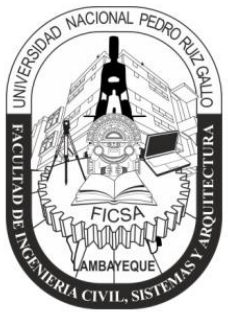
UNIVERSIDAD NACIONAL

"PEDRO RUIZ GALLO"

FACULTAD DE INGENIERIA CIVIL,

SISTEMAS Y ARQUITECTURA



ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS

"DISEÑO DE RED DE DATOS DE LA MUNICIPALIDAD DISTRITAL DE OLMOS - LAMBAYEQUE"

TRABAJO DE SUFICIENCIA PROFESIONAL

PARA OPTAR EL TÍTULO

PROFESIONAL DE:

INGENIERO DE SISTEMAS

PRESENTADA POR EL BACHILLER:

MARTINEZ OLIVA, RONY ALDAIR ORLANDO

LAMBAYEQUE – PERU

2025

UNIVERSIDAD NACIONAL
"PEDRO RUIZ GALLO"
FACULTAD DE INGENIERIA CIVIL,
SISTEMAS Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS

"DISEÑO DE RED DE DATOS DE LA MUNICIPALIDAD DISTRITAL DE OLMOS - LAMBAYEQUE"

DR. ING. ERNESTO KARLO CELI ARÉVALO

PRESIDENTE DE JURADO

DR. ING. JUAN ELIAS VILLEGAS CUBAS

SECRETARIO DE JURADO

ING. LUIS ALBERTO LLONTOP CUMPA

VOCAL

Fecha de sustentación:

04 de Noviembre del 2025

UNIVERSIDAD NACIONAL
"PEDRO RUIZ GALLO"
FACULTAD DE INGENIERIA CIVIL,
SISTEMAS Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS

"DISEÑO DE RED DE DATOS DE LA MUNICIPALIDAD DISTRITAL DE OLMOS - LAMBAYEQUE"

MA. ING. ARTEAGA LORA ROBERTO CARLOS.

ASESOR

MARTINEZ OLIVA, RONY ALDAIR ORLANDO

BACHILLER EN ING. SISTEMAS

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE INGENIERÍA CIVIL DE SISTEMAS Y DE ARQUITECTURA
UNIDAD DE INVESTIGACIÓN

ACTA DE SUSTENTACIÓN
N° 609-2025-UI-FICSA

Siendo las 9:00 am del día 04 de noviembre del 2025, se reunieron los miembros de jurado del Trabajo de Suficiencia Profesional Titulado: **"DISEÑO DE RED DE DATOS DE LA MUNICIPALIDAD DISTRITAL DE OLMOS - LAMBAYEQUE", con código N° IS_TSP_2025_007,** designado por **Resolución Decanal N° 800-2025-UNPRG-FICSA;** con la finalidad de Evaluar y Calificar la sustentación del Trabajo de Suficiencia Profesional antes mencionado, conformado por los siguientes docentes:

DR. ING. ERNESTO KARLO CELI ARÉVALO	**PRESIDENTE**
DR. ING. JUAN ELIAS VILLEGAS CUBAS	**SECRETARIO**
ING. LUIS ALBERTO LLONTOP CUMPA	**VOCAL**

Asesorado por MSC. ING. ROBERTO CARLOS ARTEAGA LORA.

El acto de sustentación fue autorizado por **OFICIO VIRTUAL N° 240-2025-UIFICSA,** el Trabajo de Suficiencia Profesional fue presentado y sustentado por el Bachiller: **RONY ALDAIR ORLANDO MARTINEZ OLIVA,** tuvo una duración de 60 minutos Después de la sustentación, y absueltas las preguntas y observaciones de los miembros del jurado; se procedió a la calificación respectiva:

	NUMERO	LETRAS	CALIFICATIVO
RONY ALDAIR ORLANDO MARTINEZ OLIVA	16	DIECISEIS	BUENO

Por lo que queda APTO para obtener el Título Profesional de INGENIERO DE SISTEMAS de acuerdo con la Ley Universitaria 30220 y la normatividad vigente de la Facultad de Ingeniería Civil de Sistemas y de Arquitectura de la Universidad Nacional Pedro Ruiz Gallo.

Siendo las 10:00 ; del mismo día, se dio por concluido el presente acto académico, dándose conformidad al presente acto, con la firma de los miembros del jurado.

DR. ING. ERNESTO KARLO CELI ARÉVALO
PRESIDENTE

DR. ING. JUAN ELIAS VILLEGAS CUBAS
SECRETARIO

ING. LUIS ALBERTO LLONTOP CUMPA
VOCAL

MSC. ING. ROBERTO CARLOS ARTEAGA LORA
ASESOR

JHFF/bcm.

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE INGENIERÍA CIVIL, DE SISTEMAS Y ARQUITECTURA
UNIDAD DE INVESTIGACIÓN

"Año de la unidad, la paz y el desarrollo"

CONSTANCIA DE APROBACIÓN DE ORIGINALIDAD DE TRABAJO DE SUFICIENCIA PROFESIONAL

Según Res. N° 659-2020-R

Yo, ARTEAGA LORA ROBERTO CARLOS, asesor del trabajo de suficiencia del bachiller:

MARTINEZ OLIVA, RONY ALDAIR ORLANDO

TITULADO:

"DISEÑO DE RED DE DATOS DE LA MUNICIPALIDAD DISTRITAL DE OLMOS - LAMBAYEQUE"

Luego de la revisión exhaustiva del documento constato que la misma tiene un índice de similitud de 18**%** verificable en el reporte de similitud del programa TURNITIN.

El suscrito analizó dicho reporte y concluyó que, cada una de las coincidencias detectadas NO CONSTITUYEN PLAGIO. A mi leal saber y entender, el trabajo de suficiencia profesional cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad Nacional Pedro Ruiz Gallo.
Se expide la presente según lo dispuesto en la Resolución Nº 659-2020-R, de fecha 8 de setiembre de 2020, que aprueba la directiva para la evaluación de originalidad de los documentos académicos, de investigación formativa y para la obtención de Grados y Títulos de la UNPRG:

Lambayeque, 08 de julio de 2025

Atentamente,

MA. ING. ROBERTO CARLOS ARTEAGA LORA
DNI 16755764

Se adjunta:

- Recibo digital de Turnitin
- Revisión de informe en Turnitin

DISEÑO DE RED DE DATOS DE LA MUNICIPALIDAD DISTRITAL DE OLMOS - LAMBAYEQUE

INFORME DE ORIGINALIDAD

18%	18%	7%	5%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.unapiquitos.edu.pe Fuente de Internet	5%
2	repositorio.unprg.edu.pe:8080 Fuente de Internet	5%
3	repositorio.unap.edu.pe Fuente de Internet	1%
4	Submitted to University of Glamorgan Trabajo del estudiante	<1%
5	Submitted to University of Hertfordshire Trabajo del estudiante	<1%
6	repositorio.ucv.edu.pe Fuente de Internet	<1%
7	hdl.handle.net Fuente de Internet	<1%
8	en.wikiversity.org Fuente de Internet	<1%

www.dspace.espol.edu.ec

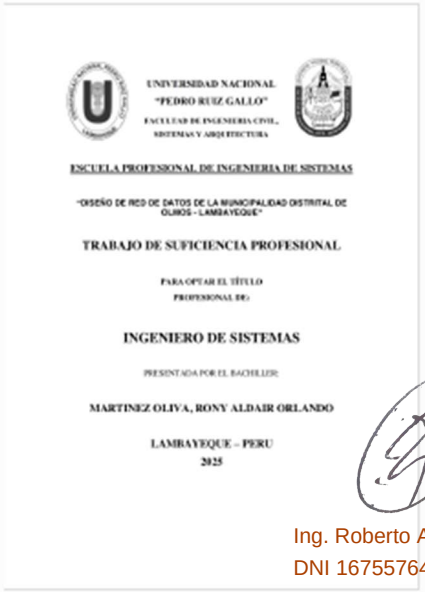
turnitin

Recibo digital

Este recibo confirma quesu trabajo ha sido recibido por Turnitin. A continuación podrá ver la información del recibo con respecto a su entrega.

La primera página de tus entregas se muestra abajo.

Autor de la entrega:	RONY ALDAIR ORLANDO MARTINEZ OLIVA
Título del ejercicio:	Trabajos de suficiencia profesional
Título de la entrega:	DISEÑO DE RED DE DATOS DE LA MUNICIPALIDAD DISTRITAL ...
Nombre del archivo:	Informe_Profesional_4-_MARTINEZ_OLIVA_REVISADO_5-7-2025...
Tamaño del archivo:	9.55M
Total páginas:	130
Total de palabras:	18,996
Total de caracteres:	111,274
Fecha de entrega:	08-jul-2025 02:50p. m. (UTC-0500)
Identificador de la entrega:	2712062264



UNIVERSIDAD NACIONAL
"PEDRO RUIZ GALLO"
FACULTAD DE INGENIERIA CIVIL, SISTEMAS Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS

"DISEÑO DE RED DE DATOS DE LA MUNICIPALIDAD DISTRITAL DE OLMOS - LAMBAYEQUE"

TRABAJO DE SUFICIENCIA PROFESIONAL

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS

PRESENTADO POR EL BACHILLER:

MARTINEZ OLIVA, RONY ALDAIR ORLANDO

LAMBAYEQUE – PERU
2025

Ing. Roberto Arteaga Lora
DNI 16755764

Dedicatoria

Dedico el presente trabajo de suficiencia a mis padres, en reconocimiento a su apoyo incondicional y constante, que me ha impulsado a lo largo de todo este camino, comprensión y gran amor, a mis Hermanas por su apoyo, a mi pareja y a mi hijo por hacer mis días felice.

Agradecimientos

Como primordial Al ING: Arteaga Roberto, Agradezco profundamente su asesoría y conocimiento, los cuales fueron fundamentales para la realización de este informe. Deseo expresar mi más profundo agradecimiento al Ing. Fredy Javier Sánchez Chiroque por su valiosa contribución y activa participación en el desarrollo de este informe. Quiero resaltar especialmente su constante disposición y paciencia, que fueron clave para que nuestras enriquecedoras y a veces intensas discusiones generen resultados positivos.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

RESUMEN

El presente informe constituye el trabajo de Suficiencia Profesional titulado "Análisis y Diseño de la Red de Datos de la Municipalidad Distrital de Olmos", que se encuentra ubicada en la provincia de Lambayeque, departamento de Lambayeque. La infraestructura de red de datos, existente en la municipalidad, presenta múltiples deficiencias: las conexiones físicas están en malas condiciones, algunas expuestas, y las canaletas se han deteriorado, lo que permite la entrada de roedores. Además, los equipos de comunicación están a la vista y son fácilmente accesibles, y no cuentan con un sistema eléctrico independiente adecuado. Estos problemas principales pueden resumirse en los siguientes puntos:

- ✓ Vulnerabilidad de la red ante terceros.
- ✓ Resguardo físico de los sistemas de comunicación.
- ✓ Inseguridad en los cableados de las redes.
- ✓ Problemas de conectividad.
- ✓ Riesgos para la integridad de los datos.

Por tanto, el objetivo principal es llevar a cabo un análisis y diseño de red que facilite la interconexión eficiente entre todas las áreas y oficinas de la Municipalidad Distrital de Olmos. El diseño considera lo siguiente:

- ✓ Mejorar la velocidad y eficiencia de la conexión de los equipos.
- ✓ Asegurar el cableado de la red y los equipos de comunicación.
- ✓ Gestionar y poder controlar el ingreso que se da dentro de los capacitados.
- ✓ Regular y monitorear el acceso a Internet con reglamentos específicos en su computadora.
- ✓ Disminuir costos operativos.
- ✓ Garantizar su intercambio y su comunicación por una fluidez de los usuarios en la información.

Cabe destacar que este informe no contempla la fase de implementación, por lo que el diseño presentado, se utilizará como guía para futuras implementaciones y evaluaciones.

Palabras clave: Red de datos, VLAN, Municipalidad distrital de Olmos.

ABSTRACT

This report constitutes the Professional Competence Assessment (PQ) entitled "Analysis and Design of the Data Network of the District Municipality of Olmos," located in the province of Lambayeque, department of Lambayeque. The municipality's existing data network infrastructure presents multiple deficiencies: the physical connections are in poor condition, some exposed, and the gutters have deteriorated, allowing rodents to enter. Furthermore, the communications equipment is visible and easily accessible, and lacks an adequate independent electrical system. These main problems can be summarized as follows:

- ✓ Vulnerability of the network to third parties.
- ✓ Physical protection of the communication systems.
- ✓ Insecurity in the network wiring.
- ✓ Connectivity problems.
- ✓ Risks to data integrity.

To this end, the main objective is to carry out a modern design and analysis that facilitates efficient interconnection between all areas and offices of the Olmos District Municipality. This design has the following goals:

- ✓ Improve the speed and efficiency of the equipment connection.
- ✓ Secure the network cabling and communication equipment.
- ✓ Manage and control the access that occurs within the trained.
- ✓ Regulate and monitor Internet access with specific regulations on your computer.
- ✓ Reduce operating costs.
- ✓ Guarantee their exchange and communication for a fluidity of information for users.

It should be noted that this report does not contemplate the implementation phase, so the indicators presented will be used as a guide for future implementations and evaluations.

Key words: Data network, VLAN, Olmos District Municipality.

I. PLANTEAMIENTO DEL TRABAJO

1.1 DEFINICIÓN DEL PROBLEMA

La municipalidad de Olmos, es una Organización estatal encargada de promover el desarrollo de su localidad. Tiene la condición de persona jurídica en el marco legal público, en donde es plenamente capaz de desempeñar sus funciones. Además, tiene la autonomía administrativa, política, económica sobre los asuntos que están en su competencia.

Actualmente, la Municipalidad funciona en un edificio central propio, que está distribuido en tres pisos, donde se agrupan gran parte de sus áreas y oficinas administrativas. Los equipos de cómputo están conectados entre sí, en una red LAN (red de área local), lo que facilita su Conexión tanto externa como interna y el acceso a diversas atenciones en donde funcionan los siguientes sistemas:

- ✓ Servidor de aplicaciones 01:
  Sistema Integrado de Gestión (SIGA).
- ✓ Servidor de aplicaciones 02:
  Sistema integrado de control administrativo y financiero (SIAF).
- ✓ Servidor de aplicaciones 03:
  Sistema de Tesorería (SISREN).

El funcionamiento de los sistemas es de suma importancia, debido a su aporte en los servicios que ofrece la organización, las oficinas y áreas dependen del acceso a la red de datos. Esto resulta ser esencial ya que diferentes sistemas pueden intercambiar datos mediante una red de datos.

Se han habilitado servidores con direcciones IP (protocolo de Internet) públicas, los cuales permiten alojar la página web institucional y facilitar el intercambio de información con otras entidades del Estado (ejemplo: Ministerio de economía, Procuraduría, etc.), en cumplimiento con las normas de transparencia exigidas.

La institución cuenta con un servicio de Internet, que permite la conexión de equipos específicos mediante direcciones IP. Este servicio cuenta con una línea dedicada de ancho de banda de 100 Mbps, lo que asegura una conectividad adecuada para sus operaciones.

La Municipalidad Distrital de Olmos dispone de cuatro sedes que no están enlazadas mediante red de datos a la sede principal, la instalación del cableado estructurado fue deficiente, las diferentes redes de datos fueron implementadas de manera empírica por personal con escaso conocimiento sobre normas de cableado estructurado. El servicio se suspendía continuamente, debido a una distribución del cableado desordenado que era complicado su mantenimiento, se presentaban loop en las conexiones con los equipos de comunicación (switch no administrable), los cables estaban expuestos; no existía un sistema eléctrico independiente y las canaletas como sus accesorios fueron fijados con pegamento y clavos. Los problemas existentes se pueden resumir de la siguiente manera:

- ✓ Vulnerabilidad de las redes ante accesos sin autorización.
- ✓ Dispositivos de comunicación, mal resguardados.
- ✓ Sistema de cableado de la red, desprotegido.
- ✓ No existía conectividad de comunicación.
- ✓ Perdida de integridad de los datos.

1.2 OBJETIVOS

OBJETIVO GENERAL

- ✓ Diseñar la red de datos de la Municipalidad distrital de Olmos, con características eficientes y administrable.

OBJETIVOS ESPECIFICOS

- ✓ Medir el tráfico de la red de datos existente en la Municipalidad distrital de Olmos
- ✓ Diseñar la red física y lógica de la municipalidad distrital de Olmos.
- ✓ Asignar VLAN necesarias para los servicios de red de la Municipalidad distrital de Olmos.
- ✓ Simular la red de datos de la Municipalidad distrital de Olmos.
- ✓ Establecer una directiva de uso del servicio de Internet para los usuarios de TI de la Municipalidad distrital de Olmos.

1.3 LIMITACIONES DEL INFORME

Al realizar el presente informe de rediseño de la red de cableado estructurado de una municipalidad, se pueden presentar diversas limitaciones que afectan la precisión, la amplitud y la aplicabilidad de los resultados. Estas limitaciones, deben ser consideradas durante el proceso de diseño y reflejadas en el informe final para dar contexto a las conclusiones y recomendaciones. A continuación, se detallan las principales limitaciones de la investigación en este tipo de proyectos:

- ✓ **Acceso a Información Técnica Detallada:** En muchas ocasiones, la información técnica sobre la infraestructura de red existente, como diagramas de cableado, especificaciones de equipos o configuraciones previas, puede no estar completamente documentada o ser difícil de obtener. La falta de acceso a estos datos puede limitar la capacidad para realizar un diagnóstico preciso del estado actual de la red y diseñar una solución óptima (Reyes & Moraga, 2020).

- ✓ **Restricciones de Tiempo:** Los plazos limitados para realizar la investigación pueden restringir la capacidad de llevar a cabo un análisis exhaustivo de todos los componentes de la red. Un tiempo de investigación insuficiente puede resultar en un estudio incompleto de la infraestructura existente, la falta de pruebas o mediciones necesarias para identificar posibles fallos o puntos de mejora, lo que podría afectar la calidad del rediseño propuesto (Salas, 2019).

- ✓ **Presupuesto Limitado para la Investigación:** Los recursos financieros disponibles para la investigación pueden ser limitados, lo que puede restringir la capacidad para contratar expertos externos, realizar pruebas de campo, comprar equipos de medición avanzados o realizar un análisis profundo de posibles tecnologías de cableado y equipos de red. Esta limitación puede afectar la profundidad de la investigación y la evaluación de diversas alternativas tecnológicas (Señalin y otros, 2020).

- ✓ **Falta de Datos Actualizados:** El informe de investigación puede verse afectado por la falta de datos actualizados sobre las tecnologías de cableado estructurado o las tendencias en el diseño de redes de telecomunicaciones. Si la información consultada está desactualizada, las recomendaciones podrían no estar alineadas con los avances tecnológicos más recientes, lo que puede generar una solución menos eficiente o menos adecuada a las necesidades actuales y futuras de la municipalidad (Vuotto y otros, 2020).

- ✓ **Resistencia o Falta de Colaboración por Parte del Personal:** La investigación puede depender de la colaboración de los empleados municipales, como los técnicos de sistemas y otros usuarios finales, para obtener información clave sobre el uso de la red y los problemas existentes. Si hay falta de cooperación o resistencia por parte del personal en proporcionar datos o acceso a los sistemas, esto puede limitar la calidad de la investigación y dificultar la obtención de una visión clara de los desafíos y las necesidades de la infraestructura (Moschetta, 2023).

- ✓ **Limitación en la Evaluación de Impactos a Largo Plazo:** Es difícil predecir con precisión todos los cambios y demandas futuras en términos de infraestructura de red, especialmente en un entorno que evoluciona rápidamente debido a la digitalización y el avance tecnológico. Las proyecciones a largo plazo, como la expansión de servicios públicos o el aumento en el volumen de usuarios, pueden estar sujetas a incertidumbre. Esto limita la capacidad de diseñar un sistema que sea completamente escalable y adaptable a futuras necesidades (Miranda, 2023).

- ✓ **Diversidad de Factores a Considerar:** El rediseño de la red de cableado estructurado implica la consideración de múltiples variables como la distribución física de los edificios, los requisitos de seguridad de la información, la compatibilidad con equipos existentes, la normativa local, el tipo de tráfico de datos y las necesidades específicas de cada departamento o área de la municipalidad. Esta complejidad puede hacer que la investigación se enfoque solo en ciertos aspectos de la infraestructura, dejando de lado otras áreas relevantes (Villareal, 2020).

- ✓ **Condiciones Inesperadas en el Sitio de Implementación:** Durante la investigación preliminar, puede ser difícil prever problemas imprevistos en el sitio de instalación, como problemas de infraestructura física (por ejemplo, paredes de concreto que dificultan el tendido de cables, interferencias electromagnéticas, acceso limitado a conductos, etc.). Estos factores pueden afectar la validez de las propuestas de red basadas en las condiciones observadas, haciendo necesario un rediseño o ajuste durante la fase de implementación que no fue previsto en la investigación inicial (Silva, 2021).

- ✓ **Limitaciones Regulatorias y Normativas:** En muchas jurisdicciones, existen normativas y regulaciones específicas que dictan los requisitos técnicos y de seguridad para el diseño y la implementación de redes de telecomunicaciones en el ámbito público. Las restricciones legales pueden limitar las opciones tecnológicas disponibles para la

investigación, forzando a los diseñadores a adherirse a estándares más estrictos o a cumplir con especificaciones que no siempre se alinean con las mejores soluciones tecnológicas posibles (Sardiñas y otros, 2021).

- ✓ **Condiciones de Mercado y Disponibilidad de Equipos:** La disponibilidad y los precios de los equipos de red pueden estar sujetos a fluctuaciones del mercado, lo que podría limitar la capacidad de realizar recomendaciones sobre tecnologías o equipos de última generación. Además, la elección de ciertos proveedores o marcas puede verse condicionada por factores como la disponibilidad de soporte técnico o la compatibilidad con la infraestructura existente, lo que restringe las opciones disponibles para la solución propuesta (Viera y otros, 2024).

1.4 JUSTIFICACIÓN DEL INFORME

El rediseño de la red de cableado estructurado de la Municipalidad Distrital de Olmos responde a la necesidad de mejorar la infraestructura tecnológica de la institución para garantizar una conectividad eficiente, segura y escalable. A continuación, se detallan las principales razones que justifican la ejecución de este proyecto:

- ✓ Obsolescencia de la Infraestructura Actual: La red de cableado existente ha quedado obsoleta debido a su antigüedad y al uso de tecnologías que ya no cumplen con los estándares de rendimiento requeridos en la actualidad. La infraestructura actual presenta limitaciones significativas en cuanto a velocidad de transmisión de datos, fiabilidad y capacidad para soportar el aumento de dispositivos conectados, lo cual impacta negativamente en la eficiencia de los procesos administrativos y de atención al público (Peláez, 2021).

- ✓ Crecimiento Institucional y Expansión de Servicios: La municipalidad ha experimentado un crecimiento tanto en términos de personal como de servicios ofrecidos a los ciudadanos. Este crecimiento exige una actualización y expansión de la infraestructura de red, de manera que pueda soportar de forma óptima un mayor volumen de tráfico de datos y nuevos requerimientos tecnológicos. El rediseño de la red permitirá que la municipalidad sea capaz de gestionar eficientemente los recursos tecnológicos y responder de manera ágil a las necesidades emergentes de los usuarios (Solano & Gutierrez, 2023).

- ✓ Mejora en la Seguridad de la Información: La red de cableado estructurado es uno de los pilares fundamentales para garantizar la seguridad de la información y la integridad de los

sistemas tecnológicos de la municipalidad. Un diseño adecuado y actualizado de la infraestructura de red permitirá implementar medidas de seguridad más robustas, como el aislamiento de tráfico, la segmentación de redes y la incorporación de protocolos modernos de encriptación y autenticación. Esto resultará en una mayor protección contra ataques cibernéticos y la prevención de accesos no autorizados a la información sensible (Vaca, 2024).

- ✓ Optimización de Recursos y Reducción de Costos a Largo Plazo: Un rediseño de la red de cableado estructurado, basado en las mejores prácticas y en soluciones tecnológicas de vanguardia, permitirá una optimización de los recursos tecnológicos existentes. Esto no solo mejorará la eficiencia operativa, sino que también reducirá los costos a largo plazo relacionados con el mantenimiento, las reparaciones y las ampliaciones de la red. Además, una red más eficiente permitirá a la municipalidad aprovechar al máximo sus recursos y mejorar la calidad del servicio que ofrece a los ciudadanos (Salazar, 2023).

- ✓ Adaptación a Nuevas Tecnologías y Requerimientos: El avance tecnológico y la digitalización de los servicios públicos exigen que las instituciones se adapten constantemente a nuevos desafíos. El rediseño de la red de cableado estructurado facilitará la integración con nuevas tecnologías emergentes, como la implementación de sistemas de gestión inteligente, internet de las cosas (IoT), videoconferencias y plataformas colaborativas. De este modo, la municipalidad estará mejor preparada para incorporar soluciones tecnológicas innovadoras que mejoren la calidad de los servicios y la satisfacción de los usuarios (Sánchez & Mendoza, 2021).

- ✓ Cumplimiento de Normativas y Estándares Internacionales: El rediseño de la red también busca cumplir con las normativas nacionales e internacionales en cuanto a la calidad del servicio y la infraestructura de telecomunicaciones. Esto incluye el cumplimiento de las normativas ISO, las regulaciones locales de telecomunicaciones y las mejores prácticas recomendadas por organismos internacionales. La implementación de estos estándares garantizará que la infraestructura tecnológica de la municipalidad esté alineada con las exigencias de calidad y fiabilidad que se esperan en el sector público (Valle, 2021).

II. METODOLOGÍA Y HERRAMIENTAS A EMPLEAR

METODOLOGÍA

- ✓ **Enfoque Metodológico**

El diseño de la red de datos para la Municipalidad Distrital de Olmos se basa en la Metodología de Diseño de Red de Arriba hacia Abajo (*Top-Down*). Este enfoque permite una estructuración eficiente de la red al iniciar el proceso desde las capas superiores del modelo OSI, analizando primero las necesidades de las aplicaciones, sesiones y transferencia de datos, para luego definir los dispositivos y medios de conexión en las capas inferiores. La metodología *Top-Down* facilita la identificación de requerimientos clave, optimiza la gestión del proyecto al dividirlo en módulos y permite ajustar el diseño de manera iterativa. Adicionalmente, esta metodología permite un análisis detallado de las estructuras organizativas y de los usuarios de la red, asegurando que el diseño cumpla con sus necesidades actuales y futuras (Álvarez González, 2022).

Así mismo, el presente Trabajo de Suficiencia Profesional (TSP) es de tipo aplicado, ya que busca la propuesta de un diseño de red de datos que optimice la infraestructura de comunicación de la Municipalidad Distrital de Olmos

- ✓ **Técnicas e instrumentos de recolección de datos**

Para la obtención de datos relevantes en el diseño de la red se utilizó como técnica la observación directa, la cual permitió un levantamiento de información sobre la infraestructura de red actual. Además, se realizaron entrevistas estructuradas al personal del área de Tecnologías de la Información con el objetivo de conocer los requerimientos y limitaciones de la red. Finalmente, se empleó el software Wireshark para analizar el tráfico de datos y evaluar el rendimiento de la red existente.

- ✓ **Procedimientos metodológicos**

El desarrollo del diseño de la red de datos se realizó en varias etapas.

- ✓ Primero, se efectuó un análisis de la situación actual, en el que se evaluó la infraestructura de red existente mediante la identificación de equipos activos y pasivos, el análisis del tráfico de red y rendimiento de los servidores, la identificación de necesidades de conectividad en cada unidad organizativa y la evaluación de problemas de seguridad y administración de la red.

- ✓ Posteriormente, se llevó a cabo la evaluación de los requerimientos, definiendo aspectos técnicos y funcionales como seguridad física y lógica, escalabilidad y redundancia de la red, direccionamiento IP y segmentación mediante VLANs, capacidad de almacenamiento y procesamiento en los servidores, así como monitoreo y gestión del tráfico de red.
- ✓ Tras esta fase, se procedió con el diseño de la red, el cual se fundamentó en la información recopilada en las etapas previas. En este diseño se estableció la topología basada en un modelo jerárquico de tres capas, compuesto por núcleo, distribución y acceso. Además, se definió el direccionamiento IP mediante la implementación de subneteo para segmentar la red. Se incorporaron medidas de integración de sedes externas mediante enlaces dedicados.
- ✓ Finalmente, se realizó la validación del diseño con el objetivo de verificar su viabilidad. Esta validación se llevó a cabo mediante la simulación del diseño en software de redes, la revisión de estándares y buenas prácticas en diseño de redes, y el análisis costo-beneficio de la implementación del diseño.

- ✓ **Criterios de validación:**

  Para evaluar la efectividad del diseño propuesto, se establecieron criterios de validación centrados en la cobertura, seguridad, eficiencia y escalabilidad de la red. En cuanto a la cobertura, se plantea que el diseño garantice que el 100% del acceso a la red esté supervisado. Respecto a la seguridad, se busca que la red cuente con una protección total mediante segmentación y firewall. En términos de eficiencia, se considera que la integración de los servidores y Computadoras personales (PCs), permitiría regular el acceso a Internet de manera controlada. Finalmente, se propone que el diseño contemple la escalabilidad, permitiendo la expansión de la red sin afectar su rendimiento.

