. Informática/ Facultad de Ciencias y Tecnología

Celular: 67675953

Correo: nunezbarbakatherineromina@gmail.com

Institución/Centro Cooperante: Subgobernación de Villa Montes

Área/línea de investigación priorizada: Redes

Duración: 8 meses

I.1.1. Antecedentes

I.1.1.1. Antecedentes de Institución

En estos últimos tiempos las tecnologías de la información está teniendo un gran crecimiento y mucha importancia en las redes LAN y en Internet debido a la gran necesidad de estar siempre conectados a diferentes servicios, estas redes actuales deben tener la capacidad de poder brindar integración de servicios tales como datos, todo esto ha llevado a que las redes actuales tengan diferentes formas y a la vez tengan cierto tipo de sofisticación para su acceso, a todo esto se suma el crecimiento constante del número de usuarios finales y la generación de grandes cantidades de información y de tráfico de estos, lo cual hace que estas redes necesitan la capacidad de poder brindar un flujo de datos constantes sin pérdidas y a la vez poder ser seguras para evitar intrusos en nuestra red.

La institución pública de la Subgobernación de Villa Montes no cuenta con ninguna topología de red normalizada en los últimos años se trató en las oficinas de utilizar internet para distintas actividades, los cuales consumen los datos generados por las aplicaciones y a la vez se incrementó los usuarios para el uso lo que genera una pérdida constante en el tráfico de red.

Para poder comprender el alcance de la Subgobernación de Villa Montes se muestra el organigrama de administración de las áreas de trabajo

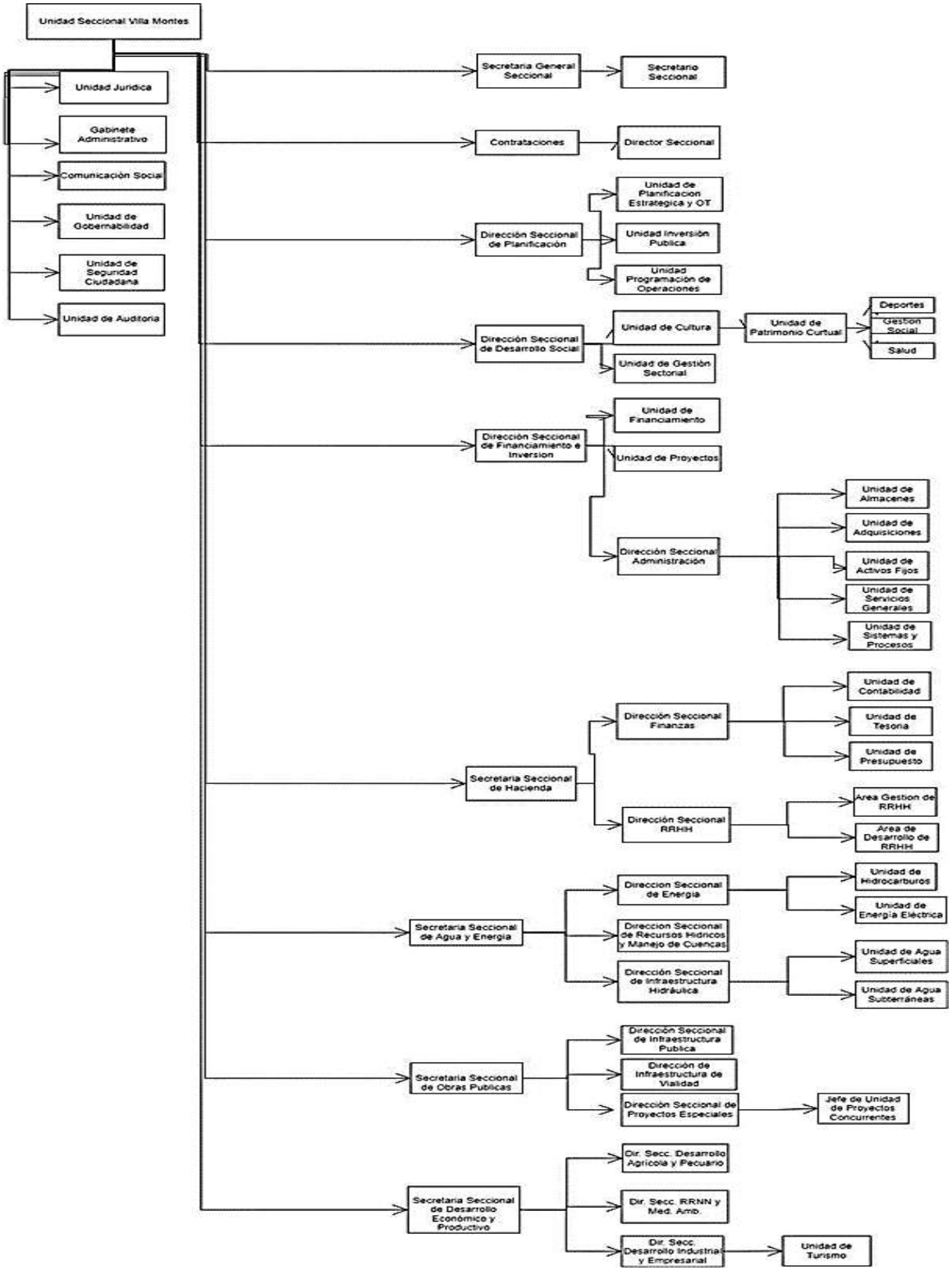


Figura 1. Organigrama Institucional

I.1.1.2. Antecedentes de Proyectos Similares

Hoy en día, las tecnologías de la comunicación se están desarrollando rápidamente, lo que obliga a las instituciones públicas y privadas a la actualización, utilizar las últimas tecnologías en el entorno de las telecomunicaciones, incluidos los equipos de conmutación, los cables, los centros de datos deben ser eficientes y rentables para brindar a los usuarios servicios de alta calidad. Mediante un análisis de proyectos e investigaciones se pretende alcanzar un mayor enfoque con respecto al desarrollo de diseño de red, además, conocer las metodologías utilizadas para la propuesta del diseño de red de datos.

En el año 2014, (Tinjaca Paola,2014) realizo el proyecto "Propuesta de mejoramiento del desempeño de la red de telecomunicaciones para la empresa KAMILION S.A" su objetivo general fue realizar la propuesta de la solución tecnológica de mejoramiento para el óptimo desempeño de la red de telecomunicaciones de la empresa prestadora de servicios Kamilion S.A., mediante la metodología PMI.

En el año 2019, (Villarreal Herrera, 2019) realizó el proyecto "Rediseño de la red de datos de la empresa Asistecom para integrar telefonía IP con calidad de servicio.", que tuvo como objetivo general realizar la simulación con GNS3 de la topología de la red de datos para la integración de telefonía IP. Además, la metodología utilizada fue PPDIOO, para diseñar redes jerárquicas de voz y datos. Los resultados que obtuvo se basan en datos de los sistemas D-ITG y PRTG en términos de latencia, con G.729.2 reduciéndose en un 82% y un 73%. Se concluyó que los tráficos de paquetes generados por los empleados de Asistecom se pudieron identificar mediante un análisis de los dispositivos y materiales de trabajo que utilizan en su día a día.

En el año 2018, (Mamani Anave, 2018) realizó el proyecto "Diseño de red Lan para predios del Colegio Don Bosco", su investigación propuso el diseño de redes LAN cableadas e inalámbricas para las instalaciones del Colegio Don Bosco. El enfoque metodológico utilizado fue un enfoque técnico orientado a descubrir nuevos conocimientos para el diseño o mejora de procesos mediante la aplicación de métodos científicos. En los resultados, se obtuvo que se necesitan 80 Mbps a Internet para la institución de promedio 2000 usuarios, donde se estiman que navegan 1600 usuarios simultáneamente. Concluyendo, se realizaron pruebas de continuidad (Punto-Punto) donde se verificó la instalación realizada antes de proceder al enlace de los dispositivos que componen la Red Local.

En el año 2020, (Aguaiza Tenelema) presentó su proyecto de tesis “Propuesta de rediseño de la Infraestructura de red de la Universidad Laica "Eloy Alfaro" de Manabí.”, su objetivo general fue realizar el rediseño de la red de la Universidad, basándose en la normativa de cableado estructurado y garantizar la calidad de servicios QoS. La metodología que aplicó fue cualitativa y cuantitativa, ya que utilizó los instrumentos como: la entrevista y la encuesta, necesarios para la recolección de información. Como resultado obtenido, demostró mediante el cálculo del ancho de banda una mejora significativa con el número de usuarios que lograron conectarse a la red sin ningún inconveniente en el tráfico de paquetes. Obteniendo como conclusión la distribución de la infraestructura de la red y la dimensión de los enlaces.

I.1.1.3. Situación Actual de la Institución

Figura 2. Situación actual de la Subgobernación de Vila Montes

Como se puede observar la imagen la Subgobernación de Villa Montes cuenta con distintos bloques o dependencia las cuales no se comunican entre ellas presentando varias limitaciones.

La situación actual de la red de la Subgobernación de Villa Montes presenta múltiples limitaciones significativas que impiden un funcionamiento óptimo y eficiente de las comunicaciones internas. En primer lugar, la estructura de la red es improvisada y carece de un diseño cohesivo y planificado, lo que resulta en una falta de interconexión efectiva entre los seis bloques de oficinas. Estos bloques están físicamente separados y no tienen comunicación entre ellos, lo que dificulta el intercambio de información y la coordinación entre las distintas áreas de trabajo. Además, el equipamiento de la red es obsoleto, lo que afecta negativamente tanto la capacidad como el rendimiento de la red. Este equipamiento anticuado no puede soportar adecuadamente la cantidad de dispositivos existentes, que incluyen 125 equipos de escritorio, 35 portátiles y 6 impresoras.

Asimismo, la seguridad de la red es insuficiente, exponiéndola a posibles accesos no autorizados y ataques, lo que pone en riesgo la integridad y confidencialidad de la información. La falta de medidas de seguridad robustas, como cortafuegos, controles de acceso y segmentación de la red, aumenta la vulnerabilidad de la infraestructura de comunicación. Finalmente, la ausencia de una infraestructura de red adecuada no solo dificulta el intercambio eficaz de información entre las áreas de trabajo, sino que también limita la capacidad de la organización para implementar nuevas tecnologías y procesos que podrían mejorar la eficiencia administrativa, la red actual no cumple con los requerimientos necesarios para soportar las operaciones diarias de la Subgobernación de Villa Montes, haciendo imperativa la necesidad de un rediseño completo y modernizado.

I.1.2. Justificación del Proyecto

I.1.2.1. Tecnológica

La Propuesta a implementar la red permite facilitar la información de la institución en la que los usuarios `puedan comunicarse y acceder a la información a través de equipos nuevos lo cual facilitara en el aumento de la productividad.

I.1.2.2. Económica

Se tiene como objetivo utilizar los equipos de computación disponibles en las áreas de trabajo para evitar una elevación de costes en la implementación de nueva infraestructura tecnológica de esta manera se controlará mejor los gastos de la institución.

I.1.2.3. Social

El proyecto pretende mejorar la Interconexión a los administrativos a través de la prestación de servicio en los usuarios finales por parte de la Subgobernación de villa montes.

I.1.2.4. Desarrollo Sostenible

La institución cuenta con los recursos tecnológicos y humanos para continuar el desarrollo del proyecto sin inconvenientes en el camino.

I.1.2.5. Medio Ambiental

Al contar con la calidad de los nuevos servicios la institución de la Subgobernación reducirá un porcentaje en el uso de algunos equipos de computación mejorando el ahorro de energía eléctrica.

I.1.3. Planteamiento del Problema

El presente proyecto busca poder presentar una propuesta de diseño de una red privada con alta disponibilidad, segura y con un menor coste. Actualmente la Subgobernación de Villa Montes presenta problemas de seguridad, disponibilidad y comunicación entre los diferentes departamentos pese a tener una red, esta misma es improvisada, reflejando esto un problema cada vez más significativo y engorroso la manera de comunicación y transferencia de archivos entre departamentos viéndose afectados el personal administrativo dentro de la institución (algunos ejemplos comunes suelen ser problemas de imprimir documentos, la incapacidad de compartir archivos con otros departamentos, la demora a los diferentes procesos administrativos y una pésima gestión de recursos derivado de esta red).

La red de comunicación administrativa es inestable y la falta de equipos tecnológicos ineficientes obstaculizan el intercambio eficaz de información entre las áreas de trabajo en la Subgobernación de Villa Montes, Se propone el diseño de una red LAN que cubra todos los departamentos facilitando el trabajo administrativo, ofreciendo por otra parte un mejor desempeño en las áreas de trabajos administrativos.

I.1.4. Análisis de Cuadro de Involucrados

Grupo	Intereses	Problemas	Recursos/Mandatos
Autoridades (Subgobernador)	Contar con un medio de información que refleje los decretos, resoluciones, leyes, Estatuto Autonómico Decretos Ejecutivos	Inestabilidad y caídas en el servicio	Publicar documentos sobre las leyes promulgadas. Documentos en formato digital. Cotización para la propuesta de implementación
Funcionarios Administrativos	Disponibilidad en la administración e información y recursos tecnológicos necesarios para el funcionamiento efectivo de la Subgobernación Colaboración Eficaz. Producir una conexión de las maquinas a la impresora por la red.	Limitaciones en la administración información y recursos tecnológicos necesarios para el funcionamiento efectivo de la Subgobernación Dificultades para la colaboración. Equipos de computación sin conexión a la impresora.	Disponibilidad para realizar pruebas de recursos implementados. Conexión fiable y sin interrupción en la red.

Funcionarios técnicos	Disposición de interconexión a los sistemas de correspondencia así también a los sistemas propios que les permiten desempeñar su trabajo de manera digital. Capacitación a los usuarios sobre la nueva tecnología de red propuesta Contar con un acceso a la red institucional para la conexión de las máquinas.	Sistemas de almacenamiento de herramientas de soporte técnico se encuentran fuera de servicio. Inestabilidad de comunicación mediante los sistemas informáticos con las diferentes oficinas para coordinación técnica entre unidades.	Conocimientos técnicos especializados. Conexión fiable y sin cortes de servicio de los diferentes sistemas institucionales

Tabla 1. *Análisis de Cuadro de Involucrados*

I.1.5. Árbol de Problemas

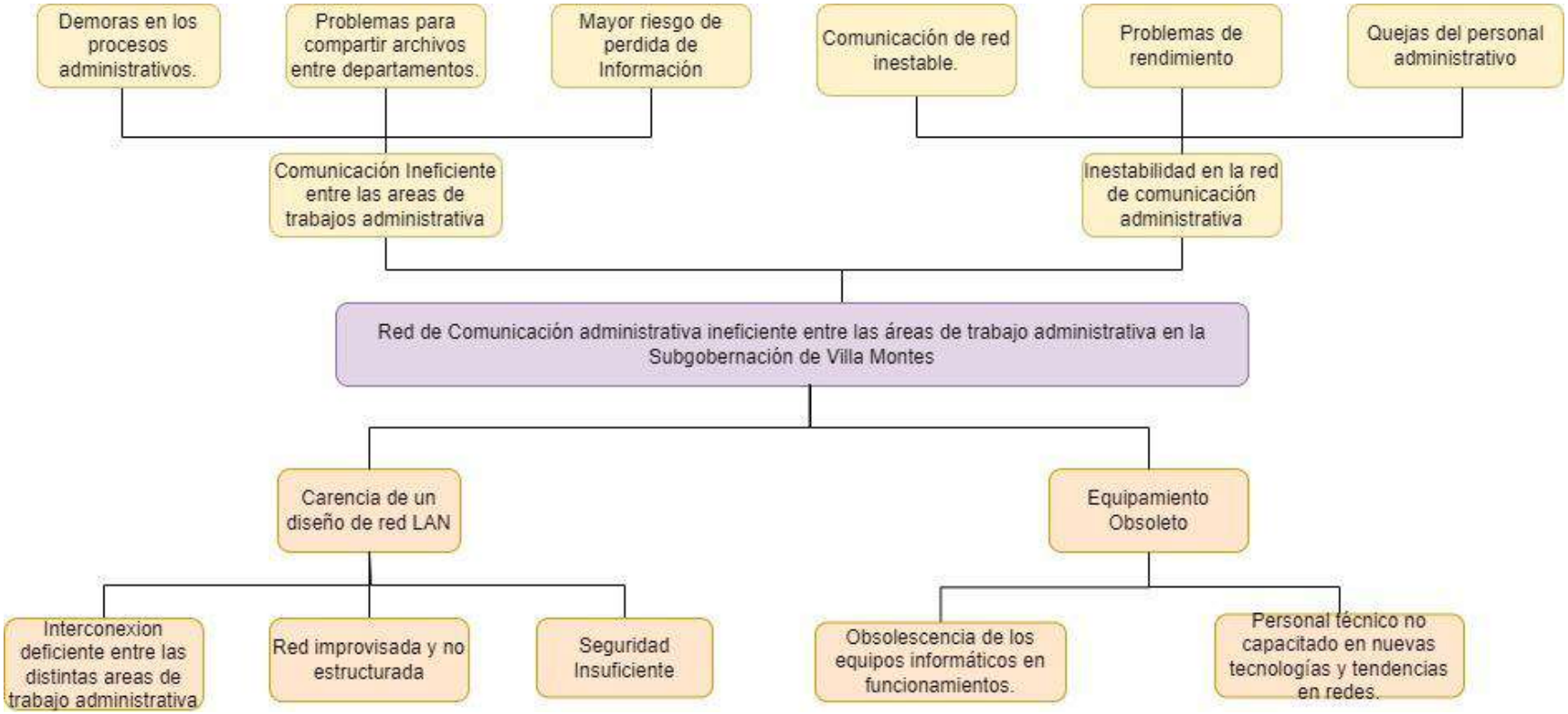


Figura 3. Árbol de Problemas

I.1.6. Árbol de Objetivos

Figura 4. Árbol de Objetivos

I.1.7. Objetivos

I.1.7.1. Objetivo General

- Proponer el diseño de una red LAN para la comunicación administrativa que permita facilitar un intercambio eficaz de información entre las áreas de trabajo en la Subgobernación de Villa Montes, en un entorno de simulación.

I.1.7.2. Objetivos Específicos

- Diseñar la red LAN de comunicación administrativa, mediante el software de simulación Packet Tracer.
- Capacitar al personal técnico sobre la nueva tecnología de red propuesta.

I.1.7.3. Alcance y Limitaciones

I.1.7.3.1. Alcance

Esta propuesta abarcará el nuevo diseño de la red de todo los bloques o dependencias de la subgobernación de Villa Montes ubicada en la zona Bolivar Kilometro 1 salida a Tarija, se enfocará en proponer la interconexión de las dependencias, el alcance del proyecto incluye:

- Estudio, análisis y solución de acuerdo a los requerimientos disponibles en cuanto a la nueva infraestructura de red en sus características más básicas y relevantes de cada tecnología.
- Lograr enlaces desde cada oficina para el uso, la nueva infraestructura de red requerirá cableado estructurado, conexiones inalámbricas por Access Point, contratos de paquetes de servicios de internet y así como materiales, equipos y configuraciones a utilizar para la correcta disponibilidad de comunicación durante la conexión establecidas.

I.1.7.3.2. Limitaciones

Teniendo en cuenta la magnitud de los problemas se limitará en no dar soluciones a los sistemas de seguimiento de trámites y configuración de VPN de accesos remotos, tampoco no cubrirá a profundidad todos los aspectos de las normas y estándares.

I.1.8. Resultados Esperados

Una vez realizada la propuesta del diseño de red con las nuevas infraestructuras tecnológicas de red se pretende lograr:

- **Propuesta de la Nueva Infraestructura tecnológica de red en las áreas de trabajo:** Se espera la elaboración de una de red que comprenda las necesidades de los funcionarios en cuanto accesos a internet y sistemas administrativos en la red, también se espera la interconexión de las distintas dependencias y normalizar la red y conexión a los sistemas.
- **Capacitación al usuario sobre la nueva tecnología de red:** Al finalizar la capacitación se espera que los funcionarios y personal de la institución tengan todo lo necesario para realizar su trabajo.

I.1.8.1 Beneficiarios

I.1.8.1.1 Beneficiarios Directos

La propuesta del diseño de red de la nueva infraestructura tecnológica de red beneficia de forma directa a los funcionarios públicos de la subgobernación de Villa Montes.

I.1.8.1.1 Beneficiarios Directos

La propuesta del diseño de red de la nueva infraestructura tecnológica de red beneficia de forma indirecta a los usuarios de Villa Montes.

I.2. Cronograma de Actividades

N.º	Actividad	N.º días	Fecha inicio	Fecha Finalización	M1	M2	M3	M4	M5	M6	M7	M8
1	**Planificación y diseño del Proyecto**	**210**	01/04/24	30/09/24	x	x	x	x	x	x	x	x
1.1.	Evaluación de la infraestructura de red existente.	**30**	01/04/24	30/04/24	x							
1.2.	Elaboración del plan de diseño de la nueva infraestructura de red.	30	01/05/24	30/05/24		x						
1.3.	Adquisición de equipos y materiales necesarios.	30	01/06/24	30/06/24			x					
1.4.	Configuración inicial de los dispositivos de red.	15	01/07/24	15/07/24				x				
1.5	Instalación de cables y dispositivos de red.	30	16/07/24	16/08/24					x			
1.6	Configuración y pruebas de seguridad de la red.	15	17/08/24	01/09/24					x	x		
1.7	Pruebas de funcionamiento y ajustes finales.	30	02/09/24	02/10/24						x	x	
1.8	Evaluación y Monitoreo del funcionamiento de la red.	30	03/10/24	02/11/24							x	x
2	**Capacitación a los encargados de informáticas sobre la nueva tecnología de red propuesta.**	**10**	04/11/24	14/11/24								x
2.1.	Definición de medios y estrategia	4	04/11/24	07/11/24								x
2.2.	Capacitación sobre la nueva infraestructura tecnológica	6	08/11/24	14/11/24								x

Tabla 2. *Cronograma de Actividades*

I.3. Presupuesto General

PARTIDA	FINALIDAD				
25200	Consultados				
#	Recurso	Aporte UAJMS	Aporte Institucional	Mensual	TOTAL (Bs)
1	Estipendio por desarrollo	0.00	2500.00	8	20000
Subtotal componente					20000.00

PARTIDA	FINALIDAD				
39700	Útiles y Materiales Eléctricos.				
#	Recurso	Aporte UAJMS	Aporte Institucional	Cantidad	TOTAL (Bs)
1	Switch (48 puertos)Capa 3 de 1 GigaBit	0.00	1100	**6**	4400
2	Adaptadores de wifi/ Access Point TP-Link de 300 Mbps	0.00	445	**6**	2670
3	Conectadores RJ-45/ Cajas de Conectores Rj45 (cada caja tiene 300 conectores)	0.00	1.12	**3**	340
4	Rack 10U	0.00	1130	1	1130
5	Patch pannel de 48 puertos	0.00	370	**6**	2220
6	Canaletas	0.00	3	50	150
7	Cable Caja de 305 metros/ Bobinas UTP cat 6	0.00	250	6	1500
8	Servidor/ Intel Xeon E5 (64 GB de RAM, 4 x 4TB de Disco duro)	0.00	31.500	6	189
9	Gabinete/Rack	0.00	336	6	2016

10	1 Router Cisco	0.00	173000	1	1730
Subtotal componente					16345.00

PARTIDA	FINALIDAD				
43120	Equipos de Computación				
#	Recurso	Aporte UAJMS	Aporte Institucional	Cantidad	TOTAL (Bs)
1	Computadoras de Escritorio	0.00	2800	12	33600
2	Impresoras	0.00	1770	6	10620
Subtotal componente					44220.00

PARTIDA	FINALIDAD				
43500	Equipo de Comunicación				
#	Recurso	Aporte UAJMS	Aporte Institucional	Anual	TOTAL (Bs)
1	INTERNET servidor Entel	0.00	1.006.620	1	1.006.620
				Subtotal componente	1006.620.00
PRESUPUESTO TOTAL en Bs.					1.087.165.00

Tabla 3. *Presupuesto General*

Condiciones

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

I.4. Matriz de Marco Lógico

Resumen Narrativo del Proyecto	**Indicadores**	**Medios de Verificación**	**Supuestos**
Fin: ▪ Comunicación eficiente entre las áreas de trabajos administrativa ▪ Estabilidad en la red de comunicación administrativa	Elaboración de la propuesta del diseño de red para la comunicación administrativa en la Subgobernación de Villa Montes.	Encuesta al personal administrativo sobre el funcionamiento de red una vez ejecutado el proyecto.	Se mantiene la infraestructura de red orgánica de la Subgobernación de Villa Montes.
Propósito (Objetivo General) Proponer el diseño de una red LAN para la comunicación administrativa que permita facilitar un intercambio eficaz de información entre las áreas de trabajo en la Subgobernación de Villa Montes	Al finalizar la propuesta de proyecto, se tiene la completitud del diseño de red evaluado mediante la simulación en Packet Tracer.	Informe técnico de la Subgobernación de Villa Monte aceptando la propuesta del diseño.	Los Técnicos de la Subgobernación de Villa Montes aceptarán y participarán activamente en la definición de requerimientos y entrega de manera oportuna la información

<table>
<tr>
<td>Componentes (Objetivos Específicos)
I. Diseñar la red LAN de comunicación administrativa, mediante el software de simulación Packet Tracer.
II. Capacitar al personal técnico sobre la nueva tecnología de red propuesta.</td>
<td colspan="2">I. Al finalizar el proyecto en la gestión 2024 se ha desarrollado la propuesta del diseño de red de acuerdo a la norma ERS IEEE830.
II. Al finalizar la propuesta del proyecto, se a implementado un plan de capacitación de las nuevas tecnologías de red propuestas al personal técnico.</td>
<td>I. La carta de aprobación del proyecto por parte del docente de taller III.
II. Carta de conformidad certificando la aceptación de la propuesta a cargo del encargado del departamento de informática de la Subgobernación de Villa Montes</td>
<td>I. Existencia del Hardware necesario para la propuesta a implementar los
equipos de computación de la Subgobernación de Villa Montes
II. Disponibilidad de tiempo e interés del personal técnico de la Subgobernación de Villa Montes para la capacitación.</td>
</tr>
<tr>
<td rowspan="3">Actividades
1. Desarrollo de la red que se propone a implementar.
1.1 Realizar un diagnóstico de la comunicación de red.
1.2 Diseño de la arquitectura de la red.
1.3 Planificación detallada de la propuesta a implementar.</td>
<td>Investigaciones</td>
<td>20000,00</td>
<td rowspan="3">Cumplimiento del cronograma establecido para la realización de cada una de las fases.</td>
<td rowspan="3">La Subgobernación de Villa Montes contará con el presupuesto requerido para la correcta propuesta de implementación del proyecto de grado.</td>
</tr>
<tr>
<td>M. Eléctricos</td>
<td>16345,00</td>
</tr>
<tr>
<td>E. Computación</td>
<td>44220,00</td>
</tr>
</table>

1.4 Adquisición de equipos tecnológicos. **1.4** Configuración de la red a implementar **1.6** Pruebas de funcionamiento. **2. Plan de Capacitación al Personal Técnico.** **2.1.** Definición de medios y estrategias **2.2.** Capacitación sobre la nueva tecnología de red al personal técnico.	E. Comunicación	1006.620,00		
	Total	1.087.165,00		

Tabla 4. *Matriz de Marco Lógico*

CAPÍTULO II
MARCO TEORICO

CAPÍTULO II: MARCO TEORICO

II.1. Elementos Físicos de la Red

En el capítulo se detalla todos los conceptos, conocimientos, metodologías y marcos utilizados, para llevar a cabo la propuesta y su posterior desarrollo de los procesos, planes y gestión del proyecto

II.1.1. Medios de Transmisión

II.1.1.1. Cable de cobre o par trenzado

El cableado de cobre y la fibra óptica son los más utilizados en la actualidad para la transmisión de datos. El cable de cobre está compuesto por hilos de cobre trenzados entre sí para mantener sus propiedades eléctricas estables y prevenir interferencias a lo largo del tiempo y del uso.

Cada par de hilos se identifica mediante un código de colores específico:

- Par 1: Blanco-Azul/Azul
- Par 2: Blanco-Naranja/Naranja
- Par 3: Blanco-Verde/Verde
- Par 4: Blanco-Marrón/Marrón

Los cables trenzados pueden estar apantallados de diferentes maneras:

- Cable UTP (Par Trenzado no Apantallado): Altamente flexible pero sensible a interferencias.
- Cable STP (Par Trenzado Apantallado Individualmente): Cada par está envuelto en una malla conductora, lo que lo hace inmune al ruido, pero bastante rígido.
- Cable FTP (Par Trenzado Apantallado Globalmente): Los cables están cubiertos por una malla conductora global, lo que lo hace poco sensible a las interferencias y tiene una rigidez intermedia.

Dependiendo de la velocidad de transmisión, los cables se clasifican en diferentes categorías:

- Categoría 1: Adecuada solo para voz, no apta para transmisiones de datos.
- Categoría 2: Especificada para transmisiones hasta 4 MHz.
- Categoría 3: Velocidad típica de 10 Mbps para Ethernet.
- Categoría 4: Velocidad de transmisión de hasta 20 Mbps.
- Categoría 5: Transmite datos hasta 100 Mbps.

- Categoría 5e: Mejora de la categoría 5, transmite datos hasta 1 Gbps.
- Categoría 6: Transmite datos hasta 1 Gbps con una frecuencia superior a 250 MHz.
- Categoría 7: Transmite datos hasta 10 Gbps con una frecuencia superior a 600 MHz.

II.1.1.2. Fibra Óptica

El cable de fibra óptica está compuesto por un núcleo de cristal rodeado por varias capas de material protector. A través del núcleo de cristal se transmite luz en lugar de señales eléctricas, lo que elimina problemas de interferencia.

Es ideal para entornos con alta interferencia eléctrica y se utiliza frecuentemente en conexiones de redes entre edificios debido a su inmunidad a la humedad y a la exposición solar.

Existen dos tipos principales de fibra óptica:

- **Multimodo:** Los haces de luz salientes de la fuente son contables, lo que significa que no generan un haz continuo dentro de la fibra. La luz entra solo en un número limitado de ángulos diferentes.
- **Monomodo:** Su principal ventaja es su ancho de banda prácticamente ilimitado, ya que solo se propaga un modo de luz, evitando la dispersión modal causada por la diferencia de velocidad de propagación de los modos en la fibra.

II.1.1.3. Transmisión Inalámbrica

La transmisión inalámbrica permite la transferencia de datos sin cables físicos, destacándose por su movilidad, flexibilidad y menor costo de implementación. Utilizada en tecnologías como Wi-Fi, Bluetooth y Zigbee, facilita despliegues rápidos y escalables, aunque enfrenta desafíos en seguridad y gestión del espectro radioeléctrico. Es crucial para la conectividad, ofreciendo beneficios significativos como:

- **Movilidad y Flexibilidad:** Permite la comunicación y transferencia de datos desde cualquier ubicación dentro del alcance de la red inalámbrica.
- **Escalabilidad:** Facilita la expansión y adaptación de la red según las necesidades cambiantes de usuarios y dispositivos.
- **Menor Costo de Implementación:** Elimina la necesidad de infraestructura cableada compleja, reduciendo los costos de instalación y mantenimiento.

- **Rapidez en la Implementación:** Permite despliegues rápidos y flexibles en comparación con las soluciones cableadas.

La transmisión inalámbrica utiliza tecnologías como Wi-Fi, Bluetooth, Zigbee, entre otras, cada una adaptada para diferentes usos y requisitos de velocidad, alcance y consumo de energía. Sin embargo, presenta desafíos como la seguridad de la red.

II.1.2. Dispositivos de Interconexión

II.1.2.1. Switches

Los computadores son dispositivos ampliamente utilizados para conectar equipos, formando lo que se conoce como una red de área local (LAN). Estas redes siguen las especificaciones técnicas del estándar Ethernet, también conocido como IEEE 802.3. Dentro de estas redes, el Switch es uno de los dispositivos fundamentales, destacando por su alto nivel de escalabilidad.

Los Switches varían en capacidad y funcionalidad, desde modelos básicos con cuatro puertos hasta dispositivos con cientos de puertos y características avanzadas. Su funcionamiento se puede resumir en los siguientes pasos:

1. Recepción de Tramas: El Switch recibe una trama de datos por cada puerto de entrada.

2. Almacenamiento en Memoria: La trama se almacena temporalmente en la memoria interna del Switch.

3. Comprobación de CRC y Estructura de Tramas: Se realiza un cálculo de CRC (Cyclic Redundancy Check) para verificar la integridad de la trama. Si la estructura de la trama es correcta y se identifica según la configuración del Switch, se procede con la transmisión; de lo contrario, la trama se descarta.

4. Validación de Dirección Destino: Se valida la dirección destino de cada trama para determinar el puerto de salida adecuado.

5. Consulta de Tabla de Direccionamiento: El Switch consulta una tabla interna de direccionamiento para determinar el puerto al que debe enviar la trama.

6. Consulta de Protocolos ARP: Si es necesario, se realiza una consulta a los protocolos ARP (Address Resolution Protocol) para completar la tabla de direccionamiento. 7.

Transmisión de Tramas: Finalmente, el Switch envía la trama únicamente al puerto que coincide con la dirección destino especificada.

Los Switches modernos no solo realizan estas funciones básicas, sino que también pueden ejecutar tareas más avanzadas, como análisis de tramas a nivel de capa de transporte, filtrado basado en protocolos de encapsulamiento como TCP y UDP, enrutamiento de paquetes, y gestión de acceso y distribución en la configuración de la red. Estas capacidades les permiten desempeñar un papel fundamental en la gestión y optimización del tráfico de datos en las redes LAN actuales.

II.1.2.2. Routers

Los Routers son dispositivos cruciales en la interconexión de redes de computadoras, como LANs, facilitando el enrutamiento de paquetes entre distintas redes según su dirección destino. Operan en la capa de red del modelo OSI o en el Modelo TCP/IP de Internet.

Existen diferentes modelos de Routers con variadas interfaces de conexión y aplicaciones específicas, adaptados para entornos empresariales que requieren un manejo eficiente de grandes volúmenes de datos.

Estos dispositivos cuentan con funciones avanzadas como la Traducción de Direcciones de Red (NAT), que permite que múltiples dispositivos internos de una LAN accedan a Internet utilizando una sola dirección IP pública proporcionada por el proveedor de servicios de Internet (ISP).

II.1.2.3. Access Point

Los Access Points (AP) o Puntos de Acceso Inalámbricos (WAP) son dispositivos utilizados para establecer conexiones inalámbricas entre equipos, formando redes inalámbricas externas (locales o de Internet) que permiten la interconexión de dispositivos móviles o tarjetas de red inalámbricas. Estas redes inalámbricas se conocen como WLAN (Wireless Local Area Network) y se utilizan para reducir la dependencia de conexiones cableadas.

Usos principales:

- Establecer un acceso inalámbrico LAN en entornos de trabajo.
- Proporcionar acceso a una red inalámbrica a clientes o usuarios externos.
- Extender la conexión a Internet a áreas previamente no cubiertas, sin pérdida de ancho de banda con repetidores.

- Cubrir grandes áreas con una conexión de calidad, minimizando el uso de cableado.
- Permitir interconexiones entre dispositivos convencionales e inalámbricos al conectar el AP a un switch.

Ventajas de un punto de acceso:

- Facilitar la conexión de dispositivos inalámbricos a la WLAN, como teléfonos móviles o computadoras portátiles.
- Utilizar emisiones de ondas de radio, capaces de atravesar muros, permitiendo la conexión de edificios cercanos dentro de la misma red.
- Tener un alcance típico de entre 30 a 100 metros.
- Proporcionar información sobre el estado de la red y descongestionarla al dividirla y enviar información de manera paralela.
- Si cuentan con conexiones PoE (Power over Ethernet), pueden proporcionar acceso a Internet con un solo cable Ethernet RJ-45, sin necesidad de conectarlo a una toma de corriente convencional.
- Permitir la conexión de más usuarios simultáneamente.

II.1.2.4. Firewalls (Fortigate)

Los firewalls Fortinet son componentes esenciales en la seguridad de redes, diseñados para controlar y filtrar el tráfico de datos con el fin de proteger activos críticos de información contra amenazas cibernéticas. Estos dispositivos destacan por su capacidad para ofrecer:

- **Control Preciso del Tráfico:** Permiten gestionar y filtrar el tráfico según criterios específicos como direcciones IP, puertos y protocolos.
- **Prevención de Intrusiones Avanzada:** Detectan y bloquean de manera proactiva tanto amenazas conocidas como nuevas, utilizando técnicas de análisis avanzado y correlación de eventos.
- **Inspección Profunda de Paquetes (DPI):** Analizan el contenido de los paquetes para identificar y mitigar ataques de malware y otras formas de amenazas.
- **Gestión Unificada de Amenazas (UTM):** Integran múltiples funciones de seguridad en un solo dispositivo, incluyendo antivirus, filtrado web y control de aplicaciones.

Estos firewalls no solo garantizan la seguridad y la integridad de los datos críticos de la organización, sino que también facilitan el cumplimiento de regulaciones y estándares de

seguridad. Sin embargo, su implementación efectiva requiere una adecuada configuración de políticas de seguridad y la continua actualización frente a nuevas amenazas.

II.2. Protocolos y Estándares de la capa de datos

Los protocolos en esta capa definen cómo se estructuran y se gestionan las tramas de datos que se envían y reciben entre dispositivos. Algunos protocolos importantes son:

- **Ethernet (IEEE 802.3):** Uno de los protocolos más comunes para redes de área local (LAN). Define cómo los datos se transmiten en forma de tramas a través de cables físicos.
- **Wi-Fi (IEEE 802.11):** Protocolo para redes inalámbricas que permite la comunicación entre dispositivos utilizando ondas de radio en lugar de cables físicos.

II.2.1. Protocolos de acceso al medio

II.2.1.2 Ethernet (IEEE 802.3)

Ethernet es el estándar predominante para redes de área local (LAN), utilizado ampliamente debido a su fiabilidad y capacidad de alta velocidad en la transmisión de datos. Este protocolo se distingue por:

- **Velocidad y Fiabilidad:** Ofrece tasas de transferencia de datos consistentes y rápidas, adecuadas para aplicaciones que requieren baja latencia.
- **Compatibilidad Universal:** Es compatible con una variedad extensa de dispositivos y tecnologías, facilitando su implementación en entornos comerciales y residenciales.
- **Seguridad Mejorada:** Proporciona robustos niveles de seguridad al ser una red cableada, minimizando riesgos de interferencias y vulnerabilidades frente a ataques externos.