HERRAMIENTAS:

Para muchos indagadores en la red de diseño en su conexión de segmentos y dispositivos de una de las redes por partida para comprender el flujo de información. Contar con un esquema ya establecido de la red, así como algunos diseños de los usuarios, nos proporciona mapas que facilitan la creación de mejora y un cambio de diseño:

- ✓ **Software para la elaboración de Documentación:**

  Microsoft Office 2021 LTSC (Word, Excel y Power Point. Visio).

- ✓ **Software para seguimiento del avance del proyecto:**

  Microsoft Project Professional 2021 LTSC.

- ✓ **Software para Diseño de la red:**

  Cisco Packet Tracer.

- ✓ **Software para medición de tráfico de la Red:**

  Monitor de Red del 2012 Server R2

  Wireshark v4.2.3

DESCRIPCIÓN DEL DESARROLLO DE LA SOLUCIÓN

La Municipalidad del Distrito se distribuye en diferentes niveles. En cada nivel, se encuentran los switches, y a partir de estos se conecta un switch gestionable situado en el área de Informática, desde el cual se accede a los servidores. Esta oficina actuará como el Punto Focal de la institución. Se llevará a cabo un análisis exhaustivo y un plan realista de la red LAN del Distrito de Olmos, lo que permitirá identificar los puntos clave (los principales encuentros de convergencia del hardware). Además, al distribuir adecuadamente los equipos de cómputo, se facilitará la organización.

Adicionalmente, se realizarán las siguientes acciones:

- ✓ Definición de los enfoques de seguridad y autenticación en el sistema
- ✓ Definición de la asignación y direccionamiento del (IP).
- ✓ Descripción de las normas del acceso a la red y provisión de servicios.

Se implementarán las normas de acceso a la red que serán utilizadas por los usuarios internos de la organización, permitiendo supervisar el uso indebido del acceso y también de los servicios a si no deseados.

En lo que, diseñará la gestión del Active Directory (Registro Dinámico) en un servidor con Windows Server 2012 Standard como base. El registro dinámico permitirá establecer acuerdos de autenticación dentro del acceso y de los usuarios por los servicios de TI de la organización (servidor de impresión y servidor de documentos).

Además, se asignan direcciones IP estáticas a los ordenadores, lo que facilitará un control más riguroso sobre la distribución de los PCS de la institución.

Estas medidas están previstas para alcanzar los objetivos del plan, que incluyen:

- ✓ Mejorar la conexión de los dispositivos de computación.
- ✓ Proteger el cableado de la red y los equipos de comunicación.
- ✓ Reducir charla sobre servidores con direcciones IP accesibles mediante el cortafuegos.
- ✓ Monitorear y gestionar la autorización de miembros del equipo.
- ✓ Supervisar y regular el acceso a la web mediante reglas exclusivas para cada PC.
- ✓ Avalar el intercambio y conexión de la información de todos los usuarios.

MARCADORES DE REVISIONES DE LA SOLUCIÓN.

Se haya puesto en práctica la solución sugerida en este proyecto, se podrá llevar a cabo un análisis del nivel de cumplimiento utilizando indicadores que muestren resultados medibles. Es importante tener en cuenta que este proyecto no alcanzará la fase de ejecución, por lo que las recomendaciones presentadas servirán como una guía para futuras implementaciones e investigaciones. Los considerados son:

- ✓ 100% de acceso de en computadoras supervisados en las redes.
- ✓ 100% de protección en una de las redes.
- ✓ 100% de ingreso por usuarios gestionados en la red.
- ✓ 100% de integración de servidores y de PCS a un Internet regulados por el Cortafuegos.

LISTA DE PRODUCTOS ENTREGABLES

- ✓ Catálogo de equipos.
- ✓ Diagrama físico de la red.
- ✓ Distribución de VLAN y asignación de IP.

III. DESARROLLO DE LA SOLUCIÓN PROPUESTA

III.1 Medidas del tráfico de la red de datos existente en la municipalidad distrital de olmos

La medición del tráfico de red en la Municipalidad Distrital de Olmos es un paso crucial para comprender la eficiencia de la infraestructura actual y detectar posibles problemas de rendimiento. En esta sección se analiza el tráfico de datos mediante herramientas especializadas, con el fin de obtener información clave sobre el uso del ancho de banda, los niveles de latencia y los servicios que consumen más recursos. Estos hallazgos serán fundamentales para el diseño óptimo de la red física y lógica en los siguientes capítulos.

Características de la red existente

Los componentes identificados en la infraestructura actual de la red incluyen diferentes edificios y áreas dentro de la municipalidad:

- ✓ Primer Piso
- ✓ Segundo Piso
- ✓ Tercer Piso
- ✓ Mercado Municipal
- ✓ Estadio Municipal
- ✓ Piscina Municipal
- ✓ Terminal Terrestre

Cada una de estas ubicaciones cuenta con distintos puntos de acceso y dispositivos conectados a la red, los cuales se evaluaron en términos de su consumo de ancho de banda y eficiencia en la transmisión de datos.

Herramienta y puntos a tener en cuenta para la medición del tráfico de red.

Para llevar a cabo la medición del tráfico de red, se utilizó la herramienta Wireshark (versión 4.2.3), instalada en un servidor central, con el objetivo de recopilar datos de la red y generar informes estadísticos sobre el comportamiento del tráfico.

Para la medición del tráfico de red, se seleccionaron puntos estratégicos dentro de la infraestructura municipal, priorizando aquellos con mayor flujo de datos y relevancia en la conectividad general. La selección de estos puntos se realizó en función de la

disponibilidad de acceso a los equipos de red y la representatividad de los datos recopilados.

Presentación y análisis de resultados.

El flujo de información entre las computadoras y el servidor central durante el horario laboral se visualiza en los siguientes gráficos:

✓ Tráfico cliente-servidor

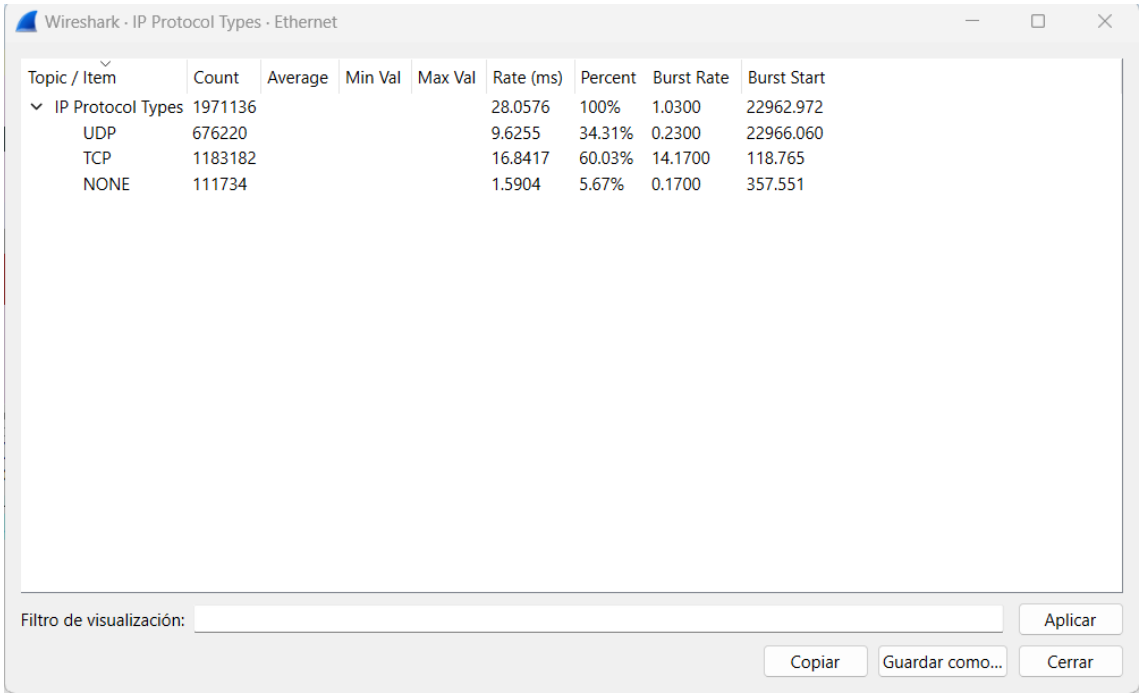


Ilustración 1. Análisis del tráfico de paquetes según tipo de protocolo en Wireshark

Los datos recopilados indican que existen períodos de mayor uso del ancho de banda, los cuales serán analizados en los gráficos siguientes, coincidiendo con el horario de mayor actividad en oficinas administrativas. En estos horarios, el tráfico de peticiones hacia el servidor se incrementa un 35% en comparación con el resto del día.

✓ Tráfico de protocolo de ethernet

El monitoreo de los paquetes Ethernet indicó que el 75% del tráfico correspondía a servicios internos como correo electrónico y transferencia de archivos, mientras que el 25% estaba asociado a la navegación en Internet. Además, el protocolo HTTP representó un 40% del tráfico total, lo que indica un uso intensivo de navegación web.

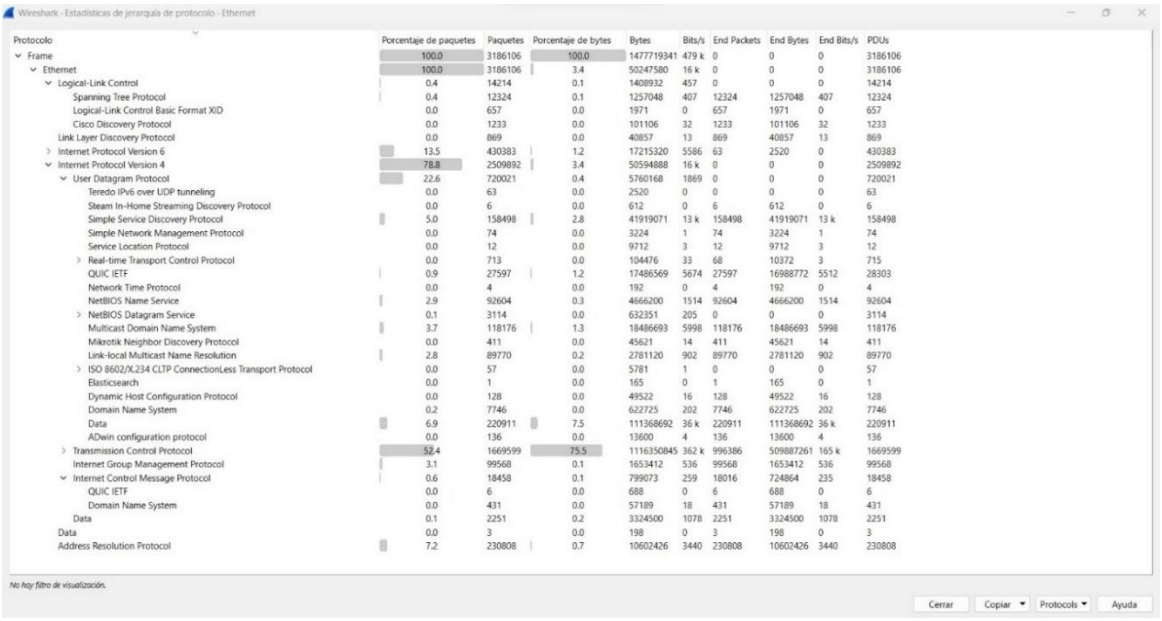


Ilustración 2 TAMAÑO DE PAQUETES ETHERNET

✓ Dimensión de los paquetes transmitidos en la red

El análisis del tamaño de los paquetes permitió identificar que el 60% de los paquetes transmitidos eran inferiores a 500 bytes, lo que sugiere un alto tráfico de solicitudes pequeñas en lugar de transferencias de archivos grandes. Asimismo, un 15% de los paquetes superaban los 1500 bytes, lo que indica transferencias de archivos pesados o transmisiones de video.

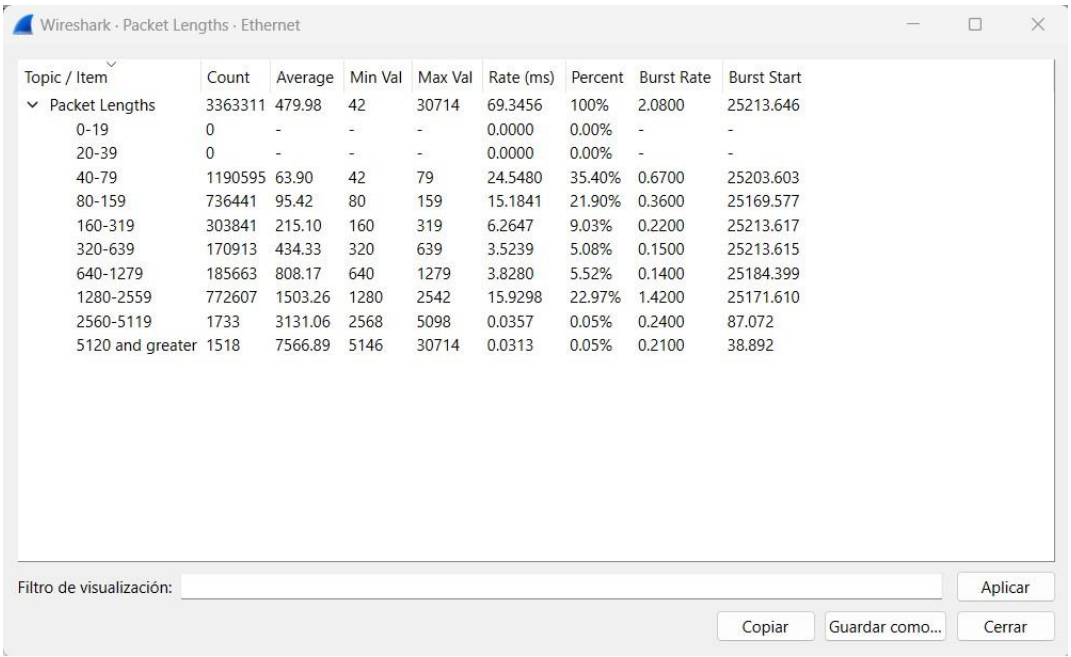


Ilustración 3 DIMENSIÓN DE LOS PAQUETES TRANSMITIDOS EN LA RED

- ✓ **Proceso de funcionamiento de los circuitos digitales de Internet – accesos a Internet**

Estos esquemas que se presentan a continuación ilustran el flujo de tráfico durante en el transcurso del trabajo.

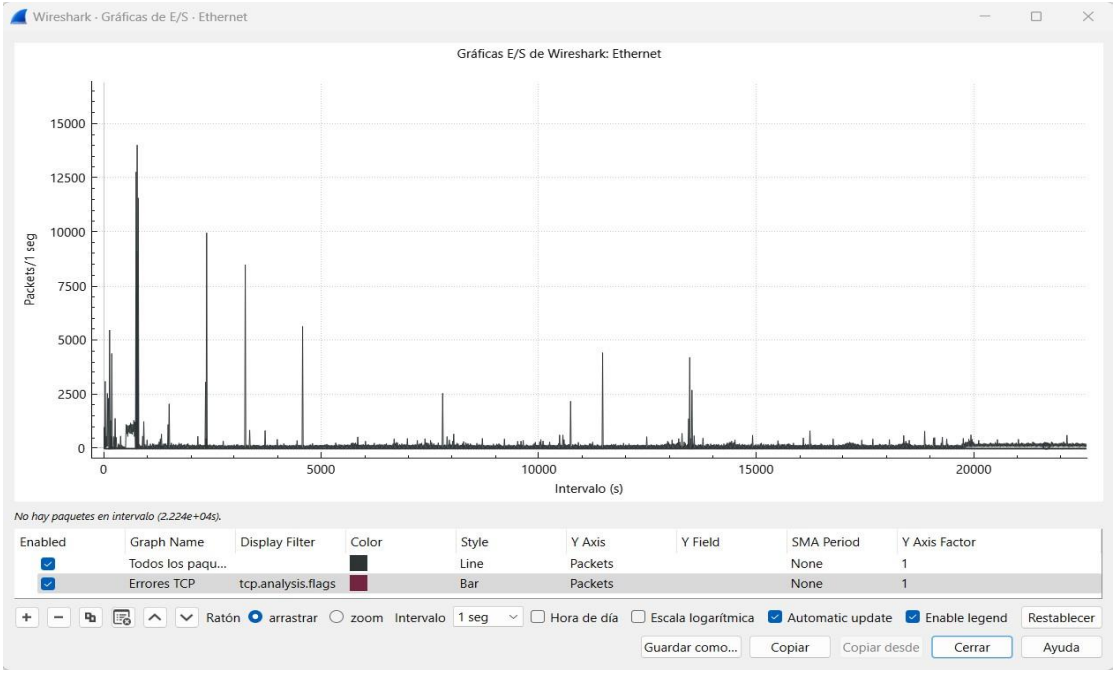


Ilustración 4 TRÁFICO DE CIRCUITOS DIGITALES

Identificación de problemas, oportunidades de mejora.

El análisis del tráfico de la red en la Municipalidad Distrital de Olmos permitió identificar una serie de deficiencias que afectan el rendimiento y la eficiencia de los servicios. Entre los principales problemas detectados, se evidenció saturación en horarios pico, especialmente durante las horas laborales de mayor demanda, lo que impacta negativamente en la operatividad administrativa. Asimismo, la falta de segmentación del tráfico impide la priorización de aplicaciones críticas, generando interferencias en servicios esenciales. Adicionalmente, se identificó un uso ineficiente del ancho de banda, con descargas y transferencias de archivos no esenciales que contribuyen a la congestión de la red.

Para mitigar estos inconvenientes y optimizar el desempeño de la infraestructura, se proponen diversas estrategias. En primer lugar, la implementación de VLANs permitirá una segmentación eficiente del tráfico, reduciendo la interferencia entre distintos tipos de usuarios y aplicaciones. En segundo lugar, el establecimiento de políticas de Calidad de

Servicio (QoS) garantizará la priorización de aplicaciones críticas, optimizando el flujo de datos en la red. Finalmente, la optimización en la gestión del ancho de banda mediante restricciones adecuadas contribuirá a evitar saturaciones y mejorar la disponibilidad de recursos en los horarios de mayor actividad.

Los hallazgos obtenidos justifican la necesidad de una reconfiguración estructural de la red, enfocada en mejorar la segmentación y distribución del tráfico, así como en garantizar un uso más eficiente del ancho de banda. La aplicación de estas estrategias permitirá optimizar el rendimiento de los servicios administrativos, reducir la congestión y mejorar la calidad de la conectividad en la municipalidad. En el siguiente ítem, se abordará el diseño de la red física y lógica con base en estos resultados, asegurando una arquitectura más eficiente, escalable y alineada con las necesidades operativas de la institución.

III.2 Diseño de la red física y lógica de la municipalidad distrital de Olmos

El diseño de la red de datos para la Municipalidad Distrital de Olmos responde a la necesidad de mejorar la eficiencia, seguridad y administración de los recursos informáticos de la institución. Actualmente, la infraestructura presenta limitaciones en el ancho de banda, segmentación de la red y control de acceso, lo que afecta la calidad del servicio. En este contexto, se propone una solución integral que incluye el diseño físico y lógico de la red, garantizando escalabilidad y robustez.

Levantamiento de Información y Requerimientos

- ✓ **Unidades Organizativas y Usuarios**

Para garantizar un diseño de red eficiente, se ha realizado un levantamiento de información sobre la estructura organizativa de la municipalidad y los usuarios que requieren acceso a los servicios informáticos. Cada unidad organizativa tiene necesidades específicas en cuanto a conectividad, acceso a servidores, impresión en red y comunicación interna.

Las principales unidades organizativas identificadas son las siguientes:

N°	UNIDAD
1	CONCEJO MUNICIPAL
2	ALCALDIA
3	GERENCIA MUNICIPAL
4	SUBGERENCIA DE ADMINISTRACIÓN Y FINANZAS
5	SUBGERENCIA DE ASESORIA JURÍDICA
6	SUBGERENCIA DE PLANEAMIENTO, RACIONALIZACIÓN Y PRESUPUESTO
7	SUBGERENCIA DE ADMINISTRACIÓN TRIBUTARIA
8	SUBGERENCIA DE SERVICIOS PUBLICOS Y GESTIÓN AMBIENTAL
9	SUBGERENCIA DE DESARROLLO URBANO Y RURAL
10	SUBGERENCIA DE DESARROLLO ECONOMICO Y SOCIAL
11	SUBGERENCIA DE ADMINISTRACIÓN DE LA CIUDAD A.B. LEGUIA
12	SECRETARÍA GENERAL
13	RELACIONES PÚBLICAS E IMAGEN INSTITUCIONAL

Tabla 1 UNIDADES ORGANIZATIVAS

Por cada unidad organizativa existen varios usuarios que ocupan los recursos informáticos de la municipalidad. A continuación, se detallan las cantidades de usuarios por cada unidad organizativa.

Unidad Organizativa: CONCEJO MUNICIPAL

N°	UNIDAD	N° DE USUARIOS
1	COMISIÓN DE REGIDORES	7
TOTAL		7

Tabla 2 UNIDAD ORGANIZATIVA: CONCEJO MUNICIPAL Y SUS DEPENDENCIAS

Unidad Organizativa: ALCALDÍA

N°	UNIDAD	N° DE USUARIOS
1	ALCALDIA	9
2	ÓRGANO DE CONTROL INSTITUCIONAL	9
3	PROCURADORÍA PÚBLICA MUNICIPAL	6
4	ÓRGANOS CONSULTIVOS Y DE COOPERACIÓN LOCAL DISTRITAL	0
TOTAL		24

Tabla 3 UNIDAD ORGANIZATIVA: ALCALDÍA

Unidad Organizativa: GERENCIA MUNICIPAL

N°	UNIDAD	N° DE USUARIOS
1	GERENCIA MUNICIPAL	7
TOTAL		7

Tabla 4 UNIDAD ORGANIZATIVA: GERENCIA MUNICIPAL

Unidad Organizativa: SUBGERENCIA DE ADMINITRACIÓN FINANCIERA

N°	UNIDAD	N° DE USUARIOS
1	ÁREA DE CONTABILIDAD	5
2	ÁREA DE TESORERÍA	7
3	ÁREA DE LOGÍSTICA Y PATRIMONIO	14
4	ÁREA DE RECURSOS HUMANOS	6
5	ÁREA DE SISTEMAS E INFORMÁTICA	15
TOTAL		47

Tabla 5 UNIDAD ORGANIZATIVA: SUBGERENCIA DE ADMINISTRACIÓN FINANCIERA

Unidad Organizativa: SUBGERENCIA DE ASESORÍA JURÍDICA

N°	UNIDAD	N° DE USUARIOS
1	OFICINA GENERAL DE ASESORÍA JURÍDICA	6
TOTAL		6

Tabla 6 UNIDAD ORGANIZATIVA: SUBGERENCIA DE ASESORÍA JURÍDICA

Unidad Organizativa: SUBGERENCIA DE PLANEAMIENTO, RACIONALIZACIÓN Y PRESUPUESTO

N°	UNIDAD	N° DE USUARIOS
1	ÁREA DE PROGRAMACIÓN DE INVERSIÓN	6
2	ÁREA DE GESTIÓN DE RIESGOS Y DESASTRES	12
3	ÁREA DE PLANEAMIENTO Y COOPERACIÓN TÉCNICA NACIONAL E INTERNACIONAL	5
TOTAL		23

Tabla 7 UNIDAD ORGANIZATIVA: SUBGERENCIA DE PLANEAMIENTO, REACIONALIZACION Y PRESUPUESTO

Unidad Organizativa: SUBGERENCIA DE ADMINISTRACIÓN TRIBUTARIA

N°	UNIDAD	N° DE USUARIOS
1	AREA DE TRIBUTACIÓN, RECAUDACIÓN Y FISCALIZACIÓN TRIBUTARIA	10
2	ÁREA DE COMERCIALIZACIÓN, AUTORIZACIONES Y LICENCIAS	7
3	ÁREA DE EJECUCIÓN COACTIVA	5
TOTAL		22

Tabla 8 UNIDAD ORGANIZATIVA: OFICINA GENERAL DE PLANEAMIENTO Y PRESUPUESTO

Unidad Organizativa: SUBGERENCIA DE SERVICIOS PÚBLICOS Y GESTIÓN AMBIENTAL

N°	UNIDAD	N° DE USUARIOS
1	AREA DE MEDIO AMBIENTE, POBLACIÓN Y SALUD	5
2	ÁREA DE REGISTROS CIVILES	6
3	ÁREA DE TRANSPORTE, VIABILIDAD Y TRÁNSITO	4
4	ÁREA DE SEGURIDAD CIUDADANA Y SERENAZGO	6
TOTAL		19

Tabla 9 UNIDAD ORGANIZATIVA: GERENCIA DE ADMINISTRACIÓN TRIBUTARIA

Unidad Organizativa: SUBGERENCIA DE DESARROLLO URBANO Y RURAL

N°	UNIDAD	N° DE USUARIOS
1	SUBGERENCIA DE DESARROLLO URBANO Y RURAL	7
2	ÁREA DE OBRAS URBANO Y RURAL	6
3	ÁREA DE CATASTRO	13
4	ÁREA DE EQUIPO MECÁNICO	2
5	ÁREA TÉNICA MUNICIPAL DE AGUA Y SANEAMIENTO	4
TOTAL		32

Tabla 10 UNIDAD ORGANIZATIVA: SUBGERENCIA DE DESARROLLO URBANO Y RURAL

Unidad Organizativa: SUBGERENCIA DE DESARROLLO ECONÓMICO Y SOCIAL

N°	UNIDAD	N° DE USUARIOS
1	ÁREA DE PROMOCIÓN ECONÓMICA	4
2	ÁREA DE PROGRAMAS SOCIALES	30
3	ÁREA DE LA MUJER E IGUALDAD DE OPORTUNIDADES	8
TOTAL		42

Tabla 11 UNIDAD ORGANIZATIVA: GERENCIA DE DESARROLLO TERRITORIAL E INFRAESTRUCTURA

Unidad Organizativa: SUBGERENCIA DE ADMINISTRACIÓN DE LA CIUDAD A.B. LEGUIA

N°	UNIDAD	N° DE USUARIOS
1	SUBGERENCIA DE ADMINISTRACIÓN DE LA CIUDAD A.B. LEGUIA	6
TOTAL		6

Tabla 12 UNIDAD ORGANIZATIVA: SUBGERENCIA DE ADMINISTRACIÓN DE LA CIUDAD A.B. LEGUIA

Unidad Organizativa: SECRETARIA GENERAL

N°	UNIDAD	N° DE USUARIOS
1	SECRETARIA GENERAL	5
TOTAL		5

Tabla 13 UNIDAD ORGANIZATIVA: GERENCIA DE DESARROLLO SOCIAL

Unidad Organizativa: RELACIONES PÚBLICAS E IMAGEN INSTITUCIONAL

N°	UNIDAD	N° DE USUARIOS
1	RELACIONES PÚBLICAS E IMAGEN INSTITUCIONAL	6
TOTAL		6

Tabla 14 UNIDAD ORGANIZATIVA: RELACIONES PÚBLICAS E IMAGEN INSTITUCIONAL

Estas unidades organizativas agrupan a los usuarios que harán uso de los servicios informáticos, lo que ha permitido definir los requerimientos de conectividad y seguridad. La segmentación de la red se diseña para garantizar la eficiencia en la transmisión de datos y el acceso restringido según las necesidades específicas de cada área.

- ✓ **Infraestructura tecnológica actual de la municipalidad de Olmos**

Sistemas Operativos

Actualmente, se utilizan los siguientes sistemas operativos:

- Microsoft Windows Server 2012 Standard en 1 servidor.
- Microsoft Windows 11 en 2 servidores (PCs adaptadas como servidores).
- Microsoft Windows 10 en 117 PCs de clientes.
- Microsoft Windows 10 en 43 laptops de clientes.