Ethernet es fundamental en la infraestructura de red para soportar la comunicación eficiente de datos, voz y video. A pesar de la necesidad de cableado físico, su rendimiento estable y predecible lo convierten en la opción preferida para entornos que demandan alta disponibilidad y capacidad de respuesta.

II.2.1.3. Wifi (IEEE 802.11)

Wi-Fi es una tecnología de comunicación inalámbrica ampliamente utilizada en la actualidad, también conocida como WLAN (Wireless LAN) o estándar IEEE 802.11. Esta tecnología se

inició en 1997 bajo el estándar IEEE 802.11 y ha evolucionado en respuesta a las demandas de los usuarios.

Algunos de los estándares más destacados de Wi-Fi son:

- 802.11g (tercera generación) (2003)
- 802.11n (cuarta generación) (2009)
- 802.11ac (quinta generación) (2013)

Estos estándares representan diferentes generaciones de Wi-Fi, cada una con mejoras en velocidad, alcance y capacidad de conexión, adaptándose a las crecientes necesidades de conectividad de los usuarios.

II.3. Enrutamiento de paquetes

II.3.1. Tablas de enrutamiento

La división en subredes es un proceso fundamental para segmentar redes grandes en unidades más pequeñas, lo que resulta en la creación de grupos más manejables de dispositivos y servicios. Este proceso se lleva a cabo con los siguientes objetivos:

- Controlar el tráfico al limitar las emisiones de broadcast dentro de cada subred.
- Reducir el tráfico general de la red y mejorar su rendimiento.

La división en subredes implica la segmentación de una red en varios espacios de red más pequeños, también conocidos como subredes. Este enfoque ayuda a optimizar el flujo de datos y a administrar de manera más efectiva los recursos de red.

II.3.2. Comunicación entre subredes

Para facilitar la comunicación entre dispositivos ubicados en diferentes redes y subredes, es fundamental contar con un router. Cada interfaz del router debe configurarse con una dirección de host IPv4 que pertenezca a la red o subred a la cual se conecta dicha interfaz.

Las funciones clave del router incluyen:

1. **Facilitar la Comunicación Interredes:** El router dirige el tráfico entre redes y subredes, asegurando que los paquetes de datos lleguen a su destino correcto.
2. **Asignar Gateway Predeterminado:** Cada dispositivo en una red o subred utiliza la interfaz del router conectada a su LAN como su puerta de enlace predeterminada, a través de la cual se dirige el tráfico fuera de la red local.

La presencia del router en una red es esencial para garantizar una comunicación eficiente y efectiva entre dispositivos ubicados en diferentes segmentos de la red.

II.3.3. Clases de direcciones IPv4

En el direccionamiento con IPv4, se emplean diferentes tipos de redes con el fin de adaptarse a diversas escalas, ya sean grandes, medianas o pequeñas. En la actualidad, los routers de Internet utilizan tanto protocolos de enrutamiento dinámico de pasarela interior (IGP) como protocolos EGP classless. Para optimizar el uso de direcciones IP y evitar desperdiciarlas, se implementa el concepto de Máscaras de Subred de Tamaño Variable (VLSM, por sus siglas en inglés).

Las clases de direcciones IPv4 más utilizadas son A, B y C, junto con las clases E para Multicast y las direcciones reservadas para uso experimental o de pruebas.

Para calcular subredes, es crucial definir el objetivo: ¿cuántas subredes se necesitan dentro de una red más grande o cómo calcular la subred en función del número máximo de hosts a alojar?

Pasos para calcular subredes dentro de una red más grande:

1. Convertir el número de redes deseado a binario.
2. Definir la máscara de subred predeterminada y convertirla a binario.
3. Reservar los bits necesarios para las nuevas subredes en la máscara de subred, comenzando desde el primer "0".
4. Ajustar la máscara de subred con los bits reservados.
5. Determinar el número de subredes posibles utilizando el valor binario de los bits reservados.
6. Calcular el rango de direcciones IP para cada subred.

Por ejemplo, al calcular 40 subredes dentro de la red 192.168.1.0/24, se reservan 6 bits en la máscara de subred, lo que resulta en una máscara /30 o 255.255.255.252. Esto permite crear 4 subredes, con rangos de direcciones IP específicos para cada una.

Este enfoque permite maximizar el uso de direcciones IP y adaptar el direccionamiento de manera eficiente a las necesidades específicas de la red.

II.3.4. Calcular subredes en función del máximo número de hosts por subred

En este ejemplo, se realiza el cálculo de cuántos hosts pueden alojarse dentro de una subred que forma parte de una red más extensa. En una red 192.168.1.0/24, se dispone de un total de 254 hosts debido a que la primera dirección es reservada para la red y la última para el broadcast.

Supongamos que se requiere alojar un total de 40 hosts en una subred, tomando como base la red principal 192.168.1.0/24. Se debe determinar la máscara de subred apropiada, el rango de direcciones IP disponibles y las direcciones de red y broadcast.

Los pasos para el cálculo son similares al ejemplo anterior, pero con un cambio crucial en el tercer paso:

1. Convertir los 40 hosts a binario, lo que resulta en 101000, indicando un total de 6 bits.
2. La máscara de subred predeterminada es /24 o 255.255.255.0, que en binario es 11111111.11111111.11111111.00000000.
3. Reservar los 6 bits calculados (40 hosts) de derecha a izquierda y completarlos con 1 hasta el extremo izquierdo.
4. La nueva máscara de subred sería: 11111111.11111111.11111111.11000000, equivalente a /26 o 255.255.255.192. La parte final de la máscara (11000000) en decimal representa 192.

Con esta información, se calculan las diferentes subredes dentro de la red 192.168.1.0/24, utilizando un incremento de 64 para cada subred.

El rango de direccionamiento IP de las subredes calculadas se muestra a continuación, donde se emplea la máscara de subred /26:

- 192.168.1.0 – 192.168.1.63 (dirección de red - dirección de broadcast)
- 192.168.1.64 – 192.168.1.127
- 192.168.1.128 – 192.168.1.191
- 192.168.1.192 – 192.168.1.255

En este escenario, solo es posible crear un total de cuatro subredes dentro de la red 192.168.1.0/24, cada una con la capacidad de alojar 40 hosts.

II.4. Tecnología de red LAN

II.4.1. DHCP

El DHCP es una herramienta de interfaz gráfica de usuario (GUI) que facilita la realización de todas las tareas de administración asociadas al servicio DHCP. Esta herramienta permite administrar el servidor DHCP y los datos que utiliza. Es necesario contar con privilegios de superusuario para ejecutar el Administrador de DHCP.

Algunas de las funciones que se pueden llevar a cabo con el Administrador de DHCP son las siguientes:

- Configurar y desconfigurar el servidor DHCP.
- Iniciar, detener y reiniciar el servidor DHCP.
- Desactivar y activar el servicio DHCP.
- Personalizar la configuración del servidor DHCP.

El Administrador de DHCP permite gestionar las direcciones IP, las macros de configuración de red y las opciones de configuración de red mediante los siguientes métodos:

- Agregar y eliminar redes en la administración de DHCP.
- Visualizar, agregar, modificar, eliminar y liberar direcciones IP en la administración de DHCP.
- Visualizar, agregar, modificar y eliminar macros de configuración de red.
- Visualizar, agregar, modificar y eliminar opciones de configuración de red que no sean estándar.

Además, el Administrador de DHCP facilita la administración de los almacenes de datos DHCP con las siguientes capacidades:

- Convertir datos a un nuevo formato de almacén de datos.
- Mover los datos de DHCP de un servidor DHCP a otro exportándolos del primer servidor e importándolos en el segundo.

El Administrador de DHCP también ofrece una amplia ayuda en línea que cubre los procedimientos que permite realizar esta herramienta.

II.5. Protocolos comunes para el transporte de datos

II.5.1. Transmission Control (TCP/IP)

El protocolo TCP/IP es un estándar abierto para aplicaciones en internet, que establece reglas estandarizadas para permitir la comunicación entre equipos en una red como Internet.

Un equipo puede realizar ciertas tareas por sí solo, pero su capacidad se incrementa significativamente cuando puede comunicarse con otros dispositivos. Muchas de las funciones que realizamos con equipos dependen de la comunicación entre ellos.

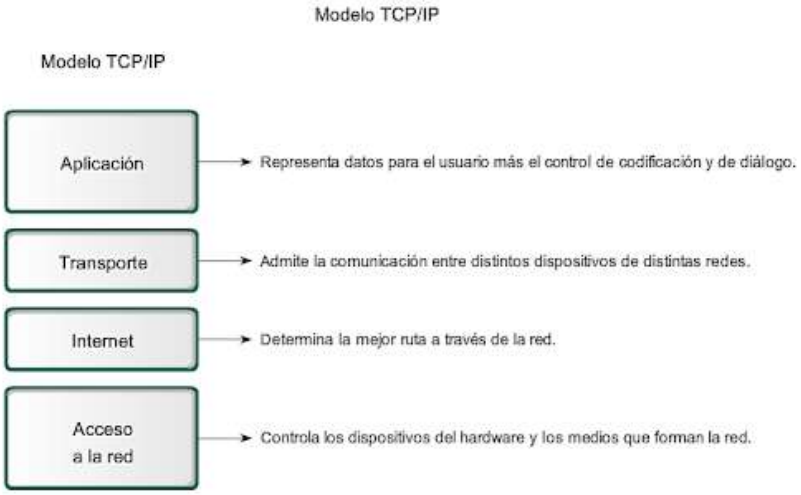


Figura 5. Modelo TCP/IP

II.6. Protocolos y servicios usados directamente en las aplicaciones

II.6.1. HTTP

HTTP es el protocolo fundamental para la comunicación de datos en la World Wide Web. Define cómo los mensajes se formatean y transmiten, y cómo los servidores y los navegadores responden a diversas solicitudes. Utiliza el modelo cliente-servidor donde un navegador web actúa como cliente que solicita recursos y un servidor web proporciona esos recursos en respuesta a las solicitudes del cliente.

II.6.2. SMTP

SMTP es un protocolo estándar utilizado para enviar correos electrónicos a través de internet. Define cómo se transmiten y reciben los mensajes de correo electrónico entre los servidores de correo. SMTP generalmente opera en el puerto 25 y utiliza un conjunto de comandos para la comunicación entre los servidores y los clientes de correo electrónico.

II.6.3. FTP

FTP es un protocolo utilizado para la transferencia de archivos entre sistemas conectados a una red TCP/IP, como internet. Permite la descarga, subida y gestión de archivos desde un servidor FTP a través de un cliente FTP. FTP opera en dos canales separados: el canal de

control para la comunicación de comandos y respuestas, y el canal de datos para la transferencia real de archivos.

II.6.4. DNS

DNS es un sistema que traduce nombres de dominio legibles por humanos (como ejemplo.com) en direcciones IP numéricas (como 192.0.2.1) que las computadoras utilizan para identificar y comunicarse entre sí en internet. Funciona como un directorio telefónico que permite a los usuarios acceder a sitios web y otros recursos utilizando nombres de dominio fáciles de recordar en lugar de direcciones IP numéricas complicadas.

II.7. Protección contra incendios

La protección contra incendios es de vital importancia debido a los posibles daños materiales y, sobre todo, a las pérdidas humanas que puede ocasionar. Por lo tanto, un sistema de prevención contra incendios debe ser eficaz para prevenir, detectar y extinguir el fuego en su fase inicial. Para lograr este objetivo, un sistema contra incendios abarca diversas áreas de diseño que deben ser consideradas, como la hidráulica, eléctrica, mecánica, entre otras.
Las características de estos sistemas se basan en normativas reconocidas a nivel mundial, como por ejemplo la NFPA (Asociación Nacional de Protección contra Incendios), cuyos códigos y normas son ampliamente adoptados debido a que son desarrollados a través de un proceso abierto y consensuado.

II.7.1. Sistemas de detección y alarma de incendios

En la actualidad, existe una amplia oferta de sistemas de detección y alarma contra incendios, con una variedad de fabricantes y sistemas muy completos disponibles en el mercado. Los precios de estos sistemas varían considerablemente dependiendo del tipo y la complejidad del sistema que se requiera instalar, abarcando un amplio rango que va desde cientos hasta miles de dólares.
Además, hay fabricantes especializados que ofrecen dispositivos específicos como sensores de gas, sensores de humo, parlantes, sirenas, entre otros. Estos dispositivos pueden ser integrados y acoplados a un sistema general de detección y alarma contra incendios, permitiendo una personalización según las necesidades específicas de cada instalación.

II.7.2. Tipos de Sistemas

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

Inteligentes: Se refieren a sistemas que permiten identificar en un panel central el lugar exacto donde se origina la alarma de incendio, emiten la alarma correspondiente a los dispositivos anunciadores adecuados y utilizan dispositivos programables para activar bombas o ventiladores.

Ubicación de los detectores: El montaje de los sensores puntuales se basa en ubicar o localizar los detectores en el centro de un rectángulo de 9x9 metros. La distancia desde el centro del detector hasta cualquier extremo no debe exceder los 6.4 metros.

II.7.3. Extintores

Los extintores son dispositivos portátiles diseñados para combatir incendios incipientes, con el propósito de controlar o extinguir cualquier tipo de fuego emergente y prevenir su propagación hacia incendios de mayor magnitud. Existen distintos tipos de extintores recomendados para cada clase de incendio, y en Soler Prevención nos encargaremos de detallar los tipos de extintores disponibles y las recomendaciones específicas para su uso.

Para comprender mejor la función de cada tipo de extintor, es importante primero entender los distintos tipos de fuegos:

- Clase A: Incendios que involucran combustibles sólidos como madera, cartón, plástico, entre otros.
- Clase B: Incendios en los que el combustible es líquido, como aceite, gasolina o pintura.
- Clase C: Fuegos en los que el combustible son gases, como butano, propano o gas natural.
- Clase D: Incendios en los que el combustible es un metal, como magnesio, sodio o aluminio en polvo.

II.8. Pruebas de la red

II.8.1. Probar la conectividad de la red

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

II.8.2. Prueba de Dispositivos

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

II.8.3. Pruebas funcionales

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

II.8.4. Pruebas de las comunicaciones

La prueba de las comunicaciones es normalmente más detallada y rigurosa que la verificación. Se requiere para asegurar que cada componente de un sistema esté operando como debe y que el sistema esté funcionando de acuerdo con los requerimientos locales específicos. Un programa de prueba integral y bien estructurado es aquel que asegura que todos los componentes del sistema sean probados. Entre las medidas de prueba que se pueden considerar figuran las siguientes:

- Desarrollar un conjunto de criterios para la prueba.
- Aplicar pruebas funcionales para determinar si se han satisfecho los criterios de prueba.
- Aplicar evaluaciones de calidad para determinar si se han satisfecho los criterios de prueba.
- Conducir pruebas en condiciones de "laboratorio" y en una variedad de condiciones "reales".
- Conducir pruebas durante un periodo prolongado, para cerciorarse que los sistemas pueden funcionar de manera consistente.
- Conducir "pruebas de carga", simulando tanto como sea posible una variedad de condiciones reales utilizando o excediendo los volúmenes de información que se pueden esperar en una situación concreta.

- Verificar que lo que entra es lo que sale, introduciendo información conocida y verificando que el resultado sea consecuente con ella.

II.9. Monitoreo de la red

El monitoreo de red es una práctica fundamental en la gestión de sistemas informáticos, consistente en la supervisión continua de una red de computadoras en busca de componentes defectuosos o con bajo rendimiento, con el objetivo de detectar problemas de manera temprana y mantener la integridad y eficiencia del sistema. Esta actividad es crucial para garantizar un funcionamiento óptimo de la red y prevenir posibles interrupciones en el servicio.

Herramientas de Monitoreo de Red

1. **Solarwinds**: Solarwinds se destaca como una de las herramientas más reconocidas en el monitoreo de redes. Su principal característica es su capacidad para realizar un mapeo automático de la red y los nodos, sin necesidad de intervención manual. Además, cuenta con una interfaz gráfica poderosa que facilita la visualización de la topología de la red y el estado de sus componentes. Solarwinds ofrece la integración de máquinas virtuales en su proceso de monitorización, lo que lo convierte en una opción atractiva para empresas medianas. Sin embargo, es importante considerar que sus licencias pueden tener un costo elevado en comparación con otras opciones disponibles en el mercado.
2. **GlassWire**: GlassWire es una herramienta especialmente destacada en el monitoreo del uso de datos en dispositivos Android. Permite supervisar el consumo de datos móviles, establecer límites de uso y analizar la actividad de la red WiFi. Esta aplicación proporciona información instantánea sobre las aplicaciones que pueden estar afectando negativamente la conexión a Internet del dispositivo o consumiendo de manera innecesaria los datos móviles.
3. **ManageEngine**: Pertenece al grupo Zoho Group, una empresa de gran renombre en el ámbito tecnológico. ManageEngine se posiciona como una herramienta de monitoreo de redes a tener en cuenta, ofreciendo diversas funcionalidades para la supervisión efectiva de los sistemas informáticos.

Estas herramientas son solo algunas de las opciones disponibles en el mercado para llevar a cabo el monitoreo de redes. La elección de la herramienta más adecuada dependerá de las

necesidades específicas de cada organización, su tamaño, infraestructura tecnológica y presupuesto disponible. Es fundamental seleccionar una herramienta que ofrezca las funcionalidades requeridas y se ajuste a los objetivos y recursos de la empresa.

II.10. Optimización de la red

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

II.11. Herramientas de Software y simulación

II.11.1. Software utilizado

II.11.1.1 Packet Tracer

Packet Tracer es una herramienta de simulación de redes desarrollada por Cisco Systems. Se utiliza principalmente para el aprendizaje y la práctica de redes informáticas. Permite a los usuarios crear topologías de red virtuales, conectar dispositivos de red (como routers, switches, PCs, etc.), configurar sus parámetros y simular el tráfico de datos dentro de estas redes. Es ampliamente utilizado en entornos educativos y académicos para enseñar conceptos de redes y para la preparación de certificaciones de redes.

II.11.1.2 GNS3

GNS3 (Graphical Network Simulator-3) es una plataforma de simulación de redes de código abierto que permite a los usuarios crear redes virtuales complejas utilizando imágenes de dispositivos reales de red, como routers y switches. A diferencia de Packet Tracer, GNS3 se utiliza más comúnmente en entornos profesionales y académicos avanzados donde se requiere la emulación de dispositivos de red más sofisticados y la integración con hardware físico para pruebas de configuración y simulación de redes complejas. GNS3 es conocido por su flexibilidad y capacidad para emular una amplia gama de dispositivos de red.

CAPÍTULO III

COMPONENTE I: Diseño y simulación de la nueva Infraestructura de la red de la Subgobernación de Villa Montes

CAPÍTULO III: COMPONENTE I DISEÑO Y SIMULACIÓN DE LA NUEVA INFRAESTRUTURA DE LA RED DE LA SUBGOBERNACIÓN DE VILLA MONTES

III.1. Componente I: Diseño y simulación de la nueva arquitectura de la red de la subgobernación de Villa Montes

III.1.1. Fase 1. Análisis de requerimientos

III.1.1.1. Análisis de las metas del negocio

III.1.1.1. Modelo de Caso de Uso del Negocio General de la Subgobernación de Villa Montes

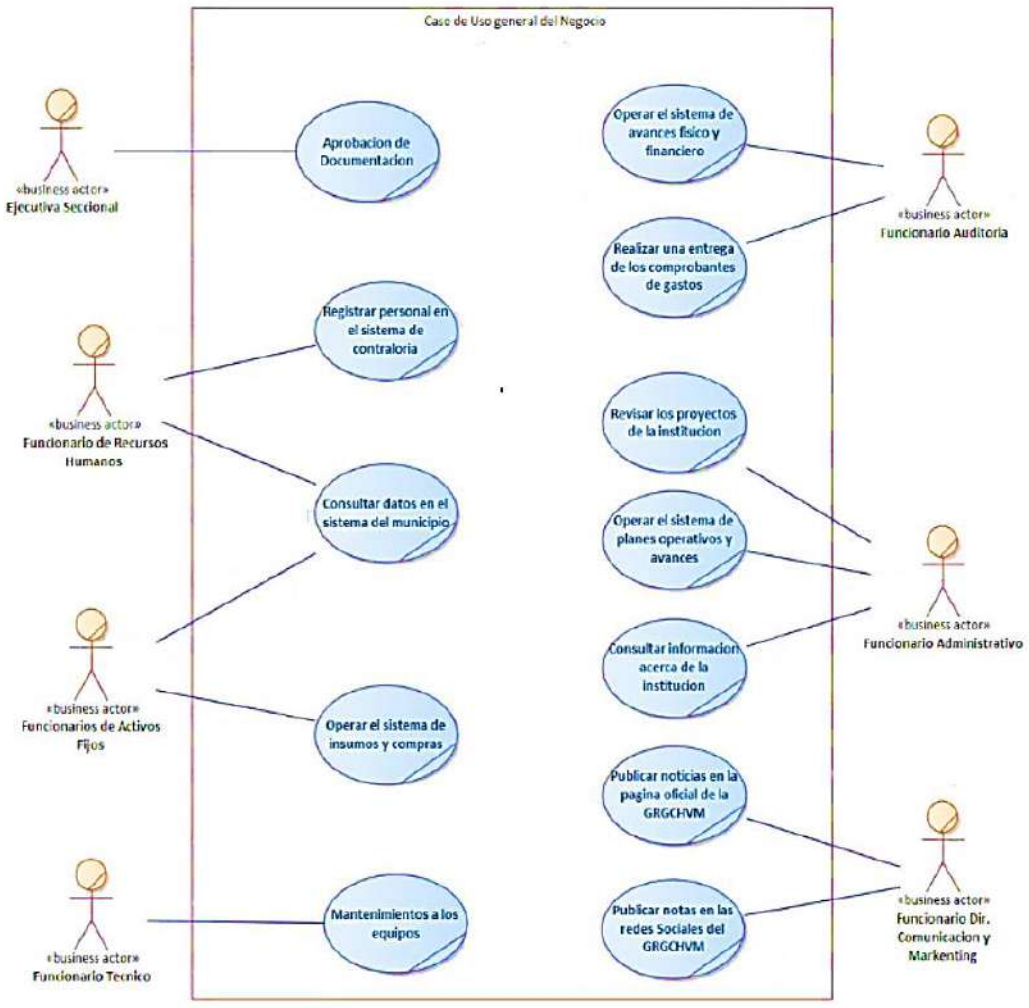


Figura 6. Caso de Uso del Negocio

III.1.1.2. Análisis de las metas técnicas

El análisis de las metas técnicas para la propuesta de un diseño de red de comunicación para la Subgobernación de Villa Montes se centra en resolver las limitaciones de la red improvisada actual, que no interconecta los 6 bloques existentes. La primera meta es interconectar todos los bloques para permitir una comunicación fluida y eficiente entre las dependencias, mejorando la coordinación y el intercambio de información. La segunda meta es estandarizar la red según normas industriales reconocidas, como IEEE 802.3 y IEEE 802.11, para garantizar compatibilidad y facilidad de mantenimiento. Se busca también asegurar la redundancia y confiabilidad mediante la implementación de mecanismos de respaldo que minimicen el impacto de posibles fallos. La seguridad de la red es otra meta clave, que incluye la protección contra amenazas internas y externas mediante firewalls y sistemas de detección de intrusos. La capacidad de expansión debe estar contemplada para soportar futuros crecimientos sin necesidad de una reestructuración completa. Finalmente, se pretende facilitar la administración y el mantenimiento mediante herramientas de gestión centralizadas para un control eficiente de la red. Estas metas se validarán mediante simulaciones en Packet Tracer, asegurando que la propuesta optimice la comunicación y mejore la infraestructura de red de la Subgobernación.

III.1.1.4. Análisis de la red Existente

La red actual de la Subgobernación de Villa Montes enfrenta diversas limitaciones debido a su estructura improvisada y la falta de interconexión entre los 6 bloques que la conforman. Cada bloque opera de manera aislada, lo que dificulta la coordinación y el intercambio de información entre dependencias. La red existente se ha desarrollado sin un diseño planificado, lo que ha resultado en una infraestructura desorganizada y obsoleta, con equipamiento antiguo que no soporta tecnologías modernas. Esta situación limita la capacidad de expansión, reduce el rendimiento durante períodos de alta demanda y presenta una seguridad insuficiente, ya que carece de firewalls y otras medidas de protección. Actualmente, la Subgobernación cuenta con 170 trabajadores distribuidos en 6 oficinas, con un total de 125 equipos de escritorio, 35 portátiles y 6 impresoras. La falta de una red unificada y moderna subraya la necesidad de una propuesta de diseño que integre los bloques, mejore el rendimiento, la seguridad y la capacidad de expansión de la red.

III.1.1.3.1. Ambiente de Distribución actual de la Oficina de Seragro

Figura 7. Ambiente de Distribución actual de la Oficina de Seragro

III.1.1.3.2. Ambiente de Distribución actual de la Oficina de despacho, recursos humanos y sistemas

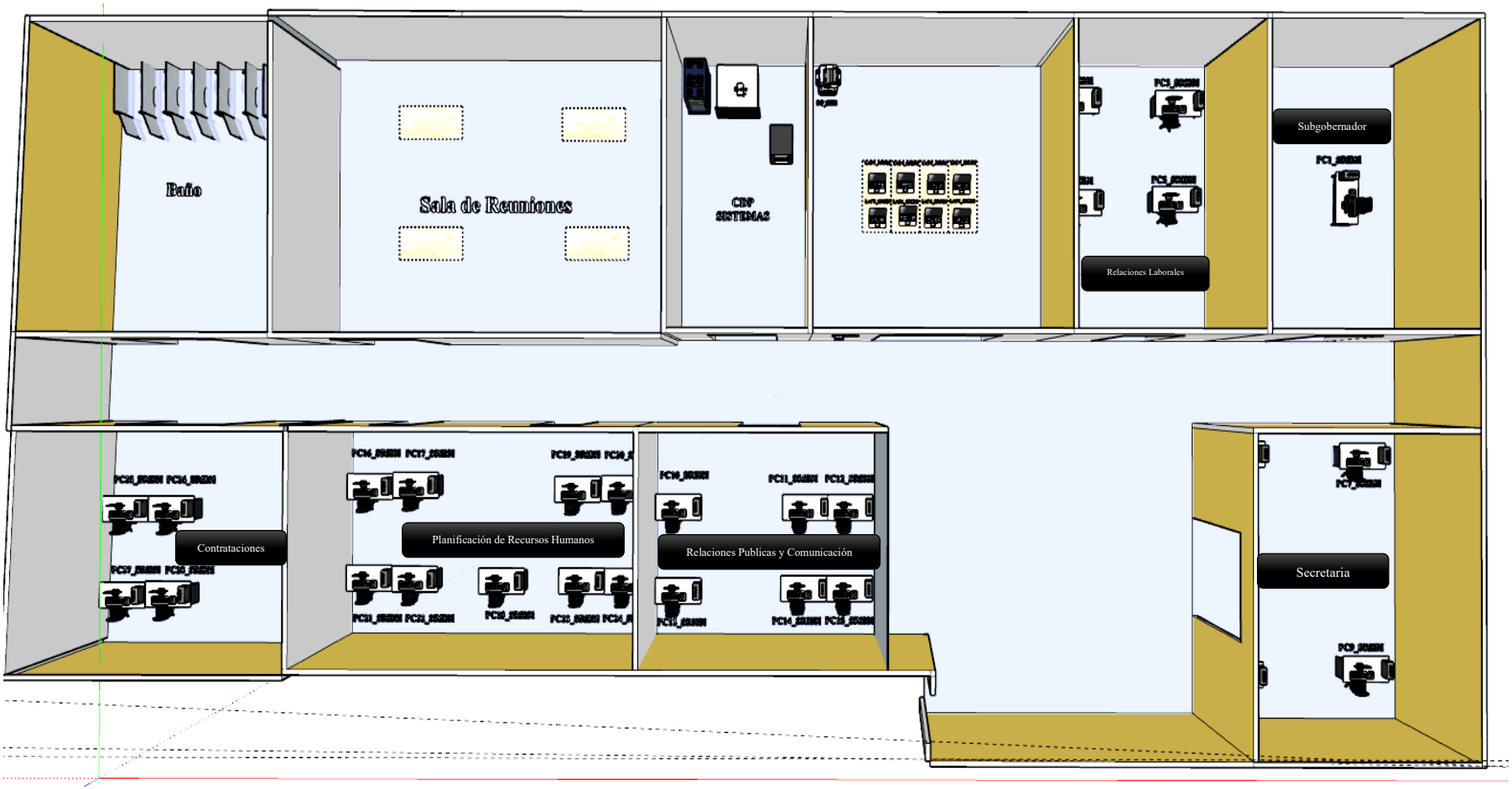


Figura 8. Ambiente de Distribución actual de la Oficina de despacho, recursos humanos y sistemas

III.1.1.3.3. Ambiente de Distribución actual de la Oficina de secretaria de Obras Publica, almacén, secretaria de Planificación

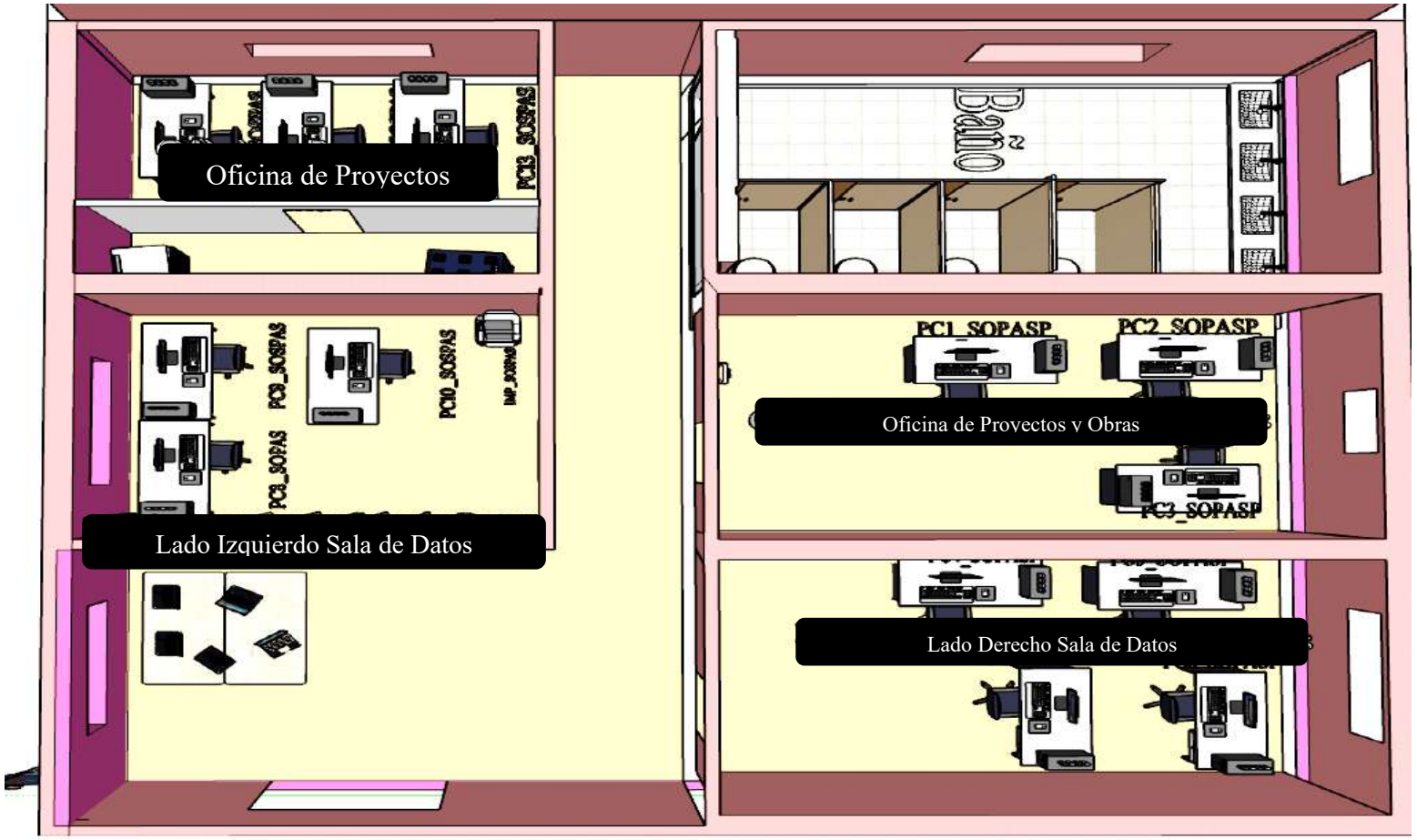


Figura 9. Ambiente de Distribución actual de la Oficina de secretaria de Obras Publica, almacén, secretaria de Planificación

III.1.1.3.4. Ambiente de Distribución actual de la Oficina de Dirección Jurídica

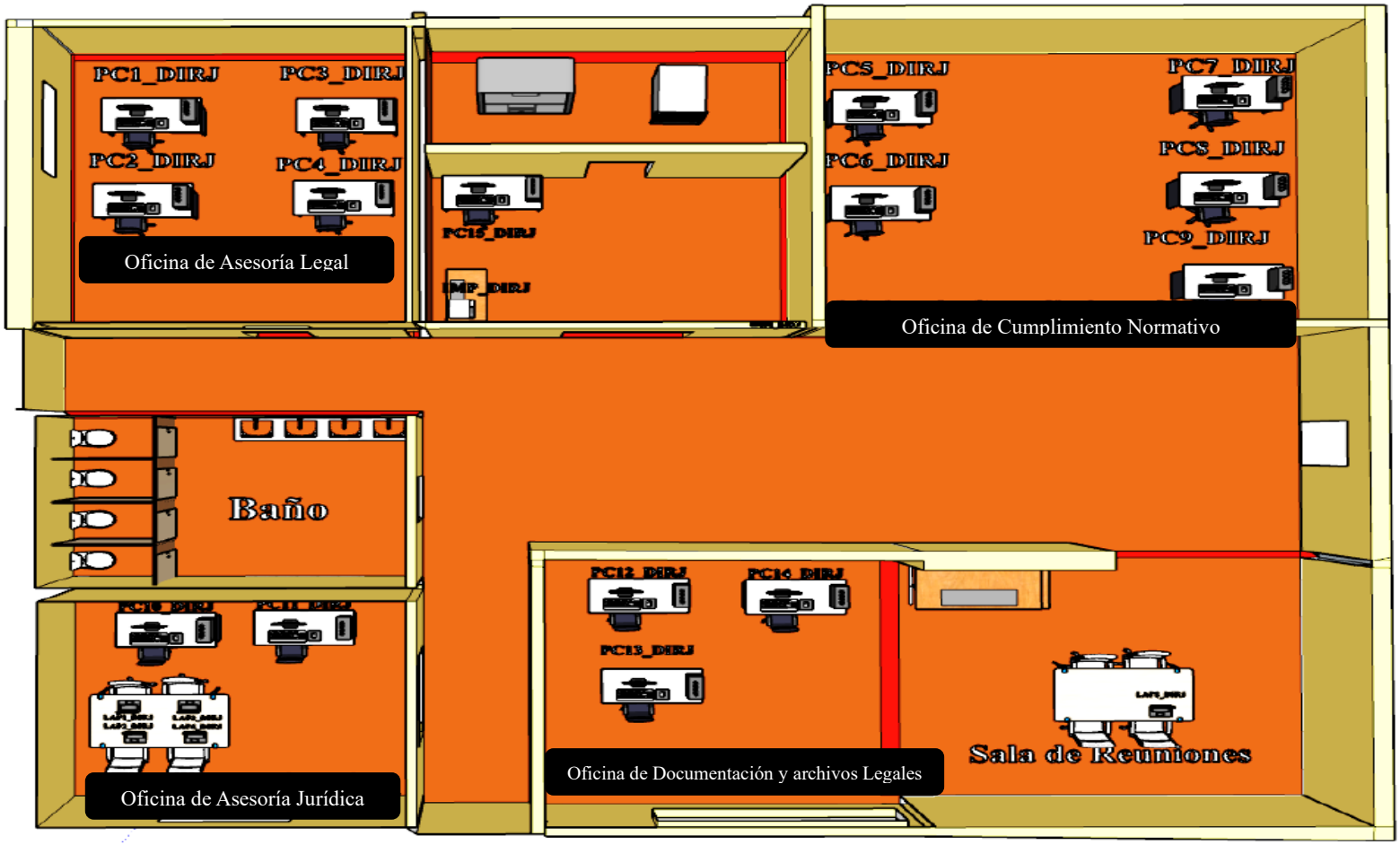


Figura 10. Ambiente de Distribución actual de la Oficina Dirección Jurídica

III.1.1.3.5. Ambiente de Distribución actual de la Oficina de economía y finanzas