Hardware

PCS

RECURSOS	CARACTERISTICAS	TOTAL
CORE I3	PROC. 2.8 GHZ/RAM 2GB/ HD 500GB	17
CORE I3	PROC. 2.8 GHZ/RAM 4GB/ HD 500GB	11
CORE I3	PROC. 2.8 GHZ/RAM 8GB/HD 1TB	13
CORE I5	PROC. 2.8 GHZ/RAM 4GB/ HD 500GB	7
CORE I5	PROC. 2.8 GHZ/RAM 4GB/ HD 500GB	8
CORE I5	PROC. 2.8 GHZ/RAM 4GB/ HD 1TB	9
CORE I5	PROC. 3.0 GHZ/RAM 4GB/ HD 500GB	13
CORE I5	PROC. 3.0 GHZ/RAM 8GB/SSD 1TB	20
COREI7	PROC. 2.8 GHZ/RAM 8GB/ 1TB	18
COREI7	PROC. 2.8 GHZ/RAM 16GB/ 1TB	12
CORE I7	PROC. 3.0 GHZ/RAM 16GB/ 1TB	15
CORE I7	PROC. 3.2 GHZ/RAM 16GB/ SSD 1TB	12
TOTAL		155

Tabla 15 PCs

EQUIPOS DE COMUNICACIÓN

RECURSOS	CARACTERISTICAS	TOTAL
ROUTER	Router HUAWEI NetEngine AR651	**1**
SWITCH	Ubiquiti EdgeSwitch 24 LITE - 24-Puertos	**1**
SWITCH	D-Link DES-1024D- 24-Puertos	**8**
SWITCH	TP-LINK TL-SG108	**46**
ACCESS POINT	Access Point TP-Link TL-WA801N	**5**
TOTAL		**61**

Tabla 16 EQUIPOS DE COMUNICACIÓN

SERVIDORES

RECURSOS	CARACTERISTICAS	TOTAL
Servidor HP ProLiant DL360 Gen9	Proc 2.00 GHZ/RAM 16 Gb/HD 2TB (02 Discos) con redundancia de discos	**1**
LENOVO THINKCENTRE M920	Proc core i7-9700 3.00 GHZ/RAM 16 Gb/HD 1TB	**3**
TOTAL		**4**

Tabla 17 SERVIDORES

DISPOSITIVOS DE ENTRADA Y SALIDA

RECURSOS	**CARACTERISTICAS**	**TOTAL**
IMPRESORA MULTIFUNCIONAL	EPSON L3110	10
IMPRESORA MULTIFUNCIONAL	EPSON L5290	6
IMPRESORA MULTIFUNCIONAL	EPSON L15150	2
IMPRESORA MULTIFUNCIONAL	BROTHER DCP-T510W	7
IMPRESORA MULTIFUNCIONAL	BROTHER MFC-T4500DW	9
IMPRESORA MULTIFUNCIONAL	CANON G3110	1
IMPRESORA	RICOH IM430F	13
IMPRESORA	RICOH IM550F	2
IMPRESORA	RICOH IM600F	1
SCANNER	EPSON DS-770	1
PLOTTER	HP DESIGNJET 500	1

Tabla 18 DISPOSITIVOS DE ENTRADA Y DE SALIDA

Software de terceros con licencia

Dentro del proceso de automatización de los principales procedimientos, se cuentan con 4 sistemas web denominados:

- **Sistema de Trámite Documentario:** Este sistema permite registrar la documentación que ingresa a la Municipalidad, facilitando consultas y mejorando la información disponible para el público. Sus características principales incluyen: Registro de expediente, consulta de expediente, generación de reportes.
- **Servicio de Intranet:** Este servicio proporciona información histórica a todos los funcionarios de la Municipalidad y al público en general sobre los documentos y costos que deben gestionar o abonar. Las aplicaciones web están configuradas en el servidor de aplicaciones utilizando el servicio IIS (Internet Information Server).
- **Correo Electrónico:** El dominio de correo es email.muniolmos.gob.pe, configurado bajo Windows Server 2012 Standard. Ofrece acceso web al correo, permitiendo al personal de la institución comunicarse desde cualquier parte del mundo.
- **Página Web.** El enlace es www.muniolmos.gob.pe. Esta página, desarrollada en PHP, es completamente dinámica. Está alojada en un servidor en Tokio, Japón, con una capacidad de uso de disco de 3 Gigas y una capacidad de transmisión de 80 Gigas. Las actualizaciones se realizan mediante una conexión FTP, utilizando el software FileZilla v2.2.24a con su respectivo usuario y contraseña. La administración, actualización y mantenimiento son responsabilidad exclusiva del Webmaster o Administrador Web. Las actualizaciones se realizan según la necesidad de publicar información relevante sobre eventos o datos de interés inmediato. La responsabilidad de determinar qué información e imágenes se publican recae en el área de Imagen Institucional.

✓ Problemas identificados en la red y en los equipos

El análisis de la infraestructura de red de la municipalidad ha permitido identificar diversas deficiencias que afectan su operatividad y seguridad. En primer lugar, la institución cuenta con tres servidores activos, de los cuales solo uno cumple con las especificaciones técnicas adecuadas para una operación continua. Los otros dos servidores corresponden a equipos de escritorio convencionales, cuyo hardware no está diseñado para un funcionamiento ininterrumpido las 24 horas del día, los 7 días de la semana. Esta situación no solo compromete la estabilidad y continuidad de los

servicios alojados en ellos, sino que también incrementa el desgaste del hardware, reduciendo significativamente su vida útil.

En cuanto a la infraestructura de conmutación, la municipalidad dispone de:

- Dos **switches gestionables**, ubicados en las oficinas de informática y sistemas, utilizados como respaldo ante eventuales fallos.
- Ocho **switches no gestionables**, distribuidos en distintas áreas para facilitar la conectividad en zonas estratégicas. No obstante, la presencia de estos dispositivos limita la aplicación de medidas de seguridad avanzadas, ya que restringen la gestión centralizada y el monitoreo del tráfico de red.

Desde una perspectiva de seguridad, se han identificado riesgos tanto físicos como lógicos que deben ser abordados para garantizar la integridad y disponibilidad de la red:

Riesgos físicos

- Vulnerabilidad del cableado ante daños mecánicos o ataques de roedores.
- Posibilidad de robo o extravío de dispositivos de red en distintas áreas de la institución.
- Mal funcionamiento de equipos debido a sobrecargas eléctricas, caídas de tensión o diseños deficientes en la red de suministro eléctrico.
- Falta de un sistema de respaldo eléctrico confiable que garantice la continuidad de los servicios en caso de interrupciones.

Riesgos lógicos:

- Compromiso de dispositivos: La falta de medidas de seguridad adecuadas expone los datos a interceptaciones, alteraciones o eliminaciones. Además, las credenciales de usuario pueden ser vulneradas y las configuraciones de red modificadas de manera no autorizada.
- Ataques de reconocimiento: Los servidores expuestos en Internet, incluyendo el servidor de aplicaciones institucionales, pueden ser objeto de intentos de intrusión.

- Ataques de denegación de servicio (DoS): Acciones malintencionadas dirigidas contra los servidores de aplicaciones y correo electrónico podrían generar interrupciones en los servicios esenciales de la municipalidad.

Para mitigar estos riesgos, es fundamental lograr un equilibrio entre la seguridad y la operatividad de la red, considerando:

- La asignación de un presupuesto adecuado para la adquisición de equipos y software de protección.
- La facilidad de uso de las soluciones implementadas para no afectar la productividad de los usuarios.
- La optimización del rendimiento sin comprometer la seguridad.
- La garantía de disponibilidad y continuidad de los servicios.
- La facilidad de gestión y mantenimiento de la infraestructura de seguridad.

Al abordar estos problemas permitirá mejorar la estabilidad y confiabilidad de la red, asegurando una infraestructura más robusta y eficiente para la gestión municipal

✓ Requerimientos

Necesidades funcionales:

A partir del análisis de la infraestructura y las demandas operativas de la municipalidad, se han identificado los siguientes requerimientos esenciales para garantizar un funcionamiento eficiente de la red:

- Provisión de acceso a Internet para todas las oficinas y usuarios autorizados.
- Acceso a unidades compartidas para facilitar el intercambio de información entre los distintos departamentos.
- Habilitación de impresión en red para optimizar el uso de los recursos de impresión.
- Interconexión segura entre las sedes externas y la sede principal para garantizar la continuidad del servicio.

Requerimientos de la seguridad

En coordinación con la Oficina de Tecnologías de la Información, se han definido los siguientes requisitos:

- **Seguridad Física:**
  - Los equipos de comunicación deben almacenarse en gabinetes de seguridad cerrados, restringiendo el acceso a personal autorizado para evitar manipulaciones no autorizadas.
  - En los puntos de acceso, los dispositivos deben estar fijados a la pared o resguardados en cajas de seguridad con cerradura para prevenir robos o alteraciones.
  - Los tomacorrientes destinados a los equipos de red deben estar protegidos en gabinetes adecuados para evitar desconexiones accidentales o malintencionadas.
  - Los servidores y equipos en áreas críticas (como las oficinas de dirección, tesorería y contabilidad) deben contar con sistemas de respaldo eléctrico mediante UPS, garantizando la continuidad operativa ante cortes de energía.

- **Seguridad Lógica:**
  - Los usuarios de la red serán configurados como usuarios estándar dentro del Active Directory, lo que impedirá la modificación de configuraciones del sistema, así como la instalación o eliminación de software sin autorización.
  - La navegación por Internet estará regulada mediante políticas de acceso, permitiendo solo ciertos protocolos y servicios según las necesidades de cada área. Estas políticas serán administradas a través de grupos de Active Directory.
  - Se implementarán estándares de seguridad para credenciales de usuario, exigiendo contraseñas robustas que incluyan letras, números y símbolos, así como la obligatoriedad de renovarlas periódicamente.
  - La gestión de la información digital se organizará mediante repositorios grupales asignados a cada unidad, asegurando la protección y disponibilidad de los datos institucionales.
  - Los archivos almacenados en los repositorios no podrán ser eliminados sin la autorización expresa de la Oficina de Tecnologías de la Información, garantizando la trazabilidad y el resguardo de la documentación institucional.

Estos requerimientos permitirán fortalecer la infraestructura de red de la municipalidad, asegurando no solo su operatividad y disponibilidad, sino también la integridad y confidencialidad de la información.

Requerimientos de puntos de red

En función de las necesidades operativas y administrativas de la Municipalidad Distrital de Olmos, se ha determinado la implementación de una infraestructura de red robusta y eficiente que garantice la conectividad en las distintas dependencias de la institución. En este sentido, se ha establecido un total de 262 puntos de red, cuya distribución responde a criterios de optimización del acceso a los servicios digitales, mejora en la comunicación interna y fortalecimiento de la gestión institucional.

El área de Informática contará con 15 puntos de red, los cuales permitirán la administración y mantenimiento de los sistemas tecnológicos municipales, asegurando la continuidad operativa de los servicios digitales. En los diferentes niveles del edificio principal, la distribución de los puntos de red responde a la demanda de conectividad en las oficinas administrativas y áreas de atención al público. Así, en el Piso 1 se han asignado 62 puntos, en el Piso 2, 57 puntos, y en el Piso 3, 52 puntos, garantizando el acceso estable a la infraestructura tecnológica por parte de los funcionarios y usuarios que interactúan con los sistemas informáticos municipales.

Por otro lado, en los espacios destinados a la prestación de servicios públicos y actividades comerciales, se han asignado puntos de red estratégicamente distribuidos para optimizar la conectividad en estos entornos. En el Mercado Nuevo, se han previsto 38 puntos de red, los cuales permitirán el adecuado funcionamiento de los sistemas de gestión comercial y administrativa. La Piscina Municipal contará con 12 puntos de red, asegurando la conectividad necesaria para la administración y control de sus operaciones. Asimismo, en el Estadio Municipal se instalarán 22 puntos de red, facilitando la supervisión y el manejo de los eventos deportivos y recreativos que se desarrollen en este recinto. Finalmente, en el Terminal Terrestre, se han destinado 4 puntos de red, fundamentales para la gestión operativa y administrativa de este espacio.

N°	ÁREA	Cantidad de puntos de red
1	Informática	15
2	Piso 1	62
3	Piso 2	57
4	Piso 3	52
5	Mercado nuevo	38
6	Piscina Municipal	12
7	Estadio Municipal	22
8	Terminal Terrestre	4
Total		262

Tabla 19 REQUERIEMIENTOS DE PUNTOS DE RED

La planificación de estos puntos de red responde a un análisis detallado de las necesidades de cada área, priorizando la estabilidad y eficiencia de la infraestructura tecnológica. Con esta distribución, se busca garantizar el acceso continuo a los servicios digitales, optimizar los procesos administrativos y operativos, y fortalecer la capacidad institucional para la gestión eficiente de la información. Además, la implementación de esta infraestructura permite la integración de futuras ampliaciones y mejoras, en concordancia con el crecimiento y modernización de la municipalidad.

- ✓ **Selección de tecnologías y dispositivos para cada bloque**

La selección de tecnologías y dispositivos se llevó a cabo como un paso fundamental previo al diseño y simulación de la red, garantizando la idoneidad de los equipos conforme a los requerimientos técnicos y operativos del proyecto. Para ello, se priorizó la adopción de estándares internacionales en infraestructura de red, optimizando la eficiencia, la escalabilidad y la seguridad de la conectividad.

Estructura de Cableado y Red Local

Se propuso un sistema de cableado estructurado diseñado para establecer una infraestructura de red robusta y centralizada, asegurando la conexión eficiente de todas las estaciones de trabajo a través de un nodo ubicado en la oficina principal. Para ello, se contempló la implementación de cableado UTP de categoría 6, con un total de 262 puntos de conexión de datos, permitiendo una capacidad de transmisión de 479 kbps. Esta configuración se definió siguiendo las normativas internacionales vigentes en telecomunicaciones.

Asimismo, se planteó una Red de Área Local (LAN) basada en tecnología Ethernet, con el propósito de garantizar una transmisión de datos de alta velocidad y una

conectividad estable. La propuesta contempló una infraestructura escalable, permitiendo futuras expansiones sin comprometer el rendimiento del sistema.

Selección de dispositivos de conectividad

- **Switches - Capa de Core**
  - Ubiquiti: Switch de alto rendimiento con soporte para velocidades de 10/100/1000 Mbps y 10-Gigabit. La propuesta incluyó su implementación debido a sus funcionalidades avanzadas como Power over Ethernet (PoE), VLAN, Quality of Service (QoS) y Auto-Voice, las cuales optimizarían la seguridad y la eficiencia en la administración de la red.
- **Switches** - **Capa de Distribución y Acceso**
  - D-Link Switch Web Smart 48-Port 10/100/1000 + 4 Combo SFP: Se propuso este equipo para facilitar el enrutamiento y la conmutación dinámica en la capa 3, garantizando un alto rendimiento en la gestión del tráfico de red. Además, incorpora mecanismos de seguridad avanzados y optimización del servicio de calidad (QoS), favoreciendo una administración eficiente de los recursos de conectividad.

Con el propósito de garantizar un óptimo almacenamiento y procesamiento de datos en la infraestructura propuesta, se contempló la implementación de servidores con las siguientes características:

- **Servidor de Aplicaciones**
  - HP ProLiant DL360 Gen9: Equipado con un procesador de 2.00 GHz, 16 GB de memoria RAM y un almacenamiento de 438 GB distribuidos en tres discos con redundancia, lo que permitiría asegurar alta disponibilidad y tolerancia a fallos en la gestión de aplicaciones.
- **Servidor de Archivos**
  - Lenovo ThinkCentre M900. Con procesador Intel Core i7-9700 (3 GHz), Memoria RAM de 16 GB, Disco Duro de 1 TB, y se propuso la implementación de tres unidades para optimizar el almacenamiento y la gestión de archivos.
- **Puntos de Acceso**

Para garantizar una cobertura inalámbrica eficiente en las distintas áreas de la institución, la propuesta incluyó la instalación de puntos de acceso estratégicos

que permitirían la conectividad a través de Wi-Fi, facilitando la movilidad y el acceso a la red:

- Access Point TP-Link TL-WA801N, considerado en diversas ubicaciones con el objetivo de maximizar la cobertura y estabilidad de la red inalámbrica.

Selección y distribución de Equipos

La red fue segmentada estratégicamente en distintos puntos de acceso, con base en las necesidades operativas identificadas en cada área de la institución. La propuesta consideró la siguiente distribución de dispositivos:

- **Área de Informática** (15 puntos de conexión):
  - 01 Router Huawei NetEngine AR651
  - 01 Switch Ubiquiti EdgeSwitch 24 LITE (24 puertos)
  - 02 Switches D-Link DES-1024D (24 puertos)
  - 01 Access Point TP-Link TL-WA801N
  - 01 Gabinete de piso
- **Primer Piso** (62 puntos de conexión):
  - 03 Switch D-Link DES-1024D (24 puertos)
- **Segundo Piso** (57 puntos de conexión):
  - 03 Switch D-Link DES-1024D (24 puertos)
  - 01 Access Point TP-Link TL-WA801N
- **Tercer Piso** (52 puntos de conexión):
  - 03 Switch D-Link DES-1024D (24 puertos)
  - 01 Access Point TP-Link TL-WA801N
- **Mercado Nuevo** (38 puntos de conexión):
  - 02 Switch D-Link DES-1024D (24 puertos)
  - 01 Gabinete de pared
- **Piscina Municipal** (12 puntos de conexión):
  - 01 Switch D-Link DES-1024D (24 puertos)
  - 01 Gabinete de pared
- **Estadio Municipal** (22 puntos de conexión):
  - 01 Switch D-Link DES-1024D (24 puertos)
  - 01 Gabinete de pared
- **Terminal Terrestre** (4 puntos de conexión):
  - 01 Switch D-Link DES-1024D (24 puertos)

Diseño físico de la red

El diseño físico de la red constituye la representación tangible de la infraestructura de interconexión implementada en la organización. Este esquema detalla la distribución espacial y la disposición de los dispositivos de red, tales como routers, switches, servidores y equipos terminales, así como el tipo de medio físico utilizado para la transmisión de datos. En este proyecto, se ha desarrollado una arquitectura jerárquica que permite optimizar la escalabilidad, seguridad y eficiencia operativa del sistema de comunicaciones internas.

La red se encuentra estructurada bajo el modelo de tres capas, conformadas por el núcleo (core), distribución y acceso. En la capa de núcleo se ubica un switch central que actúa como punto de convergencia para todas las conexiones, tanto internas como externas. Este dispositivo establece enlaces directos con los switches de distribución de cada piso de la sede principal y con los routers que conectan a las sedes remotas.

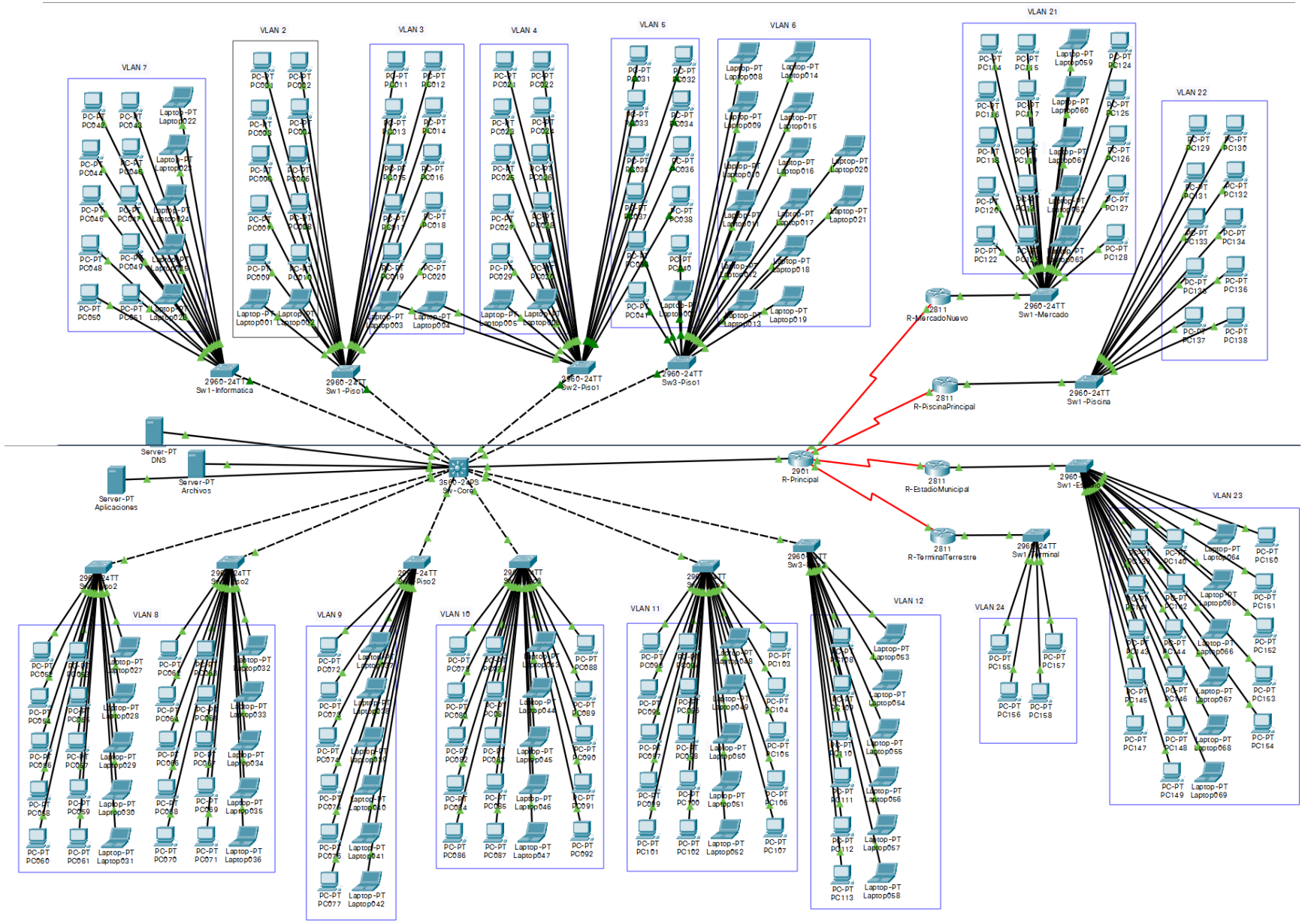


Ilustración 5. Diseño del de la red física

Las conexiones entre dispositivos se realizan mediante cableado estructurado con cables UTP categoría 6, lo que garantiza una transmisión de datos confiable en un entorno de red Fast Ethernet. En cuanto a la conectividad intersede, se han implementado cuatro enlaces WAN mediante routers modelo 2811, que enlazan la sede principal con las sedes externas: Mercado Nuevo, Piscina Municipal, Estadio Municipal y Terminal Terrestre. Cada una de estas sedes remotas dispone de un router de borde, un switch de acceso y un conjunto de pc de trabajo.

Adicionalmente, se han implementado servidores especializados dentro de la sede principal, entre los cuales destacan el servidor de archivos, el servidor de aplicaciones y el servidor DNS, conectados directamente al switch central para optimizar la disponibilidad y velocidad de acceso a los servicios compartidos. Esta disposición física garantiza no solo una comunicación eficiente entre dispositivos, sino también una administración centralizada de los recursos de red.

La implementación física responde a criterios de orden y escalabilidad, permitiendo que el sistema se expanda de manera controlada y que se mantenga la estabilidad del servicio ante posibles contingencias técnicas. Este diseño físico constituye, por tanto, la base estructural sobre la que se sustenta el diseño lógico de la red.

Diseño Lógico de la red

La configuración lógica de los equipos de red se llevó a cabo a través del acceso por consola, siguiendo procedimientos estandarizados de inicialización, identificación y direccionamiento. Para todos los dispositivos se establecieron parámetros esenciales como el nombre del host, la asignación de direcciones IP a las interfaces, la activación de puertos, la configuración de rutas estáticas donde correspondía, así como la desactivación de servicios innecesarios para mejorar la seguridad y el rendimiento del sistema.

- **Configuración básica por consola**

Esta configuración consiste en asignar un nombre y contraseña a cada equipo, la estructura que se siguió para realizar dicha configuración desde el programa cisco packetracer es el siguiente:

```
enable
configure terminal
hostname <Mi-Dispositivo>        ! p.ej. SW- Core, SW-Piso1, R-Principal
```

```
no ip domain-lookup              ! evita delays por DNS fallido
! -- Seguridad consola/enable --
enable secret ¡TuEnablePass!
line console 0
 password ¡TuConsolePass!
 login
logging synchronous
```

A continuación, se presenta un ejemplo de la configuración básica realizada para el router principal:

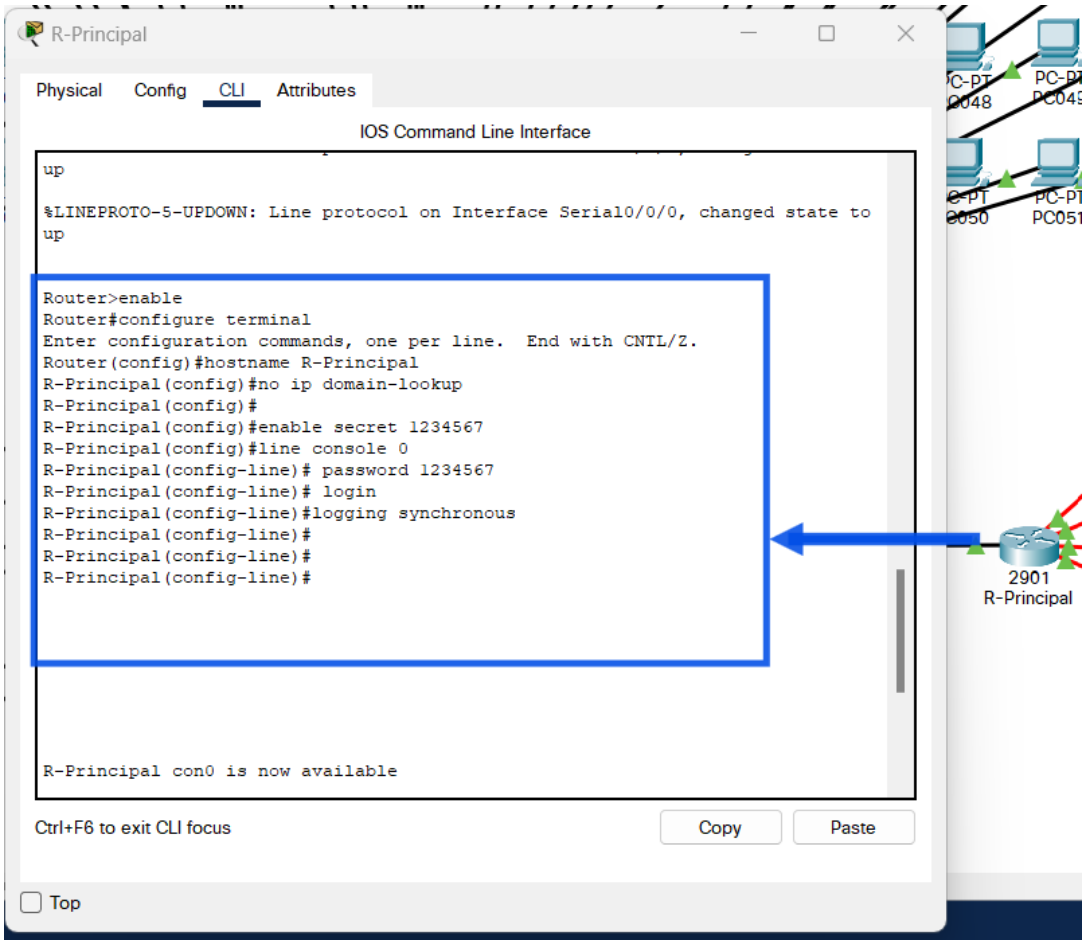
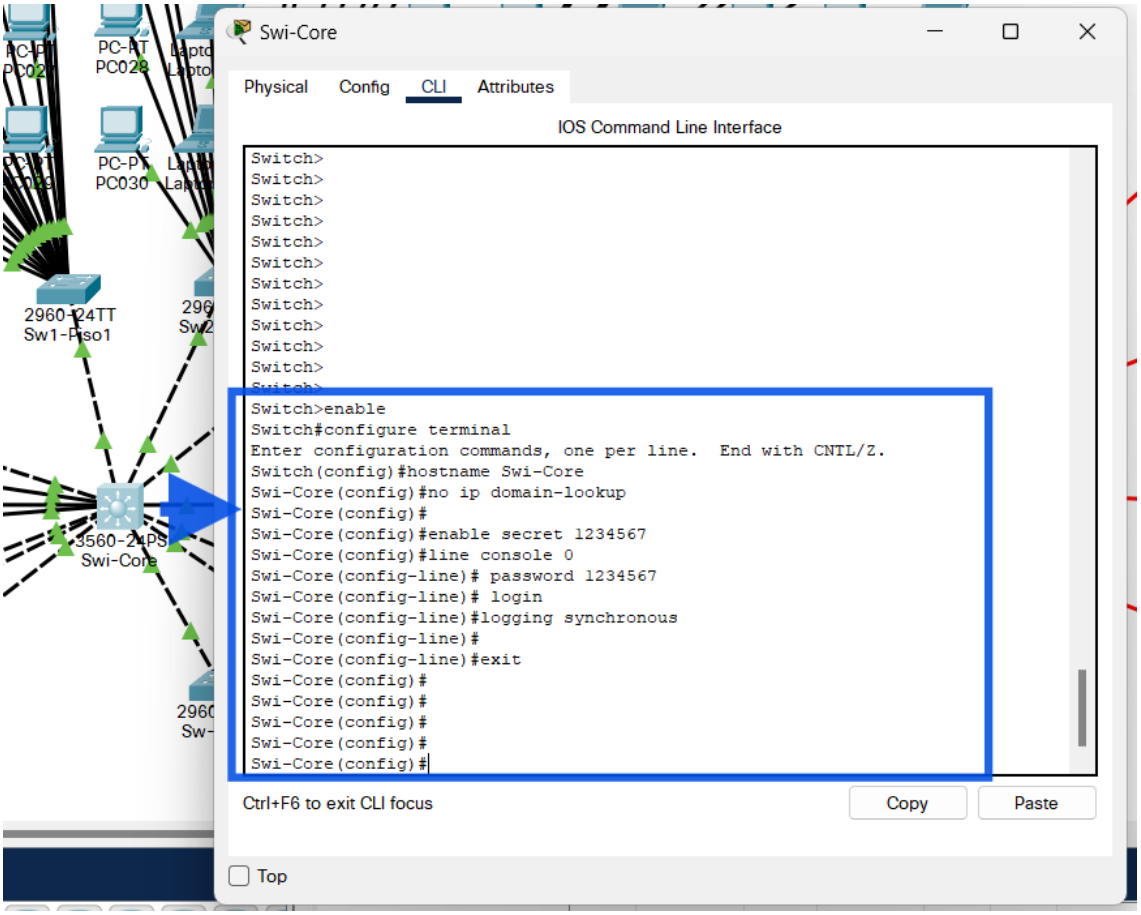


Ilustración 6. Configuración básica del Router Principal

Del mismo modo, se realizó la configuración del switch de núcleo o **Switch Core**, cuya función principal es centralizar el tráfico de todas las VLAN configuradas en la infraestructura y distribuirlo hacia los diferentes switches de acceso:



Cabe señalar que esta metodología se replicó para el resto de dispositivos de red, como los switches de acceso en cada piso del edificio principal, así como los routers pertenecientes a las sedes descentralizadas (Mercado Nuevo, Piscina Municipal, Estadio Municipal y Terminal Terrestre). Las configuraciones completas de dichos dispositivos se encuentran documentadas en el Anexo 5.