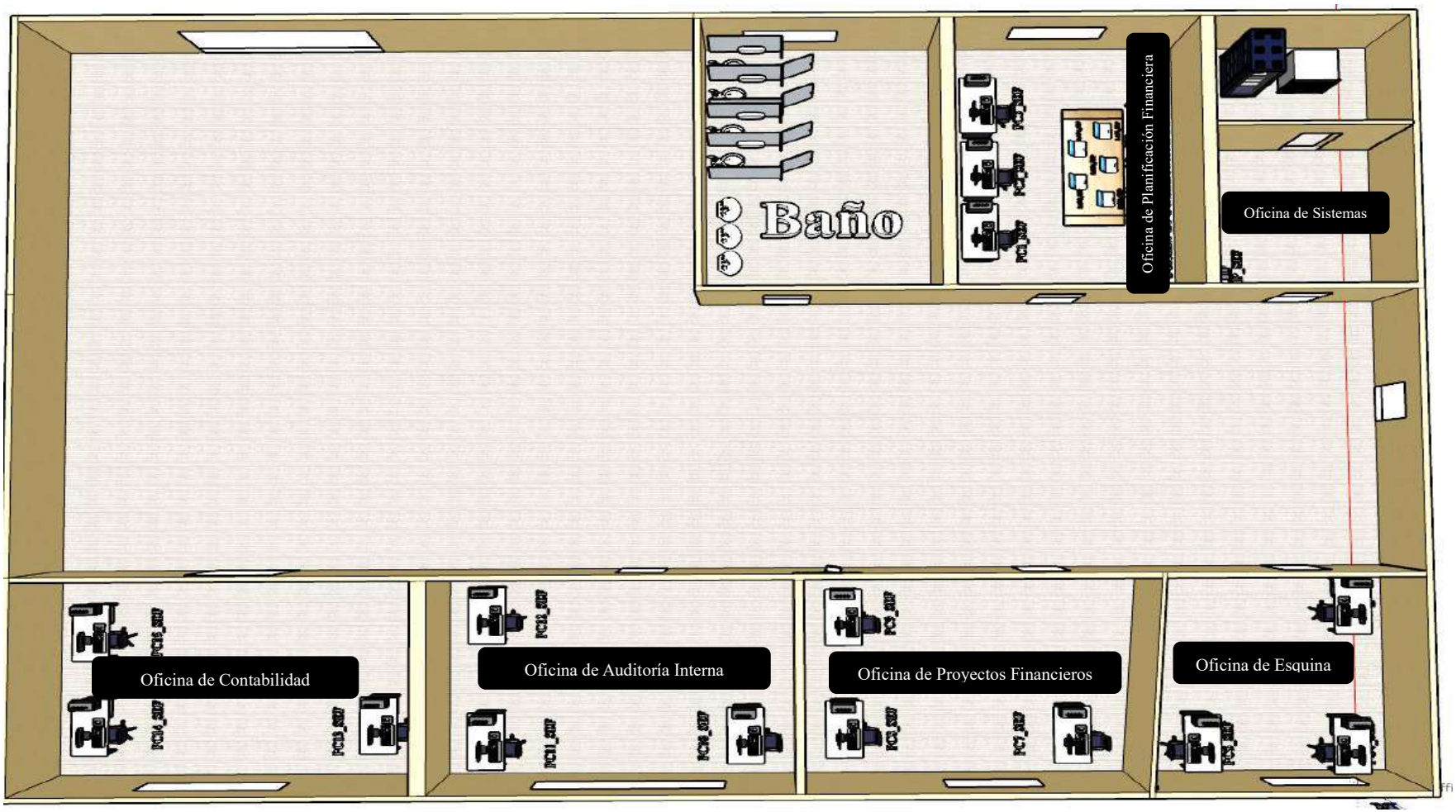


Figura 11. *Ambiente de Distribución actual de la Oficina de economía y finanzas*

III.1.1.3.6. Ambiente de Distribución actual de la Oficina de secretaria de desarrollo productivo

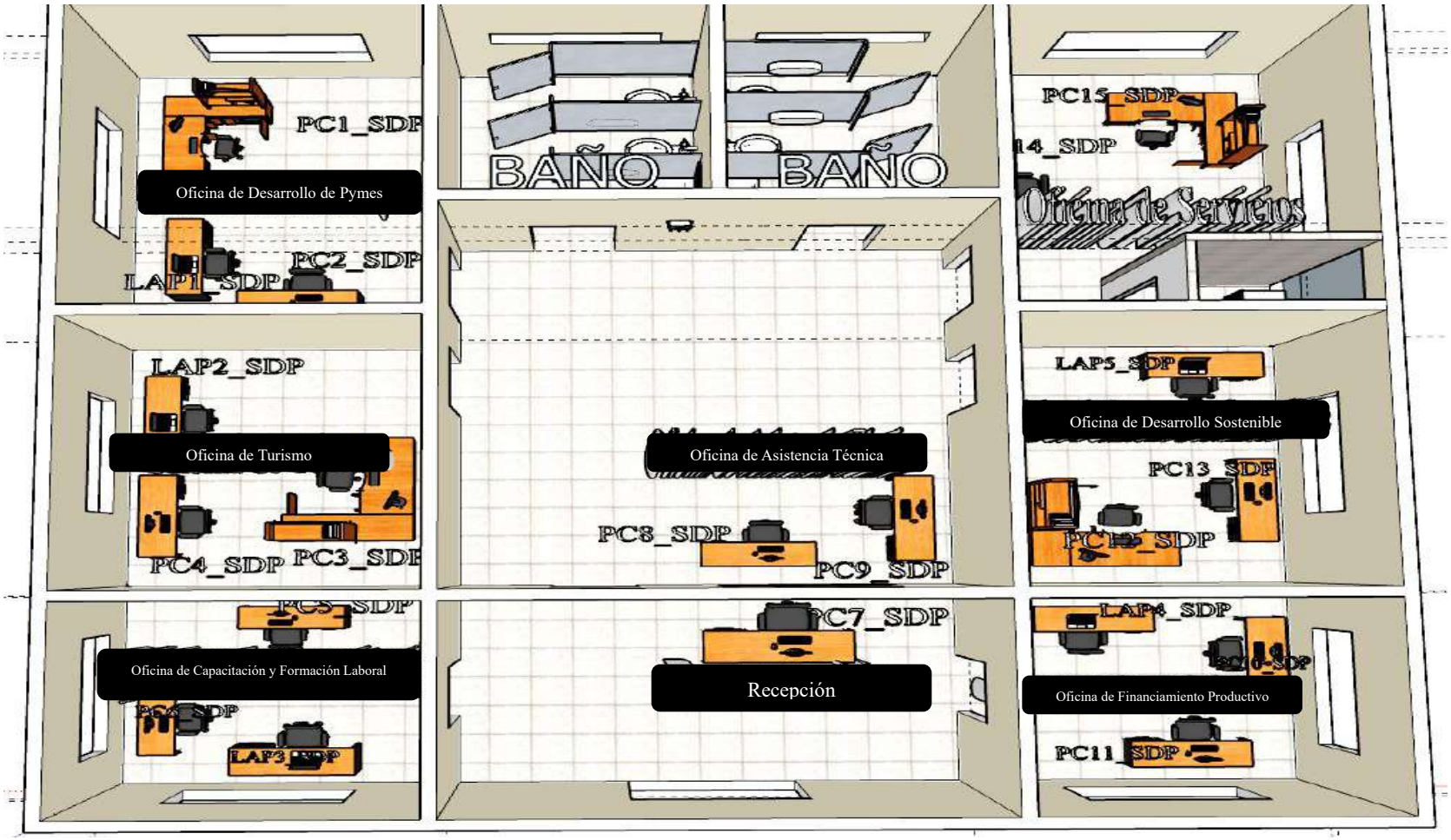


Figura 12. *Ambiente de Distribución actual de la Oficina de secretaria de desarrollo productivo*

III.1.1.4. Análisis de tráfico existente

Se evidencia un flujo de tráfico existente en la red, principalmente orientado hacia la conexión a Internet, utilizado para procesar los trámites de compras a través de las plataformas estatales, lo cual constituye la actividad principal. Asimismo, se utiliza para acceder a los sistemas internos alojados en la intranet, que abarcan áreas como compras, contabilidad, finanzas y administración. Además, se emplea para acceder a sitios gubernamentales del estado.

Por otro lado, se verificó que la red improvisada presenta vulnerabilidad en la seguridad tanto físicas como lógicas, por ejemplo, en la seguridad lógica se logra observar ataques de infiltración, contraseñas de fácil acceso, entre otros, viendo por otra parte en la seguridad física los equipos están expuestos a personal no autorizado e incluso mal intencionado debido a su ubicación y mala instalación. Otro problema físico de gran importancia en la red existente son las ubicaciones de los equipos ya que son propensos a problemas climáticos como sobrecalentamientos, humedad, entre otros.

El análisis del tráfico en la red de la Subgobernación de Villa Montes revela varios problemas significativos debido a la estructura improvisada y la falta de interconexión entre los 6 bloques. La red actual no está optimizada para manejar el tráfico de datos entre los bloques, lo que resulta en una fragmentación del tráfico y una sobrecarga en los puntos de interconexión. Esta falta de planificación ha llevado a un rendimiento subóptimo, con problemas de congestión durante períodos de alta demanda. La red también carece de herramientas adecuadas para el monitoreo y control del tráfico, lo que impide la identificación y resolución proactiva de problemas. La capacidad de ancho de banda es insuficiente para soportar el volumen de datos necesario, y la falta de segmentación adecuada contribuye a conflictos de tráfico y dificultades en la gestión del rendimiento. Estos problemas destacan la necesidad de un diseño de red que mejore la comunicación entre bloques, optimice el ancho de banda, y facilite la gestión y monitoreo del tráfico para asegurar un rendimiento eficiente y estable.

III.1.2. Fase 2: Desarrollar Diseño Lógico

III.1.2.1. Diseño de la Topología de red

Para realizar el diseño de la topología de la red para la Subgobernación de Villa Montes. La propuesta de topología contempla una topología en estrella o jerárquica, en la que cada bloque se conecta a un router central, que a su vez está interconectado con otros switches para asegurar una comunicación fluida entre todos los bloques. Esta estructura permitirá una interconexión eficiente, minimizando la congestión y mejorando el rendimiento. Además, la topología incluirá mecanismos de redundancia, como enlaces de respaldo y equipos en alta disponibilidad, para garantizar alta disponibilidad y confiabilidad. Se segmentar el tráfico y mejorar la gestión del rendimiento, y se integrarán herramientas de monitoreo para supervisar el tráfico y detectar problemas en tiempo real. La capacidad de expansión será un factor clave en el diseño, asegurando que la red pueda soportar futuros crecimientos sin necesidad de una reestructuración significativa. Esta topología será validada mediante simulaciones en Packet Tracer para asegurar que cumpla con los objetivos de comunicación, rendimiento y seguridad

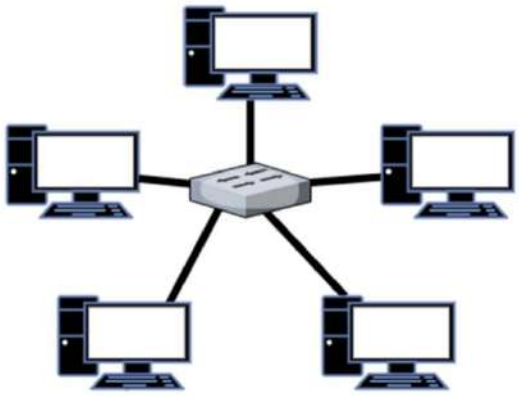


Figura 13. Topología Estrella

III.1.2.2. Diseño modelos de direccionamiento y hostname

III.1.2.2.1. Direccionamiento

Para realizar la propuesta de direccionamiento contempla el uso de un esquema de **direcciones IP privadas** donde se necesita conocer la cantidad total de host que se va a utilizar, para lo cual se considera todos los equipos que requieran un direccionamiento IP.

Cada bloque de la Subgobernación recibirá un rango específico de direcciones IP para asegurar que los dispositivos dentro de cada bloque puedan comunicarse eficazmente,

mientras se mantiene la capacidad de interconexión entre los bloques a través de subredes correctamente configuradas.

Además, se aplicarán políticas de asignación dinámica de direcciones utilizando DHCP para simplificar la administración de direcciones IP y permitir una fácil integración de nuevos dispositivos. La correcta implementación y verificación del direccionamiento serán validadas a través de simulaciones en Packet Tracer para garantizar la funcionalidad del esquema propuesto.

Los dispositivos que requieren una dirección IP son:

- 125 computadoras de escritorio
- 35 portátiles
- 6 impresoras
- 6 servidores DHCP
- 1 Router
- 6 switches
- 6 Access Points

Una vez establecido la cantidad de dispositivos que se conectarán a la red, se considera la segmentación de red asignando un rango de direcciones IP. Para lo cual se debe determinar que todos los hosts formarán parte de subredes.

Por la cantidad de dispositivos que tendrán conectividad se considera trabajar con IP privadas Clase C versión 4, la red tendrá dirección IP 192.168.1.0 /24 que se dividirá en 6 subredes que será distribuidas de la siguiente manera:

Subred	N.º de Hosts	IP de red	Máscara	Primer Host	Último Host	Broadcast
Subred A	62	192.168.1.0 /26	255.255.255.192	192.168.1.1	192.168.1.62	192.168.1.63
Subred B	62	192.168.1.64/26	255.255.255.192	192.168.1.65	192.168.1.126	192.168.1.127
Subred C	30	192.168.1.128/27	255.255.255.224	192.168.1.129	192.168.1.158	192.168.1.159
Subred D	30	192.168.1.160/27	255.255.255.224	192.168.1.161	192.168.1.190	192.168.1.191
Subred E	30	192.168.1.192/27	255.255.255.224	192.168.1.193	192.168.1.222	192.168.1.223
Subred F	30	192.168.1.224/27	255.255.255.224	192.168.1.225	192.168.1.254	192.168.1.255

Tabla 5. *División de las subredes de la institución*

Se han definido seis subredes para el direccionamiento de la red en la Subgobernación de Villa Montes, cada una optimizada para satisfacer las necesidades específicas de las diferentes oficinas. La distribución de estas subredes es la siguiente:

- **Subred A**: Diseñada para la oficina de Seragro, esta subred incluye 1 switch, 1 servidor DHCP, 35 equipos de escritorio, 10 portátiles y 1 impresora. Se asignará un rango de direcciones IP que soporte hasta 62 hosts, permitiendo la expansión futura de equipos si es necesario.
- **Subred B**: Asignada para las oficinas de Despacho, Recursos Humanos y Sistemas, así como para el cuarto de telecomunicaciones, esta subred estará equipada con 1 servidor DHCP, 1 router, 1 switch, 30 equipos de escritorio, 8 portátiles y 1 impresora. El rango de direcciones IP estará dimensionado para soportar más hosts, facilitando la adición de equipos futuros y el funcionamiento eficiente del cuarto de telecomunicaciones.
- **Subred C**: Destinada para las oficinas de Secretaría de Obras Públicas, Almacén y Secretaría de Planificación, esta subred contará con 1 switch, 1 servidor DHCP, 15 equipos de escritorio, 5 portátiles y 1 impresora. Se asignará un rango de direcciones IP con capacidad para 30 hosts, permitiendo la incorporación de equipos adicionales en el futuro.
- **Subred D**: Para la oficina de Secretaría de Economía y Finanzas, se ha previsto 1 switch, 1 servidor DHCP, 15 equipos de escritorio, 5 portátiles y 1 impresora. El rango de direcciones IP estará dimensionado para soportar hasta 30 hosts, con posibilidad de expansión.
- **Subred E**: Diseñada para la oficina de Dirección Jurídica, esta subred incluirá 1 switch, 1 servidor DHCP, 15 equipos de escritorio, 5 portátiles y 1 impresora. Se asignará un rango de direcciones IP que permita la conexión de hasta 30 hosts, con espacio para añadir equipos adicionales en el futuro.
- **Subred F**: Para la oficina de Secretaría de Desarrollo Productivo, se dispondrá de 1 switch, 1 servidor DHCP, 15 equipos de escritorio, 5 portátiles y 1 impresora. La asignación de direcciones IP permitirá la conexión de hasta 30 hosts, con previsión de expansión para futuros equipos.

Cada subred está diseñada para ser escalable y flexible, permitiendo la integración de nuevos dispositivos y adaptándose a las necesidades futuras de la Subgobernación.

III.1.2.2.2. Host-name

Con respecto a los host-name se utilizará nombres simples para asignar a los equipos:

Subred A_ Oficina De Seragro

Figura 14. Subred A_ Oficina De Seragro

Subred B _ Oficina de despacho, recursos humanos y sistemas

Figura 15. Subred B _ Oficina de despacho, recursos humanos y sistemas

Subred C _ Oficina de Secretaria de Obras Publica, almacén, Secretaria de Planificación

Figura 16. Subred C _ Oficina de Secretaria de Obras Publica, almacén, Secretaria de Planificación

Subred D_ Oficina de secretaría de economía y Finanzas

Figura 17. Subred D_ Oficina de secretaría de economía y Finanzas

Subred E_ Oficina de Dirección Jurídica

Figura 18. Subred E_ Oficina de Dirección Jurídica

Subred F_ Oficina de secretaria de desarrollo productivo

Figura 19. Subred F_ Oficina de secretaria de desarrollo productivo

Subred	Equipo	Interfaz	Dirección IP	Máscara de Red	Gateway
Subred A	SERAGRO_SWITCH	Fa	192.168.1.1	255.255.255.192	No aplicable
	SERAGRO -SWITCH	NIC	192.168.1.2	255.255.255.192	192.168.1.1
	SERAGRO -DHCP	NIC	192.168.1.3	255.255.255.192	192.168.1.1
	SERAGRO -MAQ1	NIC	192.168.1.4	255.255.255.192	192.168.1.1
	SERAGRO -MAQ2	NIC	192.168.1.5	255.255.255.192	192.168.1.1
	SERAGRO -MAQ3	NIC	192.168.1.6	255.255.255.192	192.168.1.1
	SERAGRO -MAQ 4	NIC	192.168.1.7	255.255.255.192	192.168.1.1
	SERAGRO -MAQ5	NIC	192.168.1.8	255.255.255.192	192.168.1.1
	SERAGRO -MAQ 6	NIC	192.168.1.9	255.255.255.192	192.168.1.1
	SERAGRO -MAQ7	NIC	192.168.1.10	255.255.255.192	192.168.1.1
	SERAGRO-MAQ8	NIC	192.168.1.11	255.255.255.192	192.168.1.1
	SERAGRO-MAQ9	NIC	192.168.1.12	255.255.255.192	192.168.1.1
	SERAGRO-MAQ10	NIC	192.168.1.13	255.255.255.192	192.168.1.1
	SERAGRO-MAQ11	NIC	192.168.1.14	255.255.255.192	192.168.1.1
	SERAGRO-MAQ12	NIC	192.168.1.15	255.255.255.192	192.168.1.1
	SERAGRO-MAQ13	NIC	192.168.1.16	255.255.255.192	192.168.1.1
	SERAGRO_-MAQ14	NIC	192.168.1.17	255.255.255.192	192.168.1.1
	SERAGRO-MAQ15	NIC	192.168.1.18	255.255.255.192	192.168.1.1
	SERAGRO-MAQ16	NIC	192.168.1.19	255.255.255.192	192.168.1.1
	SERAGRO-MAQ17	NIC	192.168.1.20	255.255.255.192	192.168.1.1
	SERAGRO-MAQ18	NIC	192.168.1.21	255.255.255.192	192.168.1.1
	SERAGRO-MAQ19	NIC	192.168.1.22	255.255.255.192	192.168.1.1
	SERAGRO-MAQ20	NIC	192.168.1.23	255.255.255.192	192.168.1.1
	SERAGRO-MAQ21	NIC	192.168.1.24	255.255.255.192	192.168.1.1
	SERAGRO-MAQ22	NIC	192.168.1.25	255.255.255.192	192.168.1.1
	SERAGRO-MAQ23	NIC	192.168.1.26	255.255.255.192	192.168.1.1
	SERAGRO-MAQ24	NIC	192.168.1.27	255.255.255.192	192.168.1.1
	SERAGRO-MAQ25	NIC	192.168.1.28	255.255.255.192	192.168.1.1
	SERAGRO-MAQ26	NIC	192.168.1.29	255.255.255.192	192.168.1.1
	SERAGRO-MAQ27	NIC	192.168.1.30	255.255.255.192	192.168.1.1
	SERAGRO-MAQ28	NIC	192.168.1.31	255.255.255.192	192.168.1.1
	SERAGRO-MAQ29	NIC	192.168.1.32	255.255.255.192	192.168.1.1
	SERAGRO-MAQ30	NIC	192.168.1.33	255.255.255.192	192.168.1.1
	SERAGRO-MAQ31	NIC	192.168.1.34	255.255.255.192	192.168.1.1
	SERAGRO-MAQ32	NIC	192.168.1.35	255.255.255.192	192.168.1.1

	SERAGRO-MAQ33	NIC	192.168.1.36	255.255.255.192	192.168.1.1
	SERAGRO-MAQ34	NIC	192.168.1.37	255.255.255.192	192.168.1.1
	SERAGRO-MAQ35	NIC	192.168.1.38	255.255.255.192	192.168.1.1
	SERAGRO-MAQ36	NIC	192.168.1.39	255.255.255.192	192.168.1.1
	SERAGRO-MAQ37	NIC	192.168.1.40	255.255.255.192	192.168.1.1
	SERAGRO-MAQ38	NIC	192.168.1.41	255.255.255.192	192.168.1.1
	SERAGRO-MAQ39	NIC	192.168.1.42	255.255.255.192	192.168.1.1
	SERAGRO-MAQ40	NIC	192.168.1.43	255.255.255.192	192.168.1.1
	SERAGRO-MAQ41	NIC	192.168.1.44	255.255.255.192	192.168.1.1
	SERAGRO-MAQ42	NIC	192.168.1.45	255.255.255.192	192.168.1.1
	SERAGRO-MAQ43	NIC	192.168.1.46	255.255.255.192	192.168.1.1
	SERAGRO- MAQ44	NIC	92.168.1.47	255.255.255.192	192.168.1.1

Tabla 6. *Direccionamiento de la Subred A*

Subred	Equipo	Interfaz	Dirección IP	Máscara de Red	Gateway
Subred B	DRHSI_SWITCH	Fa	192.168.1.65	255.255.255.192	No aplicable
	DRHSI_DHCP	NIC	192.168.1.66	255.255.255.192	192.168.1.65
	DRHSI_-MAQ1	NIC	192.168.1.68	255.255.255.192	192.168.1.65
	DRHSI_-MAQ2	NIC	192.168.1.68	255.255.255.192	192.168.1.65
	DRHSI_-MAQ3	NIC	192.168.1.69	255.255.255.192	192.168.1.65
	DRHSI_-MAQ4	NIC	192.168.1.70	255.255.255.192	192.168.1.65
	DRHSI_-MAQ5	NIC	192.168.1.71	255.255.255.192	192.168.1.65
	DRHSI_-MAQ6	NIC	192.168.1.72	255.255.255.192	192.168.1.65
	DRHSI_-MAQ7	NIC	192.168.1.73	255.255.255.192	192.168.1.65
	DRHSI_-MAQ8	NIC	192.168.1.74	255.255.255.192	192.168.1.65
	DRHSI_-MAQ9	NIC	192.168.1.75	255.255.255.192	192.168.1.65
	DRHSI_-MAQ10	NIC	192.168.1.76	255.255.255.192	192.168.1.65
	DRHSI_-MAQ11	NIC	192.168.1.77	255.255.255.192	192.168.1.65
	DRHSI_-MAQ12	NIC	192.168.1.78	255.255.255.192	192.168.1.65
	DRHSI_-MAQ13	NIC	192.168.1.79	255.255.255.192	192.168.1.65
	DRHSI_-MAQ14	NIC	192.168.1.80	255.255.255.192	192.168.1.65
	DRHSI_-MAQ15	NIC	192.168.1.81	255.255.255.192	192.168.1.65
	DRHSI_-MAQ16	NIC	192.168.1.82	255.255.255.192	192.168.1.65
	DRHSI_-MAQ17	NIC	192.168.1.83	255.255.255.192	192.168.1.65
	DRHSI_-MAQ18	NIC	192.168.1.84	255.255.255.192	192.168.1.65
	DRHSI_-MAQ19	NIC	192.168.1.85	255.255.255.192	192.168.1.65
	DRHSI_-MAQ20	NIC	192.168.1.86	255.255.255.192	192.168.1.65

	DRHSI_-MAQ21	NIC	192.168.1.87	255.255.255.192	192.168.1.65
	DRHSI_-MAQ22	NIC	192.168.1.88	255.255.255.192	192.168.1.65
	DRHSI_-MAQ23	NIC	192.168.1.89	255.255.255.192	192.168.1.65
	DRHSI_-MAQ24	NIC	192.168.1.90	255.255.255.192	192.168.1.65
	DRHSI_-MAQ25	NIC	192.168.1.91	255.255.255.192	192.168.1.65
	DRHSI_-MAQ26	NIC	192.168.1.92	255.255.255.192	192.168.1.65
	DRHSI_-MAQ27	NIC	192.168.1.93	255.255.255.192	192.168.1.65
	DRHSI_-MAQ28	NIC	192.168.1.94	255.255.255.192	192.168.1.65
	DRHSI_-MAQ29	NIC	192.168.1.95	255.255.255.192	192.168.1.65
	DRHSI_-MAQ30	NIC	192.168.1.96	255.255.255.192	192.168.1.65
	DRHSI_-MAQ31	NIC	192.168.1.97	255.255.255.192	192.168.1.65
	DRHSI_-MAQ32	NIC	192.168.1.98	255.255.255.192	192.168.1.65
	DRHSI_-MAQ33	NIC	192.168.1.99	255.255.255.192	192.168.1.65
	DRHSI_-MAQ34	NIC	192.168.1.100	255.255.255.192	192.168.1.65
	DRHSI_-MAQ35	NIC	192.168.1.101	255.255.255.192	192.168.1.65
	DRHSI_-MAQ36	NIC	192.168.1.102	255.255.255.192	192.168.1.65
	DRHSI_-MAQ37	NIC	192.168.1.103	255.255.255.192	192.168.1.65
	DRHSI_-MAQ38	NIC	192.168.1.104	255.255.255.192	192.168.1.65
	DRHSI_-I MAQ39	NIC	192.168.1.105	255.255.255.192	192.168.1.65

Tabla 7. *Direccionamiento de la Subred B*

Subred	Equipo	Interfaz	Dirección IP	Máscara de Red	Gateway
Subred C	SOPASP_SWITCH	Fa	192.168.1.129	255.255.255.224	No aplicable
	SOPASP_-DHCP	NIC	192.168.1.130	255.255.255.224	192.168.1.129
	SOPASP_-MAQ1	NIC	192.168.1.132	255.255.255.224	192.168.1.129
	SOPASP_-MAQ2	NIC	192.168.1.133	255.255.255.224	192.168.1.129
	SOPASP_-MAQ3	NIC	192.168.1.134	255.255.255.224	192.168.1.129
	SOPASP_-MAQ4	NIC	192.168.1.135	255.255.255.224	192.168.1.129
	SOPASP_-MAQ5	NIC	192.168.1.136	255.255.255.224	192.168.1.129
	SOPASP_-MAQ6	NIC	192.168.1.137	255.255.255.224	192.168.1.129
	SOPASP_-MAQ7	NIC	192.168.1.138	255.255.255.224	192.168.1.129
	SOPASP_-MAQ8	NIC	192.168.1.139	255.255.255.224	192.168.1.129
	SOPASP_-MAQ9	NIC	192.168.1.140	255.255.255.224	192.168.1.129
	SOPASP_-MAQ10	NIC	192.168.1.141	255.255.255.224	192.168.1.129
	SOPASP_-MAQ11	NIC	192.168.1.142	255.255.255.224	192.168.1.129
	SOPASP_-MAQ12	NIC	192.168.1.143	255.255.255.224	192.168.1.129

	SOPASP_-MAQ13	NIC	192.168.1.144	255.255.255.224	192.168.1.129
	SOPASP_-MAQ14	NIC	192.168.1.145	255.255.255.224	192.168.1.129
	SOPASP_-MAQ15	NIC	192.168.1.146	255.255.255.224	192.168.1.129
	SOPASP_-MAQ16	NIC	192.168.1.147	255.255.255.224	192.168.1.129
	SOPASP_-MAQ17	NIC	192.168.1.148	255.255.255.224	192.168.1.129
	SOPASP_-MAQ18	NIC	192.168.1.149	255.255.255.224	192.168.1.129
	SOPASP_-MAQ19	NIC	192.168.1.150	255.255.255.224	192.168.1.129
	SOPASP_-MAQ20	NIC	192.168.1.151	255.255.255.224	192.168.1.129
	SOPASP_- MAQ21	NIC	192.168.1.152	255.255.255.224	192.168.1.129

Tabla 8. *Direccionamiento de la Subred C*

Subred	Equipo	Interfaz	Dirección IP	Máscara de Red	Gateway
Subred D	SEF_SWITCH	Fa	192.168.1.161	255.255.255.224	No aplicable
	SEF_-DHCP	NIC	192.168.1.162	255.255.255.224	192.168.1.161
	SEF_-MAQ1	NIC	192.168.1.164	255.255.255.224	192.168.1.161
	SEF_-MAQ2	NIC	192.168.1.165	255.255.255.224	192.168.1.161
	SEF_-MAQ3	NIC	192.168.1.166	255.255.255.224	192.168.1.161
	SEF_-MAQ4	NIC	192.168.1.167	255.255.255.224	192.168.1.161
	SEF_-MAQ5	NIC	192.168.1.168	255.255.255.224	192.168.1.161
	SEF_-MAQ6	NIC	192.168.1.169	255.255.255.224	192.168.1.161
	SEF_-MAQ7	NIC	192.168.1.170	255.255.255.224	192.168.1.161
	SEF_-MAQ8	NIC	192.168.1.171	255.255.255.224	192.168.1.161
	SEF_-MAQ9	NIC	192.168.1.172	255.255.255.224	192.168.1.161
	SEF_-MAQ10	NIC	192.168.1.173	255.255.255.224	192.168.1.161
	SEF_-MAQ11	NIC	192.168.1.174	255.255.255.224	192.168.1.161
	SEF_-MAQ12	NIC	192.168.1.175	255.255.255.224	192.168.1.161
	SEF_-MAQ13	NIC	192.168.1.176	255.255.255.224	192.168.1.161
	SEF_-MAQ14	NIC	192.168.1.177	255.255.255.224	192.168.1.161
	SEF_-MAQ15	NIC	192.168.1.178	255.255.255.224	192.168.1.161
	SEF_-MAQ16	NIC	192.168.1.179	255.255.255.224	192.168.1.161
	SEF_-MAQ17	NIC	192.168.1.180	255.255.255.224	192.168.1.161
	SEF_-MAQ18	NIC	192.168.1.181	255.255.255.224	192.168.1.161
	SEF_-MAQ19	NIC	192.168.1.182	255.255.255.224	192.168.1.161
	SEF_-MAQ20	NIC	192.168.1.183	255.255.255.224	192.168.1.161
	SEF_-MAQ21	NIC	192.168.1.184	255.255.255.224	192.168.1.161

	SEF_-MAQ22	NIC	192.168.1.185	255.255.255.224	192.168.1.161
	SEF_- MAQ23	NIC	192.168.1.186	255.255.255.224	192.168.1.161

Tabla 9. *Direccionamiento de la Subred D*

Subred	Equipo	Interfaz	Dirección IP	Máscara de Red	Gateway
Subred E	DIRJ_SWITCH	NIC	192.168.1.193	255.255.255.224	No aplicable
	DIRJ_-DHCP	NIC	192.168.1.194	255.255.255.224	192.168.1.193
	DIRJ_-MAQ1	NIC	192.168.1.196	255.255.255.224	192.168.1.193
	DIRJ_-MAQ2	NIC	192.168.1.197	255.255.255.224	192.168.1.193
	DIRJ_-MAQ3	NIC	192.168.1.198	255.255.255.224	192.168.1.193
	DIRJ_-MAQ4	NIC	192.168.1.199	255.255.255.224	192.168.1.193
	DIRJ_-MAQ5	NIC	192.168.1.200	255.255.255.224	192.168.1.193
	DIRJ_-MAQ6	NIC	192.168.1.201	255.255.255.224	192.168.1.193
	DIRJ_-MAQ7	NIC	192.168.1.202	255.255.255.224	192.168.1.193
	DIRJ_-MAQ8	NIC	192.168.1.203	255.255.255.224	192.168.1.193
	DIRJ_-MAQ9	NIC	192.168.1.204	255.255.255.224	192.168.1.193
	DIRJ_-MAQ10	NIC	192.168.1.205	255.255.255.224	192.168.1.193
	DIRJ_-MAQ11	NIC	192.168.1.206	255.255.255.224	192.168.1.193
	DIRJ_-MAQ12	NIC	192.168.1.207	255.255.255.224	192.168.1.193
	DIRJ_-MAQ13	NIC	192.168.1.208	255.255.255.224	192.168.1.193
	DIRJ_-MAQ14	NIC	192.168.1.209	255.255.255.224	192.168.1.193
	DIRJ_-MAQ15	NIC	192.168.1.210	255.255.255.224	192.168.1.193
	DIRJ_-MAQ16	NIC	192.168.1.211	255.255.255.224	192.168.1.193
	DIRJ_-MAQ17	NIC	192.168.1.212	255.255.255.224	192.168.1.193
	DIRJ_-MAQ18	NIC	192.168.1.213	255.255.255.224	192.168.1.193
	DIRJ_-MAQ19	NIC	192.168.1.214	255.255.255.224	192.168.1.193
	DIRJ_-MAQ20	NIC	192.168.1.215	255.255.255.224	192.168.1.193
	DIRJ_-MAQ21	NIC	192.168.1.216	255.255.255.224	192.168.1.193
	DIRJ_-MAQ22	NIC	192.168.1.217	255.255.255.224	192.168.1.193
	DIR_- MAQ23	NIC	192.168.1.218	255.255.255.224	192.168.1.193

Tabla 10. *Direccionamiento de la Subred E*

Subred	Equipo	Interfaz	Dirección IP	Máscara de Red	Gateway
Subred F	SDP_SWITCH	NIC	192.168.1.225	255.255.255.224	No aplicable
	SDP_-DHCP	NIC	192.168.1.226	255.255.255.224	192.168.1.225
	SDP_-MAQ1	NIC	192.168.1.228	255.255.255.224	192.168.1.225
	SDP_-MAQ2	NIC	192.168.1.229	255.255.255.224	192.168.1.225
	SDP_-MAQ3	NIC	192.168.1.230	255.255.255.224	192.168.1.225
	SDP_-MAQ4	NIC	192.168.1.231	255.255.255.224	192.168.1.225
	SDP_-MAQ5	NIC	192.168.1.232	255.255.255.224	192.168.1.225
	SDP_-MAQ6	NIC	192.168.1.233	255.255.255.224	192.168.1.225
	SDP_-MAQ7	NIC	192.168.1.234	255.255.255.224	192.168.1.225
	SDP_-MAQ8	NIC	192.168.1.235	255.255.255.224	192.168.1.225
	SDP_-MAQ9	NIC	192.168.1.236	255.255.255.224	192.168.1.225
	SDP_-MAQ10	NIC	192.168.1.237	255.255.255.224	192.168.1.225
	SDP_-MAQ11	NIC	192.168.1.238	255.255.255.224	192.168.1.225
	SDP_-MAQ12	NIC	192.168.1.239	255.255.255.224	192.168.1.225
	SDP_-MAQ13	NIC	192.168.1.240	255.255.255.224	192.168.1.225
	SDP_-MAQ14	NIC	192.168.1.241	255.255.255.224	192.168.1.225
	SDP_-MAQ15	NIC	192.168.1.242	255.255.255.224	192.168.1.225
	SDP_-MAQ16	NIC	192.168.1.243	255.255.255.224	192.168.1.225
	SDP_-MAQ17	NIC	192.168.1.244	255.255.255.224	192.168.1.225
	SDP_-MAQ18	NIC	192.168.1.245	255.255.255.224	192.168.1.225
	SDP_-MAQ19	NIC	192.168.1.246	255.255.255.224	192.168.1.225
	SDP_-MAQ20	NIC	192.168.1.247	255.255.255.224	192.168.1.225
	SDP_-MAQ21	NIC	192.168.1.248	255.255.255.224	192.168.1.225
	SDP_-MAQ22	NIC	192.168.1.249	255.255.255.224	192.168.1.225
	SDP_- MAQ23	NIC	192.168.1.250	255.255.255.224	192.168.1.225

Tabla 11. *Direccionamiento de la Subred F*

III.1.2.3. Desarrollo de estrategias de seguridad

Las estrategias de seguridad que utilizaremos en la conexión inalámbrica y ethernet como medidas de seguridad son las siguientes:

Firewalls

El firewall que se utilizara es Fortigate, ya que un software libre y sin licencia, esto permitirá poner una barrera entre nuestra red interna de confianza y las redes externas que no son de confianza, como ser de Internet. Usan conjuntos de reglas para permitir o bloquear los tráfico y actividad dentro de la red. Desde filtrado de contenido, protección avanzada de amenazas, conectividad VPN, control de aplicaciones, optimización de ancho de banda.

Wireless security (Seguridad inalámbrica)

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

1. **Cuentas de Usuarios ID o SSID:** El Router tendrá de nombre SBVM para que se puedan conectar las personas solo de la institución.
2. **Autenticación:** Se utilizará el Cifrado WPA2-Personal todas las oficinas estarán conectadas de este modo con este tipo de seguridad la oficina de la Seragro tendrá de cifrado la contraseña **Seragro2023$**, oficina de Despachos, Recursos Humanos y Sistemas tendrá de cifrado la contraseña **humanos2023$**, oficina de Secretaria de Obras Públicas, Almacén secretaria de planificación más tendrá de cifrado la contraseña **secretaria2023$**, oficina de Secretaria de economía y Finanzas tendrá de cifrado la contraseña **economia2023$**, oficina de Dirección Jurídica tendrá de cifrado la contraseña **juridica2023$**, oficina de secretaria de desarrollo productivo tendrá cifrado la contraseña **productivo2023$** tomando en cuenta que estarán conectados por cable de red.

Fortigate

FortiGate es una plataforma de seguridad de red esencial para la Subgobernación de Villa Montes. Este dispositivo actúa como un guardián digital, protegiendo las redes locales de la subgobernación contra amenazas cibernéticas cada vez más sofisticadas.

Al implementar FortiGate, la Subgobernación de Villa Montes puede asegurar la integridad de sus datos confidenciales, así como proteger los sistemas críticos de información contra intrusiones no autorizadas. Esto incluye la defensa contra ataques de malware, intentos de piratería, así como la gestión y regulación del acceso a internet y las aplicaciones en la red.
Además de proporcionar seguridad, FortiGate también optimiza el rendimiento de la red, asegurando que los recursos digitales se utilicen de manera eficiente y que el flujo de datos sea rápido y seguro.
FortiGate es una solución esencial para garantizar la seguridad y la integridad de las operaciones digitales en la Subgobernación de Villa Montes, brindando tranquilidad y confianza en la protección de la infraestructura y los datos críticos.

III.1.2.4. Desarrollo de estrategias de administración de red

Lo primero que realizaremos para la administración de la red es la configuración de cuentas de usuarios en los equipos de las áreas de trabajo y también las laptops a pesar de que estas últimas ya tiene configurada la cuenta de usuario
Como conectaremos la red en los equipos, lo realizaremos a través de DHCP en las diferentes dependencias donde se encuentran los equipos de escritorio donde primeramente tendremos que ver que el servidor será el sistema operativo Ubuntu Server, el cual se utilizará para configurar las IP, También se usará el sistema operativo Windows 7 en todas las máquinas de la institución, esto nos permitirá conectarnos a la red interna.