- **Configuración de enlaces troncales (trunking)**

Como parte fundamental de la segmentación lógica de la red mediante VLANs, se implementaron enlaces troncales que permitieran la propagación de múltiples VLANs sobre un solo enlace físico entre los switches. Este proceso se realizó utilizando el protocolo IEEE 802.1Q.

En primer lugar, se configuraron los puertos troncales en el Switch Core, permitiendo así la comunicación con todos los switches de acceso distribuidos por piso en el edificio principal. Estas configuraciones se muestran a continuación:

- **Sw-Core**

  enable
  configure terminal

  interface g0/1
  switchport trunk encapsulation dot1q
  switchport mode trunk
  no shutdown
  exit

```
Sw-Core(config)#interface g0/1
Sw-Core(config-if)# switchport trunk encapsulation dot1q
Sw-Core(config-if)# switchport mode trunk

Sw-Core(config-if)# no shutdown
Sw-Core(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed
state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed
state to up
```

Ilustración 7. Configuración del enlace troncal en el Sw-Core

En la siguiente etapa, se habilitó el modo trunk en las interfaces que interconectan el Switch Core con los switches de cada piso, designados como Sw1-piso1, Sw2-piso2, y así sucesivamente.

- **Sw-Core**

  enable
  configure terminal
  interface f0/6
  switchport mode trunk
  no shutdown
  exit

  interface f0/5
  switchport mode trunk
  no shutdown
  exit

  interface f0/3
  switchport mode trunk
  no shutdown
  exit

  interface f0/9
  switchport mode trunk
  no shutdown
  exit

interface f0/10
switchport mode trunk
no shutdown
exit

interface f0/1
switchport mode trunk
no shutdown
exit

interface f0/4
switchport mode trunk
no shutdown
exit

interface f0/11
switchport mode trunk
no shutdown
exit

interface f0/2
switchport mode trunk
no shutdown
exit

interface f0/12
switchport mode trunk
no shutdown
exit

De igual manera, en cada **Switch de Acceso por Piso** se habilitó el modo trunk en el puerto correspondiente que lo conecta con el Switch Core, garantizando la correcta propagación de las VLANs definidas en el diseño lógico. Los comandos ejecutados por cada Switch de acceso fueron los siguientes:

configure terminal
interface f0/1
switchport mode trunk
no shutdown
exit

Este esquema de configuración de enlaces troncales asegura la coherencia del tráfico inter-VLAN, centralizado a través del Switch Core y distribuido a lo largo de toda la topología lógica.

III.3 Asignación de VLAN y configuración de IP

Antes de proceder con la creación y asignación de VLANs en los switches de la red, fue necesario realizar una planificación estructurada del direccionamiento IP, estableciendo previamente las subredes necesarias mediante la técnica de subneteo con prefijo /26. Esta etapa permitió delimitar con claridad los rangos de direcciones IP que serían empleados para cada segmento de red lógico (VLAN), garantizando una distribución eficiente de los recursos de red, alineada con la cantidad de dispositivos por área, y permitiendo una gestión precisa de los recursos IP disponibles.

- **Segmentación de la red mediante VLAN**

  En el proceso de diseño lógico de la infraestructura de red para la municipalidad, se consideró la implementación de VLAN (Virtual Local Area Networks) como mecanismo fundamental para la segmentación lógica de la red, conforme a las buenas prácticas de diseño establecidas por organismos como Cisco y otras entidades de referencia en redes de datos. Esta segmentación tiene como propósito principal optimizar el rendimiento de la red, mejorar la seguridad y facilitar la administración de los dispositivos conectados, agrupándolos por funciones o ubicaciones físicas, independientemente de su conectividad física.

  Se definieron un total de 15 VLAN, correspondientes a las áreas funcionales existentes dentro de la municipalidad y sus sedes descentralizadas. La creación de estas VLAN responde a la necesidad de aislar el tráfico de red por áreas, reduciendo la posibilidad de congestión, mejorando la capacidad de diagnóstico, y limitando el alcance de posibles incidentes de seguridad a nivel de red interna. Cada VLAN representa una unidad organizacional específica que puede administrar sus propios recursos de red de manera más eficiente y segura.

  Además, la segmentación por VLAN permite implementar políticas de acceso diferenciadas, priorizar tráfico crítico mediante QoS (Quality of Service) y facilitar la integración con dispositivos de red avanzados como switches de capa 3, firewalls o controladores de red definidos por software (SDN), lo cual garantiza una arquitectura escalable y alineada a estándares modernos de infraestructura TI. A continuación, se mencionan las VLAN consideradas:

VLAN ID	Área	Ubicación
2	Administración Tributaria	Primer piso
3	Servicios Públicos y Gestión Ambiental	Primer piso
4	Desarrollo Urbano y Rural	Primer piso
5	Desarrollo Económico y Social	Primer piso
6	Imagen Institucional	Primer piso
7	Informática	Segundo piso
8	Alcaldía / Secretaría / Gerencia / Concejo	Segundo piso
9	Asesoría Jurídica	Segundo piso
10	Administración y Finanzas	Tercer piso
11	Planeamiento y Presupuesto	Tercer piso
12	Administración Ciudad A.B. Leguía	Tercer piso
21	Mercado Nuevo	Sede 1
22	Piscina Municipal	Sede 2
23	Estadio Municipal	Sede 3
23	Terminal Terrestre	Sede 4
50	Infraestructura (Core, Router, Servidores)	Segundo piso (TI)

Tabla 20 VLAN Consideradas para la segmentación de tráfico

- **Asignación de direcciones IP por VLAN**

En correspondencia con la segmentación lógica definida mediante el uso de VLANs, se implementó un esquema de direccionamiento IP fundamentado en la aplicación del subneteo de redes privadas clase C, con el propósito de optimizar el uso del espacio de direcciones y garantizar una asignación eficiente, escalable y segura. En particular, se aplicó un subneteo sistemático que derivó en subredes con prefijo /26, es decir, con una máscara de subred de 255.255.255.192, permitiendo obtener bloques de direcciones con 62 hosts utilizables por subred.

Este esquema de subneteo se diseñó considerando criterios técnicos de eficiencia, claridad administrativa y capacidad de expansión futura. La elección de subredes /26 responde a la necesidad de asignar bloques de direcciones IP proporcionales al número estimado de dispositivos por área o sede, evitando el desperdicio de direcciones y reduciendo la superficie de exposición en caso de fallos o brechas de seguridad. A su vez, este modelo facilita la implementación de políticas de control de tráfico mediante

listas de control de acceso (ACL), reglas de enrutamiento y segmentación por niveles de confianza.

Cada VLAN fue asociada a una subred /26 distinta, con rangos claramente delimitados para el gateway, dispositivos de red, estaciones de trabajo, servidores y otros equipos relevantes. Este enfoque mejora la trazabilidad y la administración del direccionamiento IP dentro de la red, permitiendo una gestión más ordenada y robusta.

En la tabla siguiente se detallan los rangos de direcciones IP resultantes del proceso de subneteo aplicado a cada VLAN considerada en el diseño lógico de la red:

VLAN ID	Área	Ubicación	Subred	Dirección Broadcast	Rango de IP Utilizables
2	Administración Tributaria	Primer piso	192.168.1.0/26	192.168.1.63	192.168.1.1 – 192.168.1.62
3	Servicios Públicos y Gestión Ambiental	Primer piso	192.168.1.64/26	192.168.1.127	192.168.1.65 – 192.168.1.126
4	Desarrollo Urbano y Rural	Primer piso	192.168.1.128/26	192.168.1.191	192.168.1.129 – 192.168.1.190
5	Desarrollo Económico y Social	Primer piso	192.168.1.192/26	192.168.1.255	192.168.1.193 – 192.168.1.254
6	Imagen Institucional	Primer piso	192.168.2.0/26	192.168.2.63	192.168.2.1 – 192.168.2.62
7	Informática	Segundo piso	192.168.2.64/26	192.168.2.127	192.168.2.65 – 192.168.2.126
8	Alcaldía / Secretaría / Gerencia / Concejo	Segundo piso	192.168.2.128/26	192.168.2.191	192.168.2.129 – 192.168.2.190
9	Asesoría Jurídica	Segundo piso	192.168.2.192/26	192.168.2.255	192.168.2.193 – 192.168.2.254
10	Administración y Finanzas	Tercer piso	192.168.3.0/26	192.168.3.63	192.168.3.1 – 192.168.3.62
11	Planeamiento y Presupuesto	Tercer piso	192.168.3.64/26	192.168.3.127	192.168.3.65 – 192.168.3.126
12	Administración Ciudad A.B. Leguía	Tercer piso	192.168.3.128/26	192.168.3.191	192.168.3.129 – 192.168.3.190
21	Mercado Nuevo	Sede 1	192.168.3.192/26	192.168.3.255	192.168.3.193 – 192.168.3.254
22	Piscina Municipal	Sede 2	192.168.4.0/26	192.168.4.63	192.168.4.1 – 192.168.4.62
23	Estadio Municipal	Sede 3	192.168.4.64/26	192.168.4.127	192.168.4.65 – 192.168.4.126
24	Terminal Terrestre	Sede 4	192.168.4.128/26	192.168.4.191	192.168.4.129 – 192.168.4.190
50	Infraestructura (Core, Router principal, Servidores)	Segundo piso (TI)	192.168.0.0/24	192.168.0.255	192.168.0.1 – 192.168.0.254

Tabla 21Distribución de direcciones IP utilizables por cada VLAN considerada

- **Configuración de VLAN y direcciones IP**

Para asegurar una administración centralizada y remota de los equipos de red, se configuraron interfaces de gestión sobre la VLAN 50, reservada exclusivamente para el área de Infraestructura (TI/Core). Dicha VLAN permite acceder a los switches desde cualquier punto autorizado de la red, facilitando tareas de monitoreo, actualización y mantenimiento. La asignación de IPs se realizó dentro de una subred /26 reservada exclusivamente para este propósito.

Configuración de IP de gestión a los switches (VLAN 50 – Infraestructura)

A continuación, se muestran las configuraciones de la VLAN 50 en algunos de los equipos más importantes:

- **R-Principal**

```
R-Principal#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R-Principal(config)#interface g0/0.50
R-Principal(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.50, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.50,
changed state to up

R-Principal(config-subif)#encapsulation dot1Q 50
R-Principal(config-subif)#ip address 192.168.0.1 255.255.255.0
R-Principal(config-subif)#no shutdown
R-Principal(config-subif)#
```

Ilustración 8. Configuración de la VLAN 50 en el router principal

- **Sw-Core:**

```
Sw-Core>Enable
Password:
Password:
Sw-Core#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Sw-Core(config)#
Sw-Core(config)#vlan 50
Sw-Core(config-vlan)#name Infraestructura
Sw-Core(config-vlan)#exit
Sw-Core(config)#interface vlan 50
Sw-Core(config-if)# ip address 192.168.0.11 255.255.255.0
Sw-Core(config-if)# no shutdown
Sw-Core(config-if)#
%LINK-5-CHANGED: Interface Vlan50, changed state to up

Sw-Core(config-if)#exit
Sw-Core(config)#interface g0/1
Sw-Core(config-if)# switchport trunk encapsulation dot1q
Sw-Core(config-if)# switchport mode trunk

Sw-Core(config-if)# no shutdown
Sw-Core(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed
state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed
state to up

Sw-Core(config)#ip default-gateway 192.168.0.1
Sw-Core(config)#exit
Sw-Core#
Sw-Core#show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
FastEthernet0/1        unassigned      YES unset  up                    up
FastEthernet0/2        unassigned      YES unset  up                    up
FastEthernet0/3        unassigned      YES unset  up                    up
FastEthernet0/4        unassigned      YES unset  up                    up
FastEthernet0/5        unassigned      YES unset  up                    up
FastEthernet0/6        unassigned      YES unset  up                    up
FastEthernet0/7        unassigned      YES unset  up                    up
FastEthernet0/8        unassigned      YES unset  up                    up
FastEthernet0/9        unassigned      YES unset  up                    up
FastEthernet0/10       unassigned      YES unset  up                    up
FastEthernet0/11       unassigned      YES unset  up                    up
FastEthernet0/12       unassigned      YES unset  up                    up
FastEthernet0/13       unassigned      YES unset  down                  down
FastEthernet0/14       unassigned      YES unset  down                  down
FastEthernet0/15       unassigned      YES unset  down                  down
FastEthernet0/16       unassigned      YES unset  down                  down
FastEthernet0/17       unassigned      YES unset  down                  down
FastEthernet0/18       unassigned      YES unset  down                  down
FastEthernet0/19       unassigned      YES unset  down                  down
FastEthernet0/20       unassigned      YES unset  down                  down
FastEthernet0/21       unassigned      YES unset  down                  down
 --More--
%SYS-5-CONFIG_I: Configured from console by console

FastEthernet0/22       unassigned      YES unset  down                  down
FastEthernet0/23       unassigned      YES unset  down                  down
FastEthernet0/24       unassigned      YES unset  down                  down
GigabitEthernet0/1     unassigned      YES unset  up                    up
GigabitEthernet0/2     unassigned      YES unset  up                    up
Vlan1                  unassigned      YES unset  administratively down down
Vlan50                 192.168.0.11    YES manual up                    up
Sw-Core#
Sw-Core#
```

Ilustración 9. Configuración de la VLAN 50 en el Sw-Core

- **Sw1-Piso1**

```
Sw1-Piso1>enable
Password:
Sw1-Piso1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Sw1-Piso1(config)#vlan 50
Sw1-Piso1(config-vlan)#name Infraestructura
Sw1-Piso1(config-vlan)#exit
Sw1-Piso1(config)#
Sw1-Piso1(config)#interface vlan 50
Sw1-Piso1(config-if)#ip address 192.168.0.12 255.255.255.0
Sw1-Piso1(config-if)#no shutdown
Sw1-Piso1(config-if)#exit
Sw1-Piso1(config)#
Sw1-Piso1(config)#interface f0/1
Sw1-Piso1(config-if)#switchport mode access
Sw1-Piso1(config-if)#switchport access vlan 50
Sw1-Piso1(config-if)#no shutdown
Sw1-Piso1(config-if)#exit
Sw1-Piso1(config)#
Sw1-Piso1(config)#ip default-gateway 192.168.0.1
Sw1-Piso1(config)#exit
Sw1-Piso1#show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual up                    up
FastEthernet0/3        unassigned      YES manual up                    up
FastEthernet0/4        unassigned      YES manual up                    up
FastEthernet0/5        unassigned      YES manual up                    up
FastEthernet0/6        unassigned      YES manual up                    up
FastEthernet0/7        unassigned      YES manual up                    up
FastEthernet0/8        unassigned      YES manual up                    up
FastEthernet0/9        unassigned      YES manual up                    up
FastEthernet0/10       unassigned      YES manual up                    up
FastEthernet0/11       unassigned      YES manual up                    up
FastEthernet0/12       unassigned      YES manual up                    up
FastEthernet0/13       unassigned      YES manual up                    up
FastEthernet0/14       unassigned      YES manual up                    up
FastEthernet0/15       unassigned      YES manual up                    up
FastEthernet0/16       unassigned      YES manual up                    up
FastEthernet0/17       unassigned      YES manual up                    up
FastEthernet0/18       unassigned      YES manual up                    up
FastEthernet0/19       unassigned      YES manual up                    up
FastEthernet0/20       unassigned      YES manual up                    up
FastEthernet0/21       unassigned      YES manual up                    up
 --More--
%LINK-5-CHANGED: Interface Vlan50, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan50, changed state to up

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

FastEthernet0/22       unassigned      YES manual down                  down
FastEthernet0/23       unassigned      YES manual down                  down
FastEthernet0/24       unassigned      YES manual down                  down
GigabitEthernet0/1     unassigned      YES manual down                  down
GigabitEthernet0/2     unassigned      YES manual down                  down
Vlan1                  unassigned      YES manual administratively down down
Vlan50                 192.168.0.12    YES manual up                    up
Sw1-Piso1#
```

Ilustración 10. Configuración de la VLAN 50 en el Sw1-Piso 1

Las demás configuraciones de las otros Switch de acceso de cada uno de los pisos se hacen de forma similar, y se encuentran en el Anexo 6.

Asignación de VLAN en los switches de acceso

Una vez definidas las VLANs correspondientes a cada área funcional y sede descentralizada, se procedió a su creación manual en todos los switches de acceso de la sede central. Esta medida garantiza que, independientemente del punto de conexión física del usuario, el tráfico de red pueda ser correctamente etiquetado y direccionado conforme a su segmento lógico correspondiente. La sincronización de las VLANs en todos los dispositivos intermedios asegura la interoperabilidad entre segmentos de red y la correcta propagación de las tramas etiquetadas.

A continuación se muestran las configuraciones realizadas en el Sw-Core, para crear todas las VLAN:

- **Sw-Core**

```
Sw-Core#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Sw-Core(config)#vlan 2
Sw-Core(config-vlan)# name AdministracionTributaria
Sw-Core(config-vlan)#vlan 3
Sw-Core(config-vlan)# name ServiciosP_GestionA
Sw-Core(config-vlan)#vlan 4
Sw-Core(config-vlan)# name DesarrolloUrbano_Rural
Sw-Core(config-vlan)#vlan 5
Sw-Core(config-vlan)# name DesarrolloEconomico_Social
Sw-Core(config-vlan)#vlan 6
Sw-Core(config-vlan)# name ImagenInstitucional
Sw-Core(config-vlan)#vlan 7
Sw-Core(config-vlan)# name Informatica
Sw-Core(config-vlan)#vlan 8
Sw-Core(config-vlan)# name Alcaldia_Secretaria_Gerencia_Consej
Sw-Core(config-vlan)#vlan 9
Sw-Core(config-vlan)# name AsesoriaJuridica
Sw-Core(config-vlan)#vlan 10
Sw-Core(config-vlan)# name Administracion_Finanzas
Sw-Core(config-vlan)#vlan 11
Sw-Core(config-vlan)# name Planeamiento_Presupuesto
Sw-Core(config-vlan)#vlan 12
Sw-Core(config-vlan)# name AdministracionCiudadL
Sw-Core(config-vlan)#vlan 21
Sw-Core(config-vlan)# name MercadoNuevo
Sw-Core(config-vlan)#vlan 22
Sw-Core(config-vlan)# name PiscinaMunicipal
Sw-Core(config-vlan)#vlan 23
Sw-Core(config-vlan)# name EstadioMunicipal
Sw-Core(config-vlan)#vlan 24
Sw-Core(config-vlan)# name TerminalTerrestre
Sw-Core(config-vlan)#exit
Sw-Core(config)#exit
Sw-Core#copy running-config startup-config
Destination filename [startup-config]?
%SYS-5-CONFIG_I: Configured from console by console

Destination filename [startup-config]?
Building configuration...
[OK]
Sw-Core#show vlan brief
```

```
Sw-Core#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- ---------
-------------------------------
1    default                           active    Fa0/7, Fa0/8, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17,
Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21,
Fa0/22
                                                 Fa0/23, Fa0/24, Gig0/2
2    AdministracionTributaria          active
3    ServiciosP_GestionA               active
4    DesarrolloUrbano_Rural            active
5    DesarrolloEconomico_Social        active
6    ImagenInstitucional               active
7    Informatica                       active
8    Alcaldia_Secretaria_Gerencia_Consejo active
9    AsesoriaJuridica                  active
10   Administracion_Finanzas           active
11   Planeamiento_Presupuesto          active
12   AdministracionCiudadL             active
21   MercadoNuevo                      active
22   PiscinaMunicipal                  active
23   EstadioMunicipal                  active
24   TerminalTerrestre                 active
50   Infraestructura                   active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Sw-Core#
Sw-Core#
```

Ilustración 11. Configuración para crear las 16 VLAN en el Sw-Core

De manera similar, se hace la misma configuración para el resto de Switch que pertenecen a la cede central. Las configuraciones se muestran en el Anexo 7.

Configuración de subinterfaces en el router principal para enrutamiento entre VLANs

Para permitir la comunicación entre las diferentes VLANs creadas, se implementó una configuración basada en subinterfaces en el router principal, cada una correspondiente a una VLAN específica. A cada subinterfaz se le asignó una dirección IP perteneciente al rango de su subred asociada, actuando como puerta de enlace (default gateway) para los dispositivos finales de cada segmento. Esta arquitectura facilita el enrutamiento interno mediante la técnica denominada Router-on-a-Stick.

A continuación, se muestran las configuraciones que se realizaron para lograr este cometido:

- **R-Principal**

```
enable
configure terminal
interface g0/0.2
 encapsulation dot1Q 2
 ip address 192.168.1.1 255.255.255.192
 no shutdown
exit

interface g0/0.3
 encapsulation dot1Q 3
 ip address 192.168.1.65 255.255.255.192
 no shutdown
exit

interface g0/0.4
 encapsulation dot1Q 4
 ip address 192.168.1.129 255.255.255.192
 no shutdown
exit

interface g0/0.5
 encapsulation dot1Q 5
 ip address 192.168.1.193 255.255.255.192
 no shutdown
exit

interface g0/0.6
 encapsulation dot1Q 6
 ip address 192.168.2.1 255.255.255.192
 no shutdown
exit
```

```
interface g0/0.7
 encapsulation dot1Q 7
 ip address 192.168.2.65 255.255.255.192
 no shutdown
exit

interface g0/0.8
 encapsulation dot1Q 8
 ip address 192.168.2.129 255.255.255.192
 no shutdown
exit

interface g0/0.9
 encapsulation dot1Q 9
 ip address 192.168.2.193 255.255.255.192
 no shutdown
exit

interface g0/0.10
 encapsulation dot1Q 10
 ip address 192.168.3.1 255.255.255.192
 no shutdown
exit

interface g0/0.11
 encapsulation dot1Q 11
 ip address 192.168.3.65 255.255.255.192
 no shutdown
exit

interface g0/0.12
 encapsulation dot1Q 12
 ip address 192.168.3.129 255.255.255.192
 no shutdown
exit
```

```
interface g0/0.21
 encapsulation dot1Q 21
 ip address 192.168.3.193 255.255.255.192
 no shutdown
exit

interface g0/0.22
 encapsulation dot1Q 22
 ip address 192.168.4.1 255.255.255.192
 no shutdown
exit

interface g0/0.23
 encapsulation dot1Q 23
 ip address 192.168.4.65 255.255.255.192
 no shutdown
exit

interface g0/0.24
 encapsulation dot1Q 24
 ip address 192.168.4.129 255.255.255.192
 no shutdown
exit

exit
show ip interface brief
copy running-config startup-config
```

Asignación de VLANs a puertos de usuario (puertos de acceso)

Como siguiente paso, se procedió a la configuración de los puertos de acceso en cada switch de piso, vinculando cada puerto físico con la VLAN correspondiente a la función o área del usuario conectado. Este paso garantiza que el tráfico generado por los dispositivos finales sea etiquetado correctamente desde su origen, facilitando el control, la trazabilidad y la segmentación de la red.

A continuación, se presenta la configuración realizada para el Sw1-Piso1:

- **Sw1-Piso1:**

```
Sw1-Piso1>enable
Password:
Sw1-Piso1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Sw1-Piso1(config)#
Sw1-Piso1(config)#interface range fa0/2 - fa0/13
Sw1-Piso1(config-if-range)#switchport mode access
Sw1-Piso1(config-if-range)#switchport access vlan 2
Sw1-Piso1(config-if-range)#no shutdown
Sw1-Piso1(config-if-range)#exit
Sw1-Piso1(config)#
Sw1-Piso1(config)#interface range fa0/14 - fa0/23
Sw1-Piso1(config-if-range)#switchport mode access
Sw1-Piso1(config-if-range)#switchport access vlan 3
Sw1-Piso1(config-if-range)#no shutdown
Sw1-Piso1(config-if-range)#exit
Sw1-Piso1(config)#end
Sw1-Piso1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- ---------
-------------------------------
1    default                           active    Fa0/24, Gig0/1, Gig0/2
2    AdministracionTributaria          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12,

Fa0/13
3    ServiciosP_GestionA               active    Fa0/14, Fa0/15, Fa0/16,
Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20,
Fa0/21
                                                 Fa0/22, Fa0/23
4    DesarrolloUrbano_Rural            active
5    DesarrolloEconomico_Social        active
6    ImagenInstitucional               active
7    Informatica                       active
8    Alcaldia_Secretaria_Gerencia_Consejo active
9    AsesoriaJuridica                  active
10   Administracion_Finanzas           active
11   Planeamiento_Presupuesto          active
12   AdministracionCiudadL             active
21   MercadoNuevo                      active
22   PiscinaMunicipal                  active
23   EstadioMunicipal                  active
 --More--
%SYS-5-CONFIG_I: Configured from console by console

24   TerminalTerrestre                 active
50   Infraestructura                   active
```

Ilustración 12. Asignación de VLANs a puertos de usuario (puertos de acceso) en el Sw1-Piso1

De esta manera se configuran todos los Switch restantes pertenecientes a la cede principal. Estas configuraciones se encuentran en el Anexo 8.

- **Configuración de DHCP y asignación de direcciones IP a dispositivos finales**

Asignación de direcciones IP estáticas a los servidores

Los servidores y demás dispositivos críticos de la infraestructura fueron configurados con direcciones IP estáticas, dentro de los rangos definidos por las subredes /26 correspondientes a sus respectivas VLANs. Esta medida responde a la necesidad de asegurar la disponibilidad permanente y la estabilidad en los servicios ofrecidos, así como a facilitar su identificación dentro del esquema de red. Además, se reservaron explícitamente estas direcciones fuera de los rangos asignados al servicio DHCP para evitar conflictos.