III.1.3. Fase 3: Desarrollar Diseño Físico

III.1.3.1. Material de canalización

Mini canal de PVC

Descripción: Canaleta plástica 32 x 12 mm

Sus dimensiones serán 40 mm de profundidad x 24 mm ancho. Por él irán los cables con una protección frente a incidencias exteriores. La canaleta dispondrá de una tapa desmontable que se podrá poner y quitar para la instalación de los cables. Existen dos modelos con adhesivos y sin adhesivos que permitirá colocar en la pared. Si utilizara sin adhesivo puede usar un tornillo para la fijación de la canaleta.

Figura 20. Canaleta de PVC

III.1.3.1.1. Descripción de cableado, conecta rizado y rosetas

Se debe tener en cuenta una serie de características de los cables UTP:

Los cables de datos tienen una resistencia de hasta 100Ω y están formados por cuatro pares

III.1.3.1.2. Cableado

Tras un estudio de mercado, se optó por utilizar el tipo de cableado UTP para esta instalación ya que el coste no supone una inversión muy descomunal. El modelo elegido fue:

Modelo de cable Fibra Óptica

Modelo de cable UTP Cat.6e

- Número de pares: 4
- Conductor: cobre sólido (clase 1)

- Aislamiento: HDPE, PE, poliolefina
- Alambre de drenaje: Cobre estañado
- Revestimiento exterior: Polietileno de baja densidad (LDPE), LSZH

Figura 21. Cable UTP cat.5e

III.1.3.1.3. Latiguillos de parcheo

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

- Alta protección contra las interferencias electromagnéticas
- Altos valores ACR y error mínimo de velocidad
- Baja propagación de retardo
- Supera las condiciones de cat. 6 marcados por la norma

Figura 22. Latiguillo de parcheo

III.1.3.1.4. Rosetas y conectores

Las rosetas estarán debidamente instaladas respetando un destrenzado menor de 13 mm, evitando la pérdida de categoría. El tipo de conectores que se van a usar en toda la

instalación de cableado es de tipo RJ45, conector con ocho pines metálicos que están conectados con los pequeños cables.

Conectores:

RJ45

- **Contactos: 8**
- **Nª de puertos: 1**
- **Categoría LAN: CAT 6ª**
- **CHAPADO DE LOS CONTACTOS: Oro**
- **Material de contacto: Bronce**

Figura 23. Conector RJ45

III.1.3.2. Equipos de Conectividad

III.1.3.2.1. Rack de distribución principal

Distribuidor 48U:

Armario rack para instalación en pared. Capacidad para 19U rack". Diseñado para su instalación en pared, este armario rack es la solución perfecta para salvaguardar el equipamiento electrónico. Sus dimensiones normalizadas según la especificación EIA-310 permiten que sea compatible con equipos de cualquier marca o fabricante.

- Armario rack para pared
- Hasta 6U rack de 24U"
- Hasta 100 Kg de carga
- Con ventilación y pasacables
- Ventilador y bandeja incluidos

- Regleta de 6 tomas incluida

Figura 24. Rack de 24U

Componente	Tamaño	Unidades	Total
Ventilador	1U	1	1U
Patch Pannel 48 Puertos	2U	6	6U
Switch 48 Puertos	2U	4	4U
Regleta de Fuerza	1U	2	2U
Organizador de Cable	2U	4	4U
Total	8U	17	17U = 16 + 24%=24U

Tabla 12. *Rack de distribución principal*

III.1.3.2.2. Regleta de fuerza

Están fabricadas con un perfil de aluminio de alta calidad preparado para soportar temperaturas elevadas de los distribuidores de servidores.

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

Referencia F2109

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

Figura 25. Regleta de Fuerza

III.1.3.2.3. Organizador de cableado

Se utilizan fundamentalmente para organizar los cables y eliminar la congestión de los mismos. Conformado con cinco robustos anillos de acero para ofrecer mayor durabilidad y resistencia para sujetar los cables sin dañarlos.

Figura 26. Organizador de cables

Ventilador rack

Las unidades de ventilación están diseñadas para no ocupar espacio en el interior de los armarios, ya que se fijan directamente en el techo.

Figura 27. Ventilador Rack

III.1.3.2.4. Patch panel 48 puertos

Los patch panel harán de conectores intermediarios entre las rosetas y el switch que vayan conectadas. Hay varias ventajas en usar patch pannel, logrando más durabilidad en los switches, ya que se reducirán las conexiones / desconexiones.

Utilizaremos paneles de conexión de veinticuatro puertos. Es importante tener buenos paneles de conexión para que no nos limite la calidad y la velocidad de nuestra instalación. Llevan los cables de datos de los diferentes puestos de trabajo para conectarlos mediante latiguillos de parcheo directamente al switch. Panel de conexión sin blindar Cat6 de 48 puertos TC-P24C6:

- Panel de 48 puertos para instalar en bastidor, listo para conexiones Gigabit
- Los paneles de conexiones Cat6e transmiten de forma continua a 250Mhz a conmutadores Gigabit cobre.
- Solución ideal para aplicaciones Ethernet, Fast Ethernet y Gigabit.

Figura 28. Patch panel 48 puertos

III.1.3.2.5. Switch Cisco Catalysh 3400

Se utilizará uno de 48 puertos para conectar los 43 equipos que se tiene además de conectar otros equipos necesarios para una conexión de red inalámbrica este switch está pensado para un futuro y si se pueda utilizar más adelante en la conexión de otras máquinas que se puedan adquirir en el área de trabajo.

Características a que utilizara este switch es:

- Número de puertos: 48 RJ45 Ethernet.
- Número de puerto: 6 SFP
- Velocidad de transferencia de datos: 100 Mbit/s.55
- Protocolo de interconexión de datos Ethernet, Fast Ethernet.

- Seguridad: IEEE 802.1x.
- SSH / HTTPS.
- Alimentación externa.
- Ventilador

Figura 29. Switch

III.1.3.2.6. Router Cisco ASR 1002-X

El Router es utilizado para la interconexión de redes de computadores (LAN) permiten asegurar el enrutamiento de paquetes entre diferentes redes o determinar la ruta que debe tomar un determinado paquete de datos en función de la dirección destino.

Figura 30. Router

-Puertos SFP/SFP+:

Tiene hasta 6 puertos SFP para conexiones de fibra óptica a 1 Gbps o 10 Gbps.

-Rendimiento:

Ofrece hasta 36 Gbps de capacidad, expandible a 100 Gbps con actualizaciones.

-Funciones Avanzadas:

Soporta seguridad integrada, VPN, y calidad de servicio (QoS) avanzada.

Virtualización: permite la gestión segmentada de la red.

-Alta Disponibilidad:

Arquitectura modular y fuentes de alimentación redundantes para minimizar el tiempo de inactividad.

Gestión:

- Incluye herramientas robustas como Cisco IOS XE para una gestión eficiente.

III.1.3.2.7. Access Point Cisco Aironet 2800 Series

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

Usos que tendrá:

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

Característica destacada:

802.11ac Wave 2: Este punto de acceso es compatible con el estándar 802.11ac Wave 2, que ofrece velocidades inalámbricas de hasta 5.2 Gbps y proporciona un rendimiento mejorado, mayor capacidad y una mejor cobertura en comparación con los estándares anteriores.

Figura 31. Access Point

III.1.3.2.8. UPS Cisco UPS 1100W

Características del UPS:

Capacidad de salida de 1100W: Ofrece una potencia de 1100 vatios para mantener dispositivos críticos operativos durante cortes de energía.

Diseño compacto y montaje en rack: Ocupa poco espacio y se instala fácilmente en racks de equipos estándar.

Baterías de larga duración: Proporciona autonomía suficiente para mantener los dispositivos conectados durante cortes de energía prolongados.

Protección contra sobretensiones y picos de corriente: Evita daños a los equipos y garantiza una alimentación estable y segura.

Monitoreo remoto: Permite supervisar y administrar el UPS desde cualquier ubicación a través de una interfaz de red.

Notificaciones de alerta: Envía alertas en tiempo real sobre eventos críticos como cortes de energía.

Figura 32. Cisco UPS 1100W

Integración con sistemas de gestión: Se integra fácilmente en la infraestructura de red existente para una gestión centralizada de la energía.

Por lo tanto, el proveedor de servicios de internet será la empresa encargada de suministrar a sus clientes una conexión de banda ancha, a través de tecnologías como cable coaxial entre otras, ya sea de servicio como Tigo o Entel eso dependerá de los paquetes que nos ofrezcan.

UPS.

III.1.4. Simulación de la red

III.1.4.1. Topología de conexión de la red a implementar

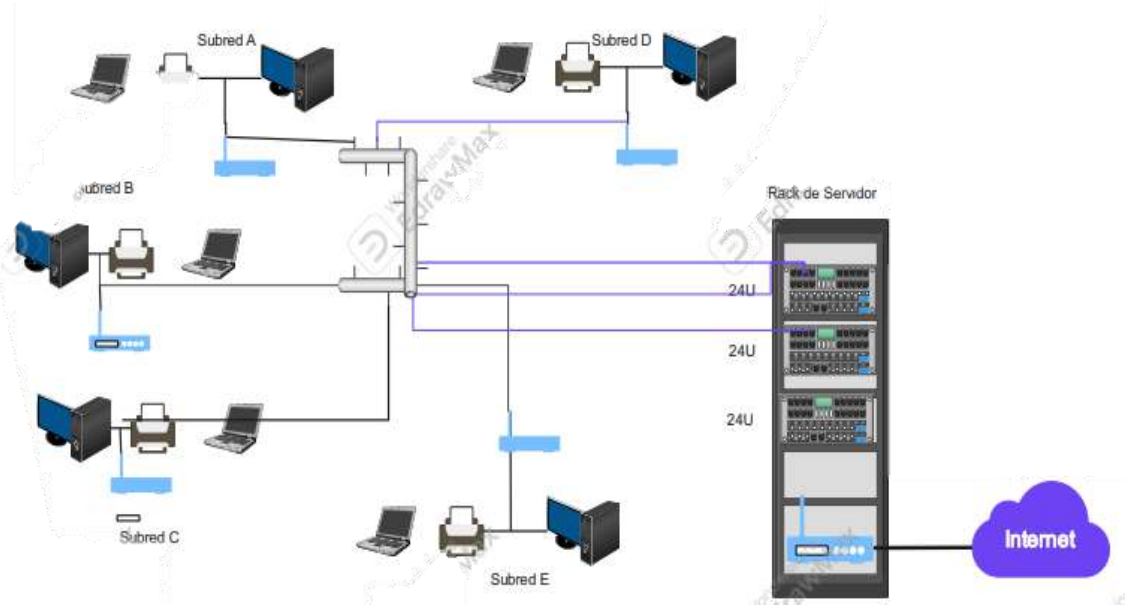


Figura 33. *Topología de la red a implementar*

III.1.4.1.1 Rack de Almacenamiento

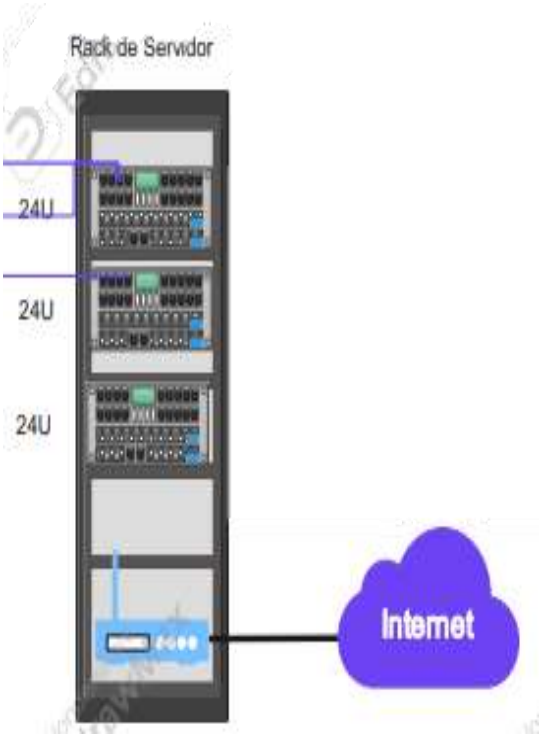


Figura 34. Rack

III.1.4.2. Simulador en Packet Tracer Lógico

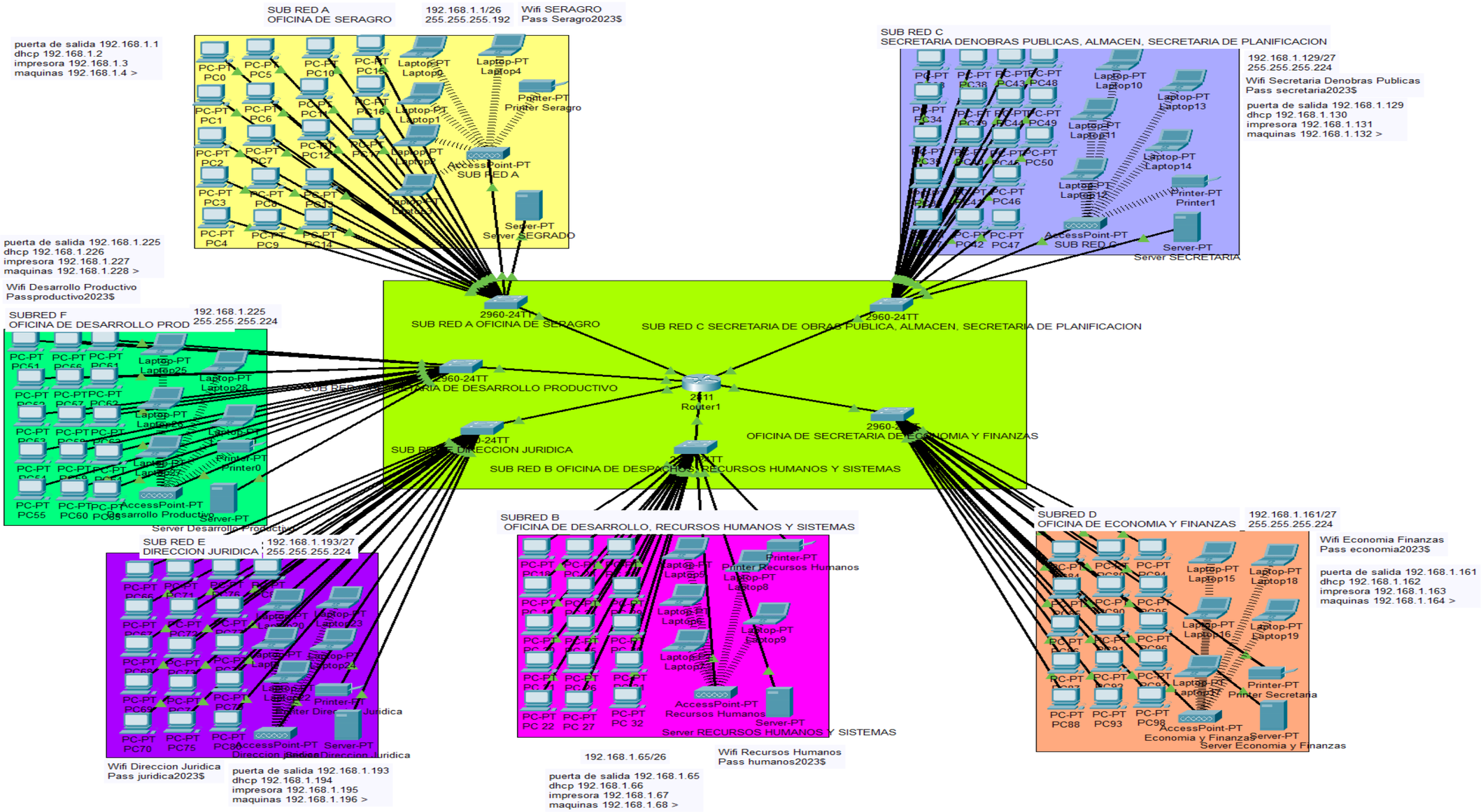


Figura 35. Simulador en Packet Tracer Lógico

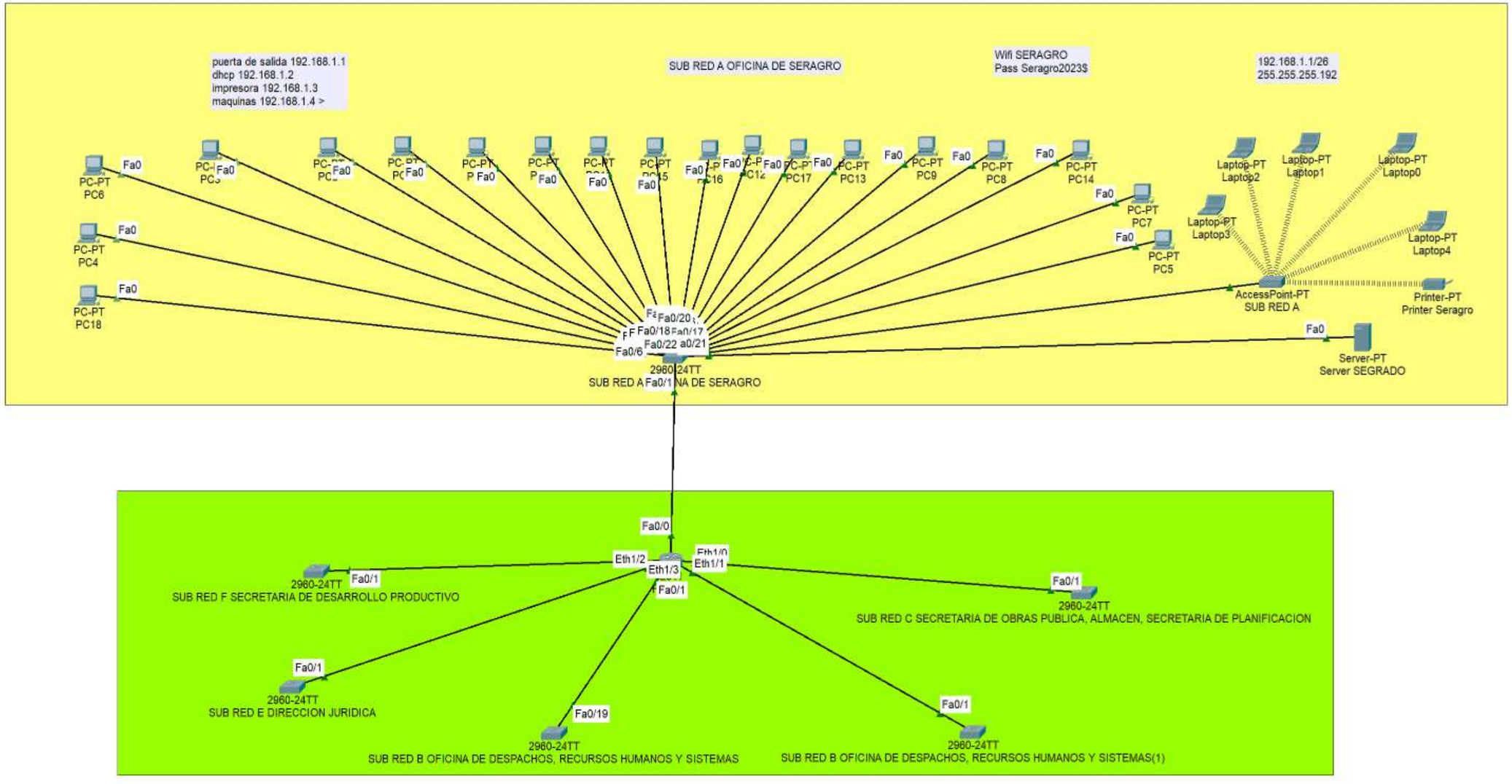


Figura 36. Packet Tracer Oficina A de Seragro

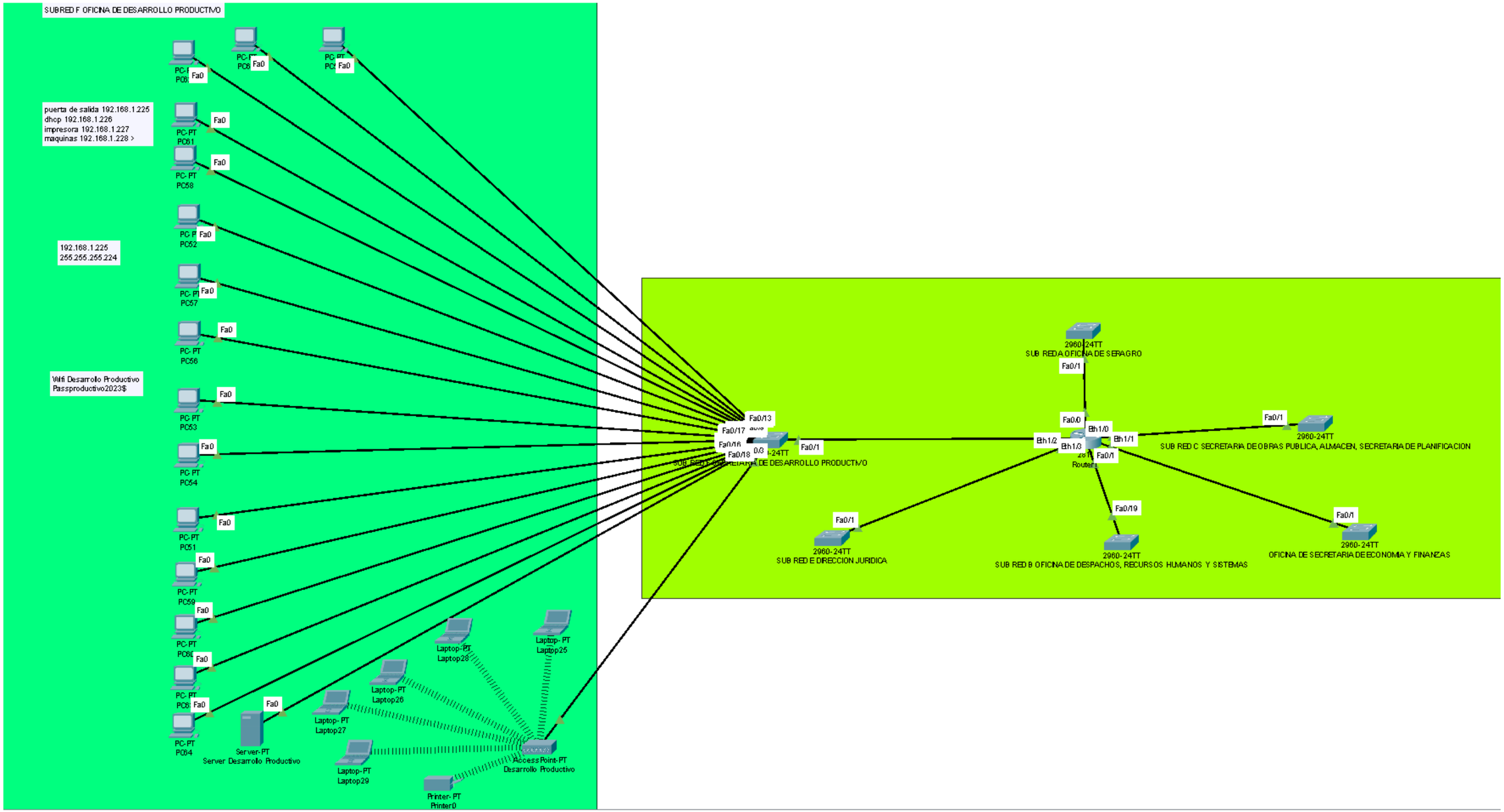


Figura 37. Packet Tracer Oficina F de Desarrollo Productivo

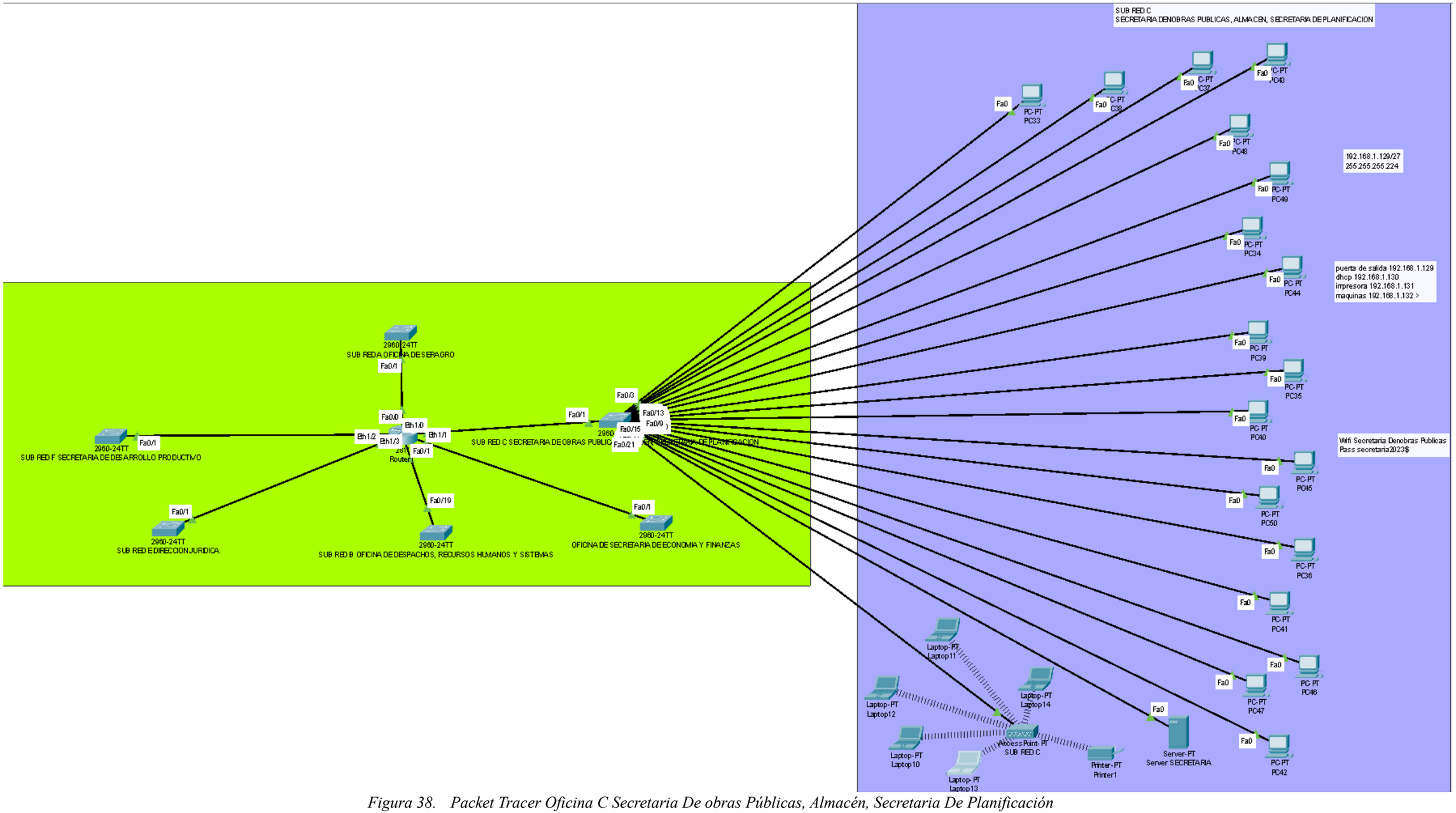


Figura 38. Packet Tracer Oficina C Secretaria De obras Públicas, Almacén, Secretaria De Planificación

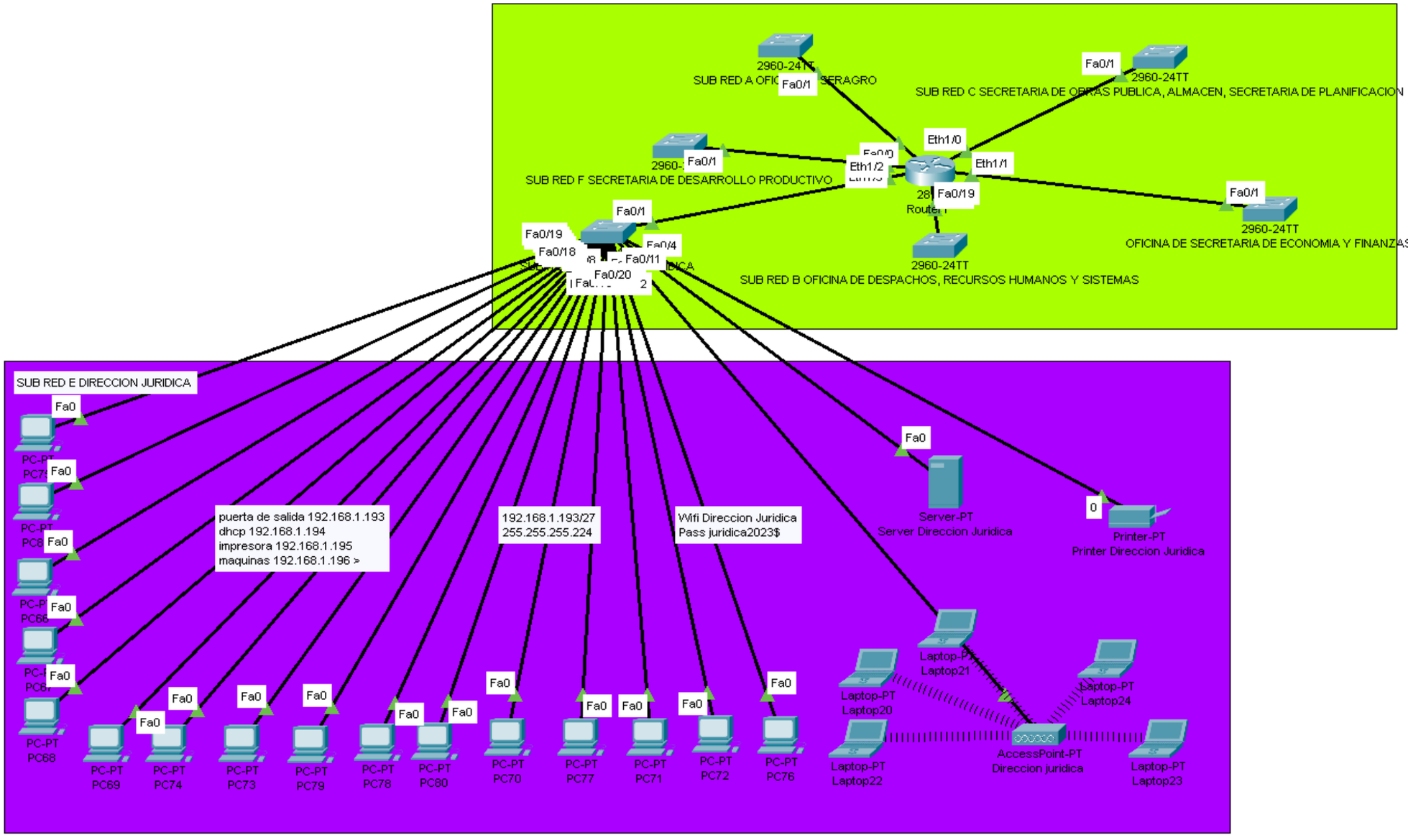


Figura 39. Packet Tracer Oficina E Dirección Jurídica

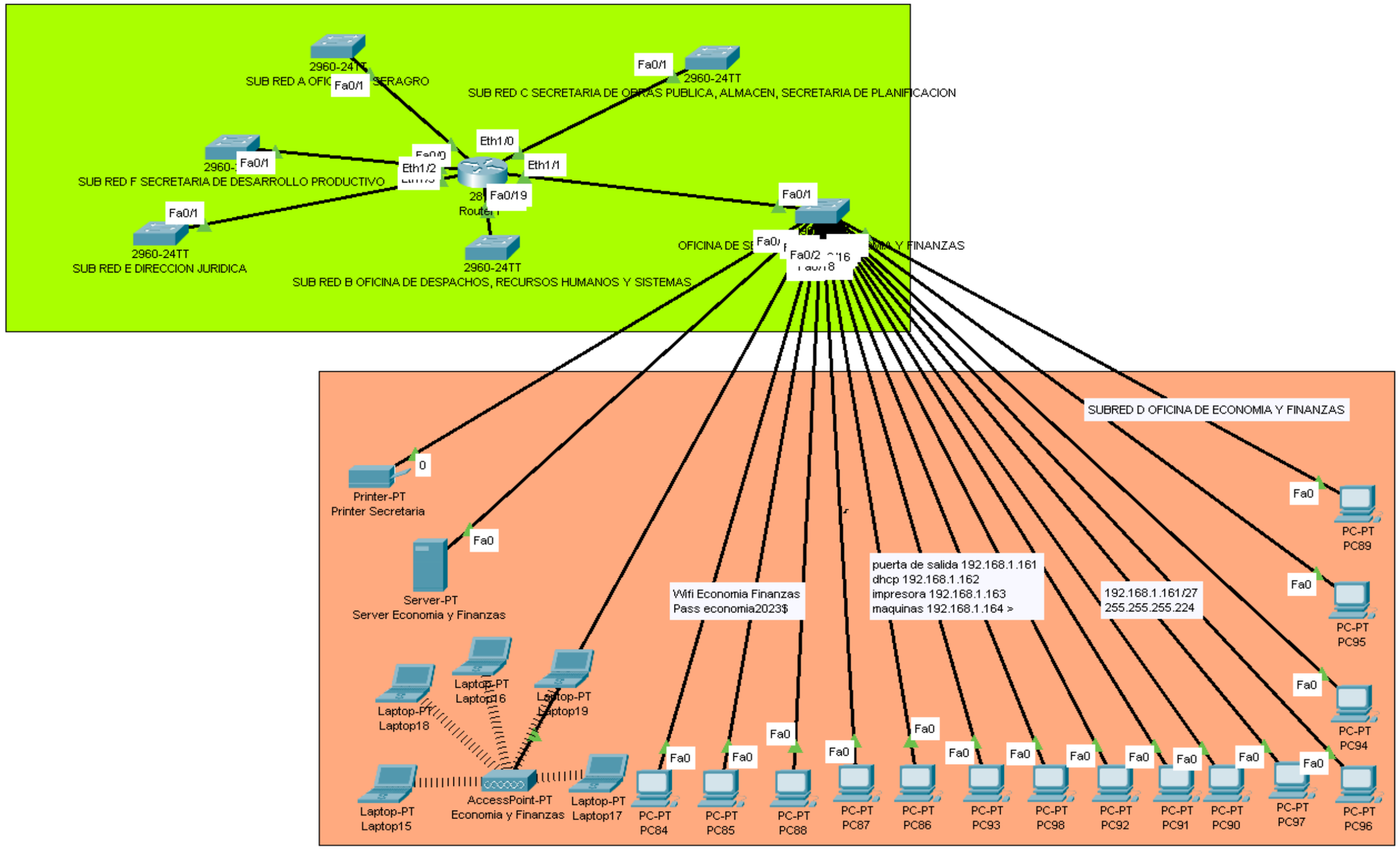


Figura 40. Packet Tracer Subred D Oficina De Economía Y Finanzas

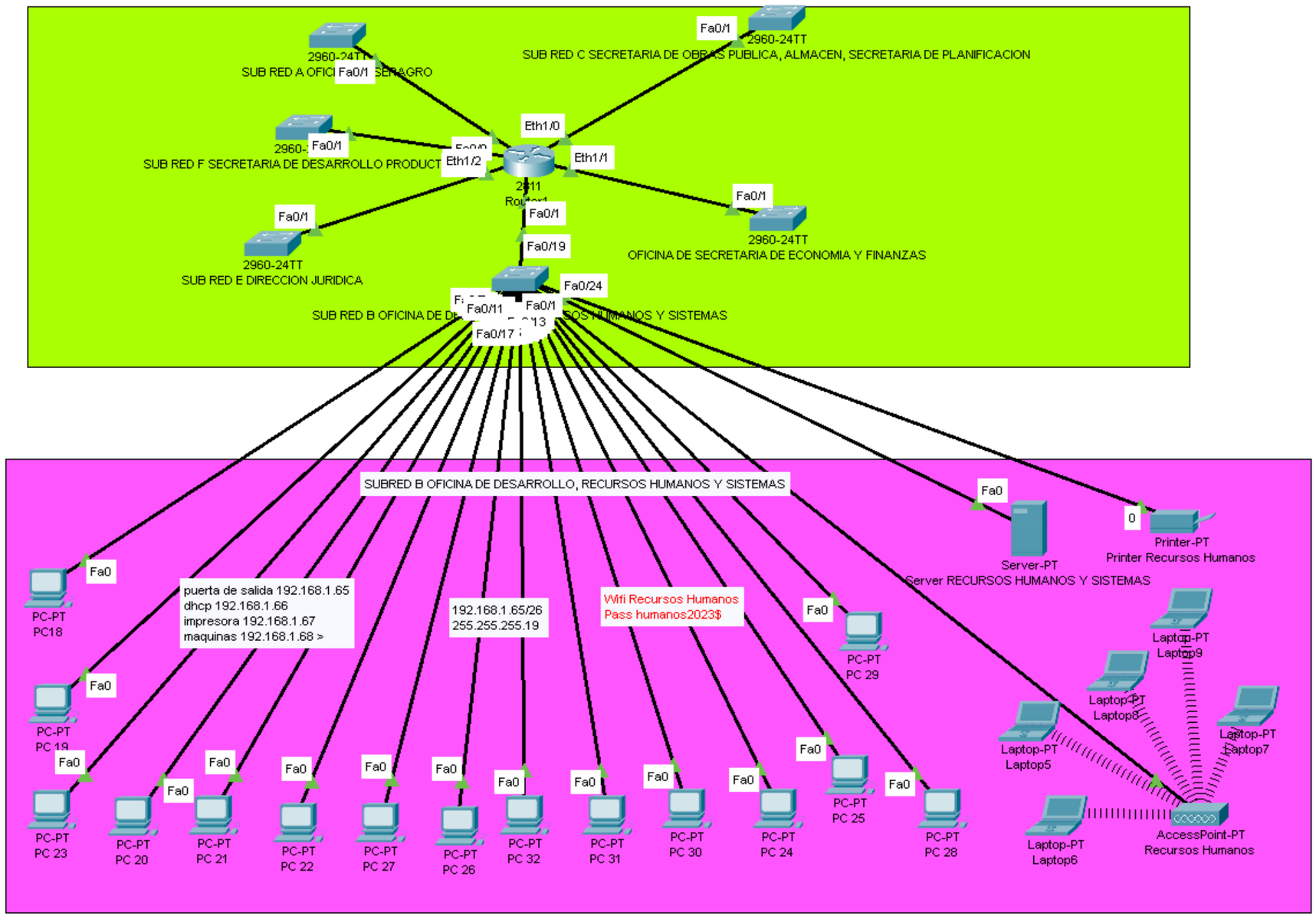


Figura 41. Pa cket Tracer SUBRED B OFICINA DE DESARROLLO, RECURSOS HUMANOS Y SISTEMAS