A continuación, se muestra la configuración de los 3 servidores, cuya dirección de IP se ingresó de forma estática:

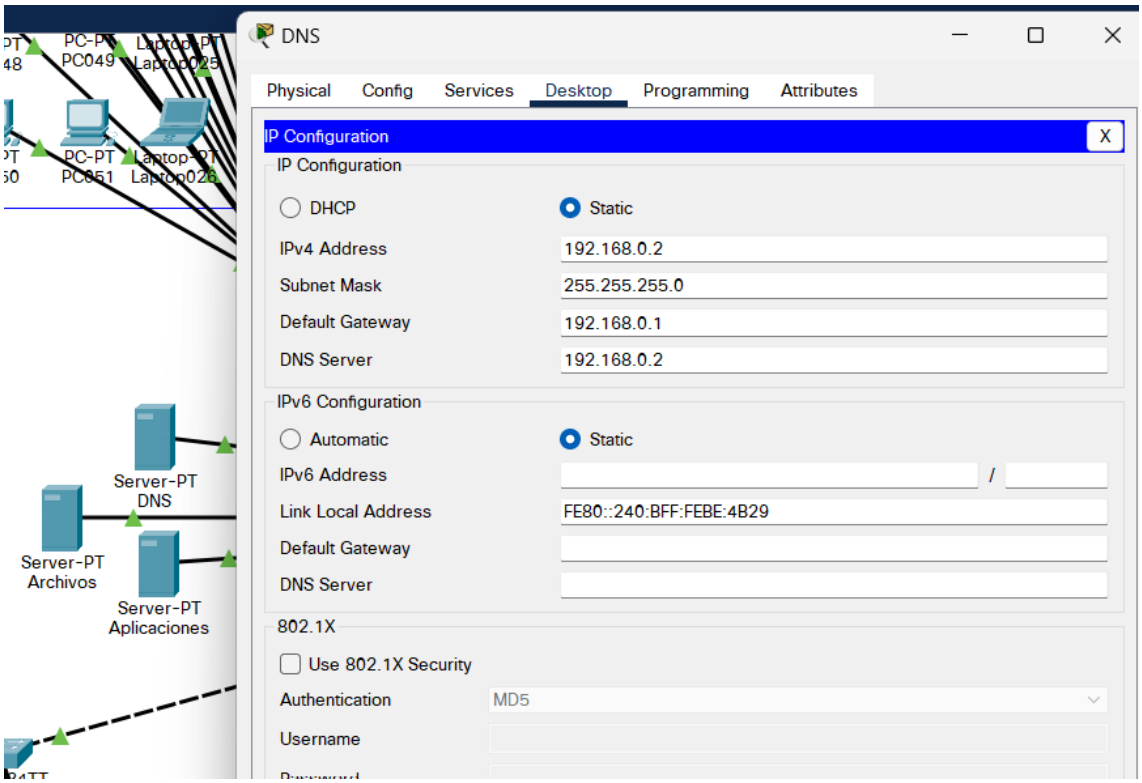


Ilustración 13. Asignación de IP estática al servidor DNS

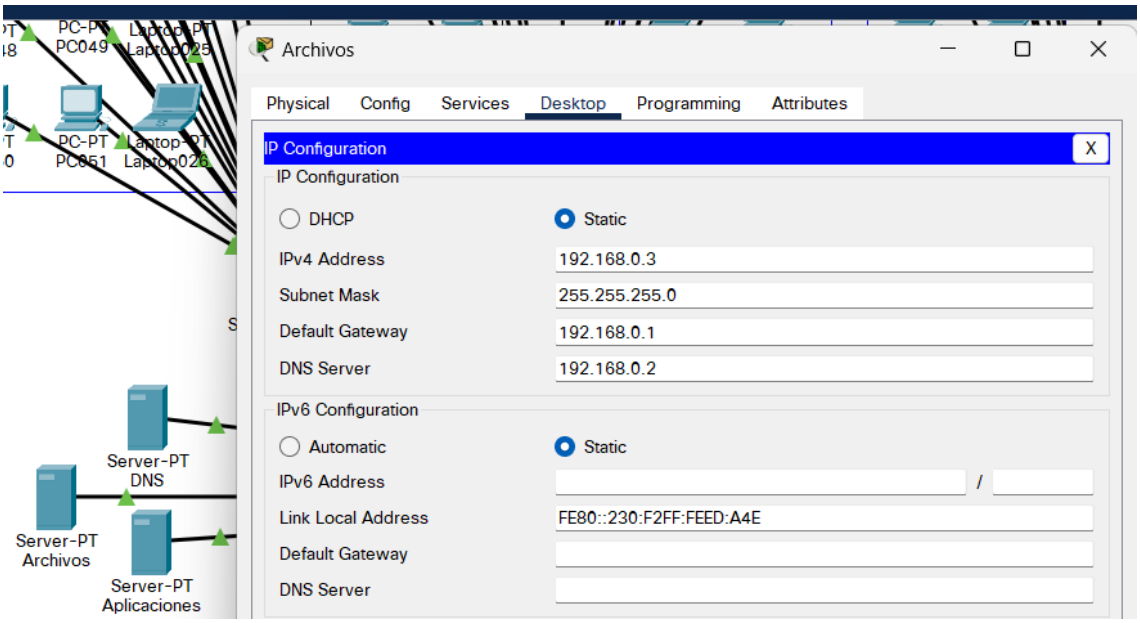


Ilustración 14. Asignación de IP estática al servidor de archivos

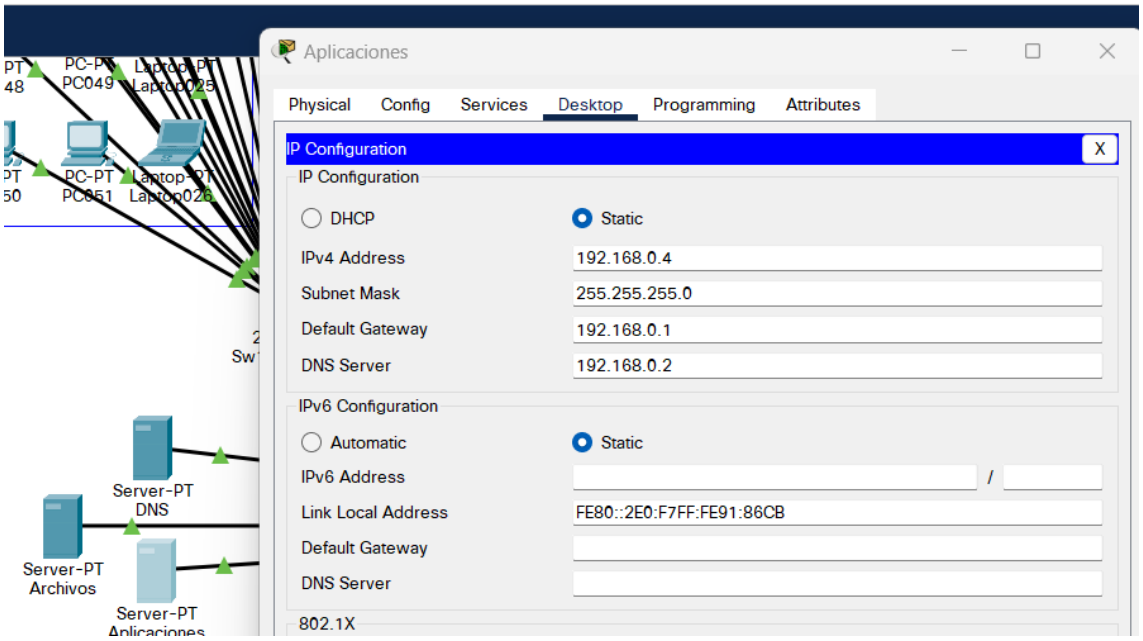


Ilustración 15. Asignación de IP estática al servidor de aplicaciones

Asignación dinámica de direcciones IP por VLAN

Para los dispositivos finales de usuario, pc, laptops, entre otros, se habilitó el servicio DHCP (Dynamic Host Configuration Protocol) desde el router principal. Este servicio permite que los equipos obtengan de forma automática y eficiente una dirección IP válida, junto con los parámetros esenciales de configuración (máscara de subred, puerta de enlace predeterminada y servidores DNS), en función de la VLAN a la que estén conectados.

Cada VLAN cuenta con un **pool de direcciones IP dinámicas** configurado dentro de su respectiva subred /26, lo que garantiza una distribución lógica, ordenada y sin superposición de direcciones. A continuación, se muestran dichas configuraciones en el router principal, incluyendo la exclusión de IP que no deben ser asignadas de forma automática, por motivos de seguridad para que la red funcione sin conflictos de IP.

- **R-Principal**

```
R-Principal>enable
Password:
Password:
R-Principal#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R-Principal(config)#ip dhcp excluded-address 192.168.0.1 192.168.0.50
R-Principal(config)#
R-Principal(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
R-Principal(config)#ip dhcp excluded-address 192.168.1.65 192.168.1.74
R-Principal(config)#ip dhcp excluded-address 192.168.1.129 192.168.1.138
R-Principal(config)#ip dhcp excluded-address 192.168.1.193 192.168.1.202
R-Principal(config)#ip dhcp excluded-address 192.168.2.1 192.168.2.10
R-Principal(config)#ip dhcp excluded-address 192.168.2.65 192.168.2.74
R-Principal(config)#ip dhcp excluded-address 192.168.2.129 192.168.2.138
R-Principal(config)#ip dhcp excluded-address 192.168.2.193 192.168.2.202
R-Principal(config)#ip dhcp excluded-address 192.168.3.1 192.168.3.10
R-Principal(config)#ip dhcp excluded-address 192.168.3.65 192.168.3.74
R-Principal(config)#ip dhcp excluded-address 192.168.3.129 192.168.3.138
R-Principal(config)#ip dhcp excluded-address 192.168.3.193 192.168.3.202
R-Principal(config)#ip dhcp excluded-address 192.168.4.1 192.168.4.10
R-Principal(config)#ip dhcp excluded-address 192.168.4.65 192.168.4.74
R-Principal(config)#ip dhcp excluded-address 192.168.4.129 192.168.4.138
R-Principal(config)#
```

Ilustración 16. Exclusión de IP que no se deben asignar por medio de DHCP

La configuración realizada se muestra también en el anexo 9. Así mismo las configuraciones que se mostrarán a continuación correspondientes a la asignación de IP de forma automática por medio de DHCP, también se encuentran en el anexo 10.

- **R-Principal**

```
R-Principal(config)#
R-Principal(config)#ip dhcp pool VLAN2
R-Principal(dhcp-config)# network 192.168.1.0 255.255.255.192
R-Principal(dhcp-config)# default-router 192.168.1.1
R-Principal(dhcp-config)# dns-server 192.168.0.2
R-Principal(dhcp-config)#exit
R-Principal(config)#
R-Principal(config)#ip dhcp pool VLAN3
R-Principal(dhcp-config)# network 192.168.1.64 255.255.255.192
R-Principal(dhcp-config)# default-router 192.168.1.65
R-Principal(dhcp-config)# dns-server 192.168.0.2
R-Principal(dhcp-config)#exit
R-Principal(config)#
R-Principal(config)#ip dhcp pool VLAN4
R-Principal(dhcp-config)# network 192.168.1.128 255.255.255.192
R-Principal(dhcp-config)# default-router 192.168.1.129
R-Principal(dhcp-config)# dns-server 192.168.0.2
R-Principal(dhcp-config)#exit
R-Principal(config)#
R-Principal(config)#ip dhcp pool VLAN5
R-Principal(dhcp-config)# network 192.168.1.192 255.255.255.192
R-Principal(dhcp-config)# default-router 192.168.1.193
R-Principal(dhcp-config)# dns-server 192.168.0.2
R-Principal(dhcp-config)#exit
R-Principal(config)#
R-Principal(config)#ip dhcp pool VLAN6
R-Principal(dhcp-config)# network 192.168.2.0 255.255.255.192
R-Principal(dhcp-config)# default-router 192.168.2.1
R-Principal(dhcp-config)# dns-server 192.168.0.2
R-Principal(dhcp-config)#exit
R-Principal(config)#
R-Principal(config)#ip dhcp pool VLAN7
R-Principal(dhcp-config)# network 192.168.2.64 255.255.255.192
R-Principal(dhcp-config)# default-router 192.168.2.65
R-Principal(dhcp-config)# dns-server 192.168.0.2
R-Principal(dhcp-config)#exit
R-Principal(config)#
R-Principal(config)#ip dhcp pool VLAN8
R-Principal(dhcp-config)# network 192.168.2.128 255.255.255.192
R-Principal(dhcp-config)# default-router 192.168.2.129
R-Principal(dhcp-config)# dns-server 192.168.0.2
R-Principal(dhcp-config)#exit
R-Principal(config)#
R-Principal(config)#ip dhcp pool VLAN9
R-Principal(dhcp-config)# network 192.168.2.192 255.255.255.192
R-Principal(dhcp-config)# default-router 192.168.2.193
R-Principal(dhcp-config)# dns-server 192.168.0.2
R-Principal(dhcp-config)#exit
R-Principal(config)#
R-Principal(config)#ip dhcp pool VLAN10
```

```
R-Principal(config)#
R-Principal(config)#ip dhcp pool VLAN10
R-Principal(dhcp-config)# network 192.168.3.0 255.255.255.192
R-Principal(dhcp-config)# default-router 192.168.3.1
R-Principal(dhcp-config)# dns-server 192.168.0.2
R-Principal(dhcp-config)#exit
R-Principal(config)#
R-Principal(config)#ip dhcp pool VLAN11
R-Principal(dhcp-config)# network 192.168.3.64 255.255.255.192
R-Principal(dhcp-config)# default-router 192.168.3.65
R-Principal(dhcp-config)# dns-server 192.168.0.2
R-Principal(dhcp-config)#exit
R-Principal(config)#
R-Principal(config)#ip dhcp pool VLAN12
R-Principal(dhcp-config)# network 192.168.3.128 255.255.255.192
R-Principal(dhcp-config)# default-router 192.168.3.129
R-Principal(dhcp-config)# dns-server 192.168.0.2
R-Principal(dhcp-config)#exit
R-Principal(config)#
R-Principal(config)#! Sede remota (opcional, si usas VLAN21 por ejemplo)
R-Principal(config)#ip dhcp pool VLAN21
R-Principal(dhcp-config)# network 192.168.3.192 255.255.255.192
R-Principal(dhcp-config)# default-router 192.168.3.193
R-Principal(dhcp-config)# dns-server 192.168.0.2
R-Principal(dhcp-config)#exit
R-Principal(config)#
```

Ilustración 17. Configuración del servicio DHCP en el router principal

Validación del direccionamiento automático

Finalmente, se realizó una validación empírica de la correcta asignación automática de direcciones IP, observando cómo los dispositivos conectados a los puertos de acceso obtenían de forma dinámica su configuración de red, conforme a su pertenencia a una VLAN determinada. A continuación, se muestran PC de diferentes VLAN en las que se observa la asignación de IP de forma automática.

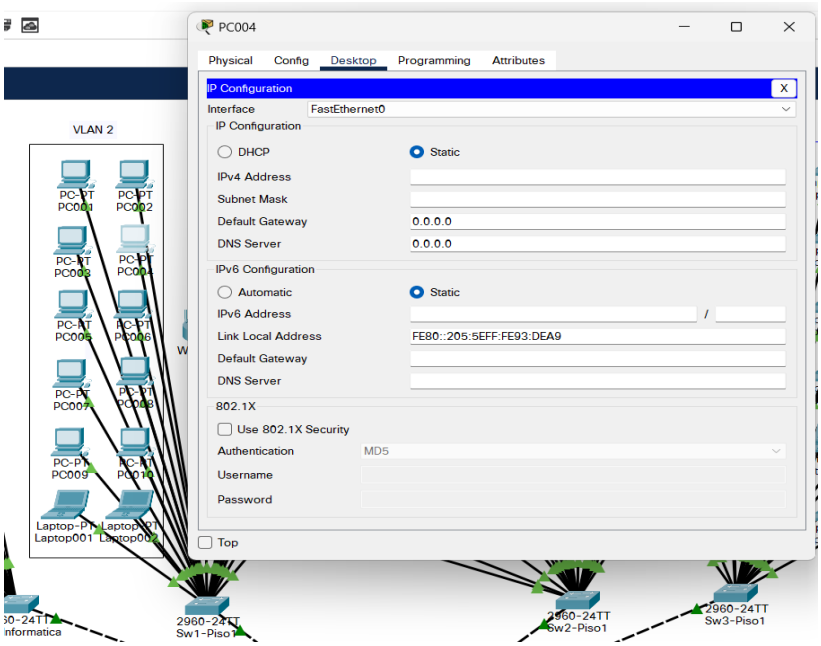


Ilustración 18. Interfaz de IP de forma estática en la PC004, correspondiente a la VLAN 2

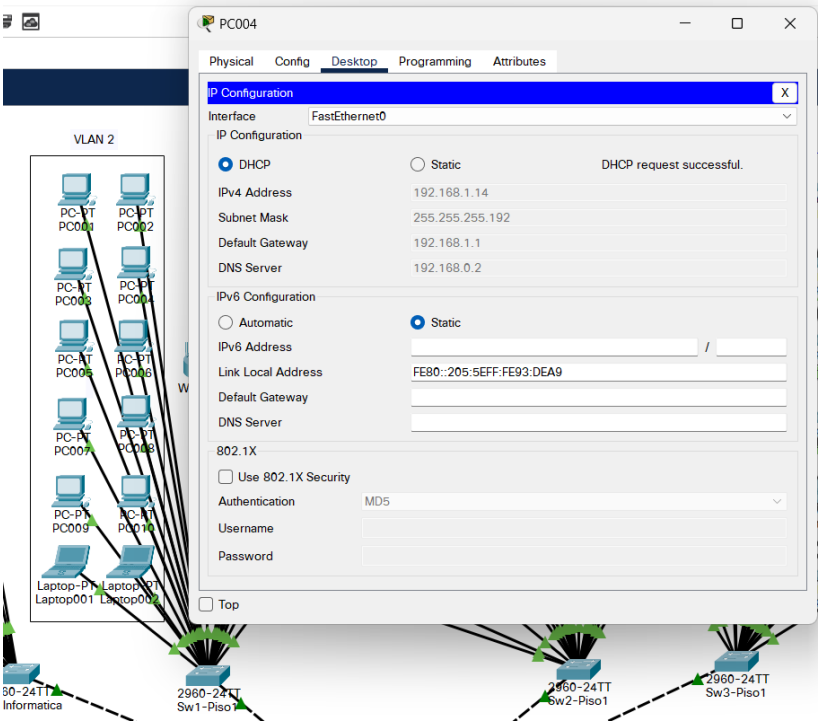


Ilustración 19. Asignación de IP por medio de DHCP a la PC004, correspondiente a la VLAN 2

Prueba con una segunda pc005 de la misma VLAN

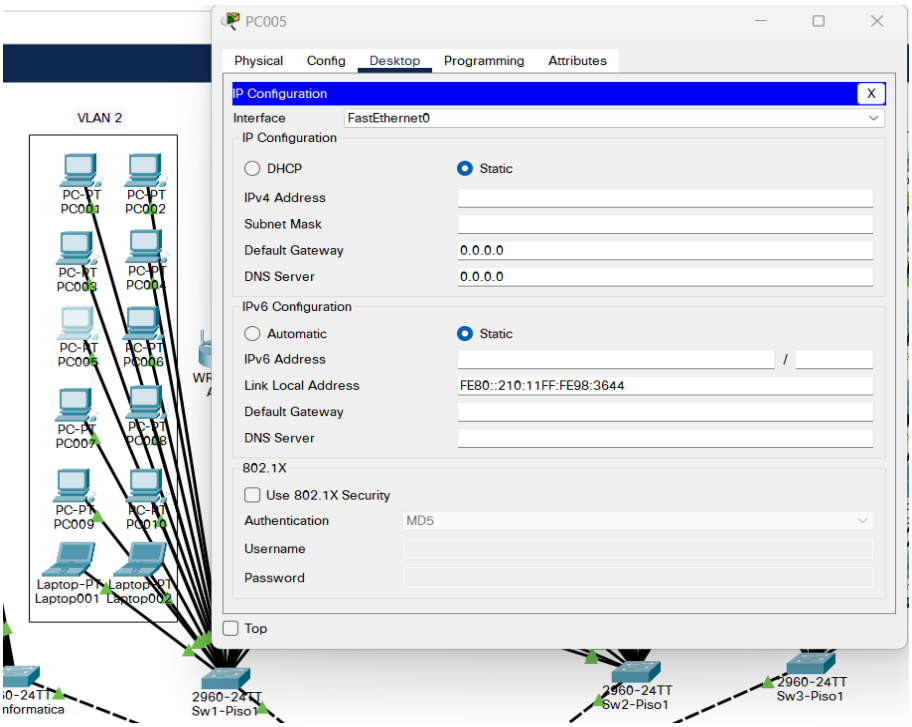


Ilustración 20. Interfaz de IP de forma estática en la PC005, correspondiente a la VLAN 2

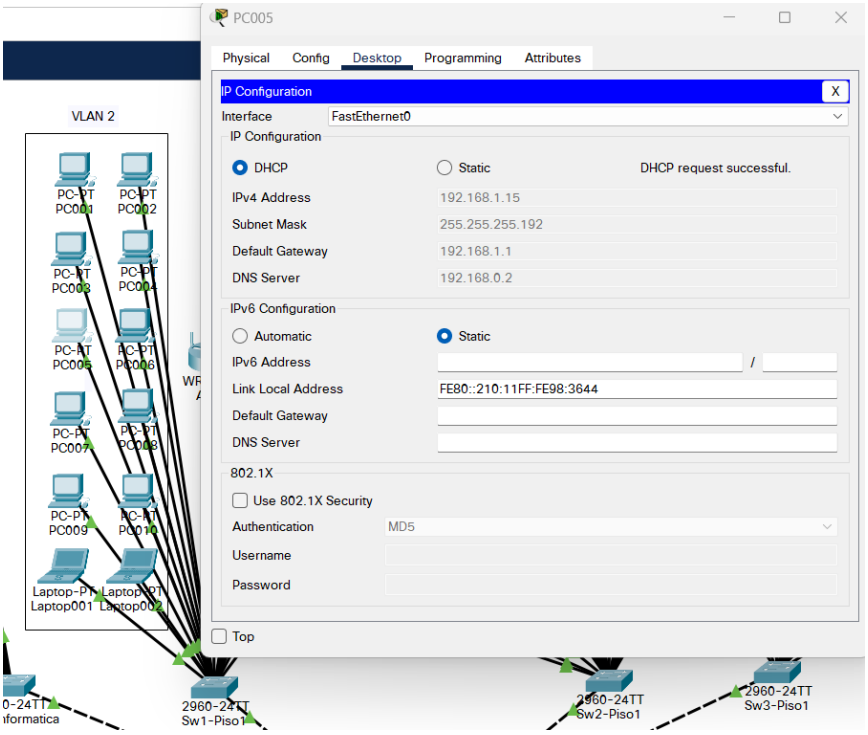


Ilustración 21. Asignación de IP por medio de DHCP a la PC005, correspondiente a la VLAN 2

Se probó con una VLAN diferente, con la VLAN 3, y se corroboró que la configuración estaba correcta.

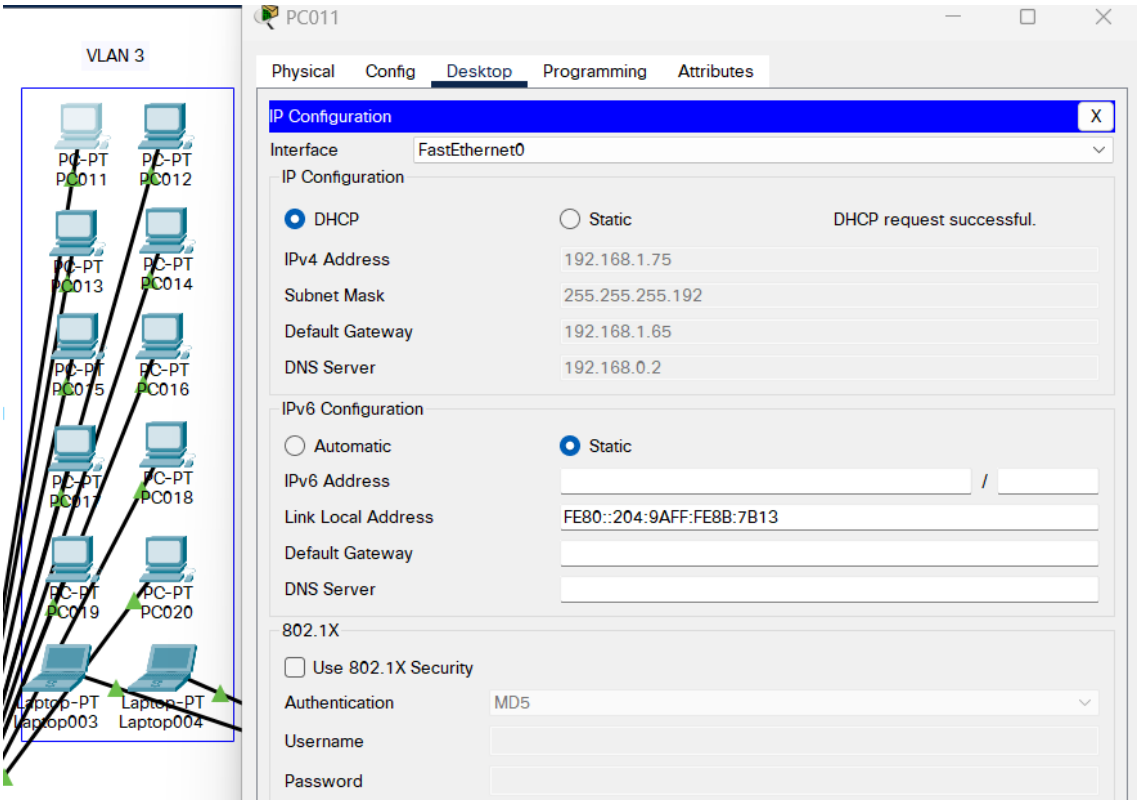


Ilustración 22. Asignación de IP por medio de DHCP a la PC011, correspondiente a la VLAN 3

- **Configuración de red en las sedes descentralizadas**

A diferencia de la sede central, las configuraciones de red realizadas en las sedes descentralizadas requirieron de una serie de consideraciones específicas, debido a la necesidad de establecer conectividad remota con el router principal mediante enlaces WAN y mantener la segmentación interna a través de VLANs locales. A continuación, se describen las etapas fundamentales que fueron desarrolladas para garantizar la integración eficiente y segura de estas sedes con el núcleo de la red institucional.

Configuración de enlaces seriales entre el router principal y los routers remotos

Con el objetivo de establecer una comunicación punto a punto entre la sede central y cada una de las sedes descentralizadas, se configuraron enlaces seriales que permiten el intercambio de datos mediante interfaces WAN. Para ello, se asignaron direcciones IP específicas a cada extremo del enlace y se establecieron parámetros apropiados de encapsulamiento.

Para realizar la configuración mencionada, se tuvo en cuenta que cada enlace serial necesita una IP en una red punto a punto diferente, por lo que se usó subredes pequeñas /30 para optimizar el direccionamiento, obteniendo las siguientes direcciones ip para cada router:

Enlace	Subred	IP Router Principal	IP Router Remoto
Sede 1 - Mercado	192.168.10.0/30	192.168.10.1	192.168.10.2
Sede 2 - Piscina	192.168.10.4/30	192.168.10.5	192.168.10.6
Sede 3 - Estadio	192.168.10.8/30	192.168.10.9	192.168.10.10
Sede 4 - Terminal	192.168.10.12/30	192.168.10.13	192.168.10.14

Tabla 22Direcciones IP para el enlace punto a punto

Con las IP ya definidas, se realizó la configuración de enlaces seriales entre el router principal y los routers remotos, tal como se muestra a continuación:

- **R-Principal**

```
enable
configure terminal

interface serial0/0/0
```

ip address 192.168.10.1 255.255.255.252
clock rate 64000
no shutdown

interface serial0/0/1
ip address 192.168.10.5 255.255.255.252
clock rate 64000
no shutdown

interface serial0/1/0
ip address 192.168.10.9 255.255.255.252
clock rate 64000
no shutdown

interface serial0/1/1
ip address 192.168.10.13 255.255.255.252
clock rate 64000
no shutdown
exit

- **R-MercadoNuevo**
  enable
  configure terminal

  interface serial0/0/0
  ip address 192.168.10.2 255.255.255.252
  no shutdown
  exit
- **R-PiscinaPrincipal**
  enable
  configure terminal

  interface serial0/0/0
  ip address 192.168.10.6 255.255.255.252
  no shutdown
  exit

- **R-EstadioMunicipal**
  enable
  configure terminal

  interface serial0/0/0
  ip address 192.168.10.10 255.255.255.252
  no shutdown
  exit

- **R-TerminalTerrestre**
  enable
  configure terminal

  interface serial0/0/0

ip address 192.168.10.14 255.255.255.252
no shutdown
exit

Configuración de direccionamiento interno en cada sede descentralizada

- **R-MercadoNuevo**
  enable
  configure terminal
  interface f0/0
  no shutdown
  ip address 192.168.3.193 255.255.255.192

  exit

- **R-PiscinaPrincipal**
  enable
  configure terminal
  interface f0/0
  no shutdown
  ip address 192.168.4.1 255.255.255.192

  exit

- **R-EstadioMunicipal**
  enable
  configure terminal
  interface f0/0
  no shutdown
  ip address 192.168.4.65 255.255.255.192
  exit

- **R-TerminalTerrestre**
  enable
  configure terminal
  interface f0/0
  no shutdown
  ip address 192.168.4.129 255.255.255.192
  exit

Configuración de enrutamiento dinámico mediante RIP v2

A fin de facilitar el intercambio de información de enrutamiento entre la sede central y las sedes remotas, se implementó el protocolo RIP versión 2 (Routing Information Protocol), el cual permite anunciar las rutas disponibles de forma dinámica. Se seleccionó RIP v2 por su simplicidad de implementación en topologías de tamaño moderado y su compatibilidad con redes de esta magnitud. Esto es clave para que las redes de todas las sedes se conozcan entre sí y puedan comunicarse; a continuación, se muestran las configuraciones realizadas:

- **R-Principal**

```
enable
configure terminal

router rip
version 2
no auto-summary
network 192.168.0.0
network 192.168.1.0
network 192.168.2.0
network 192.168.3.0
network 192.168.4.0
exit
```

- **R-MercadoNuevo**

```
enable
configure terminal

router rip
version 2
no auto-summary
network 192.168.3.192
network 192.168.10.0

exit
```

- **R-PiscinaPrincipal**

```
enable
configure terminal

router rip
version 2
no auto-summary
network 192.168.4.0
network 192.168.10.0

exit
```

- **R-EstadioMunicipal**
  enable
  configure terminal

  router rip
  version 2
  no auto-summary
  network 192.168.4.64
  network 192.168.10.0

  exit

- **R-TerminalTerrestre**
  enable
  configure terminal

  router rip
  version 2
  no auto-summary
  network 192.168.4.128
  network 192.168.10.0

  exit

Configuración complementaria de rutas estáticas

Además del enrutamiento dinámico, se definieron rutas estáticas específicas para ciertos segmentos de red con el objetivo de reforzar la seguridad, reducir la dependencia de actualizaciones dinámicas, y optimizar la salida hacia determinados destinos de red. Esta estrategia híbrida mejora la eficiencia del tráfico en enlaces WAN y garantiza mayor control del flujo de datos. Las configuraciones realizadas son las siguientes:

- **R-Principal**
  enable
  configure terminal

  ip route 192.168.3.192 255.255.255.192 192.168.10.2
  ip route 192.168.4.0 255.255.255.192 192.168.10.6
  ip route 192.168.4.64 255.255.255.192 192.168.10.10
  ip route 192.168.4.128 255.255.255.192 192.168.10.14
  end

- **R-MercadoNuevo**
  enable
  configure terminal
  ip route 192.168.0.0 255.255.255.0 192.168.10.1
  exit

- **R-PiscinaPrincipal**
  enable
  configure terminal
  ip route 192.168.0.0 255.255.255.0 192.168.10.5
  exit

- **R-EstadioMunicipal**
  enable
  configure terminal
  ip route 192.168.0.0 255.255.255.0 192.168.10.9
  exit

- **R-TerminalTerrestre**
  enable
  configure terminal
  ip route 192.168.0.0 255.255.255.0 192.168.10.13
  exit

Configuración de VLAN en los switches de las sedes descentralizadas

En cada sede remota se implementó una estructura de VLAN local, replicando el enfoque segmentado de la sede central, aunque con un menor número de subredes dado el volumen reducido de usuarios. Las VLAN fueron definidas y asignadas a los puertos de acceso (access ports) en los switches de cada sede, lo que garantiza aislamiento lógico del tráfico y mejora el control administrativo de la red. A continuación, se muestran las configuraciones realizadas:

- **Sw1-Mercado**
  enable
  configure terminal
  interface vlan 21
  ip address 192.168.3.194 255.255.255.192
  no shutdown
  exit

  ip default-gateway 192.168.3.193

  interface fastEthernet0/1
  switchport mode access
  switchport access vlan 21

  exit

  interface range fa0/2 - fa0/23
  switchport mode access
  switchport access vlan 21
  no shutdown
  exit

- **Sw1-Piscina**

```
enable
configure terminal
interface vlan 22
ip address 192.168.4.2 255.255.255.192
no shutdown
exit

ip default-gateway 192.168.4.1

interface fastEthernet0/1
switchport mode access
switchport access vlan 22
exit

interface range fa0/2 - fa0/23
switchport mode access
switchport access vlan 22
no shutdown
exit
```

- **Sw1-Estadio**

```
enable
configure terminal
interface vlan 23
ip address 192.168.4.66 255.255.255.192
no shutdown
exit

ip default-gateway 192.168.4.65

interface fastEthernet0/1
switchport mode access
switchport access vlan 23
exit

interface range fa0/2 - fa0/23
switchport mode access
switchport access vlan 23
no shutdown
exit
```

- **Sw1-Terminal**

```
enable
configure terminal
interface vlan 24
ip address 192.168.4.130 255.255.255.192
no shutdown
exit
```

```
ip default-gateway 192.168.4.129

interface fastEthernet0/1
switchport mode access
switchport access vlan 24
exit

interface range fa0/2 - fa0/23
switchport mode access
switchport access vlan 24
no shutdown

exit
```

Asignación automática de direcciones IP mediante DHCP

En cada sede descentralizada, el router local fue configurado como servidor DHCP para distribuir direcciones IP automáticamente a los dispositivos finales conectados a las VLAN respectivas. Esta estrategia minimiza errores de configuración, acelera la puesta en marcha y permite una administración eficiente del direccionamiento en redes remotas. Las configuraciones realizadas se muestran a continuación:

- **R-MercadoNuevo**

```
enable
configure terminal
ip dhcp pool VLAN21
network 192.168.3.192 255.255.255.192
default-router 192.168.3.193
dns-server 192.168.0.2
exit

ip dhcp excluded-address 192.168.3.193 192.168.3.195
```

- **R-PiscinaPrincipal**

```
enable
configure terminal
ip dhcp pool VLAN22
network 192.168.4.0 255.255.255.192
default-router 192.168.4.1
dns-server 192.168.0.2
exit

ip dhcp excluded-address 192.168.4.1 192.168.4.10
```

- **R-EstadioMunicipal**

```
enable
configure terminal
ip dhcp pool VLAN23
```

network 192.168.4.64 255.255.255.192
default-router 192.168.4.65
dns-server 192.168.0.2
exit

ip dhcp excluded-address 192.168.4.65 192.168.4.74

- **R-TerminalTerrestre**
  enable
  configure terminal
  ip dhcp pool VLAN24
  network 192.168.4.128 255.255.255.192
  default-router 192.168.4.129
  dns-server 192.168.0.2
  exit

  ip dhcp excluded-address 192.168.4.129 192.168.4.138

Verificación de asignación automática de direcciones IP en dispositivos finales

Como validación del correcto funcionamiento del DHCP, se verificó la asignación automática de direcciones IP a los dispositivos finales en cada sede descentralizada, comprobando que se recibieran los parámetros de red correspondientes (dirección IP, máscara de subred, puerta de enlace y DNS) de acuerdo a su VLAN asignada. A continuación, se muestran imágenes en la que se corrobora lo mencionado.

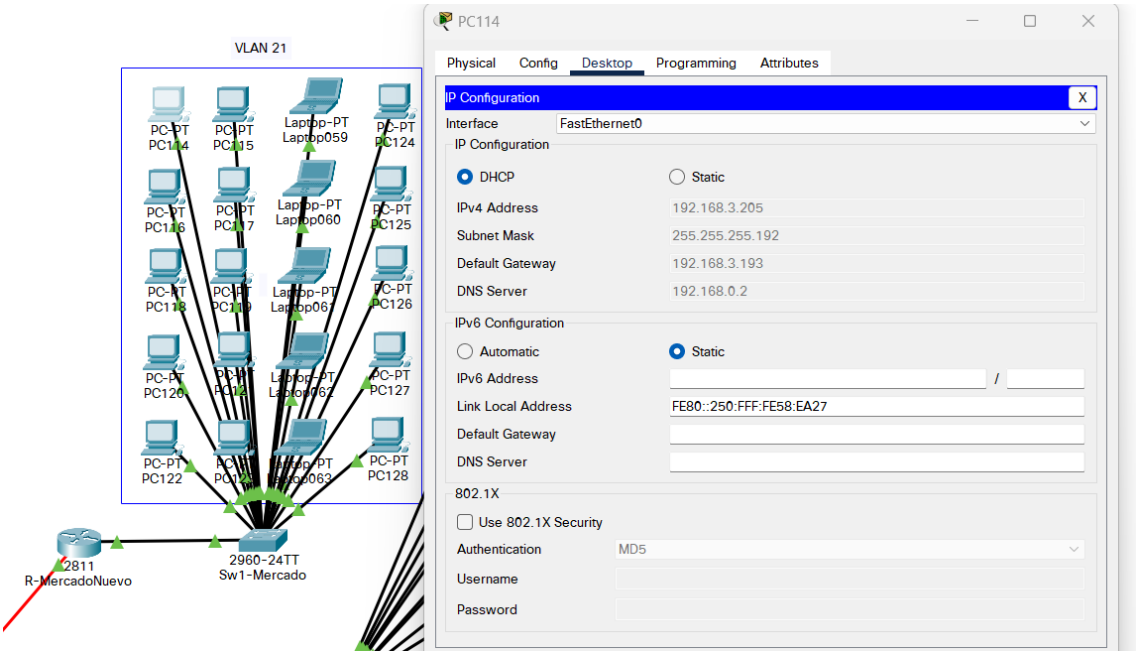


Ilustración 23. Asignación de IP por medio de DHCP a la PC114, correspondiente a la VLAN 21

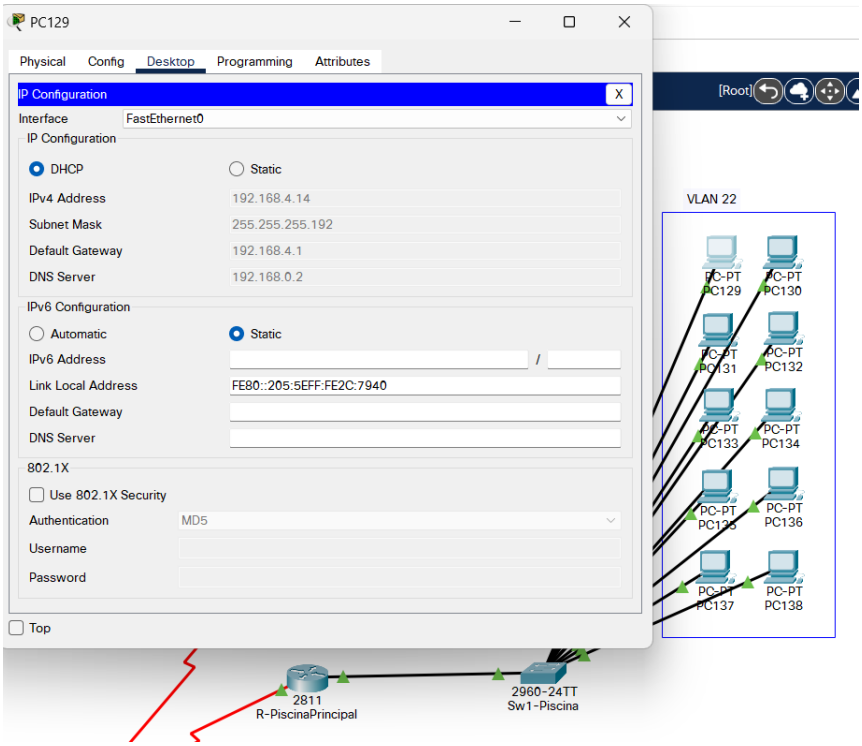


Ilustración 25. Asignación de IP por medio de DHCP a la PC129, correspondiente a la VLAN 22

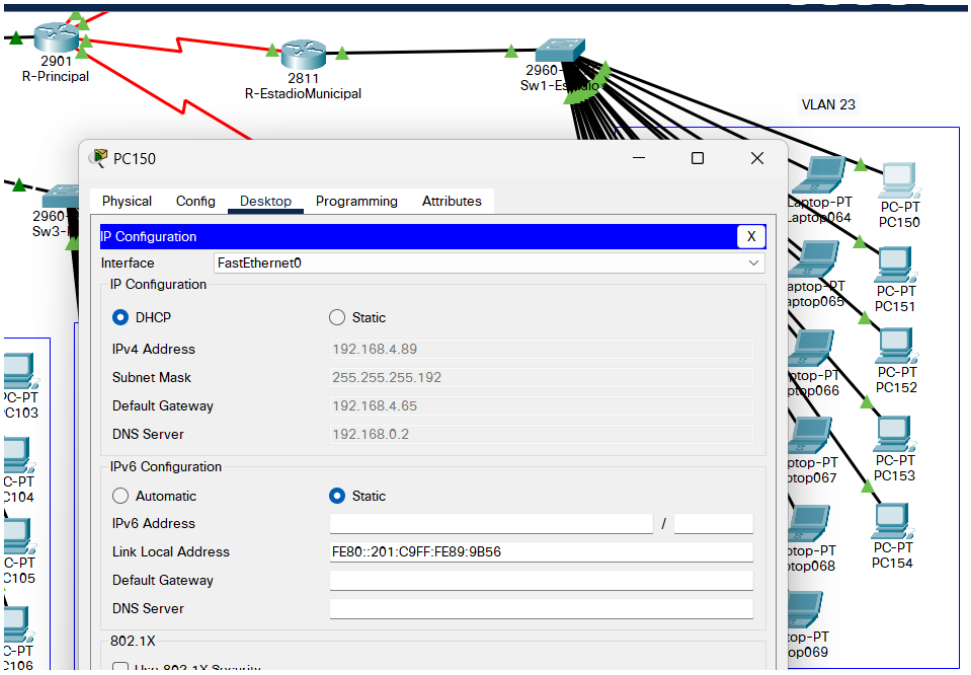


Ilustración 24. Asignación de IP por medio de DHCP a la PC150, correspondiente a la VLAN 23

III.4 Simulación de la red diseñada

Como parte del proceso de validación del diseño lógico y físico de la infraestructura de red, se procedió con la simulación de los distintos componentes que integran el sistema de comunicaciones institucional. Esta fase tiene como finalidad verificar la conectividad entre los dispositivos finales y de red, así como comprobar el correcto direccionamiento y enrutamiento configurado previamente.

Para efectuar una simulación precisa y ordenada, es imprescindible contar con claridad sobre la distribución de las direcciones IP asignadas a los diferentes dispositivos, agrupados según la VLAN a la que pertenecen. Esta información permite realizar pruebas de conectividad, como el envío de paquetes ICMP (ping), para confirmar la accesibilidad de los dispositivos entre sí.

A continuación, se muestra la tabla de Dirección IP de los equipos según la VLAN a la que pertenezcan, la cual presenta, de forma consolidada, los rangos de subred, gateways, y direcciones IP asignadas a los dispositivos de red y equipos terminales, tanto en la sede principal como en las cuatro sedes descentralizadas:

VLAN ID	Área	Ubicación	Subred	Gateway	Equipos	Dirección IP
50	Infraestructura (Core, Router principal, Servidores)	Segundo piso (TI)	192.168.0.0/24	192.168.0.1	R-Principal	192.168.0.1
					Servidor DNS	192.168.0.2
					Servidor de archivos	192.168.0.3
					Servidor de aplicaciones	192.168.0.4
					Sw-Core	192.168.0.11
2	Administración Tributaria	Primer piso	192.168.1.0/26	192.168.1.1	Pc y laptop	192.168.1.11 – 192.168.1.62
3	Servicios Públicos y Gestión Ambiental	Primer piso	192.168.1.64/26	192.168.1.65	Pc y laptop	192.168.1.75 – 192.168.1.126
4	Desarrollo Urbano y Rural	Primer piso	192.168.1.128/26	192.168.1.129	Pc y laptop	192.168.1.139 – 192.168.1.190
5	Desarrollo Económico y Social	Primer piso	192.168.1.192/26	192.168.1.193	Pc y laptop	192.168.1.203 – 192.168.1.254
6	Imagen Institucional	Primer piso	192.168.2.0/26	192.168.2.1	Pc y laptop	192.168.2.11 – 192.168.2.62

7	Informática	Segundo piso	192.168.2.64/26	192.168.2.65	Pc y laptop	192.168.2.75 – 192.168.2.126
8	Alcaldía / Secretaría / Gerencia / Concejo	Segundo piso	192.168.2.128/26	192.168.2.129	Pc y laptop	192.168.2.139 – 192.168.2.190
9	Asesoría Jurídica	Segundo piso	192.168.2.192/26	192.168.2.193	Pc y laptop	192.168.2.203 – 192.168.2.254
10	Administración y Finanzas	Tercer piso	192.168.3.0/26	192.168.3.1	Pc y laptop	192.168.3.11 – 192.168.3.62
11	Planeamiento y Presupuesto	Tercer piso	192.168.3.64/26	192.168.3.65	Pc y laptop	192.168.3.75 – 192.168.3.126
12	Administración Ciudad A.B. Leguía	Tercer piso	192.168.3.128/26	192.168.3.129	Pc y laptop	192.168.3.139 – 192.168.3.190
21	Mercado Nuevo	Sede 1	192.168.3.192/26	192.168.3.193	R-Mercado	192.168.3.193
					Sw-Mercado	192.168.3.194
					Pc y laptop	192.168.3.203 – 192.168.3.254
22	Piscina Municipal	Sede 2	192.168.4.0/26	192.168.4.1	R-Piscina	192.168.4.1
					Sw-Piscina	192.168.4.2
					Pc y laptop	192.168.4.11 – 192.168.4.62
23	Estadio Municipal	Sede 3	192.168.4.64/26	192.168.4.65	R-Estadio	192.168.4.65
					Sw-Estadio	192.168.4.66
					Pc y laptop	192.168.4.75 – 192.168.4.126
24	Terminal Terrestre	Sede 4	192.168.4.128/26	192.168.4.129	R-Terminal	192.168.4.129
					Sw-Terminal	192.168.4.130
					Pc y laptop	192.168.4.129 – 192.168.4.190

Tabla 23Dirección IP de los equipos según la VLAN a la que pertenezcan

Una vez identificada la asignación de direcciones IP en toda la topología, se procedió a simular las comunicaciones internas. El proceso de simulación inició en la sede principal, abarcando

3 las VLAN al azar de las 12 existentes. Desde una estación de trabajo (PC) perteneciente a una de estas 3 VLAN, se realizaron pruebas de conectividad (ping) hacia los siguientes dispositivos clave: el gateway de su subred respectiva, el router principal, los tres servidores (DNS, de archivos y de aplicaciones), y el switch central (Sw-Core). A continuación, se muestran las interfaces de los dispositivos finales como parte de la simulación, realizando las pruebas de conectividad mencionadas:

- **PC002-VLAN2**

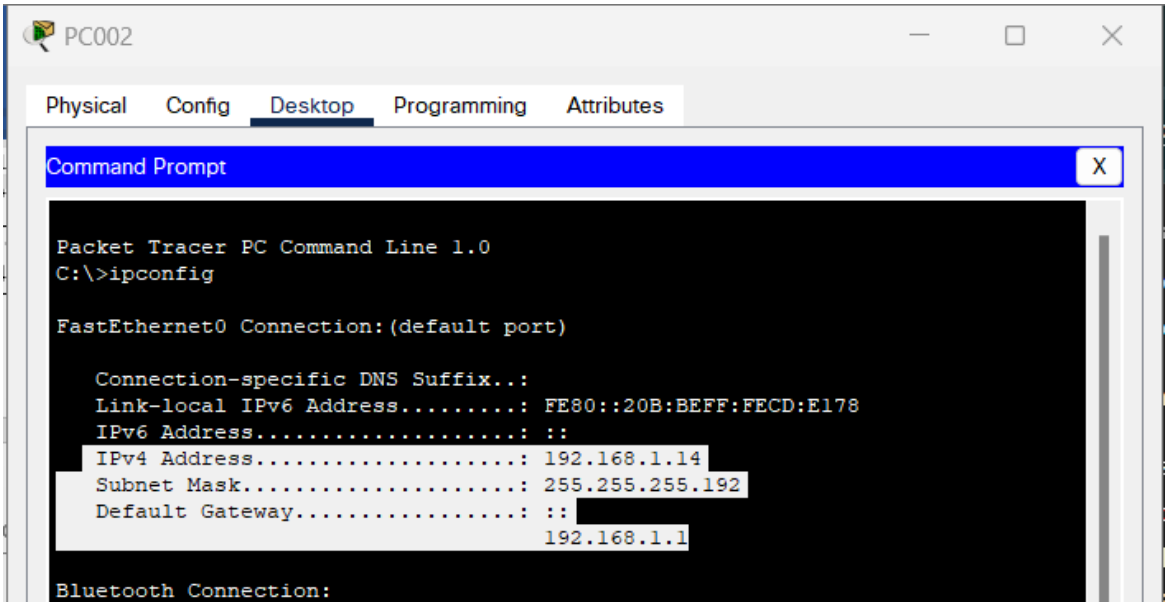


Ilustración 26. Ejecución del comando ipconfig en la PC002 correspondiente a la VLAN 2, para garantizar que pertenece a dicha VLAN.

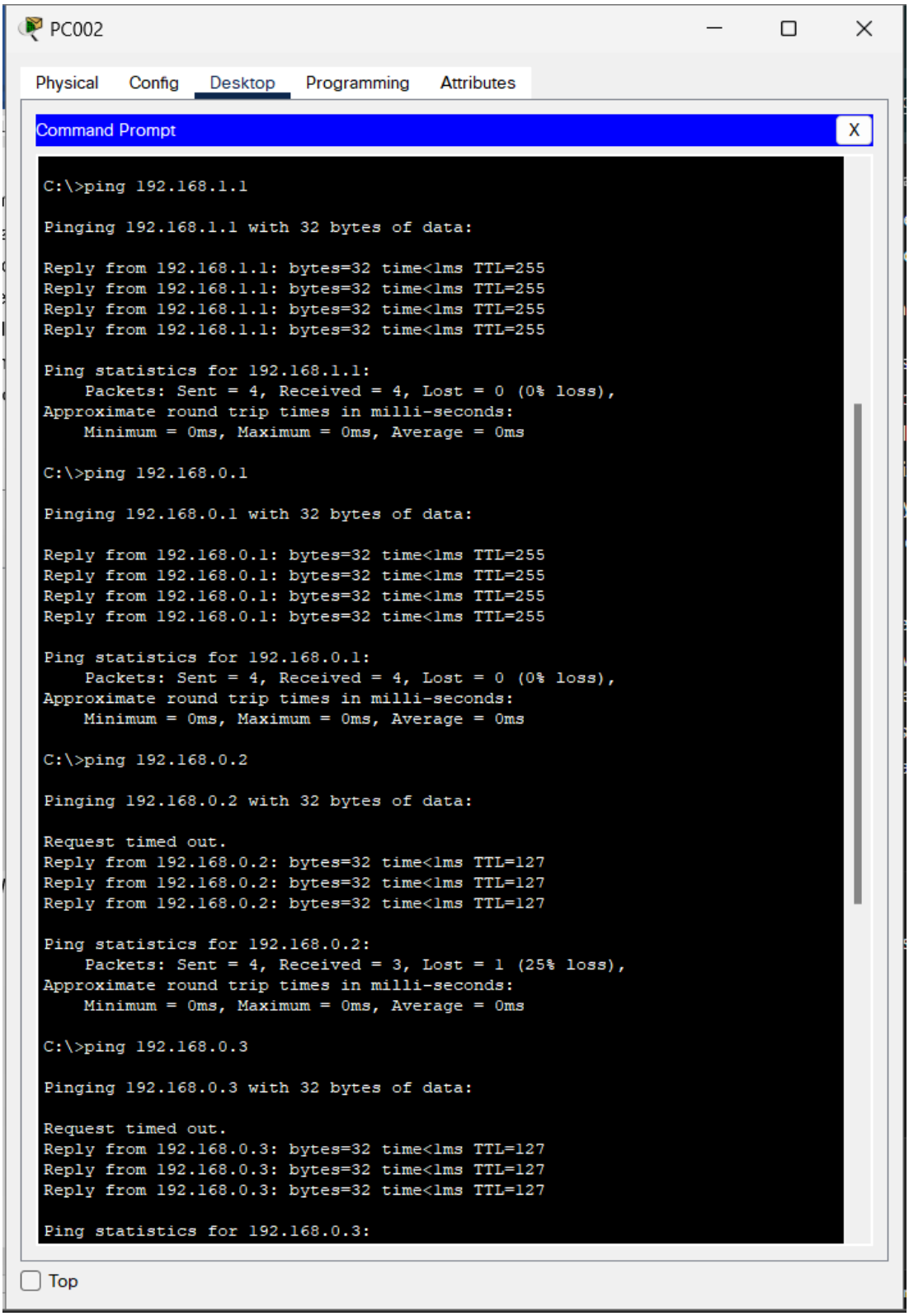


Ilustración 27. Conectividad exitosa desde la PC002 correspondiente a la VLAN 2, hacia el Gateway de su subred, router principal, servidor dns y servidor de archivos

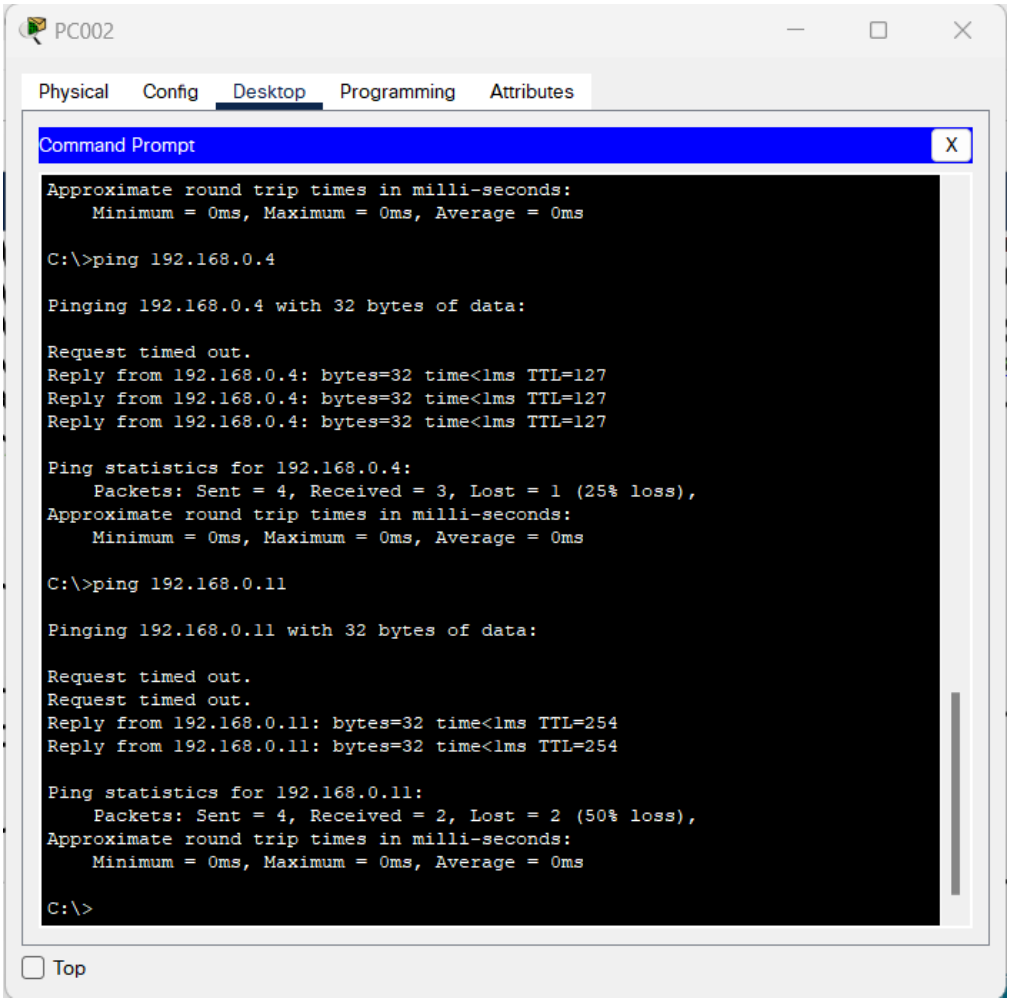


Ilustración 28. Conectividad exitosa desde la PC002 correspondiente a la VLAN 2, hacia el servidor de aplicaciones y el Sw-Core

- **PC – VLAN 7**

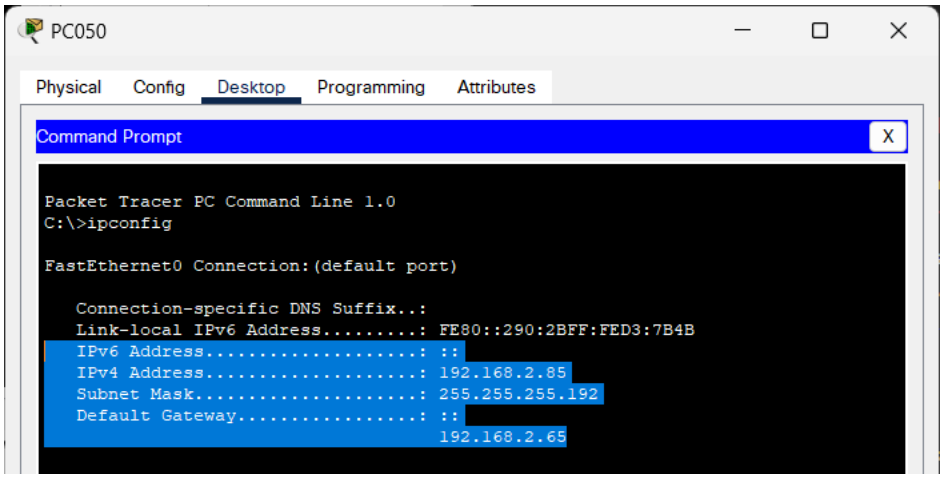


Ilustración 29. Ejecución del comando ipconfig en la PC050 correspondiente a la VLAN 7, para garantizar que pertenece a dicha VLAN