III.1.4.2.1. Comandos de la configuración del Router en packet tracer

Router>enable

Router#

Router#configure terminal

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

Router(config)#interface FastEthernet0/0

Router(config-if)#ip address 192.168.1.1 255.255.255.192

Router(config-if)#no shutdown

Router(config-if)#access-list 101 deny icmp any any host-unreachable

Router(config-if)#access-list 101 permit tcp any any eq www

Router(config-if)#ip access-group 101 in

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#exit

Router(config)#interface FastEthernet0/1

Router(config-if)#ip address 192.168.1.65 255.255.255.192

Router(config-if)#no shutdown

Router(config-if)#access-list 101 deny icmp any any host-unreachable

Router(config-if)#access-list 101 permit tcp any any eq www

Router(config-if)#ip access-group 101 in

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Router(config-if)#exit

Router(config)#interface Ethernet1/0

Router(config-if)#ip address 192.168.1.129 255.255.255.224

Router(config-if)#no shutdown

Router(config-if)#access-list 101 deny icmp any any host-unreachable

Router(config-if)#access-list 101 permit tcp any any eq www

Router(config-if)#ip access-group 101 in

%LINK-5-CHANGED: Interface Ethernet1/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0, changed state to up

Router(config-if)#exit

Router(config)#interface Ethernet1/1

Router(config-if)#ip address 192.168.1.161 255.255.255.224

Router(config-if)#no shutdown

Router(config-if)#access-list 101 deny icmp any any host-unreachable

Router(config-if)#access-list 101 permit tcp any any eq www

Router(config-if)#ip access-group 101 in

%LINK-5-CHANGED: Interface Ethernet1/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/1, changed state to up

Router(config-if)#exit

Router(config)#interface Ethernet1/2

Router(config-if)#ip address 192.168.1.193 255.255.255.224

Router(config-if)#no shutdown

Router(config-if)#access-list 101 deny icmp any any host-unreachable

Router(config-if)#access-list 101 permit tcp any any eq www

Router(config-if)#ip access-group 101 in

%LINK-5-CHANGED: Interface Ethernet1/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/2, changed state toup

Router(config-if)#exit

Router(config)#interface Ethernet1/3

Router(config-if)#ip address 192.168.1.225 255.255.255.224

Router(config-if)#no shutdown

Router(config-if)#access-list 101 deny icmp any any host-unreachable

Router(config-if)#access-list 101 permit tcp any any eq www

Router(config-if)#ip access-group 101 in

%LINK-5-CHANGED: Interface Ethernet1/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/3, changed state to up

Router(config-if)#exit

%SYS-5-CONFIG_I: Configured from console by console

III.1.4.4. Simulador en GNS3 Lógico

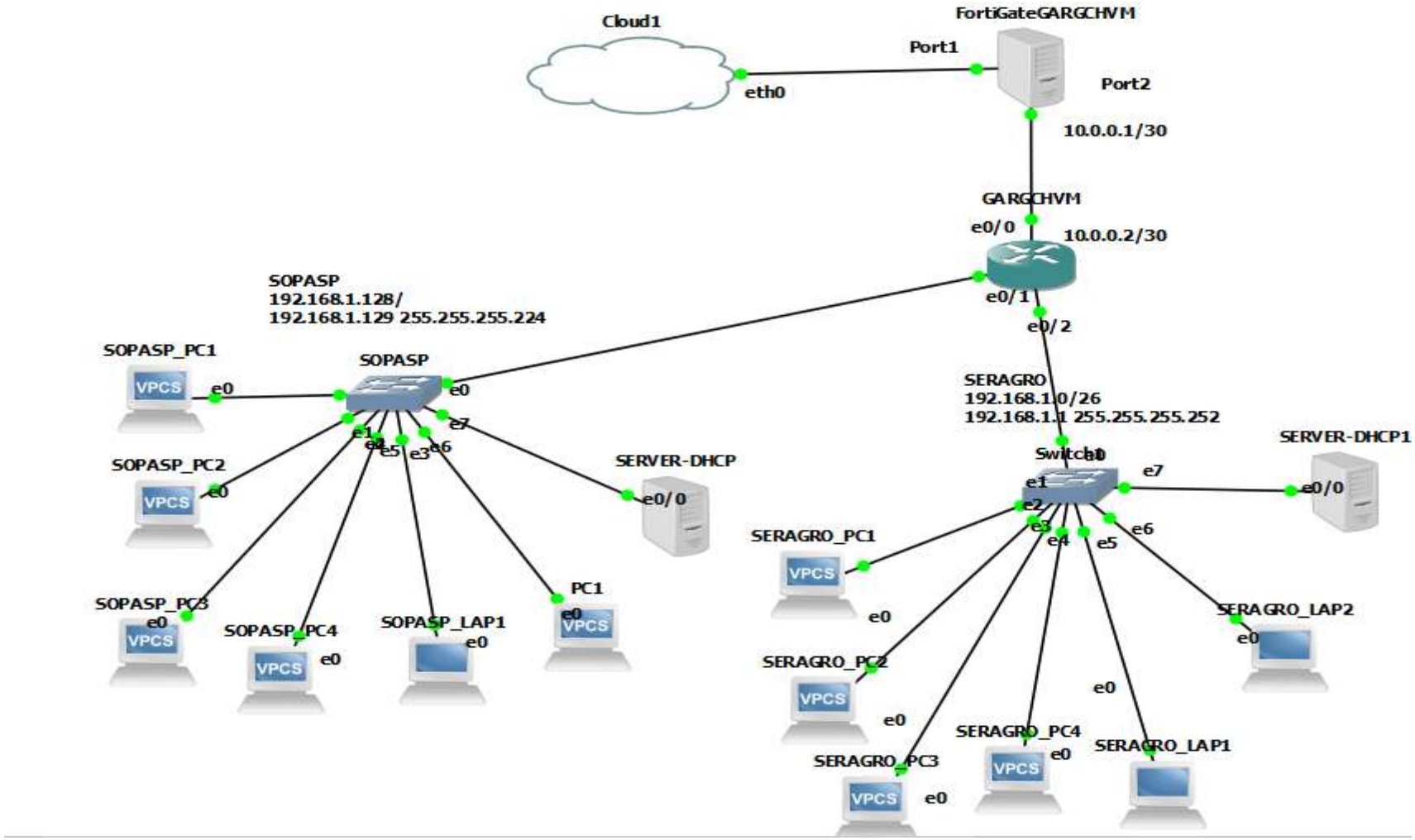


Figura 42. Simulador en GNS3 lógico

III.1.4.4.1 Simulador de la Seguridad en GNS3 con el Fortigate en la parte Lógica

Ingresamos al fortigate

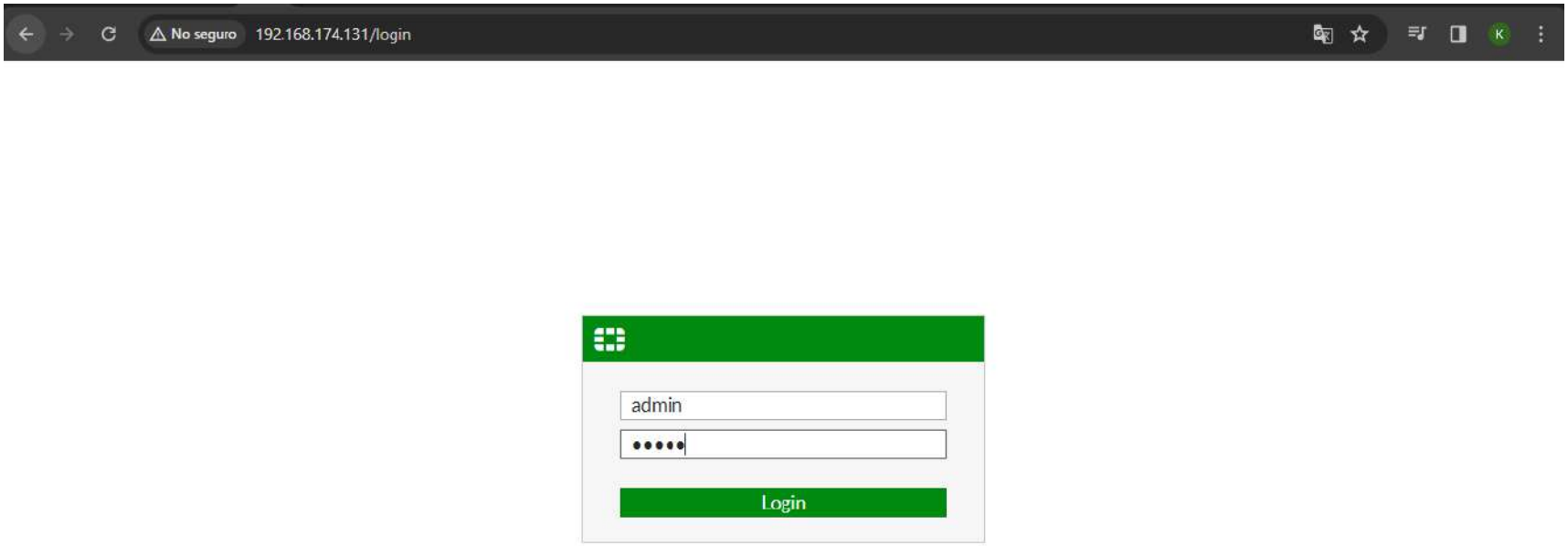


Figura 43. Ingresando al Fortigate

III.1.4.4.2. Simulador en GNS3 Lógico

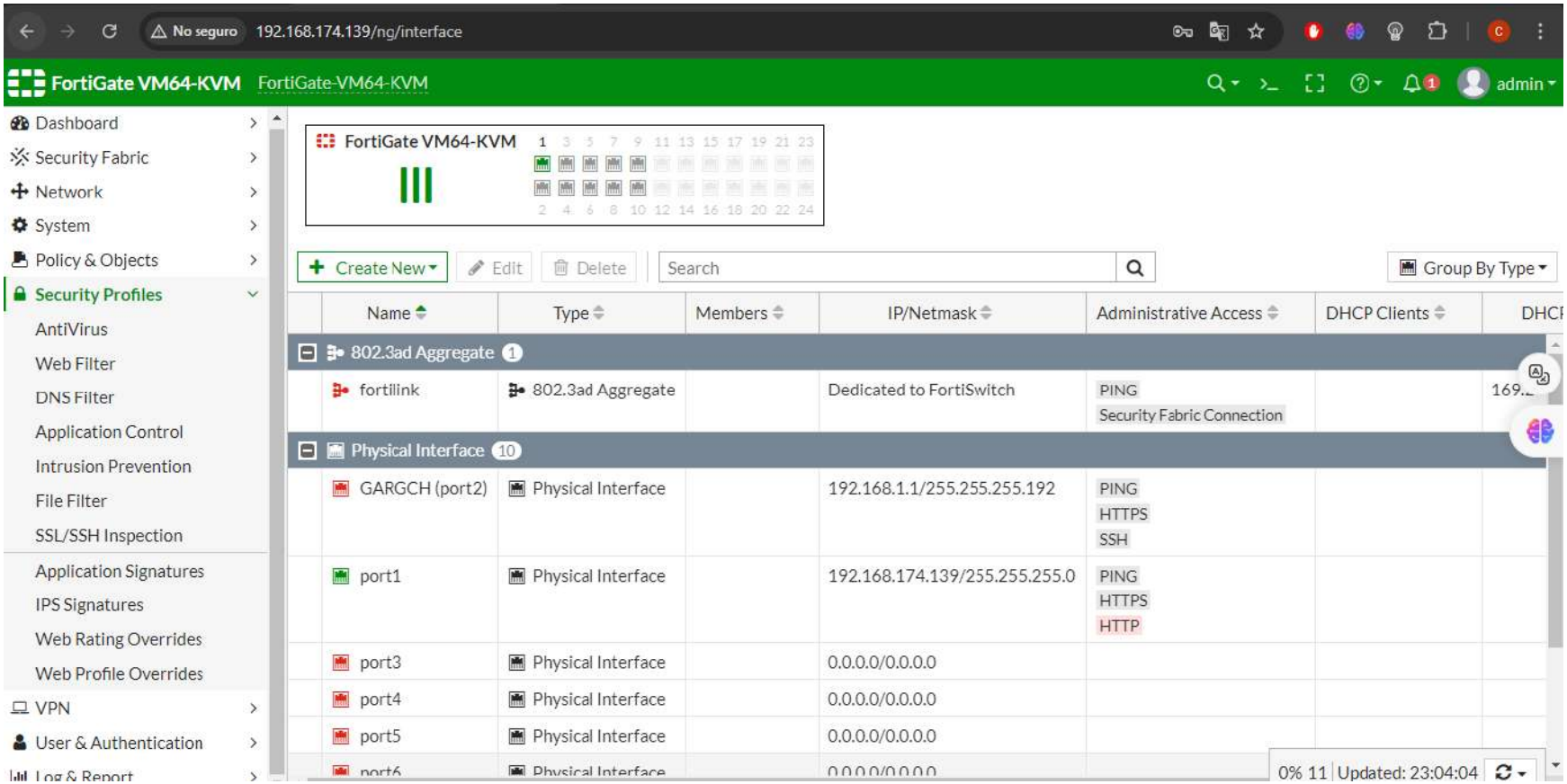


Figura 44. Configuramos la Seguridad de nuestros equipos

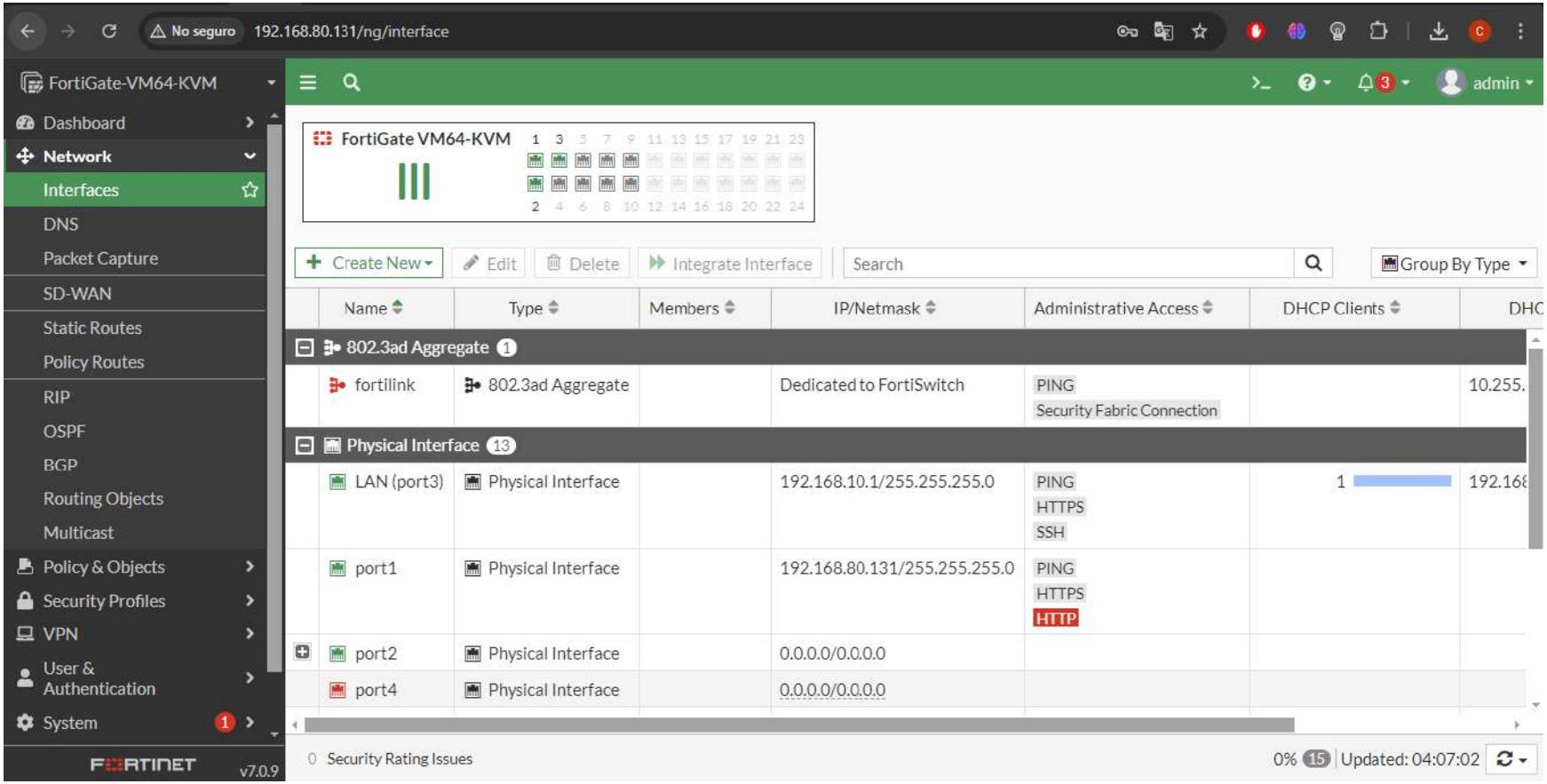


Figura 45. Fortinet Network

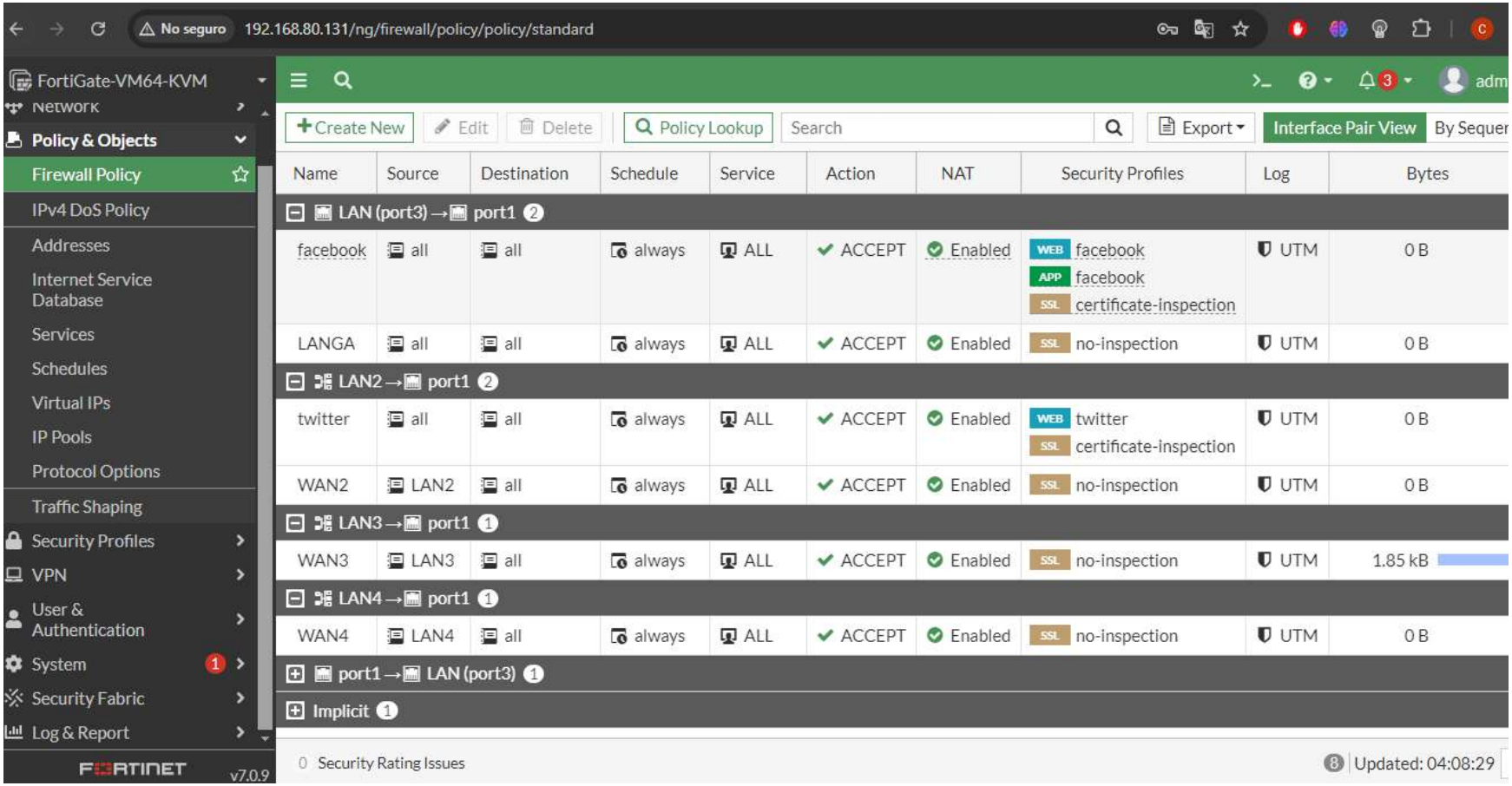


Figura 46. Fortinet Politicas

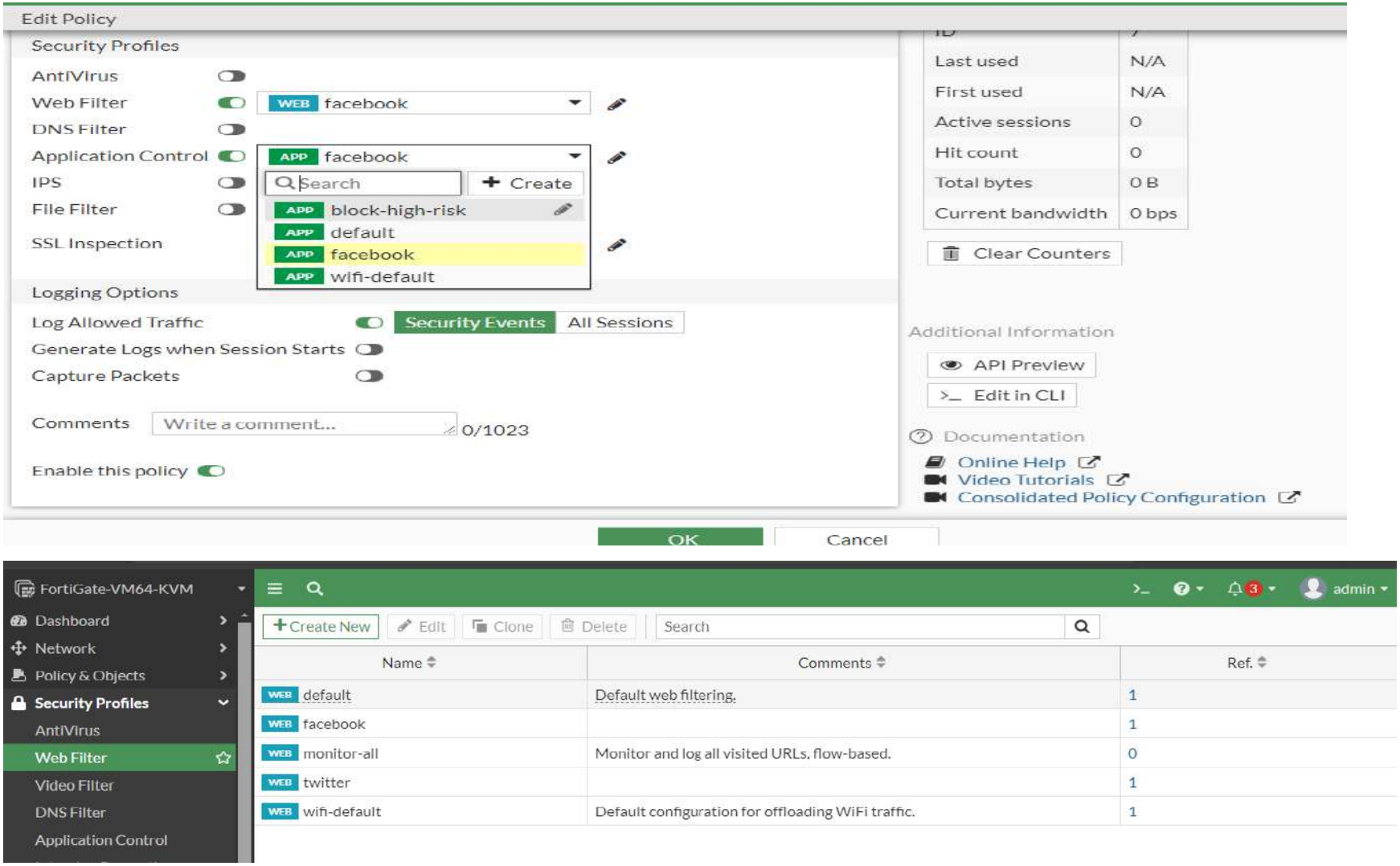


Figura 47. Fortinet Bloqueos de redes sociales

III.1.4.4.3. Script de la configuración del router y fortigate

Script de la configuración del router

```
R1#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip dhcp pool SERAGRO
R1(dhcp-config)#   network 192.168.1.0 255.255.255.192
R1(dhcp-config)#   default-router 192.168.1.1
R1(dhcp-config)#   dns-server 8.8.8.8 4.4.4.4
R1(dhcp-config)#ip dhcp pool DHRSI
R1(dhcp-config)#   network 192.168.1.64 255.255.255.192
R1(dhcp-config)#   default-router 192.168.1.65
R1(dhcp-config)#   dns-server 8.8.8.8 4.4.4.4
R1(dhcp-config)#ip dhcp pool SOPASP
R1(dhcp-config)#   network 192.168.1.128 /27
R1(dhcp-config)#   default-router 192.168.1.129
R1(dhcp-config)#   dns-server 8.8.8.8 4.4.4.4
R1(dhcp-config)#ip dhcp pool SEF
R1(dhcp-config)#   network 192.168.1.160 /27
R1(dhcp-config)#   default-router 192.168.1.161
R1(dhcp-config)#   dns-server 8.8.8.8 4.4.4.4
R1(dhcp-config)#ip dhcp pool DIRJ
R1(dhcp-config)#   network 192.168.1.192 /27
R1(dhcp-config)#   default-router 192.168.1.193
R1(dhcp-config)#   dns-server 8.8.8.8 4.4.4.4
R1(dhcp-config)#
R1(dhcp-config)#inter e0/0
R1(config-if)#ip add 192.168.1.1 255.255.255.192
R1(config-if)#no shut
R1(config-if)#inter e0/1
R1(config-if)#ip add 192.168.1.65 255.255.255.192
R1(config-if)#no shut
```

```
R1(config-if)#inter e0/2
R1(config-if)#ip add 192.168.1.129 255.255.255.224
R1(config-if)#no shut
R1(config-if)#inter e0/3
R1(config-if)#ip add 192.168.1.161 255.255.255.224
R1(config-if)#no shut
R1(config-if)#inter e1/0
R1(config-if)#ip add 192.168.1.193 255.255.255.224
R1(config-if)#no shut
R1(config-if)#inter e1/1
R1(config-if)#ip add 192.168.1.225 255.255.255.224
R1(config-if)#no shut
R1(config-if)#
*Apr  8 20:54:25.502: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*Apr  8 20:54:25.516: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to up
*Apr  8 20:54:25.525: %LINK-3-UPDOWN: Interface Ethernet0/2, changed state to up
*Apr  8 20:54:25.525: %LINK-3-UPDOWN: Interface Ethernet0/3, changed state to up
*Apr  8 20:54:25.543: %LINK-3-UPDOWN: Interface Ethernet1/0, changed state to up
*Apr  8 20:54:26.510: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0,
changed state to up
*Apr  8 20:54:26.519: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1,
changed state to up
*Apr  8 20:54:26.533: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2,
changed state to up
*Apr  8 20:54:26.533: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3,
changed state to up
*Apr  8 20:54:26.547: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0,
changed state to up
R1(config-if)#end
R1#sh ip int brie
Interface              IP-Address      OK? Method Status                Protocol
```

```
Ethernet0/0            192.168.1.1     YES manual up                    up
Ethernet0/1            192.168.1.65    YES manual up                    up
Ethernet0/2            192.168.1.129   YES manual up                    up
Ethernet0/3            192.168.1.161   YES manual up                    up
Ethernet1/0            192.168.1.193   YES manual up                    up
Ethernet1/1            192.168.1.225   YES manual up                    up
Ethernet1/2            unassigned      YES NVRAM  administratively down down
Ethernet1/3            unassigned      YES NVRAM  administratively down down
Serial2/0              unassigned      YES NVRAM  administratively down down
Serial2/1              unassigned      YES NVRAM  administratively down down
Serial2/2              unassigned      YES NVRAM  administratively down down
Serial2/3              unassigned      YES NVRAM  administratively down down
Serial3/0              unassigned      YES NVRAM  administratively down down
R1#sh ip dhc bin
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.168.1.2         0100.5079.6668.1a       Apr 09 2024 08:55 PM    Automatic
R1#
R1#sh ip dhc bin
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.168.1.2         0100.5079.6668.1a       Apr 09 2024 08:55 PM    Automatic
192.168.1.66        0100.5079.6668.1b       Apr 09 2024 08:56 PM    Automatic
192.168.1.130       0100.5079.6668.15       Apr 09 2024 08:56 PM    Automatic
192.168.1.162       0100.5079.6668.18       Apr 09 2024 08:57 PM    Automatic
192.168.1.194       0100.5079.6668.14       Apr 09 2024 08:57 PM    Automatic
R1#sh ip dhc bin
```

Bindings from all pools not associated with VRF:

IP address	Client-ID/ Hardware address/ User name	Lease expiration	Type
192.168.1.2	0100.5079.6668.1a	Apr 09 2024 08:55 PM	Automatic
192.168.1.66	0100.5079.6668.1b	Apr 09 2024 08:56 PM	Automatic
192.168.1.130	0100.5079.6668.15	Apr 09 2024 08:56 PM	Automatic
192.168.1.162	0100.5079.6668.18	Apr 09 2024 08:57 PM	Automatic
192.168.1.194	0100.5079.6668.14	Apr 09 2024 08:57 PM	Automatic

```
R1#write
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R1#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#net
R1(config-router)#network 192.168.1.0 0.0.0.255 are
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0
R1(config-router)#end
R1#
*Apr  8 20:59:29.754: %SYS-5-CONFIG_I: Configured from console by console
R1#sh ip int brie
```

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0/0	192.168.1.1	YES	manual	up	up
Ethernet0/1	192.168.1.65	YES	manual	up	up
Ethernet0/2	192.168.1.129	YES	manual	up	up
Ethernet0/3	192.168.1.161	YES	manual	up	up
Ethernet1/0	192.168.1.193	YES	manual	up	up

```
Ethernet1/1            192.168.1.225   YES manual up                    up
Ethernet1/2            unassigned      YES NVRAM  administratively down down
Ethernet1/3            unassigned      YES NVRAM  administratively down down
Serial2/0              unassigned      YES NVRAM  administratively down down
Serial2/1              unassigned      YES NVRAM  administratively down down
Serial2/2              unassigned      YES NVRAM  administratively down down
Serial2/3              unassigned      YES NVRAM  administratively down down
R1#
R1#sh ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            192.168.1.1     YES manual up                    up
Ethernet0/1            192.168.1.65    YES manual up                    up
Ethernet0/2            192.168.1.129   YES manual up                    up
Ethernet0/3            192.168.1.161   YES manual up                    up
Ethernet1/0            192.168.1.193   YES manual up                    up
Ethernet1/1            192.168.1.225   YES manual up                    up
Ethernet1/2            unassigned      YES NVRAM  administratively down down
Ethernet1/3            unassigned      YES NVRAM  administratively down down
Serial2/0              unassigned      YES NVRAM  administratively down down
Serial2/1              unassigned      YES NVRAM  administratively down down
Serial2/2              unassigned      YES NVRAM  administratively down down
R1#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#inter e1/1
R1(config-if)#ip add 172.16.1.2 255.255.255.252
R1(config-if)#end
R1#
*Apr  9 02:26:13.819: %SYS-5-CONFIG_I: Configured from console by console
R1#ping 172.16.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
```

```
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 2/2/2 ms
R1#ping 172.16.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
R1#
R1#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R1#trace
R1#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#do sh run
Building configuration...

Current configuration : 2705 bytes
!
! Last configuration change at 02:26:13 UTC Tue Apr 9 2024
!
version 15.7
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
```

```
boot-end-marker
!
no aaa new-model
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
no ip icmp rate-limit unreachable
!
ip dhcp pool SERAGRO
 network 192.168.1.0 255.255.255.192
 default-router 192.168.1.1
 dns-server 8.8.8.8 4.4.4.4
!
ip dhcp pool DHRSI
 network 192.168.1.64 255.255.255.192
 default-router 192.168.1.65
 dns-server 8.8.8.8 4.4.4.4
!
ip dhcp pool SOPASP
 network 192.168.1.128 255.255.255.224
 default-router 192.168.1.129
 dns-server 8.8.8.8 4.4.4.4
!
ip dhcp pool SEF
 network 192.168.1.160 255.255.255.224
 default-router 192.168.1.161
 dns-server 8.8.8.8 4.4.4.4
!
```

```
ip dhcp pool DIRJ
 network 192.168.1.192 255.255.255.224
 default-router 192.168.1.193
 dns-server 8.8.8.8 4.4.4.4
!
no ip domain lookup
no ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
redundancy
!
ip tcp synwait-time 5
!
interface Ethernet0/0
 ip address 192.168.1.1 255.255.255.192
 duplex auto
!
interface Ethernet0/1
 ip address 192.168.1.65 255.255.255.192
 duplex auto
!
interface Ethernet0/2
 ip address 192.168.1.129 255.255.255.224
 duplex auto
!
interface Ethernet0/3
 ip address 192.168.1.161 255.255.255.224
 duplex auto
!
```

```
interface Ethernet1/0
 ip address 192.168.1.193 255.255.255.224
 duplex auto
!
interface Ethernet1/1
 ip address 172.16.1.2 255.255.255.252
 duplex auto
!
interface Ethernet1/2
 no ip address
 shutdown
 duplex auto
!
interface Ethernet1/3
 no ip address
 shutdown
 duplex auto
!
interface Serial2/0
R1(config)#do sh ip rou
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is not set
```

```
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.0/30 is directly connected, Ethernet1/1
L       172.16.1.2/32 is directly connected, Ethernet1/1
     192.168.1.0/24 is variably subnetted, 10 subnets, 3 masks
C       192.168.1.0/26 is directly connected, Ethernet0/0
L       192.168.1.1/32 is directly connected, Ethernet0/0
C       192.168.1.64/26 is directly connected, Ethernet0/1
L       192.168.1.65/32 is directly connected, Ethernet0/1
C       192.168.1.128/27 is directly connected, Ethernet0/2
L       192.168.1.129/32 is directly connected, Ethernet0/2
C       192.168.1.160/27 is directly connected, Ethernet0/3
L       192.168.1.161/32 is directly connected, Ethernet0/3
C       192.168.1.192/27 is directly connected, Ethernet1/0
L       192.168.1.193/32 is directly connected, Ethernet1/0
R1(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.1
R1(config)#end
R1#pi
*Apr  9 03:49:08.328: %SYS-5-CONFIG_I: Configured from console by console
R1#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R1#sh ip dhc
R1#sh ip dhcp bin
R1#sh ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.168.1.2         0100.5079.6668.1a       Apr 10 2024 01:36 AM    Automatic
```

```
192.168.1.3         0100.5079.6668.19       Apr 10 2024 01:37 AM    Automatic
192.168.1.66        0100.5079.6668.1b       Apr 10 2024 01:37 AM    Automatic
192.168.1.130       0100.5079.6668.15       Apr 10 2024 01:37 AM    Automatic
192.168.1.162       0100.5079.6668.18       Apr 10 2024 01:37 AM    Automatic
192.168.1.194       0100.5079.6668.14       Apr 10 2024 01:37 AM    Automatic
R1#
R1#ping 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/41/114 ms
R1#
R1#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R1#tracer
R1#traceroute 8.8.8.8
Type escape sequence to abort.
Tracing the route to 8.8.8.8
VRF info: (vrf in name/id, vrf out name/id)
  1  *  *  *
R1#
R1#sh ip rou
R1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
      a - application route
      + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is 172.16.1.1 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 172.16.1.1
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.0/30 is directly connected, Ethernet1/1
L       172.16.1.2/32 is directly connected, Ethernet1/1
     192.168.1.0/24 is variably subnetted, 10 subnets, 3 masks
C       192.168.1.0/26 is directly connected, Ethernet0/0
L       192.168.1.1/32 is directly connected, Ethernet0/0
C       192.168.1.64/26 is directly connected, Ethernet0/1
L       192.168.1.65/32 is directly connected, Ethernet0/1
C       192.168.1.128/27 is directly connected, Ethernet0/2
L       192.168.1.129/32 is directly connected, Ethernet0/2
C       192.168.1.160/27 is directly connected, Ethernet0/3
L       192.168.1.161/32 is directly connected, Ethernet0/3
C       192.168.1.192/27 is directly connected, Ethernet1/0
L       192.168.1.193/32 is directly connected, Ethernet1/0
R1#
R1#wr
Building configuration...
[OK]
R1#ping sou
R1#ping sour
R1#ping source
R1#ping 8.8.8.8 sour
R1#ping 8.8.8.8 source 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
```

```
Packet sent with a source address of 192.168.1.1
.....
Success rate is 0 percent (0/5)
R1#trace
R1#traceroute 8.8.8.8 sou
R1#traceroute 8.8.8.8 source 192.168.1.1
Type escape sequence to abort.
Tracing the route to 8.8.8.8
VRF info: (vrf in name/id, vrf out name/id)
  1  *  *  *
  2  *  *  *
R1#
R1#sh ip int bri
R1#sh ip int brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            192.168.1.1     YES manual up                    up
Ethernet0/1            192.168.1.65    YES manual up                    up
Ethernet0/2            192.168.1.129   YES manual up                    up
Ethernet0/3            192.168.1.161   YES manual up                    up
Ethernet1/0            192.168.1.193   YES manual up                    up
Ethernet1/1            172.16.1.2      YES manual up                    up
Ethernet1/2            unassigned      YES NVRAM  administratively down down
Ethernet1/3            unassigned      YES NVRAM  administratively down down
Serial2/0              unassigned      YES NVRAM  administratively down down
Serial2/1              unassigned      YES NVRAM  administratively down down
Serial2/2              unassigned      YES NVRAM  administratively down down
Serial2/3              unassigned      YES NVRAM  administratively down down
R1#sh ip rou
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
      a - application route
      + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is 172.16.1.1 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 172.16.1.1
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.0/30 is directly connected, Ethernet1/1
L       172.16.1.2/32 is directly connected, Ethernet1/1
     192.168.1.0/24 is variably subnetted, 10 subnets, 3 masks
C       192.168.1.0/26 is directly connected, Ethernet0/0
L       192.168.1.1/32 is directly connected, Ethernet0/0
C       192.168.1.64/26 is directly connected, Ethernet0/1
L       192.168.1.65/32 is directly connected, Ethernet0/1
C       192.168.1.128/27 is directly connected, Ethernet0/2
L       192.168.1.129/32 is directly connected, Ethernet0/2
C       192.168.1.160/27 is directly connected, Ethernet0/3
L       192.168.1.161/32 is directly connected, Ethernet0/3
C       192.168.1.192/27 is directly connected, Ethernet1/0
L       192.168.1.193/32 is directly connected, Ethernet1/0
R1#
R1#
R1#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R1#
R1#sh run
```

```
Building configuration...

Current configuration : 2741 bytes
!
! Last configuration change at 03:49:08 UTC Tue Apr 9 2024
!
version 15.7
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
no ip icmp rate-limit unreachable
!
ip dhcp pool SERAGRO
 network 192.168.1.0 255.255.255.192
 default-router 192.168.1.1
 dns-server 8.8.8.8 4.4.4.4
!
ip dhcp pool DHRSI
```

```
 network 192.168.1.64 255.255.255.192
 default-router 192.168.1.65
 dns-server 8.8.8.8 4.4.4.4
!
ip dhcp pool SOPASP
 network 192.168.1.128 255.255.255.224
 default-router 192.168.1.129
 dns-server 8.8.8.8 4.4.4.4
!
ip dhcp pool SEF
 network 192.168.1.160 255.255.255.224
 default-router 192.168.1.161
 dns-server 8.8.8.8 4.4.4.4
!
ip dhcp pool DIRJ
 network 192.168.1.192 255.255.255.224
 default-router 192.168.1.193
 dns-server 8.8.8.8 4.4.4.4
!
no ip domain lookup
no ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
redundancy
!
ip tcp synwait-time 5
!
!
interface Ethernet0/0
```

```
 ip address 192.168.1.1 255.255.255.192
 duplex auto
!
interface Ethernet0/1
 ip address 192.168.1.65 255.255.255.192
 duplex auto
!
interface Ethernet0/2
 ip address 192.168.1.129 255.255.255.224
 duplex auto
!
interface Ethernet0/3
 ip address 192.168.1.161 255.255.255.224
 duplex auto
!
interface Ethernet1/0
 ip address 192.168.1.193 255.255.255.224
 duplex auto
!
interface Ethernet1/1
 ip address 172.16.1.2 255.255.255.252
 duplex auto
!
interface Ethernet1/2
 no ip address
 shutdown
 duplex auto
!
interface Ethernet1/3
 no ip address
 shutdown
```

```
 duplex auto
!
interface Serial2/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/3
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/1
 no ip address
 shutdown
 serial restart-delay 0
```

```
!
interface Serial3/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/3
 no ip address
 shutdown
 serial restart-delay 0
!
router ospf 1
 network 192.168.1.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 172.16.1.1
!
ipv6 ioam timestamp
!
R1#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#no router ospf 1
R1(config)#end
R1#
*Apr  9 04:29:12.606: %SYS-5-CONFIG_I: Configured from console by console
R1#
R1#sh run
Building configuration...
```

```
Current configuration : 2687 bytes
!
! Last configuration change at 04:29:12 UTC Tue Apr 9 2024
!
version 15.7
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
no ip icmp rate-limit unreachable
!
ip dhcp pool SERAGRO
 network 192.168.1.0 255.255.255.192
 default-router 192.168.1.1
 dns-server 8.8.8.8 4.4.4.4
!
ip dhcp pool DHRSI
 network 192.168.1.64 255.255.255.192
 default-router 192.168.1.65
```

```
 dns-server 8.8.8.8 4.4.4.4
!
ip dhcp pool SOPASP
 network 192.168.1.128 255.255.255.224
 default-router 192.168.1.129
 dns-server 8.8.8.8 4.4.4.4
!
ip dhcp pool SEF
 network 192.168.1.160 255.255.255.224
 default-router 192.168.1.161
 dns-server 8.8.8.8 4.4.4.4
!
ip dhcp pool DIRJ
 network 192.168.1.192 255.255.255.224
 default-router 192.168.1.193
 dns-server 8.8.8.8 4.4.4.4
!
no ip domain lookup
no ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
redundancy
!
ip tcp synwait-time 5
!
interface Ethernet0/0
 ip address 192.168.1.1 255.255.255.192
 duplex auto
!
```

```
interface Ethernet0/1
 ip address 192.168.1.65 255.255.255.192
 duplex auto
!
interface Ethernet0/2
 ip address 192.168.1.129 255.255.255.224
 duplex auto
!
interface Ethernet0/3
 ip address 192.168.1.161 255.255.255.224
 duplex auto
!
interface Ethernet1/0
 ip address 192.168.1.193 255.255.255.224
 duplex auto
!
interface Ethernet1/1
 ip address 172.16.1.2 255.255.255.252
 duplex auto
!
interface Ethernet1/2
 no ip address
 shutdown
 duplex auto
!
interface Ethernet1/3
 no ip address
 shutdown
 duplex auto
!
interface Serial2/0
```

```
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/3
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/2
 no ip address
```

```
 shutdown
 serial restart-delay 0
!
interface Serial3/3
 no ip address
 shutdown
 serial restart-delay 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 172.16.1.1
!
ipv6 ioam timestamp
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
R1#copy run sta
R1#copy run startup-config
Destination filename [startup-config]?
```

Building configuration...

[OK]

R1#reload

Proceed with reload? [confirm]

*Apr 9 04:30:05.805: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.

unix_reload()

UNIX ERR:tcgetattr:Inappropriate ioctl for device

Restricted Rights Legend

Use, duplication, or disclosure by the Government is

subject to restrictions as set forth in subparagraph

(c) of the Commercial Computer Software - Restricted

Rights clause at FAR sec. 52.227-19 and subparagraph

(c) (1) (ii) of the Rights in Technical Data and Computer

Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.

170 West Tasman Drive

San Jose, California 95134-1706

Cisco IOS Software, Linux Software (I86BI_LINUX-ADVENTERPRISEK9-M), Version 15.7(3)M2, D EVELOPMENT

TEST SOFTWARE

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2018 by Cisco Systems, Inc.

Compiled Wed 28-Mar-18 11:18 by prod_rel_team

This product contains cryptographic features and is subject to United

States and local country laws governing import, export, transfer and

use. Delivery of Cisco cryptographic products does not imply

third-party authority to import, export, distribute or use encryption.

Importers, exporters, distributors and users are responsible for

compliance with U.S. and local country laws. By using this product you

agree to comply with applicable laws and regulations. If you are unable

to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
Linux Unix (Intel-x86) processor with 76825K bytes of memory.Installed image archive
Processor board ID 2048002
8 Ethernet interfaces
8 Serial interfaces
64K bytes of NVRAM.
Press RETURN to get started!
*Apr 9 04:30:17.118: %LINEPROTO-5-UPDOWN: Line protocol on Interface VoIP-Null0, change d state to up
*Apr 9 04:30:17.118: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*Apr 9 04:30:17.118: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to up
*Apr 9 04:30:17.119: %LINK-3-UPDOWN: Interface Ethernet0/2, changed state to up
*Apr 9 04:30:17.119: %LINK-3-UPDOWN: Interface Ethernet0/3, changed state to up
*Apr 9 04:30:17.119: %LINK-3-UPDOWN: Interface Ethernet1/0, changed state to up
*Apr 9 04:30:17.119: %LINK-3-UPDOWN: Interface Ethernet1/1, changed state to up
*Apr 9 04:30:17.120: %LINK-3-UPDOWN: Interface Ethernet1/2, changed state to up
*Apr 9 04:30:17.120: %LINK-3-UPDOWN: Interface Ethernet1/3, changed state to up
*Apr 9 04:30:17.120: %LINK-3-UPDOWN: Interface Serial2/0, changed state to up
*Apr 9 04:30:17.120: %LINK-3-UPDOWN: Interface Serial2/1, changed state to up
*Apr 9 04:30:17.120: %LINK-3-UPDOWN: Interface Serial2/2, changed state to up
*Apr 9 04:30:17.120: %LINK-3-UPDOWN: Interface Serial2/3, changed state to up
*Apr 9 04:30:17.120: %LINK-3-UPDOWN: Interface Serial3/0, changed state to up
*Apr 9 04:30:17.120: %LINK-3-UPDOWN: Interface Serial3/1, changed state to up
*Apr 9 04:30:17.120: %LINK-3-UPDOWN: Interface Serial3/2, changed state to up
*Apr 9 04:30:17.120: %LINK-3-UPDOWN: Interface Serial3/3, changed state to up
*Apr 9 04:30:17.415: %SYS-5-CONFIG_I: Configured from memory by console
*Apr 9 04:30:17.465: %SYS-5-RESTART: System restarted --

Cisco IOS Software, Linux Software (I86BI_LINUX-ADVENTERPRISEK9-M), Version 15.7(3)M2, D EVELOPMENT
TEST SOFTWARE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Wed 28-Mar-18 11:18 by prod_rel_team
*Apr 9 04:30:17.516: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
*Apr 9 04:30:17.516: %CRYPTO-6-GDOI_ON_OFF: GDOI is OFF
*Apr 9 04:30:18.126: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, chang ed state to up
*Apr 9 04:30:18.127: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, chang ed state to up
*Apr 9 04:30:18.127: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2, chang ed state to up
*Apr 9 04:30:18.127: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3, chang ed state to up
*Apr 9 04:30:18.127: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0, chang ed state to up
*Apr 9 04:30:18.127: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/1, chang ed state to up
*Apr 9 04:30:18.127: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/2, chang ed state to down
*Apr 9 04:30:18.127: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/3, chang ed state to down
*Apr 9 04:30:18.127: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to down
*Apr 9 04:30:18.127: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/1, changed state to down
*Apr 9 04:30:19.372: %LINK-5-CHANGED: Interface Ethernet1/2, changed state to administr atively down

*Apr 9 04:30:19.386: %LINK-5-CHANGED: Interface Ethernet1/3, changed state to administr atively down
*Apr 9 04:30:19.396: %LINK-5-CHANGED: Interface Serial2/0, changed state to administrat ively down
*Apr 9 04:30:19.396: %LINK-5-CHANGED: Interface Serial2/1, changed state to administrat ively down
*Apr 9 04:30:19.405: %LINK-5-CHANGED: Interface Serial2/2, changed state to administrat ively down
*Apr 9 04:30:19.405: %LINK-5-CHANGED: Interface Serial2/3, changed state to administrat ively down
*Apr 9 04:30:19.405: %LINK-5-CHANGED: Interface Serial3/0, changed state to administrat ively down
*Apr 9 04:30:19.413: %LINK-5-CHANGED: Interface Serial3/1, changed state to administrat ively down
*Apr 9 04:30:19.413: %LINK-5-CHANGED: Interface Serial3/2, changed state to administrat ively down
*Apr 9 04:30:19.413: %LINK-5-CHANGED: Interface Serial3/3, changed state to administrat ively down
*Apr 9 04:30:23.047: %PNP-6-PNP_DISCOVERY_STOPPED: PnP Discovery stopped (Startup Confi g Present)
R1#sh ip inter bri

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0/0	192.168.1.1	YES	NVRAM	up	up
Ethernet0/1	192.168.1.65	YES	NVRAM	up	up
Ethernet0/2	192.168.1.129	YES	NVRAM	up	up
Ethernet0/3	192.168.1.161	YES	NVRAM	up	up
Ethernet1/0	192.168.1.193	YES	NVRAM	up	up
Ethernet1/1	172.16.1.2	YES	NVRAM	up	up
Ethernet1/2	unassigned	YES	NVRAM	administratively down	down
Ethernet1/3	unassigned	YES	NVRAM	administratively down	down
Serial2/0	unassigned	YES	NVRAM	administratively down	down

Serial2/1	unassigned	YES NVRAM	administratively down	down
Serial2/2	unassigned	YES NVRAM	administratively down	down
Serial2/3	unassigned	YES NVRAM	administratively down	down
Serial3/0	unassigned	YES NVRAM	administratively down	down
Serial3/1	unassigned	YES NVRAM	administratively down	down
Serial3/2	unassigned	YES NVRAM	administratively down	down
Serial3/3	unassigned	YES NVRAM	administratively down	down

Script de la configuración del fortigate

```
FortiGate-VM64-KVM login: admin
Password:
You are forced to change your password. Please input a new password.
New Password:
Confirm Password:
Welcome!
FortiGate-VM64-KVM # config system interface
FortiGate-VM64-KVM (interface) # show
config system interface
    edit "port1"
        set vdom "root"
        set mode dhcp
        set allowaccess ping https ssh fgfm
        set type physical
        set snmp-index 1
    next
    edit "port2"
        set vdom "root"
        set type physical
        set snmp-index 2
    next
```

```
edit "port3"
    set vdom "root"
    set type physical
    set snmp-index 3
next
edit "port4"
    set vdom "root"
    set type physical
    set snmp-index 4
next
edit "port5"
    set vdom "root"
    set type physical
    set snmp-index 5
next
edit "port6"
    set vdom "root"
    set type physical
    set snmp-index 6
next
edit "port7"
    set vdom "root"
    set type physical
    set snmp-index 7
next
edit "port8"
    set vdom "root"
    set type physical
    set snmp-index 8
next
edit "port9"
```

```
        set vdom "root"
        set type physical
        set snmp-index 9
    next
    edit "port10"
        set vdom "root"
        set type physical
        set snmp-index 10
    next
    edit "ssl.root"
FortiGate-VM64-KVM (interface) # get
== [ port1 ]
name: port1  mode: dhcp  ip: 192.168.122.77 255.255.255.0  status: up  netbios-forward:
ng-rx: 0  ring-tx: 0  netflow-sampler: disable  sflow-sampler: disable  src-check: enablle
explicit-ftp-proxy: disable  proxy-captive-portal: disable  mtu-override: disable  ped-
fragment: disable  drop-fragment: disable
== [ port2 ]
name: port2  mode: static  ip: 0.0.0.0 0.0.0.0  status: up  netbios-forward: disable  ring-
tx: 0  netflow-sampler: disable  sflow-sampler: disable  src-check: enable  expliccit-ftp-
proxy: disable  proxy-captive-portal: disable  mtu-override: disable  wccp: disat: disable
drop-fragment: disable
== [ port3 ]
name: port3  mode: static  ip: 0.0.0.0 0.0.0.0  status: up  netbios-forward: disable  ring-
tx: 0  netflow-sampler: disable  sflow-sampler: disable  src-check: enable  expliccit-ftp-
proxy: disable  proxy-captive-portal: disable  mtu-override: disable  wccp: disat: disable
drop-fragment: disable
== [ port4 ]
name: port4  mode: static  ip: 0.0.0.0 0.0.0.0  status: up  netbios-forward: disable  ring-
tx: 0  netflow-sampler: disable  sflow-sampler: disable  src-check: enable  expliccit-ftp-
proxy: disable  proxy-captive-portal: disable  mtu-override: disable  wccp: disat: disable
drop-fragment: disable
```

```
== [ port5 ]
FortiGate-VM64-KVM (interface) # end
FortiGate-VM64-KVM # execute ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=127 time=67.5 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=68.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=67.1 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=73.2 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=127 time=66.6 ms
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 66.6/68.6/73.2 ms
FortiGate-VM64-KVM # conf system interface
FortiGate-VM64-KVM (interface) # edit port10
FortiGate-VM64-KVM (port10) # set ip 172.16.1.1 255.255.255.0
FortiGate-VM64-KVM (port10) # set allowaccess http ping https icmp
command parse error before 'icmp'
Command fail. Return code -61
FortiGate-VM64-KVM (port10) # set allowaccess http ping https telnet
FortiGate-VM64-KVM (port10) # net
Unknown action 0
FortiGate-VM64-KVM (port10) # show
config system interface
    edit "port10"
        set vdom "root"
        set ip 172.16.1.1 255.255.255.0
        set allowaccess ping https http telnet
        set type physical
        set snmp-index 10
    next
end
```

```
FortiGate-VM64-KVM (port10) #
FortiGate-VM64-KVM (port10) # end
FortiGate-VM64-KVM # conf router
access-list       Configure access lists.
access-list6      Configure IPv6 access lists.
aspath-list       Configure Autonomous System (AS) path lists.
auth-path         Configure authentication based routing.
bfd               Configure BFD.
bfd6              Configure IPv6 BFD.
bgp               Configure BGP.
community-list    Configure community lists.
isis              Configure IS-IS.
key-chain         Configure key-chain.
multicast         Configure router multicast.
multicast-flow    Configure multicast-flow.
multicast6        Configure IPv6 multicast.
ospf              Configure OSPF.
ospf6             Configure IPv6 OSPF.
policy            Configure IPv4 routing policies.
policy6           Configure IPv6 routing policies.
prefix-list       Configure IPv4 prefix lists.
prefix-list6      Configure IPv6 prefix lists.
rip               Configure RIP.
ripng             Configure RIPng.
route-map         Configure route maps.
setting           Configure router settings.
static            Configure IPv4 static routing tables.
static6           Configure IPv6 static routing tables.
FortiGate-VM64-KVM # conf router ospf 1
command parse error before '1'
Command fail. Return code 1
```

FortiGate-VM64-KVM # conf router ospf

<Enter>

FortiGate-VM64-KVM # conf router ospf

FortiGate-VM64-KVM (ospf) #

config Configure object.

set Modify value.

unset Set to default value.

select Select multi-option values.

unselect Unselect multi-option values.

append Append values to multi-option.

clear Clear multi-option values.

get Get dynamic and system information.

show Show configuration.

abort End and discard last config.

end End and save last config.

FortiGate-VM64-KVM (ospf) # Timeout

FortiGate-VM64-KVM login: admin

Password:

Welcome!

FortiGate-VM64-KVM # get system interface

== [port1]

name: port1 mode: dhcp ip: 192.168.122.77 255.255.255.0 status: up netbios-forward: ng-rx: 0 ring-tx: 0 netflow-sampler: disable sflow-sampler: disable src-check: enablle explicit-ftp-proxy: disable proxy-captive-portal: disable mtu-override: disable ped-fragment: disable drop-fragment: disable

== [port2]

name: port2 mode: static ip: 0.0.0.0 0.0.0.0 status: up netbios-forward: disable ring-tx: 0 netflow-sampler: disable sflow-sampler: disable src-check: enable expliccit-ftp-proxy: disable proxy-captive-portal: disable mtu-override: disable wccp: disat: disable drop-fragment: disable

== [port3]

name: port3 mode: static ip: 0.0.0.0 0.0.0.0 status: up netbios-forward: disable ring-tx: 0 netflow-sampler: disable sflow-sampler: disable src-check: enable expliccit-ftp-proxy: disable proxy-captive-portal: disable mtu-override: disable wccp: disat: disable drop-fragment: disable

== [port4]

name: port4 mode: static ip: 0.0.0.0 0.0.0.0 status: up netbios-forward: disable ring-tx: 0 netflow-sampler: disable sflow-sampler: disable src-check: enable expliccit-ftp-proxy: disable proxy-captive-portal: disable mtu-override: disable wccp: disat: disable drop-fragment: disable

== [port5]

FortiGate-VM64-KVM # get system interface

== [port1]

name: port1 mode: dhcp ip: 192.168.122.77 255.255.255.0 status: up netbios-forward: ng-rx: 0 ring-tx: 0 netflow-sampler: disable sflow-sampler: disable src-check: enablle explicit-ftp-proxy: disable proxy-captive-portal: disable mtu-override: disable ped-fragment: disable drop-fragment: disable

== [port2]

name: port2 mode: static ip: 0.0.0.0 0.0.0.0 status: up netbios-forward: disable ring-tx: 0 netflow-sampler: disable sflow-sampler: disable src-check: enable expliccit-ftp-proxy: disable proxy-captive-portal: disable mtu-override: disable wccp: disat: disable drop-fragment: disable

== [port3]

name: port3 mode: static ip: 0.0.0.0 0.0.0.0 status: up netbios-forward: disable ring-tx: 0 netflow-sampler: disable sflow-sampler: disable src-check: enable expliccit-ftp-proxy: disable proxy-captive-portal: disable mtu-override: disable wccp: disat: disable drop-fragment: disable

== [port4]

name: port4 mode: static ip: 0.0.0.0 0.0.0.0 status: up netbios-forward: disable ring-tx: 0 netflow-sampler: disable sflow-sampler: disable src-check: enable expliccit-ftp-proxy: disable proxy-captive-portal: disable mtu-override: disable wccp: disat: disable drop-fragment: disable

== [port5]

name: port5 mode: static ip: 0.0.0.0 0.0.0.0 status: up netbios-forward: disable ring-tx: 0 netflow-sampler: disable sflow-sampler: disable src-check: enable expliccit-ftp-proxy: disable proxy-captive-portal: disable mtu-override: disable wccp: disat: disable drop-fragment: disable

== [port6]

name: port6 mode: static ip: 0.0.0.0 0.0.0.0 status: up netbios-forward: disable ring-tx: 0 netflow-sampler: disable sflow-sampler: disable src-check: enable expliccit-ftp-proxy: disable proxy-captive-portal: disable mtu-override: disable wccp: disat: disable drop-fragment: disable

== [port7]

name: port7 mode: static ip: 0.0.0.0 0.0.0.0 status: up netbios-forward: disable ring-tx: 0 netflow-sampler: disable sflow-sampler: disable src-check: enable expliccit-ftp-proxy: disable proxy-captive-portal: disable mtu-override: disable wccp: disat: disable drop-fragment: disable

== [port8]

name: port8 mode: static ip: 0.0.0.0 0.0.0.0 status: up netbios-forward: disable ring-tx: 0 netflow-sampler: disable sflow-sampler: disable src-check: enable expliccit-ftp-proxy: disable proxy-captive-portal: disable mtu-override: disable wccp: disat: disable drop-fragment: disable

== [port9]

name: port9 mode: static ip: 0.0.0.0 0.0.0.0 status: up netbios-forward: disable ring-tx: 0 netflow-sampler: disable sflow-sampler: disable src-check: enable expliccit-ftp-proxy: disable proxy-captive-portal: disable mtu-override: disable wccp: disat: disable drop-fragment: disable

== [port10]

name: port10 mode: static ip: 172.16.1.1 255.255.255.0 status: up netbios-forward: dg-rx: 0 ring-tx: 0 netflow-sampler: disable sflow-sampler: disable src-check: enablee explicit-ftp-proxy: disable proxy-captive-portal: disable mtu-override: disable ed-fragment: disable drop-fragment: disable

== [ssl.root]

name: ssl.root ip: 0.0.0.0 0.0.0.0 status: up netbios-forward: disable type: tunnel sflow-sampler: disable src-check: enable explicit-web-proxy: disable explicit-ftp-proortal: disable wccp: disable

== [fortilink]

name: fortilink mode: static ip: 169.254.1.1 255.255.255.0 status: up netbios-forwar netflow-sampler: disable sflow-sampler: disable src-check: enable explicit-web-proxxy: disable proxy-captive-portal: disable mtu-override: disable wccp: disable drop drop-fragment: disable

FortiGate-VM64-KVM #

FortiGate-VM64-KVM # Timeout

FortiGate-VM64-KVM login:

GRGCHVM login: en

Password:

Login incorrect

GRGCHVM login: admin

Password:

Welcome!

WARNING: File System Check Recommended! An unsafe reboot may have caused an inconsistenc y in the disk drive.

It is strongly recommended that you check the file system consistency before proceeding.

Please run 'execute disk list' and then 'execute disk scan <ref#>'.

Note: The device will reboot and scan the disk during startup. This may take up to an ho ur.

GRGCHVM #

GRGCHVM # execute ping 8.8.8.8

PING 8.8.8.8 (8.8.8.8): 56 data bytes

64 bytes from 8.8.8.8: icmp_seq=0 ttl=127 time=72.7 ms

64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=70.3 ms

64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=67.8 ms

64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=70.5 ms

64 bytes from 8.8.8.8: icmp_seq=4 ttl=127 time=68.1 ms

--- 8.8.8.8 ping statistics ---

5 packets transmitted, 5 packets received, 0% packet loss

round-trip min/avg/max = 67.8/69.8/72.7 ms

GRGCHVM # execute ping 192.168.1.2

PING 192.168.1.2 (192.168.1.2): 56 data bytes

64 bytes from 192.168.1.2: icmp_seq=0 ttl=63 time=38.3 ms

64 bytes from 192.168.1.2: icmp_seq=1 ttl=63 time=2.4 ms

64 bytes from 192.168.1.2: icmp_seq=2 ttl=63 time=9.1 ms

64 bytes from 192.168.1.2: icmp_seq=3 ttl=63 time=1.0 ms

64 bytes from 192.168.1.2: icmp_seq=4 ttl=63 time=2.5 ms

--- 192.168.1.2 ping statistics ---

5 packets transmitted, 5 packets received, 0% packet loss

round-trip min/avg/max = 1.0/10.6/38.3 ms

GRGCHVM # execute ping 192.168.1.194

PING 192.168.1.194 (192.168.1.194): 56 data bytes

64 bytes from 192.168.1.194: icmp_seq=0 ttl=63 time=78.5 ms

64 bytes from 192.168.1.194: icmp_seq=1 ttl=63 time=3.3 ms

64 bytes from 192.168.1.194: icmp_seq=2 ttl=63 time=1.8 ms

64 bytes from 192.168.1.194: icmp_seq=3 ttl=63 time=1.8 ms

64 bytes from 192.168.1.194: icmp_seq=4 ttl=63 time=0.9 ms

--- 192.168.1.194 ping statistics ---

5 packets transmitted, 5 packets received, 0% packet loss

round-trip min/avg/max = 0.9/17.2/78.5 ms

GRGCHVM # Timeout

GRGCHVM login: admin

Password:

Welcome!

WARNING: File System Check Recommended! An unsafe reboot may have caused an inconsistenc y in the disk drive.

It is strongly recommended that you check the file system consistency before proceeding.

Please run 'execute disk list' and then 'execute disk scan <ref#>'.

Note: The device will reboot and scan the disk during startup. This may take up to an ho ur.

GRGCHVM # execute traceroute 8.8.8.8

traceroute to 8.8.8.8 (8.8.8.8), 32 hops max, 3 probe packets per hop, 84 byte packets

1 192.168.122.1 <192.168.122.1> 1.560 ms 3.527 ms 2.349 ms

2 192.168.88.2 <192.168.88.2> 1.302 ms 2.122 ms 2.441 ms

3 192.168.1.1 <gpon.net> 4.579 ms 4.174 ms 5.814 ms

4 10.11.254.119 <10.11.254.119> 8.647 ms 10.934 ms 9.957 ms

5 10.149.222.38 <10.149.222.38> 15.574 ms 9.755 ms 10.424 ms

6 10.149.220.162 <10.149.220.162> 7.899 ms 13.899 ms 23.266 ms

7 190.129.248.231 19.477 ms 17.706 ms 16.276 ms

8 190.129.248.5 15.142 ms 15.668 ms 16.101 ms

9 190.129.248.17 17.851 ms 16.047 ms 21.485 ms

10 209.85.149.62 74.459 ms 85.910 ms 83.268 ms

11 142.250.62.21 82.364 ms 80.066 ms 73.741 ms

12 72.14.237.143 74.566 ms 74.395 ms 72.219 ms

13 8.8.8.8 <dns.google> 68.329 ms 69.649 ms 72.180 ms

GRGCHVM # Timeout

GRGCHVM login: admin

Password:

Welcome!

WARNING: File System Check Recommended! An unsafe reboot may have caused an inconsistenc y in the disk drive.

It is strongly recommended that you check the file system consistency before proceeding.

Please run 'execute disk list' and then 'execute disk scan <ref#>'.

Note: The device will reboot and scan the disk during startup. This may take up to an ho ur.

GRGCHVM # execute traceroute 8.8.8.8

traceroute to 8.8.8.8 (8.8.8.8), 32 hops max, 3 probe packets per hop, 84 byte packets

1 192.168.122.1 <192.168.122.1> 1.053 ms 0.940 ms 1.228 ms

2 192.168.88.2 8.928 ms 0.954 ms 2.698 ms

3 192.168.1.1 <gpon.net> 5.318 ms 7.877 ms 4.878 ms

4 10.11.254.119 5.644 ms 6.401 ms 5.944 ms

5 10.149.222.38 <10.149.222.38> 6.785 ms 5.138 ms 6.595 ms

6 10.149.220.162 7.157 ms 8.819 ms 6.479 ms

7 190.129.248.231 20.692 ms 15.506 ms 14.208 ms

8 190.129.248.5 16.050 ms 15.302 ms 14.776 ms

9 190.129.248.17 17.176 ms 16.238 ms 16.328 ms

10 209.85.149.62 73.589 ms 73.531 ms 72.558 ms

11 142.250.62.21 71.236 ms 76.095 ms 72.269 ms

12 72.14.237.143 72.763 ms 74.997 ms 73.653 ms

13 8.8.8.8 <dns.google> 69.021 ms 67.492 ms 66.786 ms

GRGCHVM # execute traceroute 8.8.8.8

traceroute to 8.8.8.8 (8.8.8.8), 32 hops max, 3 probe packets per hop, 84 byte packets

1 127.0.0.1 2997.460 ms !H 1436.679 ms !H 2992.618 ms !H

GRGCHVM # execute traceroute 8.8.8.8

traceroute to 8.8.8.8 (8.8.8.8), 32 hops max, 3 probe packets per hop, 84 byte packets

1 192.168.122.1 0.911 ms 1.877 ms 1.458 ms

2 192.168.88.2 <192.168.88.2> 3.636 ms 1.971 ms 2.927 ms

3 192.168.1.1 5.142 ms 6.114 ms 6.144 ms

4 10.11.254.119 6.418 ms 18.728 ms 5.416 ms

5 10.149.222.38 <10.149.222.38> 5.629 ms 4.983 ms 5.373 ms

6 10.149.220.162 5.958 ms 6.504 ms 6.740 ms

7 190.129.248.231 15.985 ms 14.966 ms 14.399 ms

8 190.129.248.5 15.199 ms 15.978 ms 15.623 ms

9 190.129.248.17 15.260 ms 21.744 ms 15.947 ms

10 209.85.149.62 73.412 ms 71.516 ms 73.145 ms

11 142.250.62.21 73.477 ms 73.337 ms 71.475 ms

12 72.14.237.143 72.841 ms 72.819 ms 72.239 ms

13 8.8.8.8 <dns.google> 68.234 ms 66.416 ms 67.232 ms

GRGCHVM # execute ping 192.168.1.2

PING 192.168.1.2 (192.168.1.2): 56 data bytes

--- 192.168.1.2 ping statistics ---

5 packets transmitted, 0 packets received, 100% packet loss

GRGCHVM # execute ping 192.168.1.2

PING 192.168.1.2 (192.168.1.2): 56 data bytes

--- 192.168.1.2 ping statistics ---

5 packets transmitted, 0 packets received, 100% packet loss

GRGCHVM # Timeout

GRGCHVM login: admin

Password:

Welcome!

WARNING: File System Check Recommended! An unsafe reboot may have caused an inconsistenc y in the disk drive.

It is strongly recommended that you check the file system consistency before proceeding.

Please run 'execute disk list' and then 'execute disk scan <ref#>'.

Note: The device will reboot and scan the disk during startup. This may take up to an ho ur.

GRGCHVM # execute ping 8.8.8.8

PING 8.8.8.8 (8.8.8.8): 56 data bytes

64 bytes from 8.8.8.8: icmp_seq=0 ttl=127 time=70.3 ms

64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=69.6 ms

64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=68.4 ms

64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=67.8 ms

64 bytes from 8.8.8.8: icmp_seq=4 ttl=127 time=71.6 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 67.8/69.5/71.6 ms
GRGCHVM # execute ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=4.5 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=1.1 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.7 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=5.1 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.7 ms
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.7/2.4/5.1 ms
GRGCHVM # execute ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2): 56 data bytes
64 bytes from 192.168.1.2: icmp_seq=0 ttl=63 time=3.1 ms
64 bytes from 192.168.1.2: icmp_seq=1 ttl=63 time=1.4 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=63 time=1.2 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=63 time=1.3 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=63 time=1.2 ms
--- 192.168.1.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.2/1.6/3.1 ms
GRGCHVM # execute ping 192.168.1.66
PING 192.168.1.66 (192.168.1.66): 56 data bytes
64 bytes from 192.168.1.66: icmp_seq=0 ttl=63 time=77.1 ms
64 bytes from 192.168.1.66: icmp_seq=1 ttl=63 time=1.2 ms
64 bytes from 192.168.1.66: icmp_seq=2 ttl=63 time=1.1 ms
64 bytes from 192.168.1.66: icmp_seq=3 ttl=63 time=1.9 ms
64 bytes from 192.168.1.66: icmp_seq=4 ttl=63 time=17.9 ms
--- 192.168.1.66 ping statistics ---

5 packets transmitted, 5 packets received, 0% packet loss

round-trip min/avg/max = 1.1/19.8/77.1 ms

GRGCHVM # Timeout

GRGCHVM login:

The system is going down NOW !!

Please stand by while rebooting the system.

Restarting system.

System is starting...