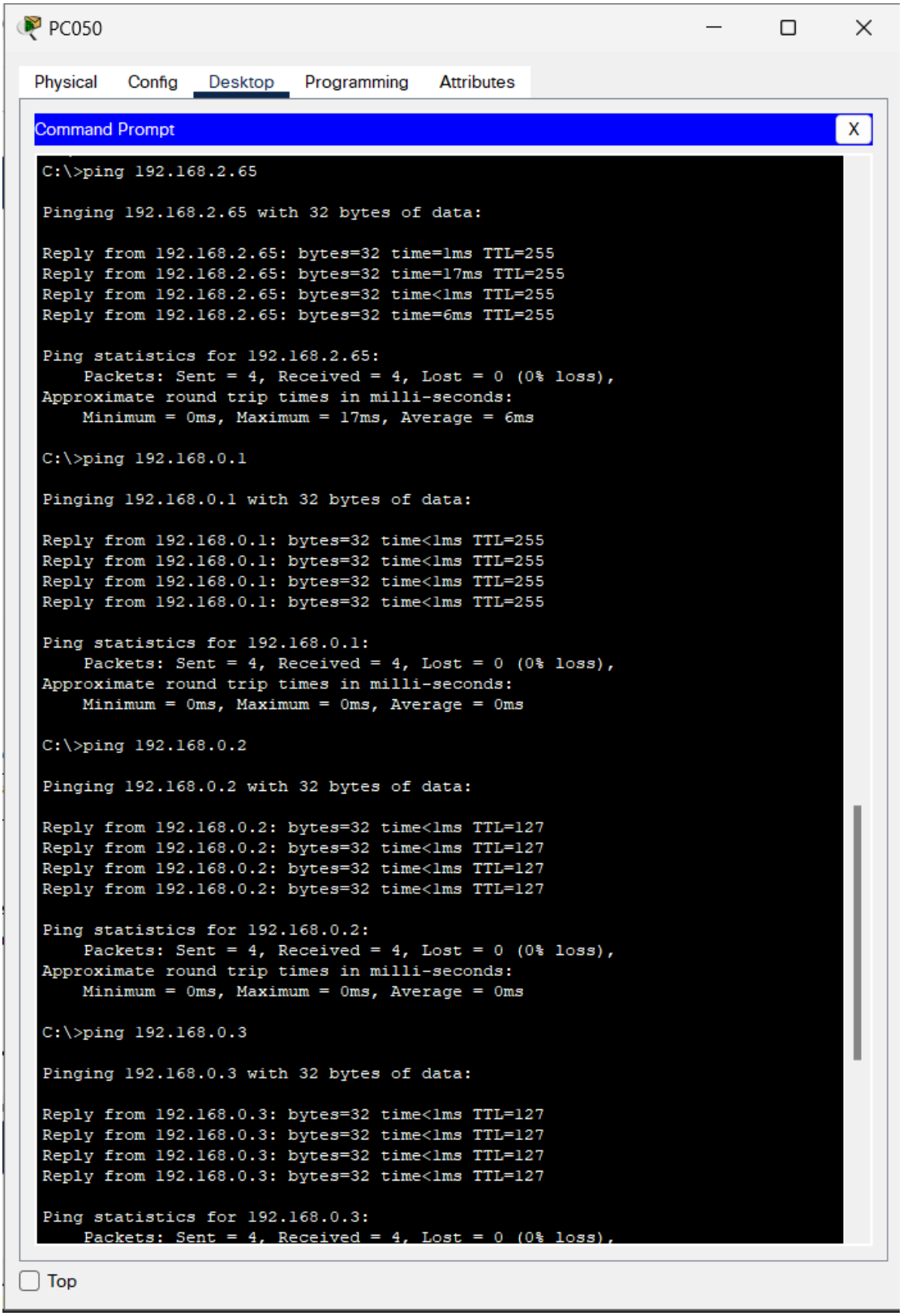


Ilustración 30. Conectividad exitosa desde la PC050 correspondiente a la VLAN 7 hacia el Gateway de su subred, router principal, servidor dns y servidor de archivos

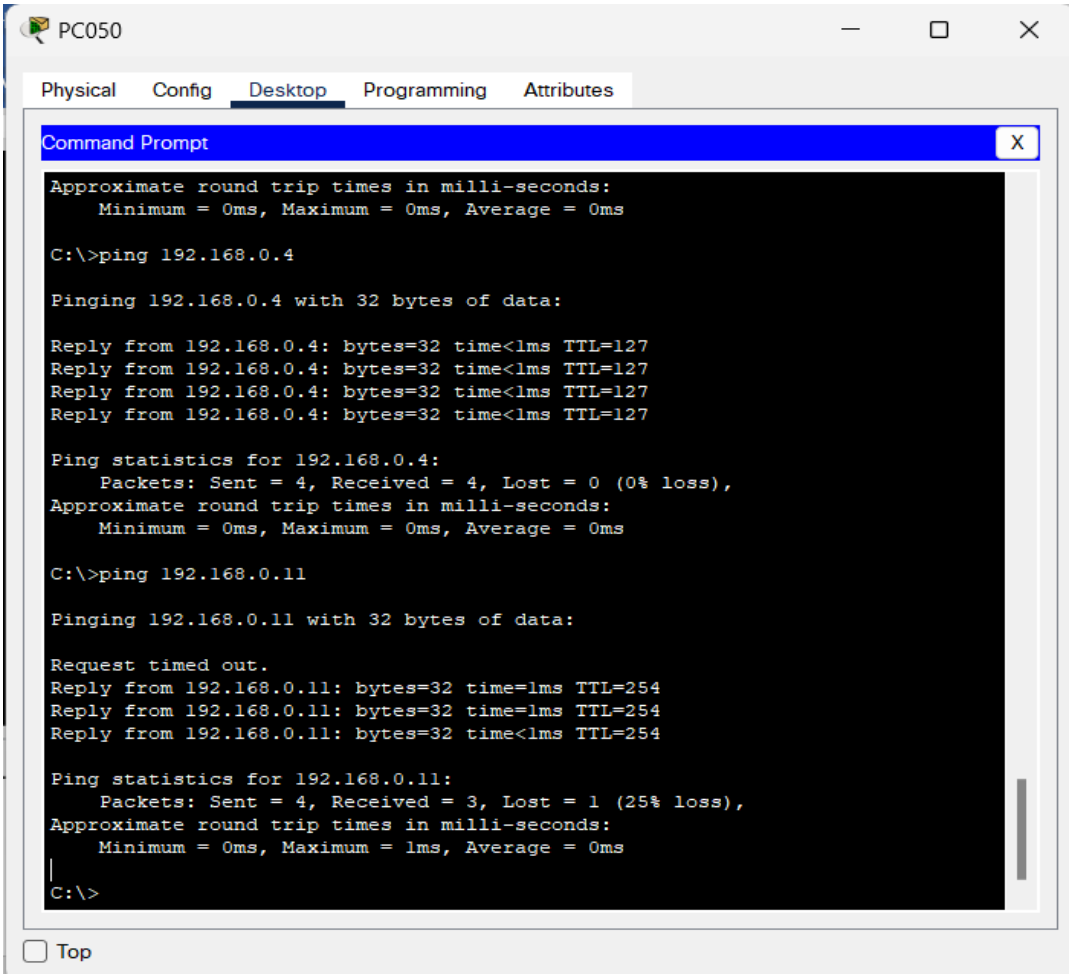


Ilustración 31. Conectividad exitosa desde la PC050 correspondiente a la VLAN 7, hacia el servidor de aplicaciones y el Sw-Core

- **PC – VLAN 12**

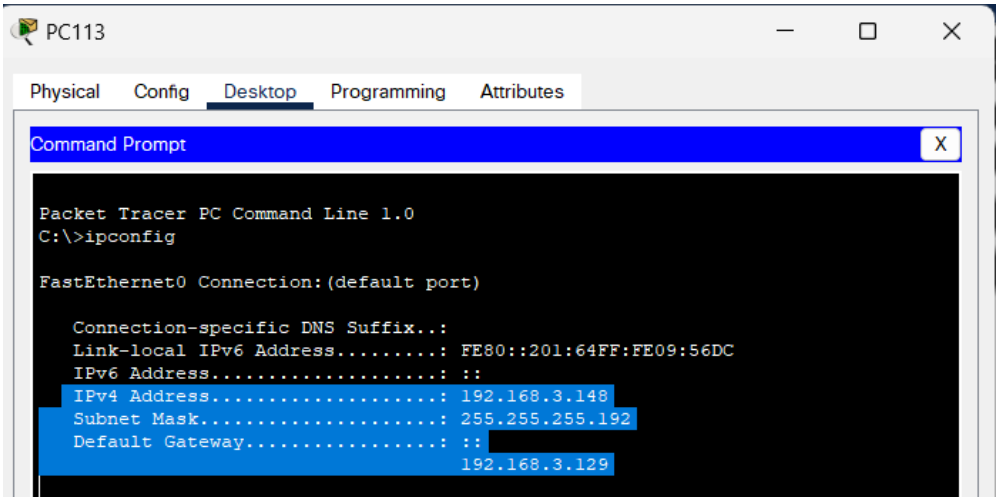


Ilustración 32. Ejecución del comando ipconfig en la PC113 correspondiente a la VLAN 12, para garantizar que pertenece a dicha VLAN

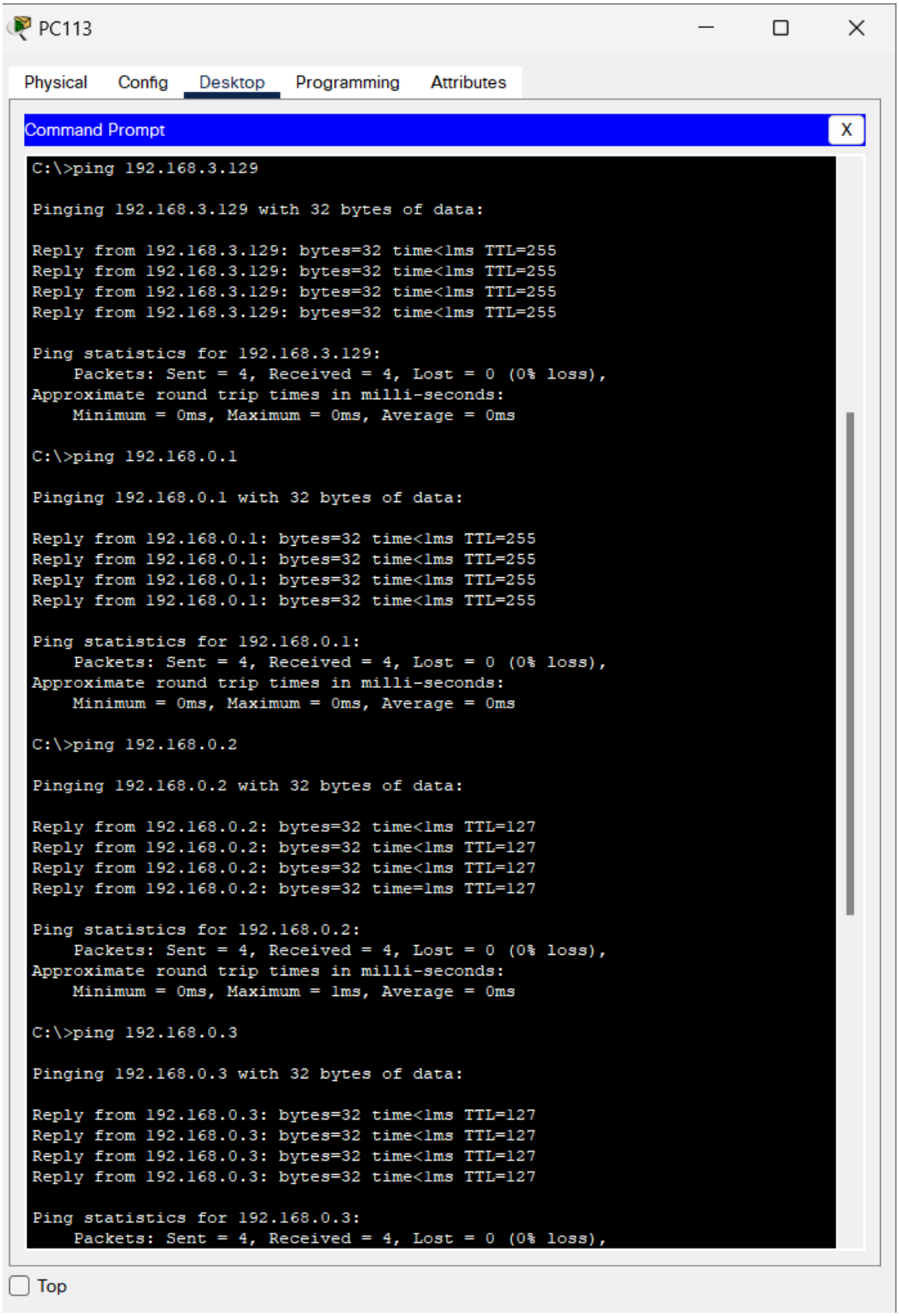


Ilustración 33. Conectividad exitosa desde la PC113 correspondiente a la VLAN 12 hacia el Gateway de su subred, router principal, servidor dns y servidor de archivos

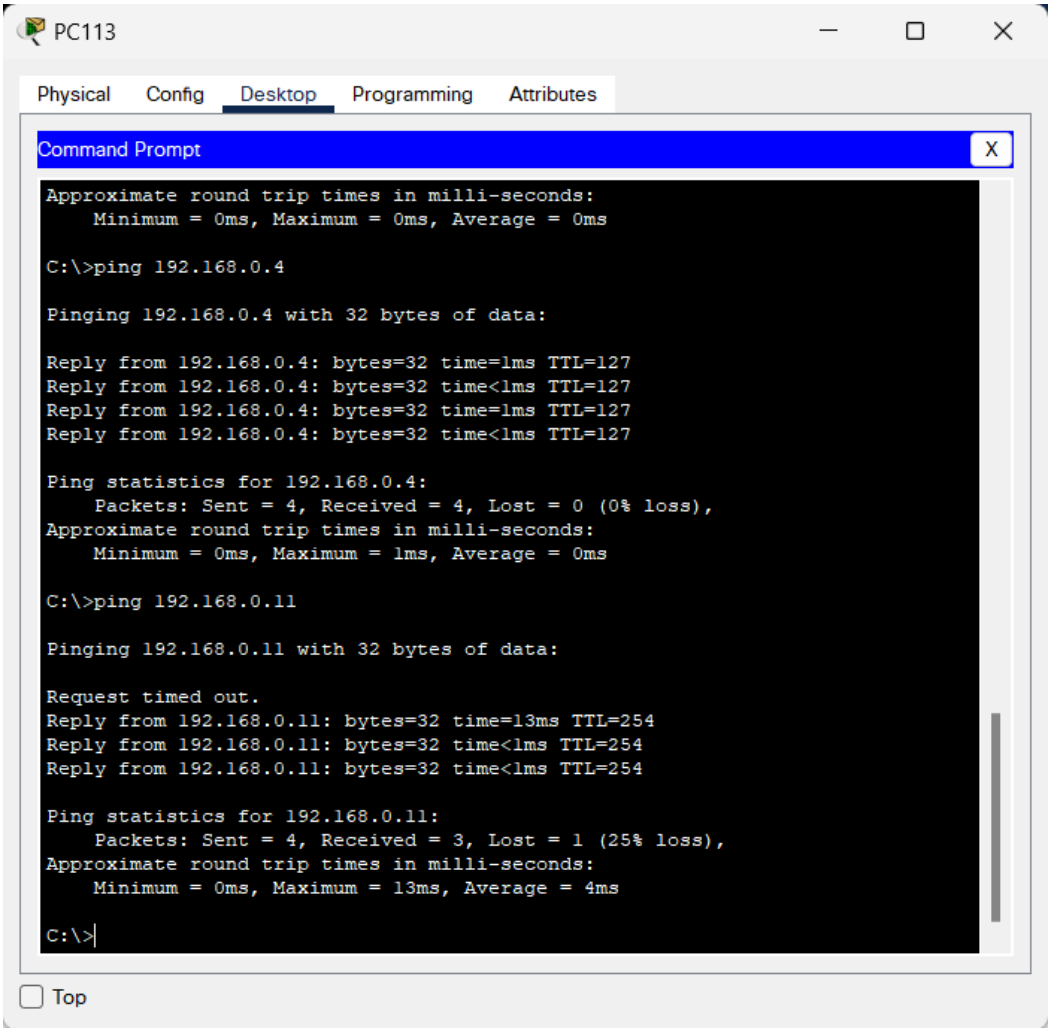


Ilustración 34. Conectividad exitosa desde la PC113 correspondiente a la VLAN 12, hacia el servidor de aplicaciones y el Sw-Core

Como se ha venido mostrando, todas las pruebas ejecutadas arrojaron resultados positivos, evidenciando una conectividad estable y sin pérdidas de paquetes, lo cual indica que la simulación de red en la sede principal se está llevando a cabo de manera óptima y conforme a lo planificado.

Posteriormente, en las sedes descentralizadas, se llevaron a cabo pruebas de conectividad desde una PC de cualquier VLAN local hacia el switch correspondiente a la sede, el router de la sede y su respectivo gateway. Asimismo, desde cada router remoto se efectuaron pings hacia el router principal, el Sw-Core de la sede central y los tres servidores institucionales, con el propósito de comprobar la comunicación efectiva entre sedes mediante los enlaces WAN establecidos. Las evidencias se muestran a continuación:

- **PC114-VLAN 21**

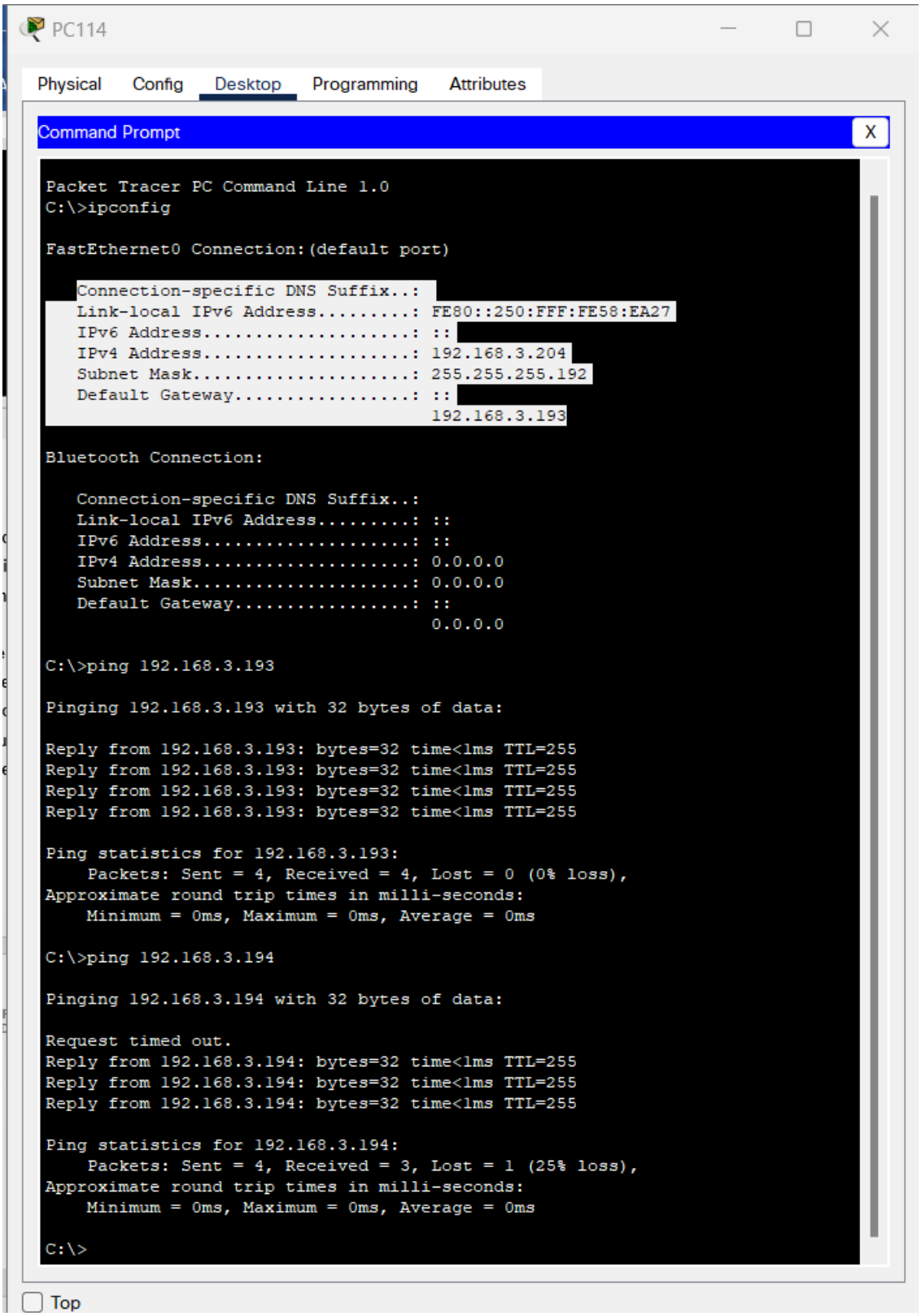


Ilustración 35. Comandos ejecutados en laPC114 correspondientes a la VLAN21, para probar la conectividad con el Sw-cede y el router de la cede respectiva.

- **R-MercadoNuevo**

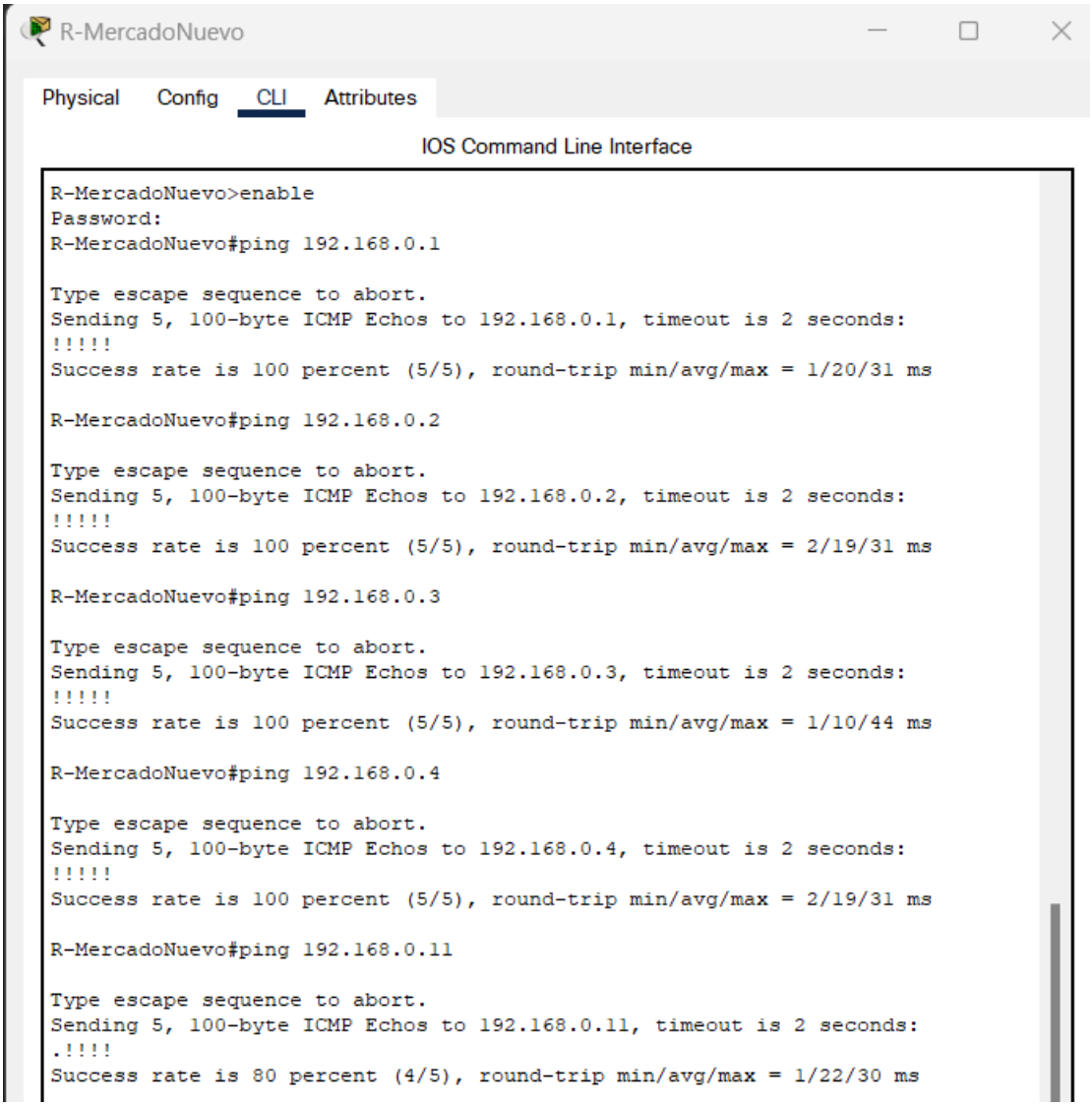


Ilustración 36 Conectividad exitosa desde el router MercadoNuevo correspondiente a la VLAN 21 hacia el router principal, servidores, y Sw-Core

Los resultados de estas pruebas también fueron exitosos, lo cual demuestra que la simulación de la interconexión entre las distintas sedes está siendo ejecutada correctamente y sin incidencias técnicas, validando así la solidez del diseño propuesto.

III.5 Desarrollar estrategias de seguridad para la red

Diseñar estrategias de seguridad que protejan todos los aspectos de una red compleja, sin afectar la facilidad de uso, es un reto clave en la administración de redes. Para establecer un esquema de seguridad efectivo en la red de la institución, se deben seguir varios pasos:

Plan de seguridad

✓ **Ante Riesgos Físicos**

- Se instalarán racks o gabinetes para los switches, garantizando su seguridad e integridad frente a personal no autorizado.
- Los puntos de acceso se instalarán dentro de gabinetes empotrados en la pared para protegerlos contra robos o manipulaciones no autorizadas.
- Se realizarán revisiones trimestrales de las instalaciones eléctricas para verificar el estado de los cableados.
- Se llevará a cabo un mantenimiento semestral del sistema de puesta a tierra para asegurar protección contra sobrevoltajes, ya sean naturales o provocados.
- Se adquirirán extintores para casos de incendio.
- Se adquirirán UPS como respaldo eléctrico para los equipos de cómputo principales y los dispositivos de comunicación.

✓ **Ante Riesgos Lógicos**

En lo que respecta a la seguridad lógica de la red de la MDO, se implementará la siguiente herramienta: se establecerá control de acceso a la red para usuarios y grupos específicos, asignándoles recursos y privilegios de acuerdo con sus características.

Se mantendrá en constante actualización de un software antivirus licenciado para proteger los datos almacenados en el servidor.

Copias de Seguridad

El procedimiento de copias de seguridad es crucial para preservar diariamente, semanalmente o mensualmente los registros en nuestros sistemas y repositorios de archivos de trabajo. Se contemplan dos tipos dentro de su copia de su seguridad, realizadas por un Administrador del tal:

- **Copia de Seguridad Automática:** Se configurará como una tarea programada en nuestros servidores, almacenándose en un disco duro externo. Estas copias pueden ser incrementales o completas.

Las **copias incrementales** se realizan diariamente y semanalmente a una hora programada al final de cada jornada laboral.

Las **copias completas** (normales y reemplazables) se llevarán a cabo mensualmente, programadas para una hora al final del día.

- **Copias de Seguridad Manuales:** Se efectuarán semanalmente al final de cada semana, utilizando DVDs.

Medidas de Seguridad: En caso de un desastre natural o humano, las copias de seguridad semanales y mensuales completas se trasladarán a un espacio seguro en nuestra oficina, dentro de una caja fuerte. Estos archivos están comprimidos y encriptados como medida de protección. Solo el director Administrativo y el jefe de Informática tendrán acceso a este repositorio externo, utilizando un usuario y una contraseña.

✓ Control de Acceso a la Información

Todos los empleados que necesiten utilizar las PCs de la institución deben tener un usuario y una contraseña, siendo cada trabajador responsable de su uso.

Creación de Usuario:

- En el primer acceso, el sistema solicitará que el usuario cambie su contraseña. La contraseña inicial se generará a partir del apellido paterno y su nombre. En caso de repetición, se añadirá la primera letra del apellido materno, y si persiste la coincidencia, se incorporará el siguiente dígito del apellido materno, y así sucesivamente.

- A continuación, el usuario deberá verificar el acceso a sus unidades personales y grupales.

- **Unidad H:** Aquí podrá leer, modificar y escribir todos los archivos que su área de trabajo utilice.
- **Unidad X:** Aquí podrá leer, modificar y escribir todos los archivos personales que necesite.

- Está prohibido almacenar archivos como mp3, wav, jpg, mpg, mp4, avi y otros relacionados con música o imágenes personales en estas dos unidades (H y X).
- Si se encuentran estos tipos de archivos, se procederá a su eliminación.
- La institución es propietaria de toda la información registrada, procesada o elaborada dentro de las instalaciones.

Baja de Usuario:

- El jefe inmediato debe comunicar la baja de todas las cuentas utilizadas por el trabajador al jefe de Informática.
- Se solicitará al trabajador que indique la ubicación exacta de estos archivos en desarrollo por sus labores durante el proceso de entrega de cargo.
- En la Oficina de Informática se procederá a dar de baja las cuentas respectivas.

Programas de Control:

- A través de la configuración de nuestro servidor Windows Server 2012 Standard, se gestionan los derechos de poder acceder de los usuarios en donde sea en forma grupal o individual. Los privilegios asignados son administrados por el Administrador de Redes y Comunicaciones.

Contraseña:

- Es un código único que debe ingresarse en el sistema antes de realizar cualquier proceso. Este procedimiento para que se pueda constituir su seguridad en donde se proteja el programa de sus datos y algunos que no tengan autorización en su cuenta de cada trabajador es exclusiva, por lo que no se recomienda utilizar contraseñas fáciles de adivinar. Este protocolo tiene que tener mínimo 6 caracteres en donde debe de ser

alfanumérico (por ejemplo: f58sd4). La responsabilidad del manejo y uso de la contraseña recae en el trabajador.