Serial number is FGVMEVPNT-IRPPF3

Scanning /dev/vdb1... (100%)

III.1.4.4.3. Cantidad de Recursos que se compartirán en la red

Departamento	Cantidad de Recursos	Números de Puntos de Red
Seragro	-1 Switch -1 Impresora - 35PC -1 DHCP	48(1 Impresora Compartida + 35PC + 1 Switch + 1 DHCP + 10 puntos Extras
SRHSI (Oficina De Despacho, Recursos Humanos Y Sistemas)	-1 Switch -1 Impresora -1 DHCP - 35PC -1 Router	48(1 Impresora Compartida + 30PC + 1 Switch + 1 DHCP + 1 Router + 15 puntos Extras
SOPASP (Oficina de Secretaria de Obras Publica, almacén, Secretaria de Planificación)	-1 Switch -1 Impresora - 35PC -1 DHCP	48(1 Impresora Compartida + 15PC + 1 Switch + 1 DHCP + 30 puntos Extras
SEF (Oficina De Secretaría de Economía Y Finanzas)	-1 Switch -1 Impresora - 35PC -1 DHCP	48(1 Impresora Compartida + 15PC + 1 Switch + 1 DHCP + 30puntos Extras
DIRJ (Oficina De Dirección Jurídica)	-1 Switch -1 Impresora - 35PC -1 DHCP	48(1 Impresora Compartida + 15PC + 1 Switch + 1 DHCP +30puntos Extras
SDP (Oficina De Secretaria de Desarrollo Productivo)	-1 Switch -1 Impresora - 35PC -1 DHCP	48(1 Impresora Compartida + 15PC + 1 Switch + 1 DHCP +30 puntos Extras
Total, de Puntos Físicos de Red		143 puntos y 145 el resto se conectará por wifi

Tabla 13. *Cantidad de Recursos que se compartirán en la red*

III.1.4.5. Simulador en packet tracer Físico

Figura 48. Simulador en Packet Tracer Físico

III.1.4.5.1. Cableado de la Oficina Subred A SERAGRO

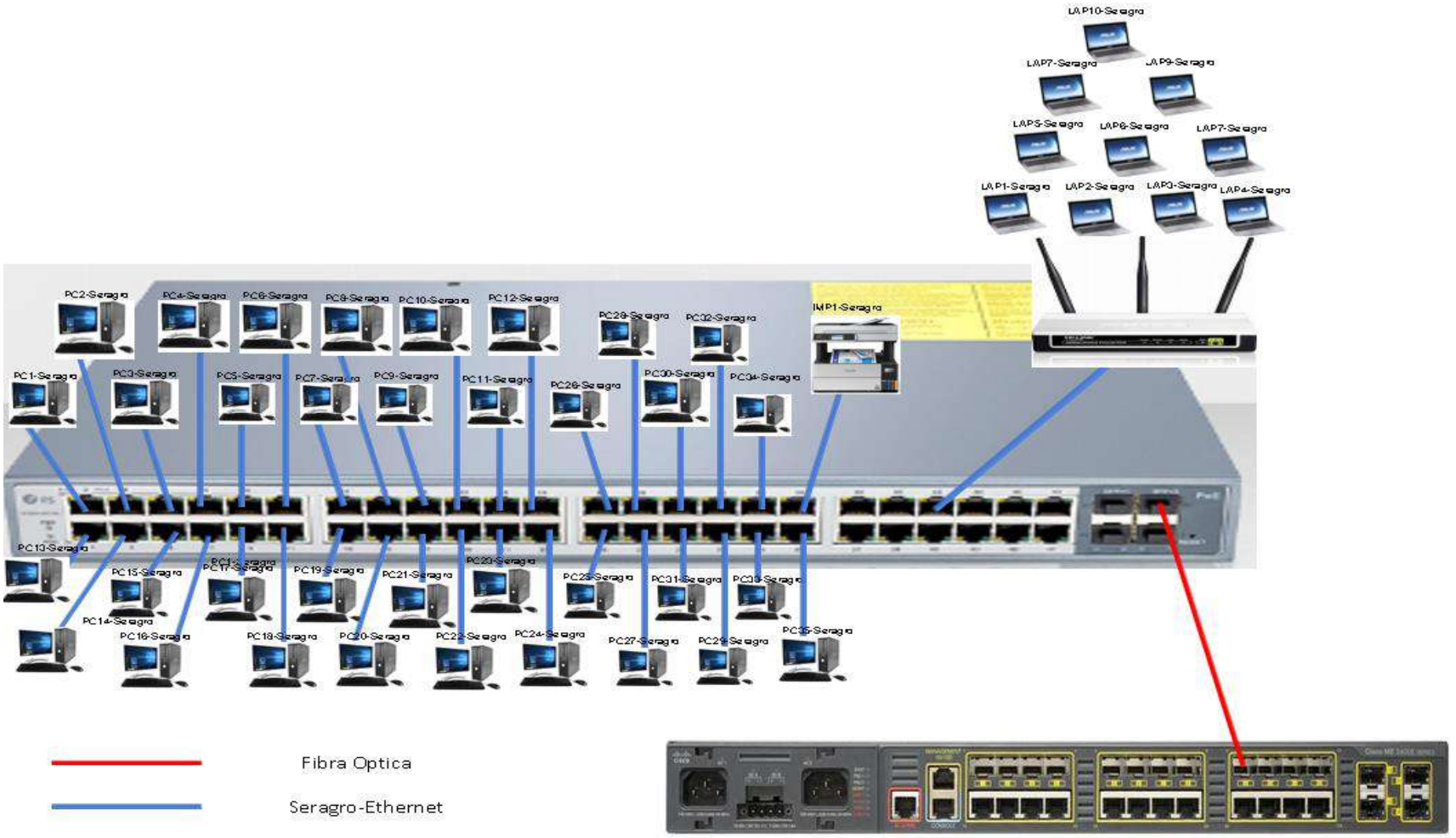


Figura 49. Cableado de red de la Oficina Subred A SERAGRO

Figura 50. Ambiente de Distribución del Cableado de la Oficina de Seragro

Información detallada en la pag139-144

Figura 51. Oficina Seragro/Oficina de Apoyos a Pequeños Productos

Figura 52. Oficina de Seragro/Oficina de Fomento y Desarrollo Rural

Figura 53. Oficina de Seragro/Oficina de Certificación Orgánica

Figura 54. Oficina de Seragro/ Oficina de Asesoramiento Legal

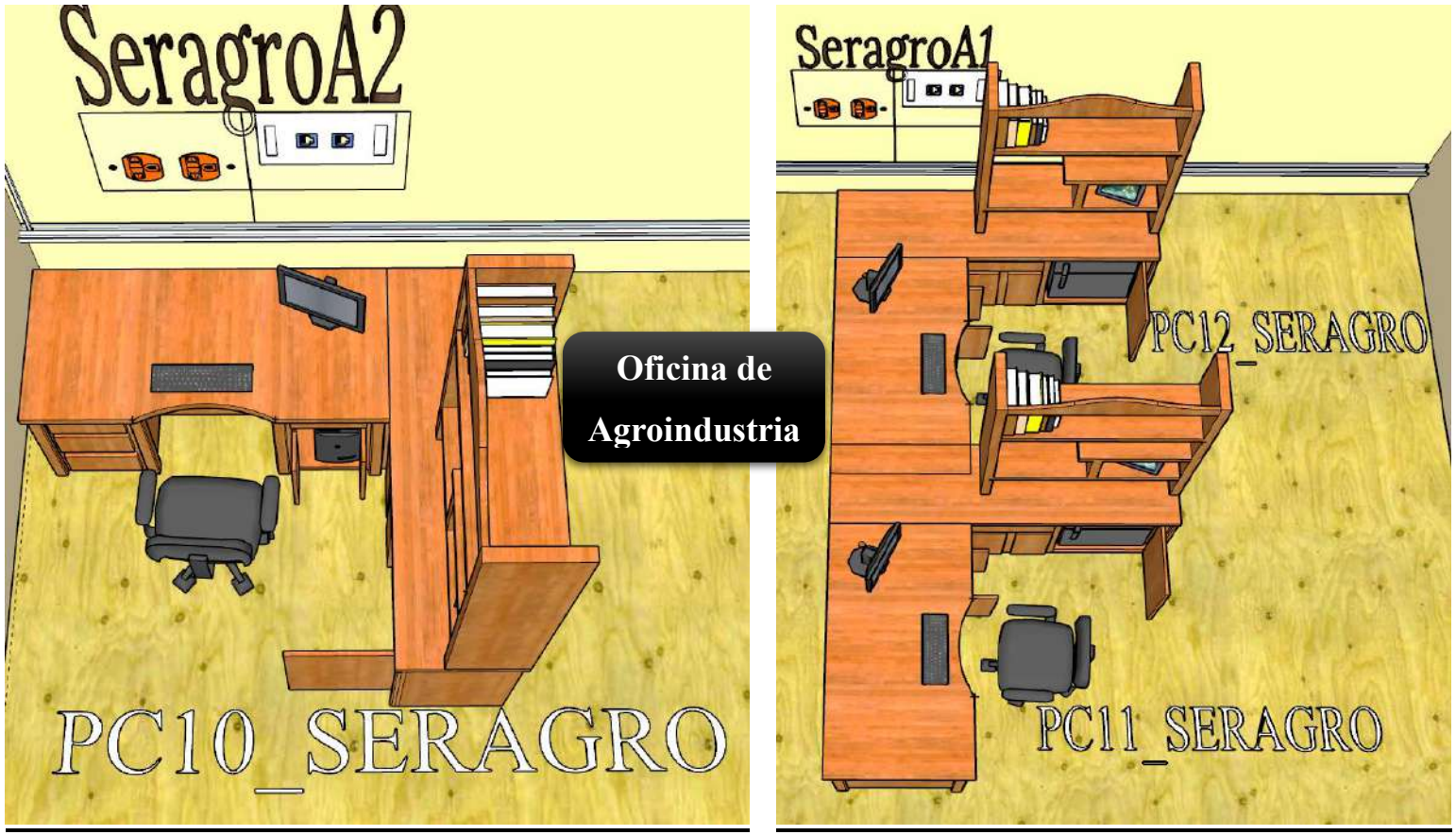


Figura 55. Oficina de Seragro/ Oficina de Agroindustria

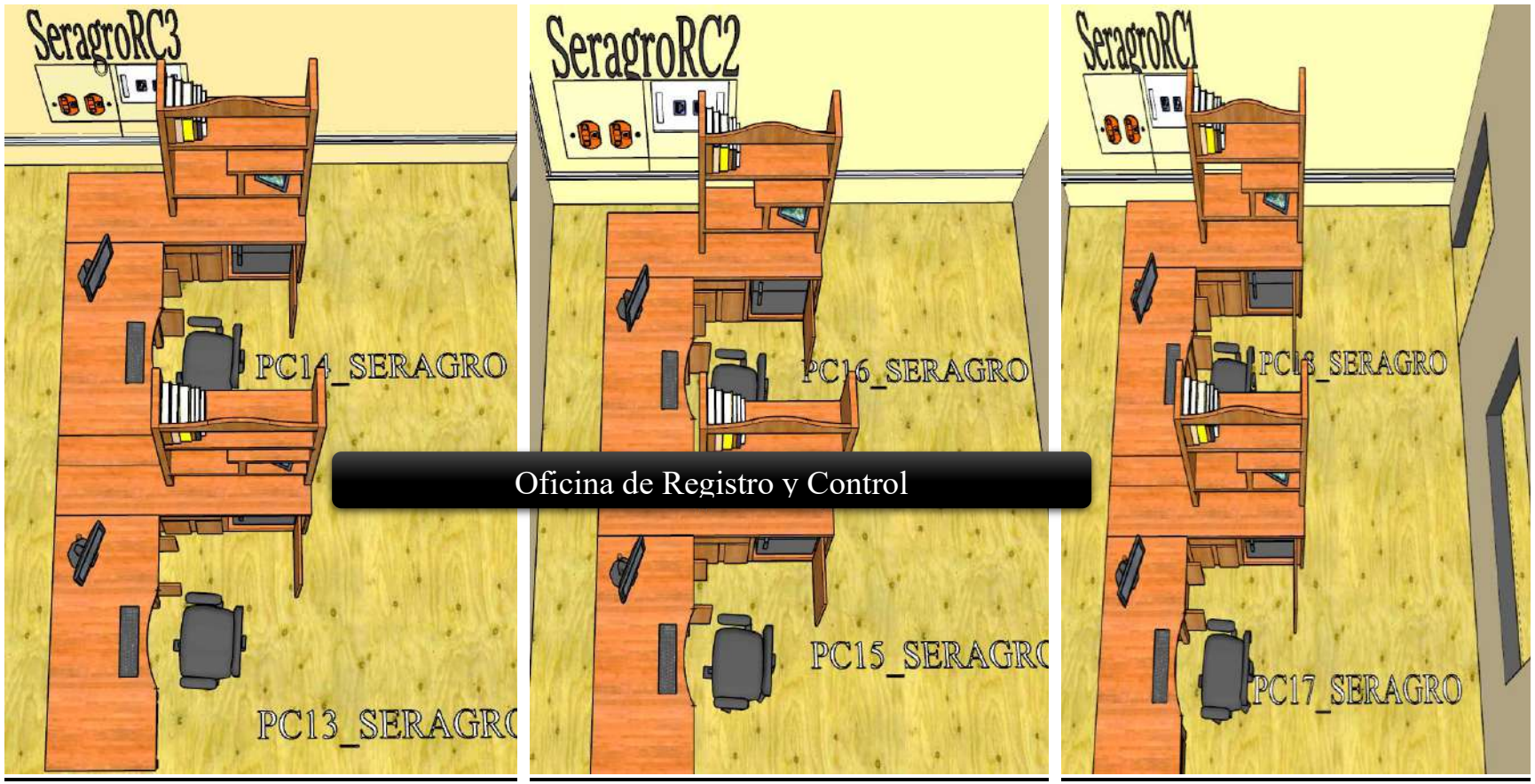


Figura 56. Oficina de Seragro/Oficina de Registro y Control

Figura 57. Oficina de Seragro/ Oficina Desarrollo Productivo

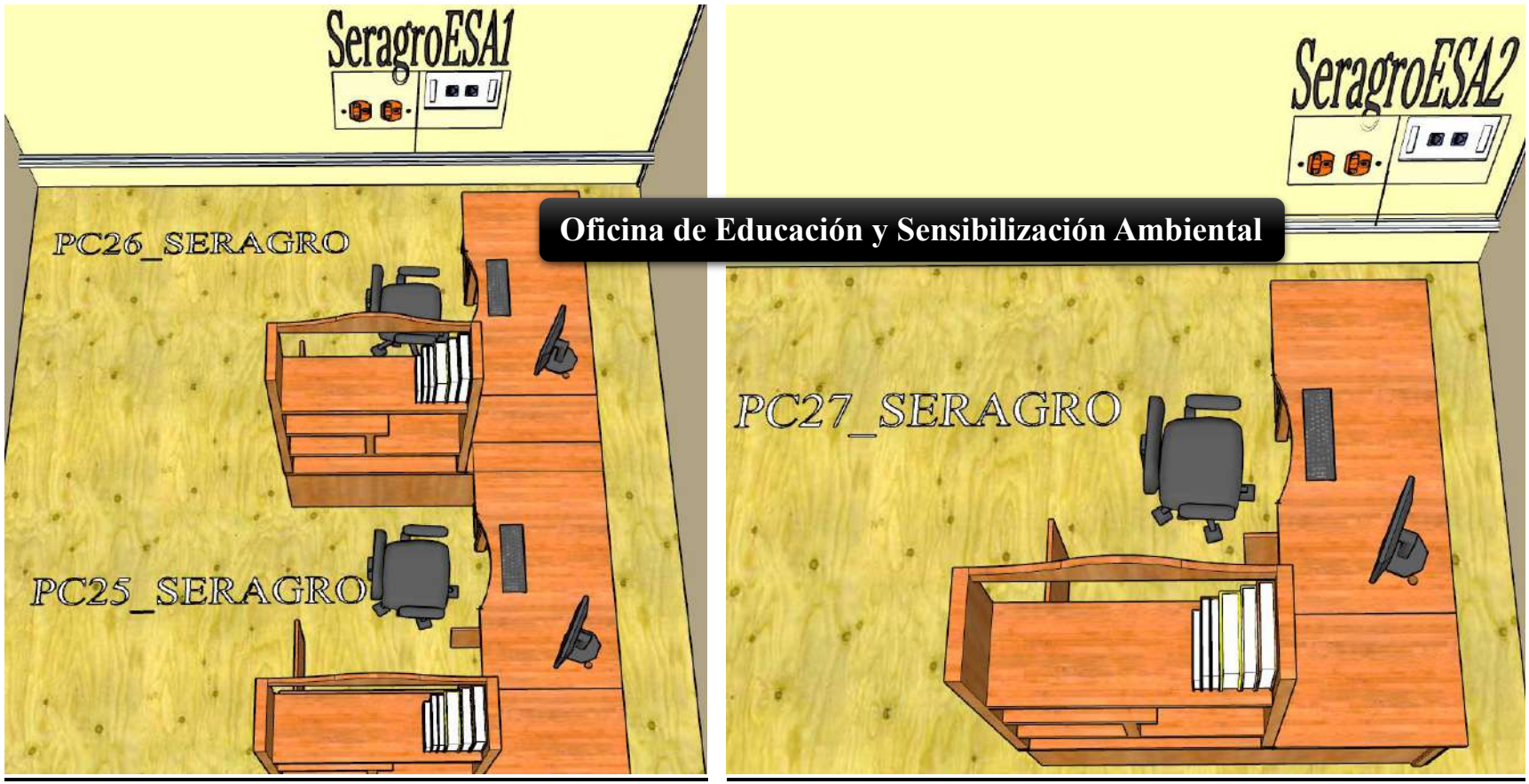


Figura 58. Oficina de Seragro/Oficina de Educación y Sensibilización ambiental

Figura 59. Oficina de Seragro/ Oficina de Administración de Recursos

Figura 60. Oficina de Seragro/Oficina de Política y Normativa

OFICINAS POLITICAS NORMATIVAS **Tamaño aprox**

Materiales	Cantidad
Cortapicos	6
Patch Cords RJ45 -3 metros	3
Cable canal	12
Cable UTP cat 6	168
Rosetas RJ 45	3
Keystone RJ45	6

Puntos de Red		
SeragroPN1	192.168.1.4	OCUPADO
SeragroPN1	192.168.1.5	LIBRE
SeragroPN2	192.168.1.6	OCUPADO
SeragroPN2	192.168.1.7	LIBRE
SeragroPN3	192.168.1.8	OCUPADO
SeragroPN3	192.168.1.9	LIBRE

OF. PEQUEÑOS PRODUCTORES **Tamaño aprox**

Materiales	Cantidad
Cortapicos	3
Patch Cords RJ45 -3 metros	3
Cable canal	12
Cable UTP cat 6	132
Rosetas RJ 45	3
Keystone RJ45	6

Puntos de Red		
SeragroAPP1	192.168.1.10	OCUPADO
SeragroAPP1	192.168.1.11	LIBRE
SeragroAPP2	192.168.1.12	OCUPADO
Serag2oAPP1	192.168.1.13	LIBRE
SeragroAPP3	192.168.1.14	OCUPADO
SeragroAPP3	192.168.1.15	LIBRE

OFICINA DESARROLLO PRODUCTIVO **Tamaño aprox**

Materiales	Cantidad
Cortapicos	6

OF. FOMENTO AL DESARROLLO **Tamaño aprox**

Materiales	Cantidad
Cortapicos	2

Patch Cords RJ45 -3 metros	6
Cable canal	12
Cable UTP cat 6	138
Rosetas RJ 45	3
Keystone RJ45	6

Puntos de Red		
SeragroDP1	192.168.1.16	OCUPADO
SeragroDP1	192.168.1.17	LIBRE
SeragroDP2	192.168.1.18	OCUPADO
SeragroDP2	192.168.1.19	LIBRE
SeragroDP3	192.168.1.20	OCUPADO
SeragroDP3	192.168.1.21	LIBRE

Patch Cords RJ45 -3 metros	2
Cable canal	8
Cable UTP cat 6	94
Rosetas RJ 45	2
Keystone RJ45	4

Puntos de Red		
SeragroFDR1	192.168.1.22	OCUPADO
SeragroFDR1	192.168.1.23	LIBRE
SeragroFDR2	192.168.1.24	OCUPADO
SeragroFDR2	192.168.1.25	LIBRE

OFICINAS REGISTRO CONTROL **Tamaño aprox**

Materiales	Cantidad
Cortapicos	6
Patch Cords RJ45 -3 metros	6
Cable canal	12
Cable UTP cat 6	138
Rosetas RJ 45	3

OFICINA CERT. ORGANICA **Tamaño aprox**

Materiales	Cantidad
Cortapicos	2
Patch Cords RJ45 -3 metros	2
Cable canal	4
Cable UTP cat 6	38
Rosetas RJ 45	2

Keystone RJ45	6		Keystone RJ45	4	
Puntos de Red			**Puntos de Red**		
SeragroRC1	192.168.1.26	OCUPADO	SeragroCO1	192.168.1.32	OCUPADO
SeragroRC1	192.168.1.27	LIBRE	SeragroCO1	192.168.1.33	LIBRE
SeragroRC2	192.168.1.28	OCUPADO	SeragroCO2	192.168.1.34	OCUPADO
SeragroRC2	192.168.1.29	LIBRE	SeragroCO2	192.168.1.35	LIBRE
SeragroRC3	192.168.1.30	OCUPADO			
SeragroRC3	192.168.1.31	LIBRE			

OF. AMBIENTAL **SENSIBILIZACION** **Tamaño aprox**

Materiales	**Cantidad**
Cortapicos	2
Patch Cords RJ45 -3 metros	2
Cable canal	8
Cable UTP cat 6	62
Rosetas RJ 45	2
Keystone RJ45	4
Puntos de Red	
SeragroESA1	192.168.1.36 OCUPADO

SALA DE REUNIONES **Tamaño aprox**

Materiales	**Cantidad**
Cortapicos	3
Patch Cords RJ45 -3 metros	0
Cable canal	0
Cable UTP cat 6	0
Rosetas RJ 45	0
Keystone RJ45	0

SeragroESA1	192.168.1.37	LIBRE
SeragroESA2	192.168.1.38	OCUPADO
SeragroESA2	192.168.1.39	LIBRE

OF. AGROINDUSTRIA	**Tamaño aprox**
Materiales	**Cantidad**
Cortapicos	2
Patch Cords RJ45 -3 metros	2
Cable canal	8
Cable UTP cat 6	62
Rosetas RJ 45	2
Keystone RJ45	4

LAP SERAGRO	**Tamaño aprox**
Materiales	**Cantidad**
Cortapicos	6
Patch Cords RJ45 -3 metros	0
Cable canal	0
Cable UTP cat 6	0
Rosetas RJ 45	0
Keystone RJ45	0

Puntos de Red		
SeragroA1	192.168.1.40	OCUPADO
SeragroA1	192.168.1.41	LIBRE
SeragroA2	192.168.1.42	OCUPADO
SeragroA1	192.168.1.43	LIBRE

Of. Ad. Recursos	**Tamaño aprox**
Materiales	**Cantidad**
Cortapicos	2
Patch Cords RJ45 -3 metros	2

Of. Asesoramiento legal	**Tamaño aprox**
Materiales	**Cantidad**
Cortapicos	2
Patch Cords RJ45 -3 metros	2

Cable canal	8
Cable UTP cat 6	46
Rosetas RJ 45	2
Keystone RJ45	4

Puntos de Red		
SeragroAR1	192.168.1.44	OCUPADO
SeragroAR1	192.168.1.45	LIBRE
SeragroAR2	192.168.1.46	OCUPADO
SeragroAR2	192.168.1.47	LIBRE

Cable canal	8
Cable UTP cat 6	46
Rosetas RJ 45	2
Keystone RJ45	4

Puntos de Red		
SeragroAL1	192.168.1.48	OCUPADO
SeragroAL1	192.168.1.49	LIBRE
SeragroAL2	192.168.1.50	OCUPADO
SeragroAL2	192.168.1.51	LIBRE

Materiales adicionales	CANTIDAD
ESCALERILLA HORIZONTAL HACIA SALA DE EQUIPOS	54
Cable UTP Cat 6 Instalacion router wifi	47
Conecor Rj 45 Cat 6	2
Cable Canal	5
EQUIPO WIFI	3

SALA DE SISTEMAS

	Patch Panel 12 puertos	**Switch L2 12 GE - 2 SFP/GE Patch Cords RJ45**	**Patch Cords RJ45**	**Roseta Optica 4 Puertos**	**Patch - cords Duplex LC-LC/SM**	**Acopladores LC/SM Duplex**	**Acopladores LC/SM Duplex**	**Fibra 4 hilos DROP metros**	Tensores Fibra Drop

OFICINA DIRECCION JURIDICA	2	1	24	1	1	2	4	89	**8**
OFICINA ECONOMIA Y FINANZAS	2	1	24	1	1	2	4	60	**4**
SECRETARIA DESARROLO PRODUCTIVO	2	1	24	1	1	2	4	295	**20**
SECRETARIA O.PUBLICAS-ALM-PLAN	2	1	24	1	1	2	4	85	**8**
OFICINA SRHI	2	1	24	1	1	2	4		
SERAGRO	**2**	**1**	**24**	**1**	**1**	**2**	**4**	**320**	**30**

OFICINA SISTEMAS	Cant.
Switch Core L3 48 Puertos GE/SFP	1
Router / Firewall GE-2SFP	1
Bandejan ODF 48 Puertos LC-LC /SM	1
Acopladoresv LC/SM Duplex	12
Pigtails LC-LC/SM	24
Patch Cords LC-LC/SM duplex	12
Fibra 24 Hilos	150 metros
Caja de Empalme fibas 24 Hilos	1
Cruceta de Reserva Fibra Optica	1

III.1.4.5.2. Cableado de la Oficina Subred B (DESARROLLO, RECURSOS HUMANOS Y SISTEMAS)

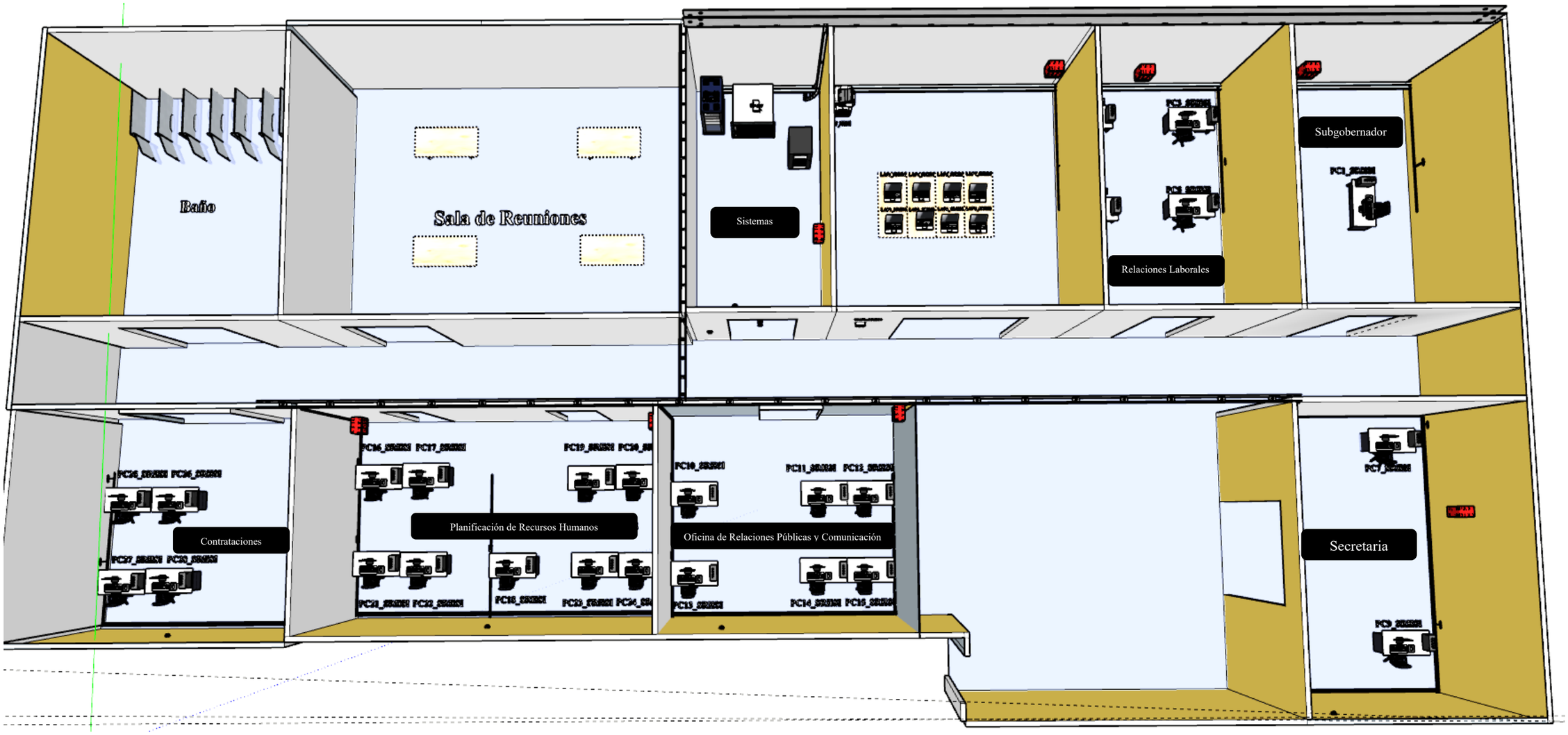


Figura 61. Ambiente de distribución del Cableado de la Oficina de Desarrollo, Recursos Humanos Y Sistemas

Información detallada en la pag154-157

Figura 62. Oficina de Desarrollo, Recursos Humanos Y Sistemas/Oficina del Sugbobernador

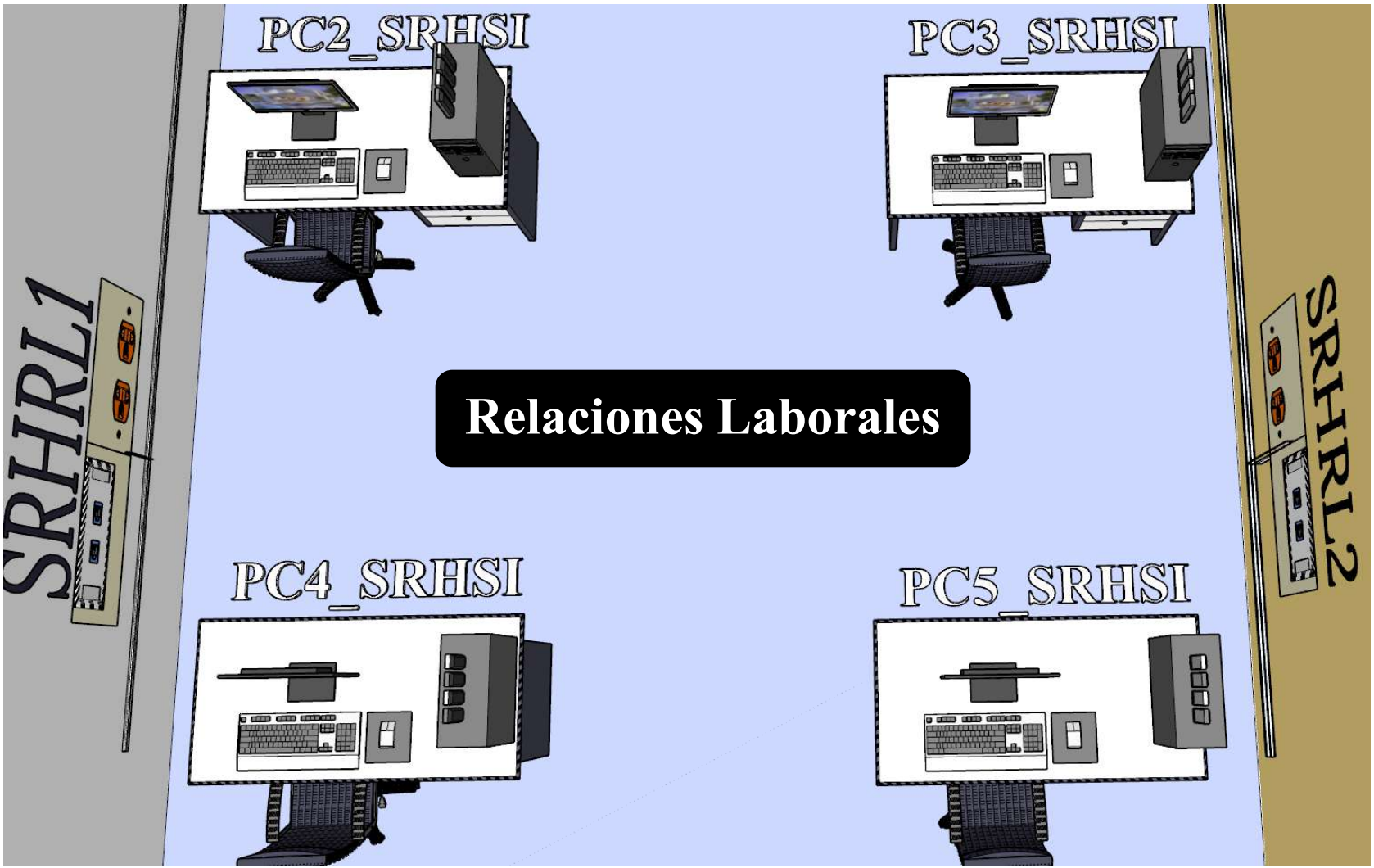


Figura 63. Oficina de Desarrollo, Recursos Humanos Y Sistemas/Relaciones Laborales

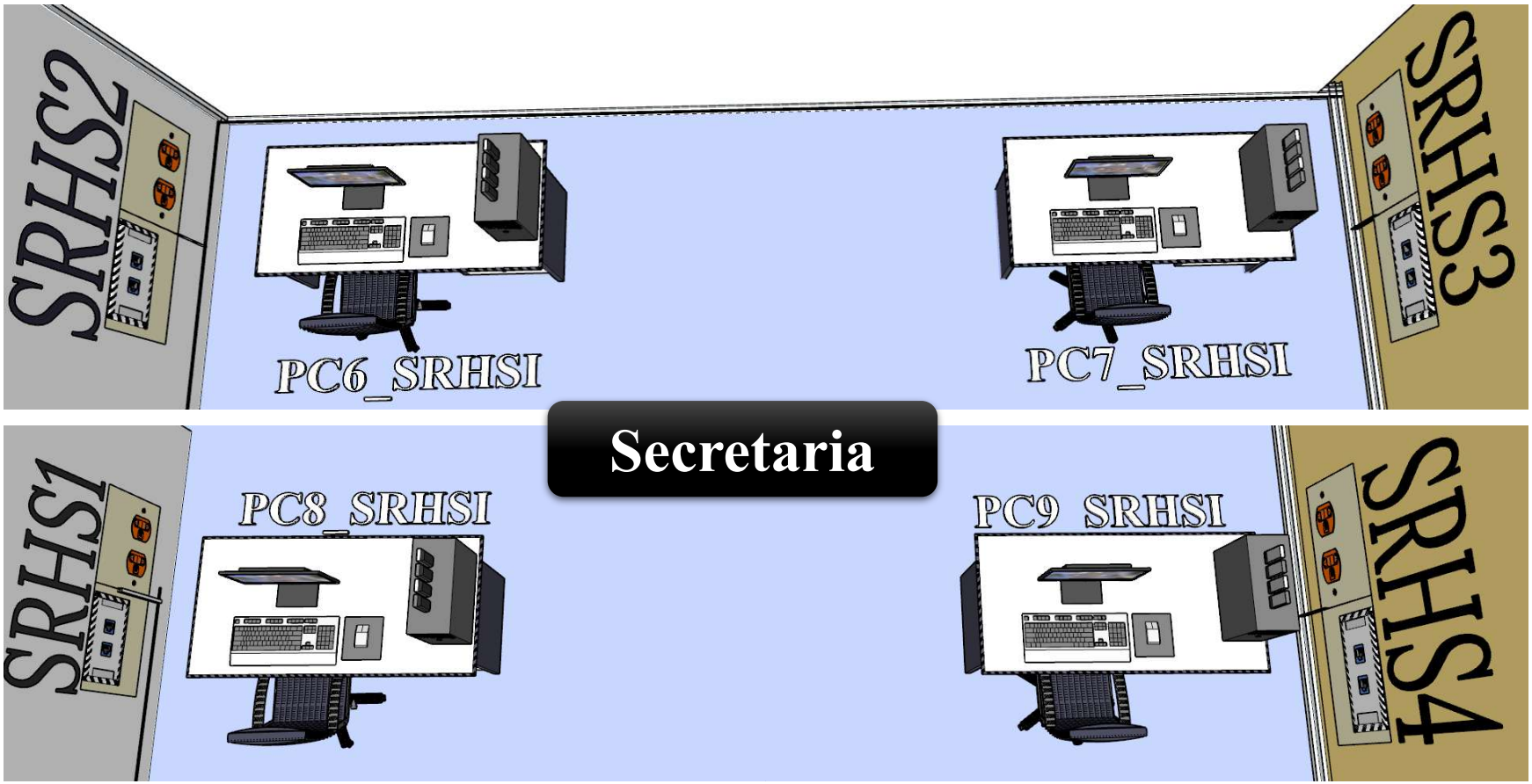


Figura 64. Oficina de Desarrollo, Recursos Humanos Y Sistemas/Secretaria

Figura 65. Oficina de Desarrollo, Recursos Humanos Y Sistemas/Oficina de Relaciones Publicas y Comunicación

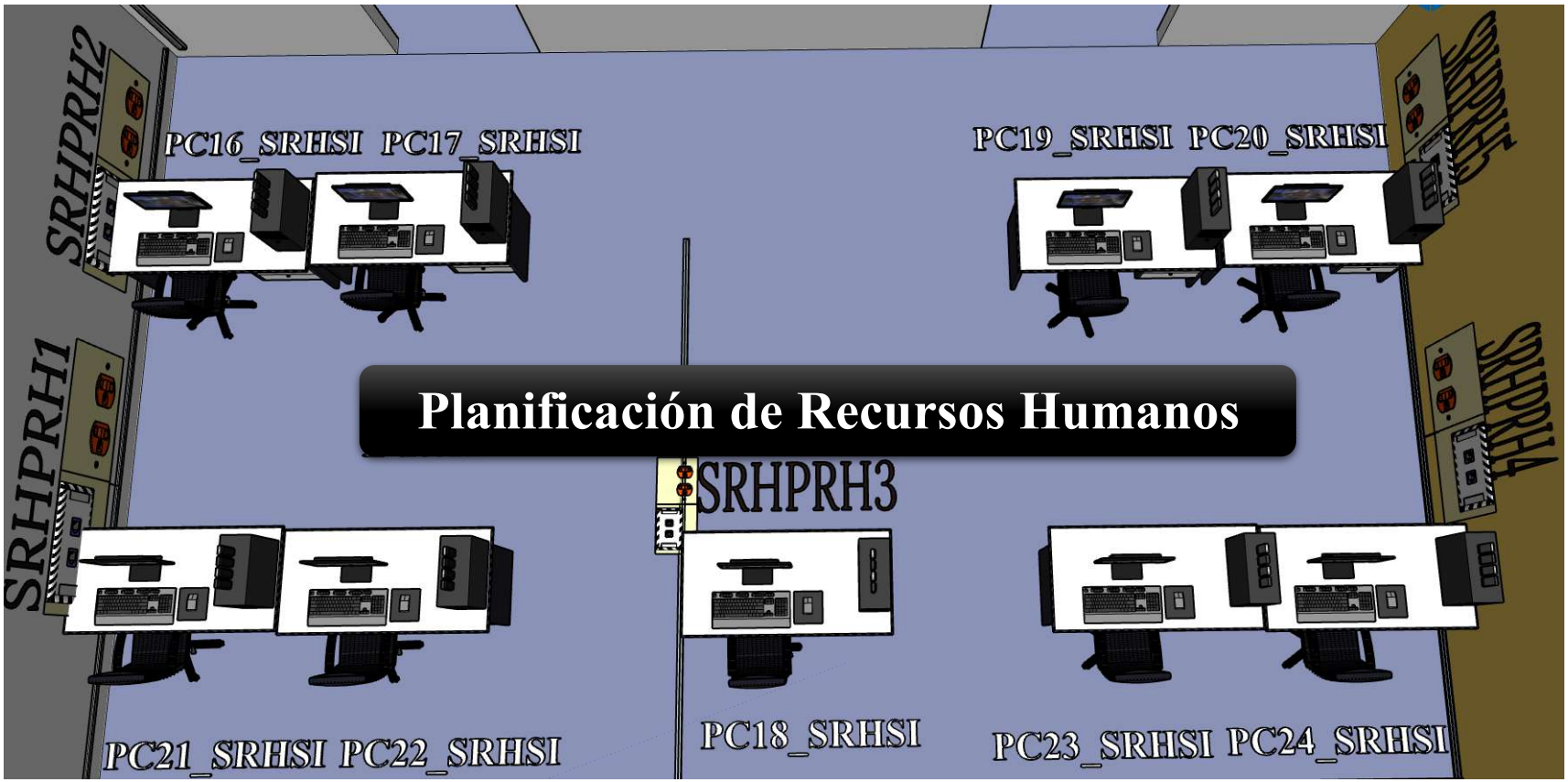


Figura 66. Oficina de Desarrollo, Recursos Humanos Y Sistemas/Planificación de Recursos Humanos

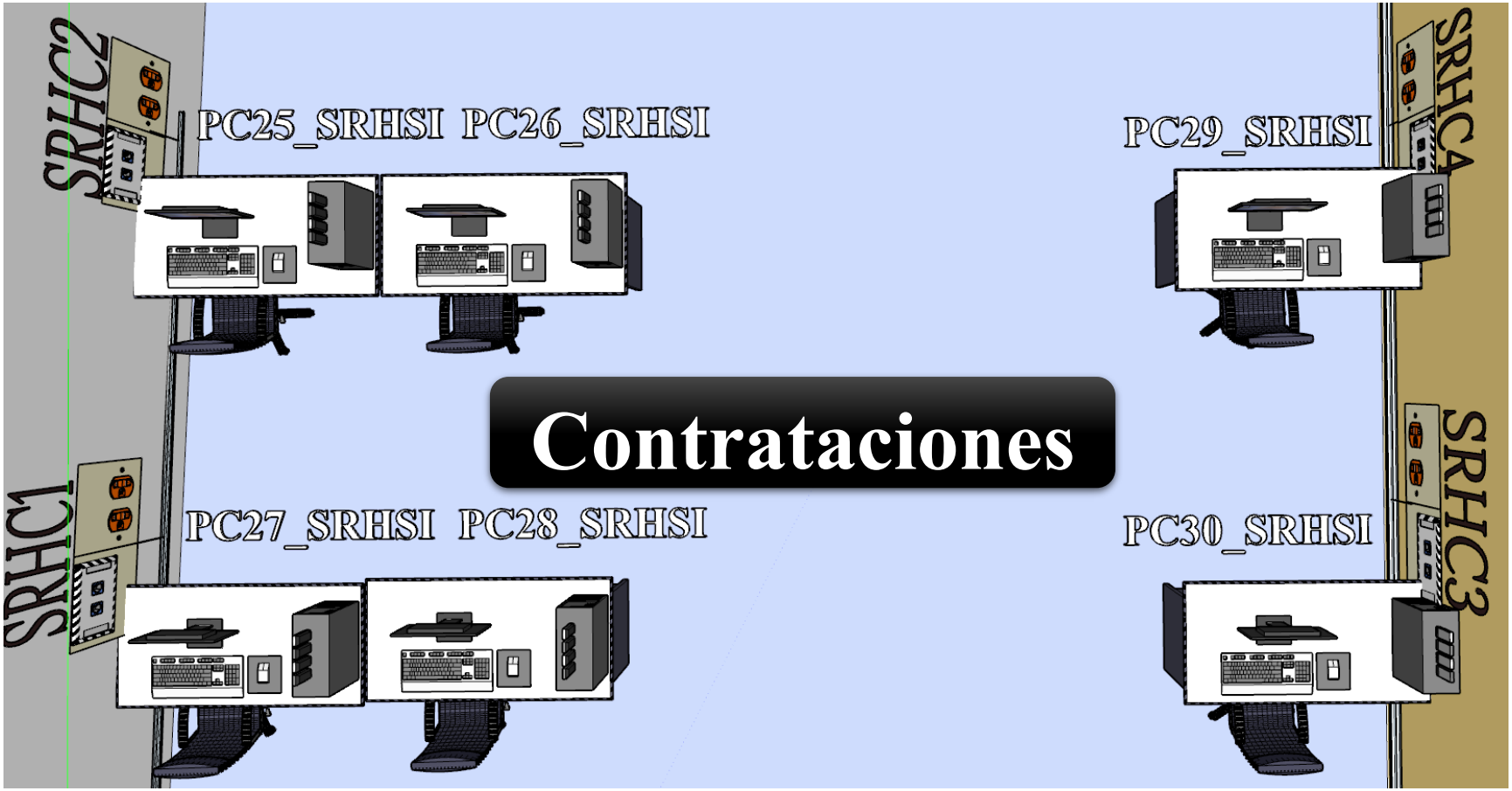


Figura 67. Oficina de Desarrollo, Recursos Humanos Y Sistemas/Contrataciones

Figura 68. Oficina de Desarrollo, Recursos Humanos Y Sistemas/Sala de Reuniones

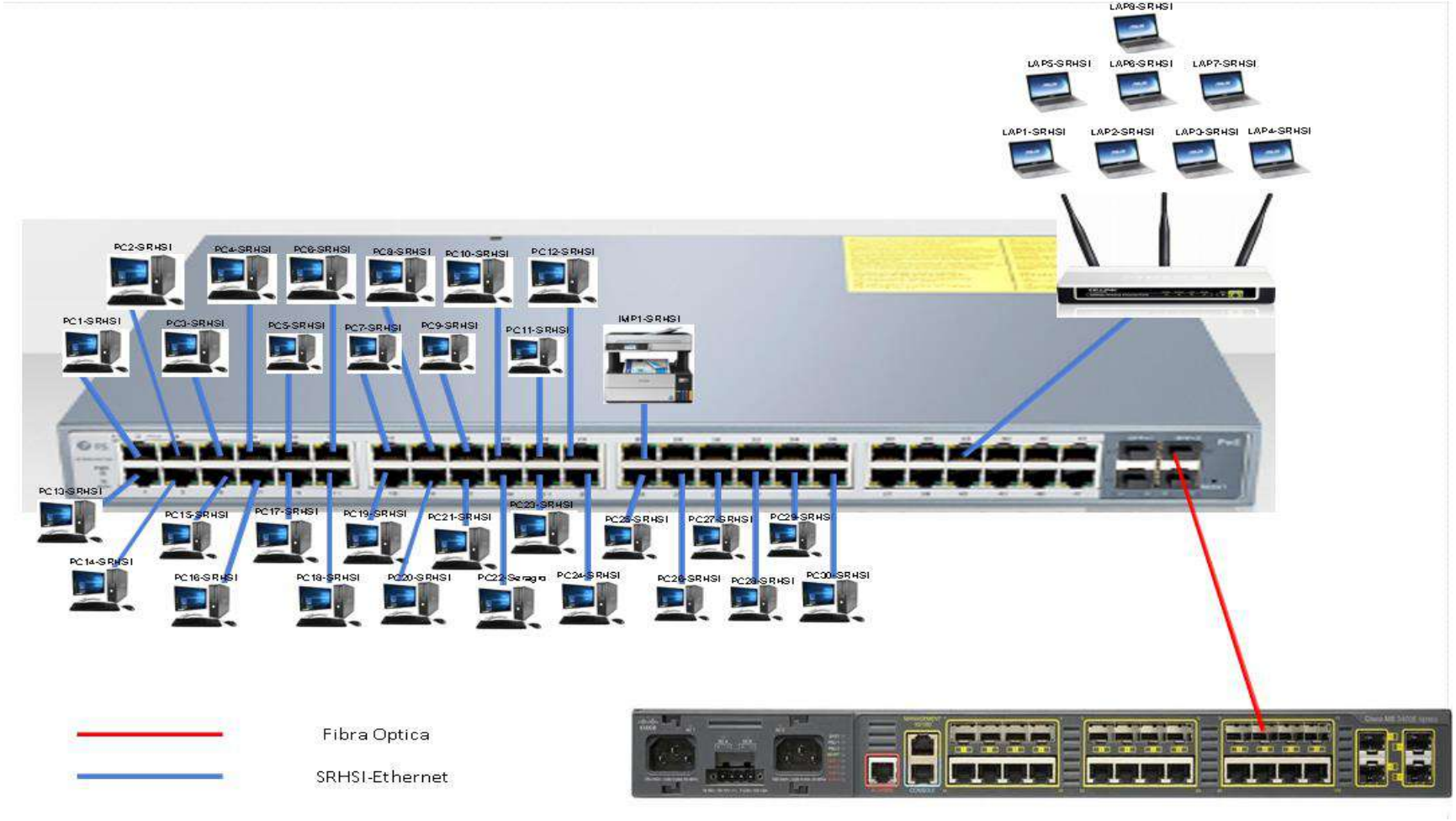


Figura 69. Cableado de red de la oficina Subred B (DESARROLLO, RECURSOS HUMANOS Y SISTEMAS)

CONTRATACIONES	Tamaño aprox	3*3.5
Materiales	**Cantidad**	
Cortapicos	6	
Patch Cords RJ45 -3 metros	6	
Cable canal	11,5	
Cable UTP cat 6	44	
Rosetas RJ 45	4	
Keystone RJ45	8	
PUNTOS DE RED		
SRHC1	192.168.1.67	OCUPADO
SRHC1	192.168.1.68	OCUPADO
SRHC2	192.168.1.69	OCUPADO
SRHC2	192.168.1.70	OCUPADO
SRHC3	192.168.1.71	OCUPADO
SRHC3	192.168.1.72	LIBRE
SRHC4	192.168.1.73	OCUPADO
SRHC4	192.168.1.74	LIBRE

OFICINA SUB GOBERNADOR	Tamaño aprox	3*3.5
Materiales	**Cantidad**	
Cortapicos	1	
Patch Cords RJ45 -3 metros	1	
Cable canal	4,5	
Cable UTP cat 6	26	
Rosetas RJ 45	1	
Keystone RJ45	2	
PUNTOS DE RED		
SRHG1	192.168.1.75	OCUPADO
SRHG1	192.168.1.76	LIBRE

PLANIFICACION RECURSOS HUMANOS **Tamaño aprox** 4.5*3

Materiales	Cantidad
Cortapicos	9
Patch Cords RJ45 -3 metros	9
Cable canal	13
Cable UTP cat 6	118
Rosetas RJ 45	4
Keystone RJ45	8

PUNTOS DE RED		
SRHPRH1	192.168.1.77	OCUPADO
SRHPRH1	192.168.1.78	OCUPADO
SRHPRH2	192.168.1.79	OCUPADO
SRHPRH2	192.168.1.80	OCUPADO
SRHPRH3	192.168.1.81	OCUPADO
SRHPRH3	192.168.1.82	LIBRE
SRHPRH4	192.168.1.83	OCUPADO
SRHPRH4	192.168.1.84	OCUPADO
SRHPRH5	192.168.1.85	OCUPADO
SRHPRH5	192.168.1.86	OCUPADO

OFICINA RELACIONES LABORALES **Tamaño aprox** **3*3.5**

Materiales	Cantidad
Cortapicos	4
Patch Cords RJ45 -3 metros	4
Cable canal	5,5
Cable UTP cat 6	31
Rosetas RJ 45	2
Keystone RJ45	4

PUNTOS DE RED		
SRHRL1	192.168.1.87	OCUPADO
SRHRL	192.168.1.88	LIBRE
SRHRL2	192.168.1.89	OCUPADO
SRHRL2	192.168.1.90	LIBRE

SRHI **Tamaño aprox** **3*3.5**

Materiales	Cantidad
Cortapicos	3
Patch Cords RJ45 -3 metros	2
Cable canal	1
Cable UTP cat 6	5,5

RELACIONES PUBLICAS Y COMUNICACIÓN

Materiales	**Cantidad**	**Tamaño aprox**
Cortapicos	6	
Patch Cords RJ45 -3 metros	6	
Cable canal	11,5	3.5*3
Cable UTP cat 6	160	
Rosetas RJ 45	4	
Keystone RJ45	8	

PUNTOS DE RED		
SRHC1	192.168.1.91	OCUPADO
SRHC1	192.168.1.92	LIBRE
SRHC2	192.168.1.93	OCUPADO
SRHC2	192.168.1.94	LIBRE
SRHC3	192.168.1.95	OCUPADO
SRHC3	192.168.1.96	OCUPADO
SRHC4	192.168.1.97	OCUPADO
SRHC4	192.168.1.98	OCUPADO

Rosetas RJ 45	1	
Keystone RJ45	2	

SALA DE REUNIONES

Materiales	**Cantidad**	**Tamaño aprox**
Cortapicos		
Patch Cords RJ45 -3 metros		
Cable canal		
Cable UTP cat 6		
Rosetas RJ 45		
Keystone RJ45		

PUNTOS DE RED		
SRHSR1	192.168.1.105	OCUPADO
SRHSR1	192.168.1.106	LIBRE

SECRETARIA	**Tamaño aprox**	**3.5*3**
Materiales	**Cantidad**	
Cortapicos	4	
Patch Cords RJ45 -3 metros	4	
Cable canal	14,5	
Cable UTP cat 6	189	
Rosetas RJ 45	4	
Keystone RJ45	8	
PUNTOS DE RED		
SRHS1	192.168.1.99	OCUPADO
SRHS1	192.168.1.100	LIBRE
SRHS2	192.168.1.101	OCUPADO
SRHS2	192.168.1.102	LIBRE
SRHS3	192.168.1.103	OCUPADO
SRHS3	192.168.1.104	LIBRE

Materiales adicionales	**CANTIDAD**
ESCALERILLA HORIZONTAL HACIA SALA DE EQUIPOS	18,5
Cable UTP Cat 6 Instalacion router wifi	14
Conecor Rj 45 Cat 6	2
Cable Canal	2
WIFI _SRHSI/PASILLO	2

III.1.4.5.3. Cableado de la Oficina Subred C (SECRETARIA DE OBRAS PÚBLICAS, ALMACÉN, SECRETARIA DE PLANIFICACIÓN)

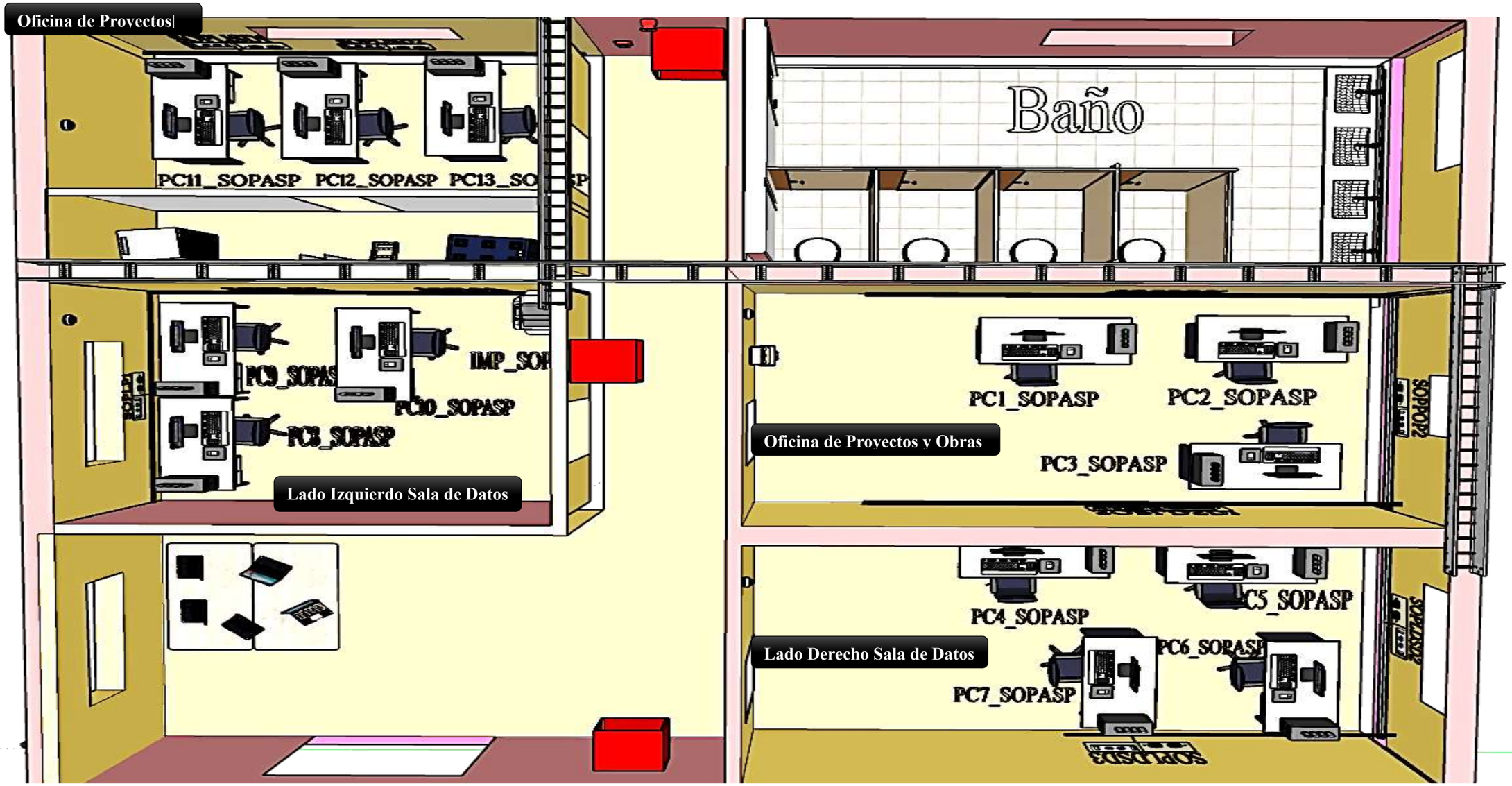


Figura 70. Ambiente de Distribución del Cableado de la Oficina de Secretaria de Obras Públicas, Almacén, Secretaria de Planificación

Información detallada en la pag164-165

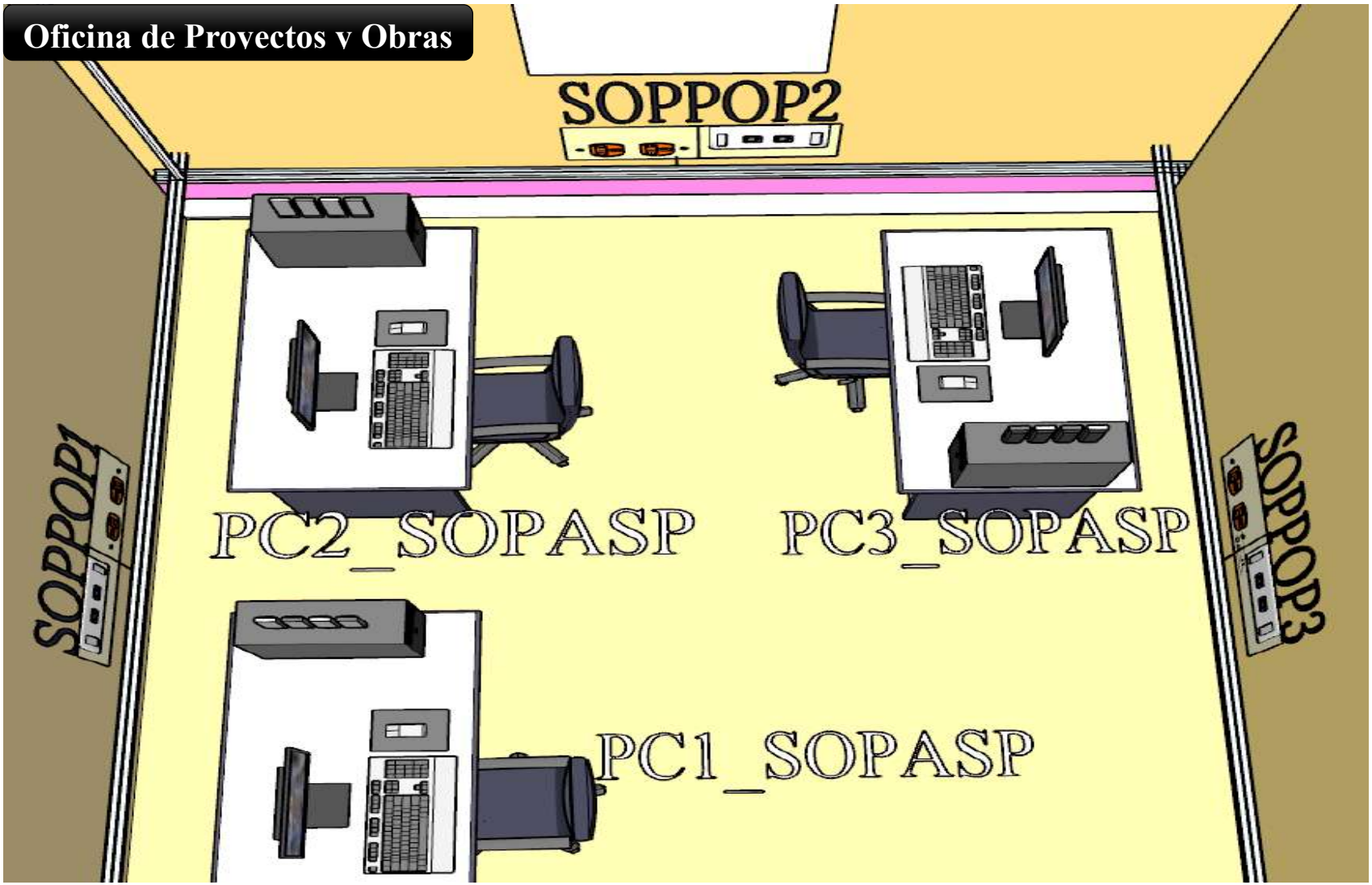
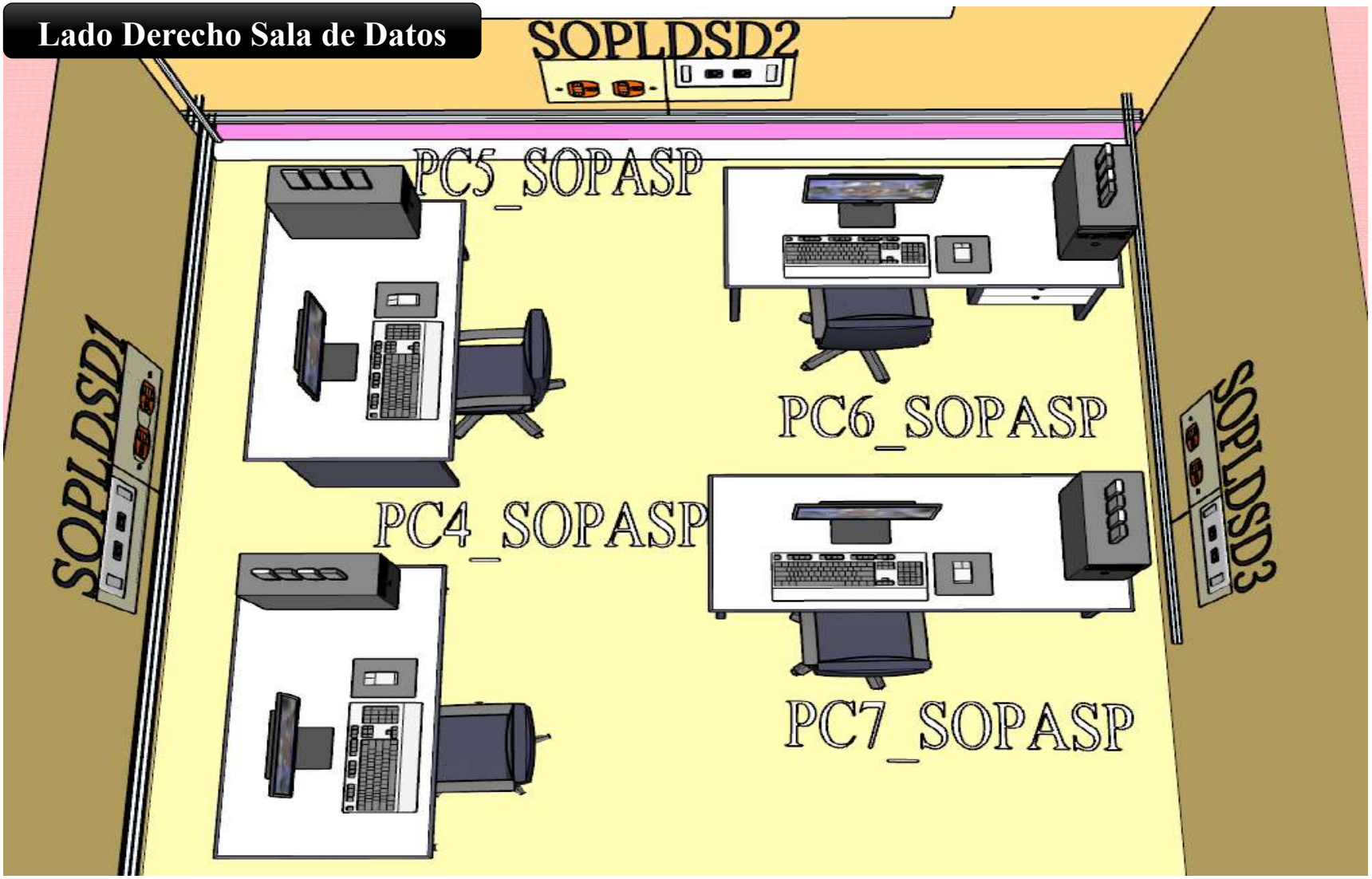


Figura 71. Oficina de Secretaria de Obras Públicas, Almacén, Secretaria de Planificación/Oficina de Proyectos y Obras



Oficina de Secretaria de Obras Públicas, Almacén, Secretaria de Planificación/ Lado Derecho Sala de Datos

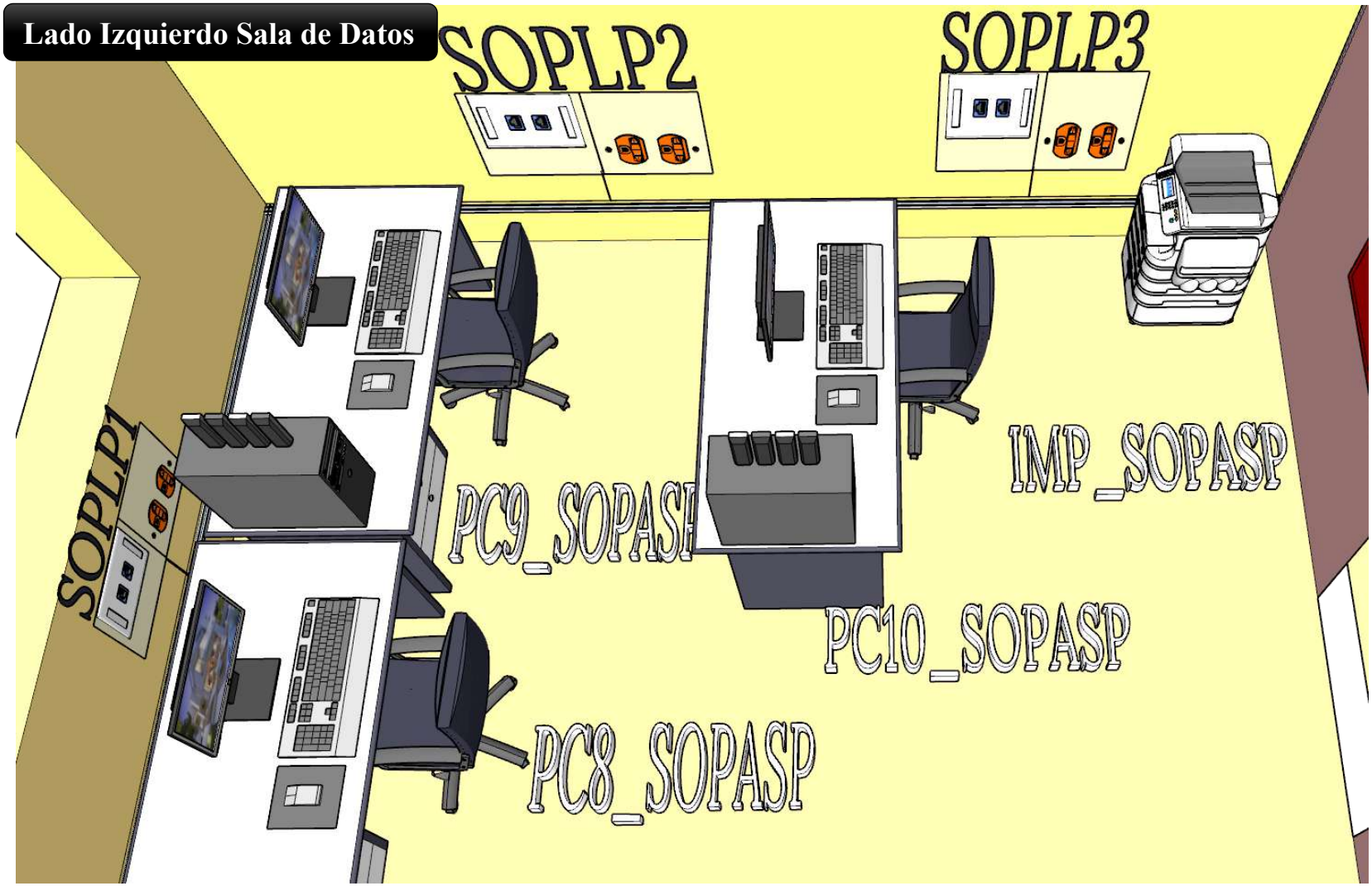


Figura 72. Oficina de Secretaria de Obras Públicas, Almacén, Secretaria de Planificación/ Lado Izquierdo Sala de Datos

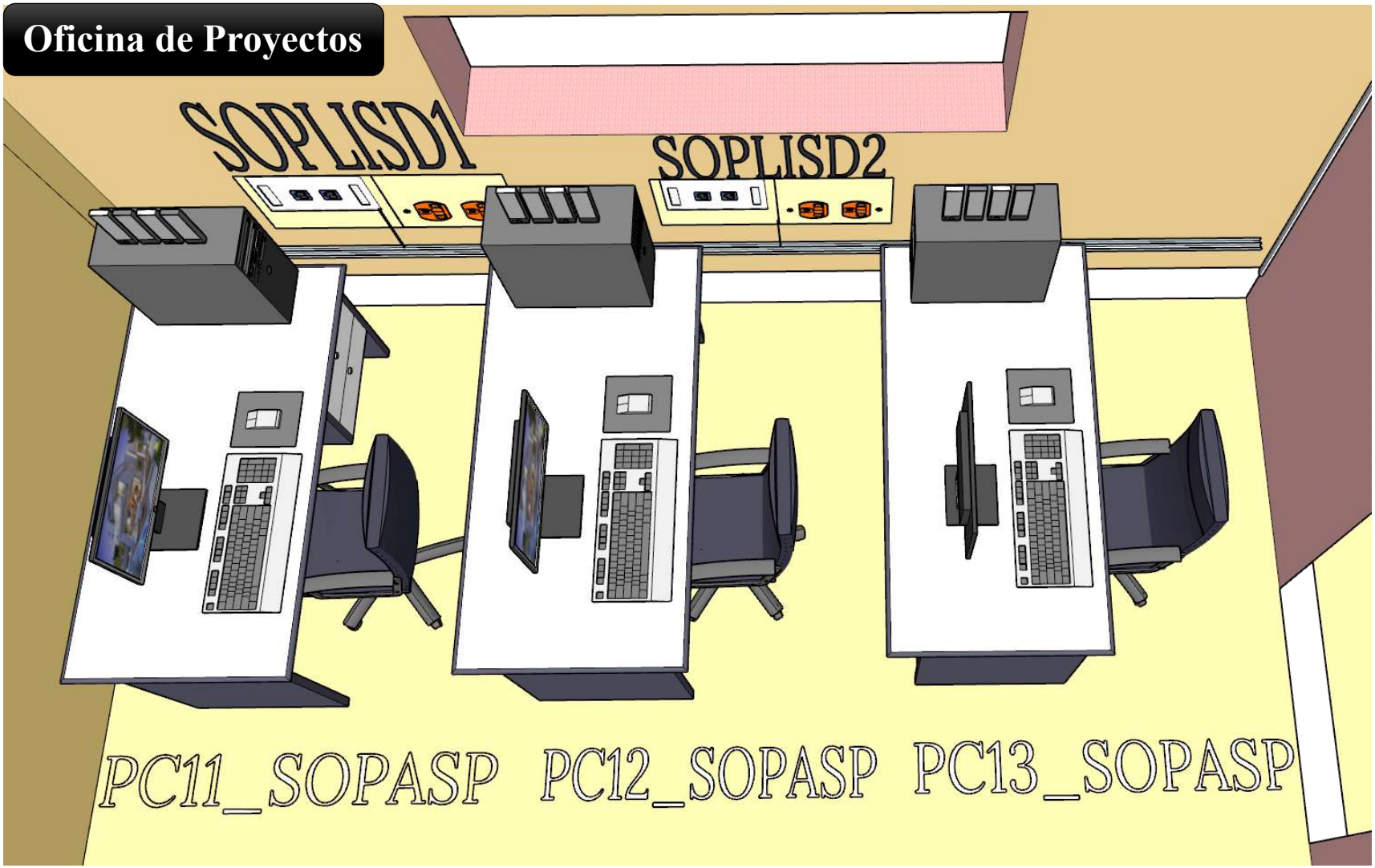


Figura 73. Oficina de Secretaria de Obras Públicas, Almacén, Secretaria de Planificación/Oficina de Proyectos

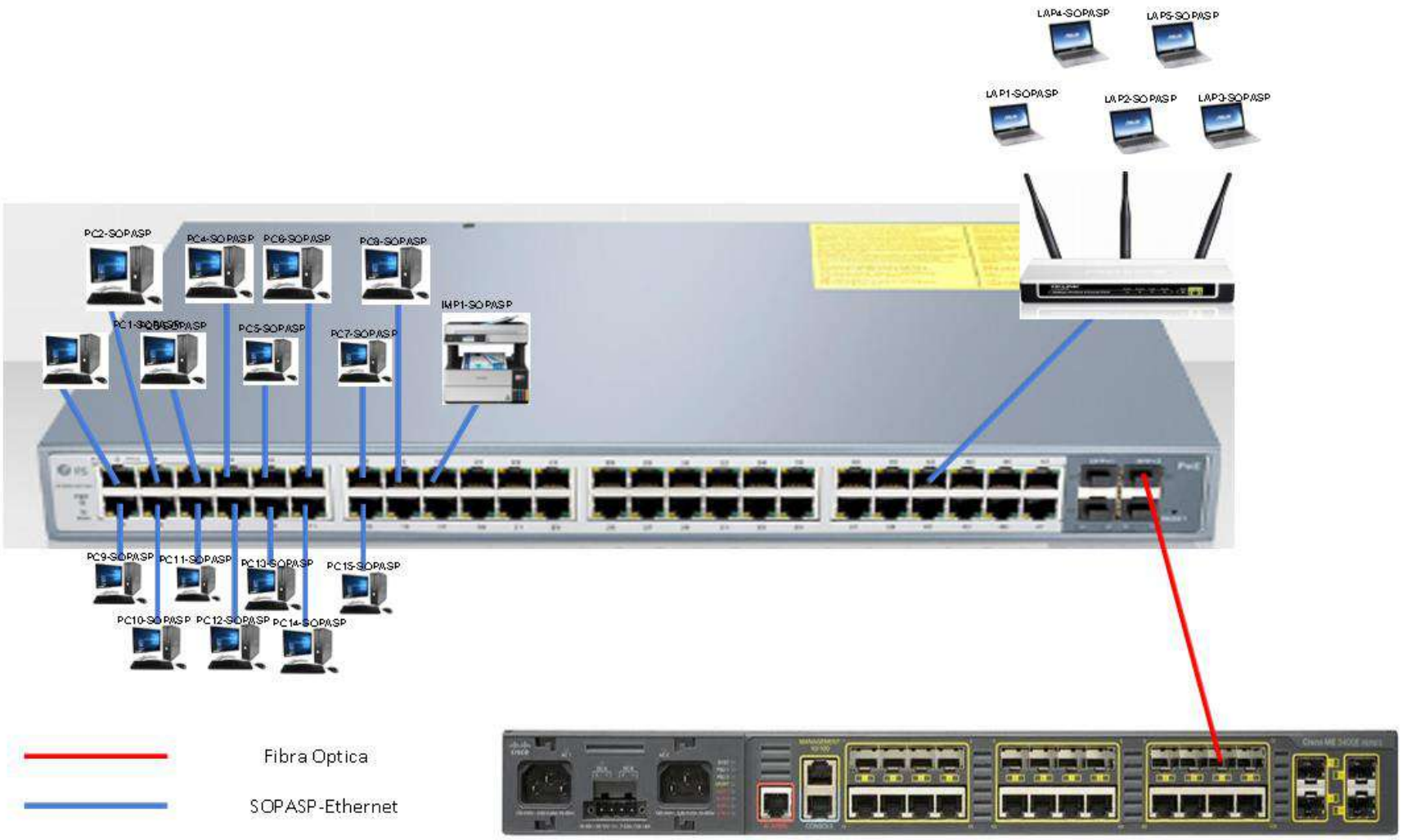


Figura 74. Cableado de red SECRETARIA DE OBRAS PÚBLICAS, ALMACÉN, SECRETARIA DE PLANIFICACIÓN

OFICINA PROYECTOS OBRAS PUBLICAS **Tamaño aprox**

Materiales	Cantidad
Cortapicos	4
Patch Cords RJ45 -3 metros	4
Cable canal	6,5
Cable UTP cat 6	50
Rosetas RJ 45	2
Keystone RJ45	4

PUNTOS DE RED		
SOPPOP1	192.168.1.131	OCUPADO
SOPPOP1	192.168.1.132	LIBRE
SOPPOP2	192.168.1.133	OCUPADO
SOPPOP2	192.168.1.134	LIBRE
SOPPOP3	192.168.1.135	OCUPADO
SOPPOP3	192.168.1.136	LIBRE

Materiales adicionales	CANTIDAD
ESCALERILLA HORIZONTAL HACIA SALA DE EQUIPOS	9
Cable UTP Cat 6 Instalacion router wifi	4,5
Conecor Rj 45 Cat 6	1
Cable Canal	1,5
EQUIPOS WIFI	1

LADO DERECHO SALA DATOS **Tamaño aprox**

Materiales	Cantidad
Cortapicos	3
Patch Cords RJ45 -3 metros	3
Cable canal	5,5
Cable UTP cat 6	32
Rosetas RJ 45	2
Keystone RJ45	4

PUNTOS DE RED		
SOPLDSD1	192.168.1.137	OCUPADO
SOPLDSD1	192.168.1.138	OCUPADO
SOPLDSD2	192.168.1.139	OCUPADO
SOPLDSD2	192.168.1.140	LIBRE
SOPLDSD3	192.168.1.141	OCUPADO
SOPLDSD3	192.168.1.142	LIBRE

LADO OFICINA PROYECTOS	Tamaño aprox		LADO IZQUIERDO SALA DATOS	Tamaño aprox	
Materiales	**Cantidad**		**Materiales**	**Cantidad**	
Cortapicos	3		Cortapicos	3	
Patch Cords RJ45 -3 metros	3		Patch Cords RJ45 -3 metros	3	
Cable canal	6,5		Cable canal	5,5	
Cable UTP cat 6	42		Cable UTP cat 6	35	
Rosetas RJ 45	2		Rosetas RJ 45	2	
Keystone RJ45	4		Keystone RJ45	4	
PUNTOS DE RED			PUNTOS DE RED		
SOPLP1	192.168.1.143	OCUPADO	SOPLISD1	192.168.1.149	OCUPADO
SOPLP1	192.168.1.144	LIBRE	SOPLISD1	192.168.1.150	LIBRE
SOPLP2	192.168.1.145	OCUPADO	SOPLISD2	192.168.1.151	OCUPADO
SOPLP2	192.168.1.146	LIBRE	SOPLISD2	192.168.1.152	OCUPADO
SOPLP3	192.168.1.147	OCUPADO			
SOPLP3	192.168.1.148	OCUPADO			