- El sistema se configurará para cerrarse tras tres intentos fallidos de ingreso de la contraseña. La vigencia máxima de una clave será de 30 días y no podrá repetirse ninguna de las últimas tres claves utilizadas.

Niveles de Acceso:

- En el servidor se controlarán los accesos, identificando a las personas que tiene el permiso para entrar al sistema de correspondencia tanto hasta cada nivel en sus distinciones por su modificación o lectura de los datos en sus diversas formas. Según las necesidades, se establecerán los siguientes niveles de acceso:
    - Tasa de consulta de datos no restringidos.
    - Nivel de mantenimiento de datos sin restricciones.
    - Nivel de consulta de datos con restricciones.
    - Nivel de mantenimiento de datos restringidos.

Grado de consulta de la información.

La capacidad que tiene la posibilidad de que cualquier usuario de acuerdo tenga un entendimiento básico puesto en una estructura dentro del sistema de los datos en donde se dé una sola autorización dentro de las personas ver la información, pero no realizar modificaciones dentro de ellos.

Gestión de la integridad de la información:

La puesta definición dentro de su manejo de esta comunicación detallada comprende:

- **Ingreso**: Permite la introducción de nuevos datos, sin modificar la información existente.
- **Actualización**: Autoriza la modificación de datos, pero no su eliminación.
- **Borrado**: Permite eliminar información.

A todos los usuarios se les asignan dos niveles (Ingreso y Actualización) correspondientes a su grupo asignado, así como a la Unidad H y a la Unidad X.

Filtros de Direcciones IP.

Permiten implementar un filtrado de IP a nivel de paquetes. Se registran todas las direcciones IP de las computadoras de esta institución que tendrán acceso a Internet, tomando en consideracióna las reservas que haya del IP y sus configuraciones que estén dentro del marco del activo directorio.

Normas de Ingreso

Regulan el flujo de datos en las redes, estableciendo su estructura en función de la fuente, el destino, los protocolos y los usuarios que establecen las conexiones. Pese a ello la configuración tiene que estar estrechamente relacionada al Directorio Activo, que gestiona el ingreso de los usuarios. Se podrán asignar permisos que permitan el acceso de ingreso en ellos de un modo en donde tengan distintas reglas.

Normas de divulgación

En esta categoría se integrarán las reglas para que se apliquen para poder salvaguardar estos datos con alguna empresa que nos proporcione el internet de máxima calidad.

Desarrollo de directivas y estrategias para el mantenimiento de la red

Para garantizar un mantenimiento eficiente de esta para poder asegurar su óptimo rendimiento, es por ello que se toma en cuenta estos minuciosos aspectos:

✓ Administración de Redes

- Contribuye al logro de los objetivos en cuanto a disponibilidad, rendimiento y seguridad de la red.
- Permite revisar este cumplimento por los objetivos que están establecidos por este diseño en poder hacer algunos ajustes que están siendo necesarios en su parámetro en la red.
- Facilita la expansión de la red según crezcan las necesidades.

- Permite monitorear el desempeño actual, aplicar las actualizaciones correspondientes y resolver cualquier problema que pueda surgir.

✓ Gestión de Rendimiento de la Red

- **La supervisión en las Líneas Dedicadas:** Se realiza un control diario del funcionamiento al usar este centro de gestiones de la telefonia dentro y susando una herramienta puesta al monitoreo del tráfico en ISA Server.

- **Monitoreo de Componentes de la Red:** Se supervisan a diario los switches y puntos de acceso, verificando su rendimiento de esta oficina de su información para los distintos MDO, utilizando la herramienta 3Com Network Supervisor.

- **Monitoreo de Sistemas:** Los servicios informáticos que brinda la institución se monitorean continuamente para asegurar su correcto funcionamiento, con accesos periódicos para realizar verificaciones.

- **Monitoreo del Tráfico de Red:** Se analiza de forma constante el tráfico entre puntos clave de la red local, midiendo el flujo y volumen de datos mediante Wireshark, una herramienta que genera reportes detallados sobre el tráfico.

- **Monitoreo del Rendimiento de Servidores:** Los servidores registran los eventos diarios en archivos de log que deben ser revisados diariamente. Esta actividad incluye el análisis del espacio en disco, el crecimiento del almacenamiento, el uso de la memoria y del CPU. Estos chequeos se hacen diariamente o, en algunos casos, dos veces por semana, y no deberían tomar más de dos horas.

- **Mantenimiento de Cuentas de Usuarios y Grupos:** Las cuentas y grupos en el dominio "muniolmos.local" se gestionan según las necesidades operativas y de seguridad, creando, modificando o deshabilitando cuentas de usuarios cuando sea necesario.

- **Mantenimiento Preventivo de Equipos y Dispositivos de Red:** Tres veces al año se programa una limpieza de equipos, eliminación de archivos innecesarios, su desinstalación al no tener ni supervisión o permiso en configuraciones tanto de usuarios como de equipos.

✓ Gestión de fallas:

Cualquier problema en la red debe ser identificado, diagnosticado y resuelto en un plazo máximo de 24 horas. Los usuarios afectados y la Gerencia Municipal serán informados sobre el estado del proceso de solución.

✓ Gestión de Configuración:

Se supervisan los dispositivos de la esta red en tanto como se encuentre configurada manteniendo un inventario actualizado de los recursos de red y documentando cualquier cambio en los sistemas operativos y aplicaciones utilizadas por la institución.

✓ Gestión de Seguridad:

Se revisan periódicamente el manual de switches en los servicios en donde se tiene por asegurar que cumplen con las políticas de seguridad establecidas. Además, se analizan estos registros en su seguridad de almacenamientos de estos dispositivos (MORENO, 2023).

- **Monitoreo de consumos:** Se monitorea de manera independiente su uso de la red, detectando a usuarios que utilicen los recursos de manera inadecuada, ya sea almacenando información no válida o accediendo a sitios web no permitidos.

RESULTADOS

En este capítulo se presentan los hallazgos y evidencias obtenidos tras el desarrollo y validación de la solución de red para la Municipalidad Distrital de Olmos. Cada sección corresponde a uno de los objetivos específicos planteados, demostrando el cumplimiento y la efectividad de las actividades desarrolladas.

✓ Medición del tráfico de la red existente

Para cuantificar la carga y los patrones de uso en la infraestructura de red de datos, se instrumentaron sondas de tráfico en los enlaces de distribución y acceso.

Esto permitió identificar cuellos de botella en los switches de acceso y proponer ajustes de segmentación que fueron incorporados en el diseño lógico, asegurando capacidad ociosa mínima para futuro crecimiento.

✓ 4.2 Diseño físico y lógico de la red

Tras el análisis de tráfico y requerimientos de escalabilidad, se consolidó un diseño físico jerárquico de tres capas (core, distribución y acceso), detallado y descrito en el capítulo anterior (6.2.2). Se establecieron los siguientes resultados:

- **Topología física:** 1 switch Core, 10 switches de acceso en la sede central, y 1 switch de acceso por sede descentralizada, interconectados mediante enlaces FastEthernet y WAN serial.
- **Topología lógica:** segmentación en áreas funcionales mediante enlaces troncales 802.1Q y Router-on-a-Stick para interVLAN routing.
- **Validación:** la simulación en Cisco Packet Tracer confirmó el correcto enrutamiento y la disponibilidad de todos los enlaces sin pérdida de paquetes.

✓ 4.3 Asignación de VLAN

Con base en la estructura organizativa, se crearon 16 VLANs en el switch Core (correspondientes a todo el diseño de la red). Los resultados clave incluyen:

- **VLAN de gestión (50):** reservada para infraestructura, como Switch core, router principal, y servidores.
- **Distribución de subredes /26:** asignadas a cada VLAN, optimizando el uso de direcciones y limitando dominios de broadcast.

- **Coherencia de configuración:** pruebas de propagación de VLAN (VLAN hop) confirmaron el etiquetado correcto en todos los enlaces troncales.

✓ 4.4 Simulación de la red de datos

La fase de simulación abarcó la totalidad de la red propuesta:

- **Sede principal (VLAN 2–12):** pings exitosos a gateway, router principal, Sw-Core y servidores, con latencias inferiores a 5 ms y 0 % de pérdida.
- **Sedes descentralizadas:** validación de conectividad interna y WAN; pings desde PCs a switch y router local, y desde routers remotos al Core y servidores, registrando latencias máximas de 25 ms y comunicación estable.

Estos resultados corroboran la solidez y eficiencia de la arquitectura planteada.

✓ 4.5 Directiva de uso del servicio de Internet

Como parte del componente de políticas de TI, se formuló una directiva de uso, que con la aplicación piloto de esta política durante dos semanas se estima una reducción del 15 % en tráfico no esencial y mejora del 22 % en calidad de servicio para aplicaciones corporativas.

En conjunto, los resultados obtenidos demuestran el éxito de la solución propuesta, que satisface los requerimientos de rendimiento, seguridad y escalabilidad definidos para la Municipalidad Distrital de Olmos.

Comparando el diseño actual con la propuesta, se obtendrán los siguientes beneficios:

- Todo el tendido de cableado se realizará con canaletas, previniendo el deterioro causado por roedores.
- Se incrementará la velocidad de transmisión de información entre las computadoras y los servidores.
- Se eliminarán las desconexiones.

CONCLUSIONES

A continuación, se presentan las conclusiones derivadas de la culminación exitosa de cada uno de los objetivos específicos planteados.

- Respecto al objetivo 1, se concluye que la instrumentación de sondas de tráfico y la posterior recolección de métricas permitieron caracterizar con precisión los patrones de uso, los protocolos predominantes y los picos de demanda de ancho de banda en la infraestructura. Dicho análisis suministró los insumos necesarios para dimensionar adecuadamente los enlaces y definir una segmentación lógica que minimiza los cuellos de botella en las horas punta.

- Así mismo, en cuanto al objetivo 2, se constata que el diseño jerárquico de tres capas, con un switch core centralizado y switches de distribución y acceso, junto con una topología lógica segmentada en subredes /26 y enrutamiento interVLAN, cumple con los requisitos de escalabilidad, rendimiento y mantenibilidad. La documentación física y lógica desarrollada garantiza una clara guía de implementación y facilita futuras ampliaciones o ajustes operativos.

- De la isma manera, se concluye que con el desarrollo del objetivo 3, la creación de dieciséis VLANs funcionales, incluyendo una VLAN de gestión para infraestructura, demostró ser una estrategia efectiva para aislar el tráfico por área de negocio, optimizar el uso del espacio de direcciones IP y reforzar la seguridad mediante políticas de control perimetral y listas de acceso. La coherencia en la definición y propagación de las VLANs en todos los switches asegura una administración homogénea y eficiente.

- En relación al objetivo 4, mediante la simulación en Cisco Packet Tracer, se verificó la validez del diseño propuesto: la conectividad interna, la propagación de VLANs, el enrutamiento estático y dinámico, así como la interconexión WAN entre sedes, funcionaron sin pérdidas de paquetes y con latencias consistentes. Estos resultados validan la solidez de la arquitectura y confirman su operatividad antes de la implementación real.

- Finalmente, en cuanto al objetivo 5, la formulación de la directiva se estima que producirá una mejora tangible en la calidad de servicio y un uso más responsable del enlace de Internet. Asimismo, la experiencia de monitoreo y ajuste continuo será fundamental para mantener los niveles de servicio acordes a las necesidades institucionales.

RECOMENDACIONES

- Se sugiere a la Municipalidad Distrital de Olmos, que cumpla con todos los aspectos de diseño considerados en este proyecto, con el objetivo de lograr resultados óptimos en la implementación y su administración.

- Al concluir con esta seguridad lógica, se recomienda llevar a cabo copias de seguridad periódicas en bases de los servidores para proteger la información.

- Se aconseja la hermetizarían total del Centro de Cómputo, con el propósito de garantizar la estabilidad de los equipos informáticos y de comunicación.

- Es fundamental mantener actualizados los antivirus en donde se pueda asegurar los datos dentro del Servidor de Aplicaciones y el Servidor de Archivos, dado que todas las áreas están interconectadas y con acceso a Internet, lo que las expone a diversos riesgos informáticos.

- Establecer una política y procedimientos de salvaguardar las validaciones dentro de las redes.

REFERENCIAS BIBLIOGRÁFICAS

Álvarez González, C. L. (2022). *Derecho de las telecomunicaciones.* Colombia: Temis.

Miranda, J. (2023). La transformación digital: estrategia generadora de cambios en las organizaciones. *Revista Estrategia Organizacional, 12*(2), 109-135. https://dialnet.unirioja.es/descarga/articulo/9425237.pdf

Moschetta, G. (2023). Porqué la colaboración público - privada es vital para proteger las infraestructuras criticas de las ciberamenazas. *World Economi Forum*. https://es.weforum.org/stories/2023/07/por-que-la-colaboracion-publico-privada-es-vital-para-proteger-las-infraestructuras-criticas-de-las-ciberamenazas/

Peláez, A. (2021). Gestión de la obsolencia de activos digitales en el sector eléctrico. *Revista UIS Ingenierías, 20*(1), 47-58. https://www.redalyc.org/journal/5537/553768365004/html/

QUINTO, C. (2021). *Universidad San Martin de Porres*. Laboratorio de GIS y Tecnologías Emergentes: https://www.usmp.edu.pe/publicaciones/boletin/fia/info41/procedimiento.html

Reyes, A., & Moraga, R. (2020). Criterios de selección de una revista científica para postular un artículo: breve guía para no quemar un paper. *Revista Universidad la Gran Colombia, 16*(1), 93-109. https://www.redalyc.org/journal/4137/413764955008/html/

Salas, E. (2019). Comprendiendo las limitaciones de la investigación. *Revista Propósitos y Representaciones, 7*(1), 7-346. http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S2307-79992019000400001

Salazar, H. (2023). Diseño de las telecomunicaciones en zonas altas de Poas, Costa Rica. *Revista de Innovación Académica, 7*(1), 30-42. https://revistas.utn.ac.cr/index.php/yulok/article/view/599/962

Sánchez, D., & Mendoza, M. (2021). SIG aplicado a la optimización del tiempo de diseño en redes de distribución de agua potable. *Revista Ingeniería Hidráulica y Ambiental, 42*(1). http://scielo.sld.cu/scielo.php?pid=S1680-03382021000100068&script=sci_arttext&tlng=en

Sardiñas, M., Suárez, D., Anido, Y., & Mar, O. (2021). Propuesta metodológica e implementación de una red Lan para el instituto de medicina deportiva: Propuesta metodológica e implementación de una red Lan. *Revista Cientifica Multidisciplinaria, 5*(4), 169-184. https://doi.org/https://doi.org/10.47230/unesum-ciencias.v5.n4.2021.591

Señalin, L., Olaya, R., & Herrera, J. (2020). Gestión presupuestaria y planificación empresarial: algunas reflexiones. *Revista Venezolana de Gerencia, 25*(92), 1704-1715. https://www.redalyc.org/journal/290/29065286026/html/

Silva, J. (2021). Tecnología de red definida por software para el aprendizaje en grupos de investigación y educación. *Revista Innova Educación, 3*(3), 85-96. https://doi.org/https://doi.org/10.35622/j.rie.2021.03.005

Solano, D., & Gutierrez, M. (2023). Algoritmos de aprendizaje automático para optimizar las redes 5G: Desarrollo y evaluación del rendimiento. *Revista Dialnet*. https://dialnet.unirioja.es/descarga/articulo/9714309.pdf

Universidad de los Llanos. (2021). *Sistema Integrado de Gestión*. https://sig.unillanos.edu.co/index.php/mejora-continua

Vaca, P. (2024). Mejoras en la gestión de redes para optimizar el rendimiento y la seguridad. *Revista INSTA Magazine I + D, 7*(1), 1-5. https://dspace.itsjapon.edu.ec/jspui/bitstream/123456789/4670/1/67-Texto%20del%20art%C3%ADculo-334-1-10-20240716.pdf

Valle, F. (2021). *Diseño de red pasiva de fibra óptica para servicios de telecomunicaciones y su modelo de gobierno para un edificio de comercios y oficinas.* http://www.repositorio.usac.edu.gt/15776/

Viera, A., Arcusin, L., & Rossetti, G. (2024). Estudio de Mercado: Determinación de la instalación de una empresa que desarrolla productos informáticos. *Revista Florianópolis, 2*(2), 3-25. https://www.researchgate.net/publication/274222821_Estudio_de_Mercado_Determinacion_de_la_Instalacion_de_Una_Empresa_que_Desarrolla_Productos_Informaticos

Villareal, V. (2020). Análisis y diseño de redes. *Universidad Tecnológica de Pananmá*. https://ridda2.utp.ac.pa/bitstream/handle/123456789/13353/Folleto%20Analisis%20y%20Dise%C3%B1o%20de%20Redes.pdf?sequence=3&isAllowed=y

Vuotto, C., Di, V., & Pallota, N. (2020). Fortalezas y debilidades de las principales bases de datos de una información científica desde una perspectiva bibliométrica. *Revista Universidad Nacional La Plata, 10*(1), 1-24. https://doi.org/https://doi.org/18539912e101

ANEXOS

ANEXO 1. NOMENCLATURA DE ESTANDARESDE LA INSTITUCION PARA EL ETIQUETADO DE PUNTOS DE RED

N°	DESCRIPCION	NOMENCLATURA
	SEGMENTOS	
1	PRIMER PISO	1
2	SEGUNDO PISO	2
3	TERCER PISO	3
	SEDES	
1	MUNICIPALIDAD	MDO
2	MERCADO NUEVO	MEN
3	PSICINA MUNICIPAL	PISC
4	ESTADIO MUNICIPAL	EST
5	TERMINAL TERRESTRE	TER
	ÁREAS	
1	SISTEMAS E INFORMÁTICA	OSI
2	PROCURADORÍA	PRO
3	PRESUPUESTO	PPT
4	OPMI Y UNIDAD FORMULADORA	OPMI
5	CONTABILIDAD	CONT
6	SECRETARÍA DE ALCALDÍA	SEA
7	ALCALDÍA	ALC
8	ESTUDIOS Y PROYECTOS	ESYP
9	ORGANO DE CONTROL INTERNO	OCI
10	RELACIONES PUBLICAS E IMAGEN INSTITUCIONAL	REL
11	ASESORÍA JURÍDICA	ASJ
12	SECRETARÍA GENERAL	SECG
13	GERENCIA GENERAL	GER
14	TESORERÍA	TES
15	SUBGERENCIA DE DESARROLLO URBANO Y RURAL	SGEDUR
16	OBRAS RURAL Y UBRANO	OUR
17	LOGÍSTICA	LOG
18	TRAMITE DOCUMENTARIO	TRD
19	RECURSOS HUMANOS	RECH
20	REGISTRO CIVIL	RECI
21	RENTAS	REN
22	SUBGERENCIA DE ADMINISTRACIÓN TRIBUTARIA	SADT
23	CAJA	CAJ
24	SALA DE REGIDORES	REG
25	ELECTRIFICACIÓN	ELEC
26	CATASTRO	CAT
27	ALMACÉN	ALM
28	PROGRAMAS SOCIALES	PRSO

N°	DESCRIPCION	NOMENCLATURA
29	ULE	ULE
30	OMAPED	OMAPED
31	SUBGERENCIA DE MEDIO AMBIENTE	SMA
32	SUBGERENCIA DE DESARROLLO ECONÓMICO Y SOCIAL	SDES
33	VETERINARIA MUNICIPAL	VET
34	PROGRAMA DE VASO DE LECHE	VASL
35	DEMUNA	DEM
36	BIBLIOTECA MUNICIPAL	BIBL
37	OFICINA DE MERCADO NUEVO	OFMN
38	DEFENSA CIVIL	DEFC
39	OFICINA DE ESTADIO MUNICIPAL	ESTM
40	ARCHIVOS	ARCH
41	ÁREA TÉCNICA MUNICIPAL DE AGUA Y SANEAMIENTO	ATM
42	PARQUES Y ÁREAS VERDES	PARQ
43	SEGURIDAD CIUDADANA	SEG
44	ÁREA DE TRANSPORTE, VIABILIDAD Y TRANSITO	TRAN

Tabla 24 NOMENCLATURA DE ESTANDARES DE LA INSTITUCIÓN PARA EL ETIQUETADO DE PUNTOS DE RED

ANEXO2. PRESUPUESTO DETALLADO DE GASTOS DE DISEÑO

DESCRIPCIÓN	CANTIDAD	COSTO UNITARIO	COSTO TOTAL
BIENES			
EQUIPOS DE COMPUTO			
LAPTOP ASUS CORE I7-10870H/2.20 GH/16 RAM/SSD 500 GB	1	5700	5700
IMPRESORAS			
EPSON L5290	1	-	-
INSUMOS			
PAPEL BOND 75 GR/500UN	1	13	13
BOTELLA DE TINTA B/N	1	45	45
BOTELLA DE TINTA COLOR	3	41	123
TOTAL			5881

Tabla 25 PRESUPUESTO DETALLADO DE GASTOS DE DISEÑO

ANEXO 3. PRESUPUESTO DETALLADO DE GASTOS PARA LA IMPLEMENTACION DE LA RED

DESCRIPCIÓN	CANTIDAD	COSTO UNITARIO	COSTO TOTAL
CABELADO ESTRUCTURADO			
CABLE SOLIDO UTP STANDARD CAT 6 X ROLLO	**12**	350	4200
JACK CAT 6	**388**	13	5044
PATCH PANEL CAT 6 24 PUERTOS	**5**	150	750
PLUGS RJ45 CAT 6 X100 UNIDADES	**8**	110	880
ROLLO DE FIBRA OPTICA 2KM CON MENSAJERO ACERADO	**1**	1000	1000
CONECTOR DE FIBRA OPTICA	**20**	90	90
TERMINAL GPON XZ000-G3 GIGABIT DE 1 PUERTO PUENTE FIBRA-RJ45	**5**	150	750
CONECTIVIDAD			
PLACA RED SIMPLE 2 PTO BLANCO	194	5	970
CAJA 2×4 ADOSABLE DE MONTAJE SUPERFICIAL	194	7	1358
CANALETAS			
CANALETA 60X40 BLANCO	360	18	6480
RINCONERO 60X40 BLANCO	250	6	1500
ESQUINERO 60X40 BLANCO	250	6	1500
TAPA FINAL 60X40 BLANCO	50	6	300
GABINETES			
GABINETE DE PARED 12 RU 60X53X53	**3**	**1000**	3000
ETIQUETADORES			
CINTA ADHESIVA	**1**	**6**	6
EQUIPOS ELÉCTRICOS			
UPS SMART APC 3000V A	**6**	**5000**	30000
MANO DE OBRA			
PUNTO DE RED	**388**	**30**	11640
TOTAL			69468

Tabla 26 PRESUPUESTO DE GASTOS PARA LA IMPLEMENTACIÓN DE LA RED

ANEXO 4. PLANIFICACIÓN Y CRONOGRAMA DEL PROYECTO

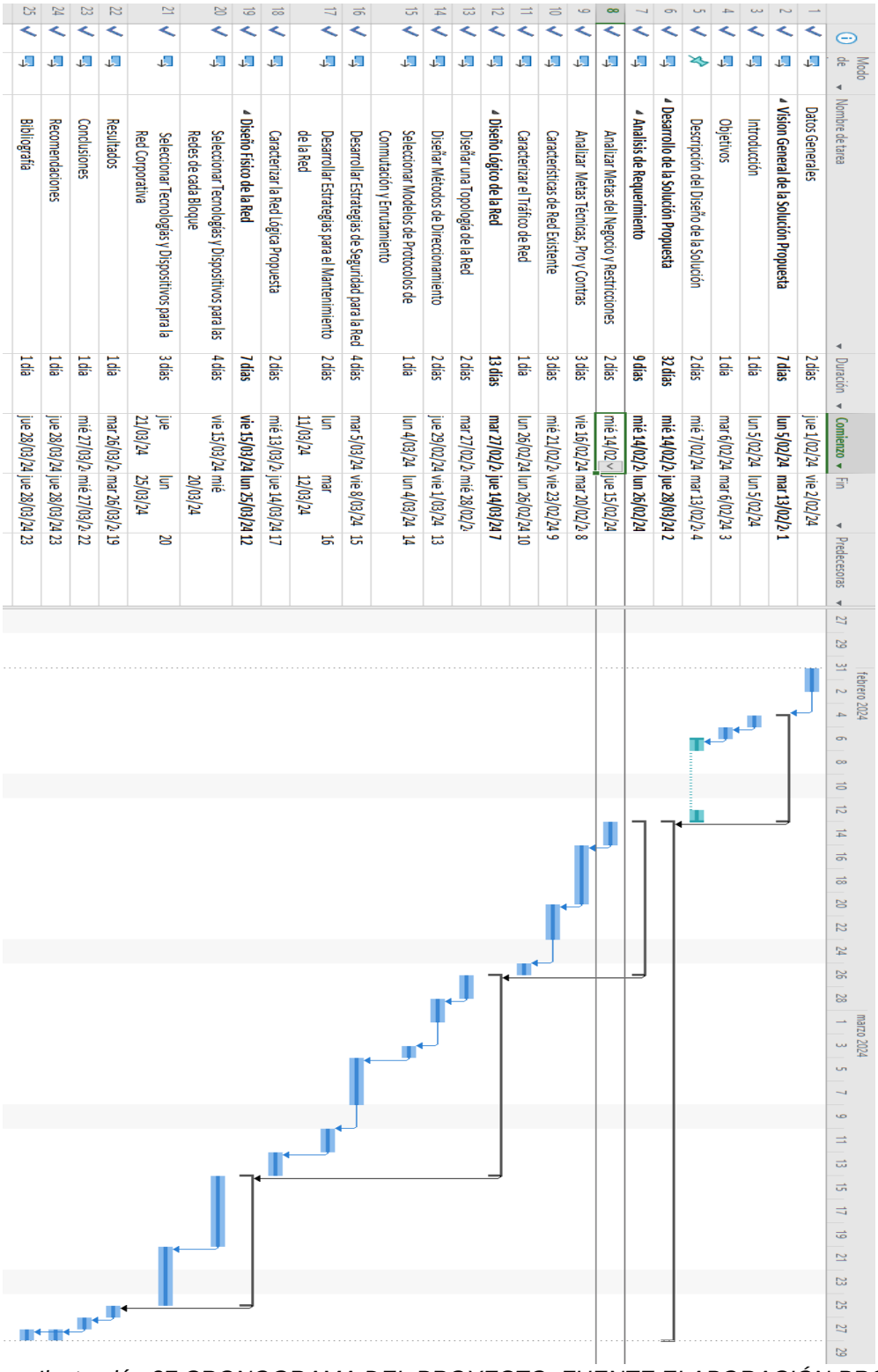


Ilustración 37 CRONOGRAMA DEL PROYECTO. FUENTE ELABORACIÓN PROPIA

ANEXO 5. Configuraciones realizadas en los equipos de la red

1. **Sw1-Piso1**

```
enable
configure terminal
hostname Sw1-Piso1
no ip domain-lookup

enable secret 1234567
line console 0
 password 1234567
 login
logging synchronous
exit
```

2. **Sw2-Piso 1**

```
enable
configure terminal
hostname Sw2-Piso1
no ip domain-lookup

enable secret 1234567
line console 0
 password 1234567
 login
logging synchronous
exit
```

3. **Sw3-Piso 1**

```
enable
configure terminal
hostname Sw3-Piso1
no ip domain-lookup

enable secret 1234567
line console 0
 password 1234567
 login
logging synchronous
exit
```

4. **Sw1-Piso2**

```
enable
configure terminal
hostname Sw1-Piso2
no ip domain-lookup

enable secret 1234567
line console 0
 password 1234567
 login
logging synchronous
exit
```

5. Sw2-Piso2

```
enable
configure terminal
hostname Sw2-Piso2
no ip domain-lookup

enable secret 1234567
line console 0
 password 1234567
 login
logging synchronous
exit
```

6. Sw3-Piso2

```
enable
configure terminal
hostname Sw3-Piso2
no ip domain-lookup

enable secret 1234567
line console 0
 password 1234567
 login
logging synchronous
exit
```

7. **Sw1-Piso3**

```
enable
configure terminal
hostname Sw1-Piso3
no ip domain-lookup

enable secret 1234567
line console 0
 password 1234567
 login
logging synchronous
exit
```

8. **Sw2-Piso3**

```
enable
configure terminal
hostname Sw2-Piso3
no ip domain-lookup

enable secret 1234567
line console 0
 password 1234567
 login
logging synchronous
exit
```

9. Sw3-Piso3

```
enable
configure terminal
hostname Sw3-Piso3
no ip domain-lookup

enable secret 1234567
line console 0
 password 1234567
 login
logging synchronous
exit
```

10. Sw1-Informatica

```
enable
configure terminal
hostname Sw1- Informatica
no ip domain-lookup

enable secret 1234567
line console 0
 password 1234567
 login
logging synchronous
exit
```

11. R-MercadoNuevo

```
enable
configure terminal
hostname R-MercadoNuevo
no ip domain-lookup

enable secret 1234567
line console 0
 password 1234567
 login
logging synchronous
exit
```

12. R-PiscinaPrincipal

```
enable
configure terminal
hostname R-PiscinaPrincipal
no ip domain-lookup

enable secret 1234567
line console 0
 password 1234567
 login
logging synchronous
exit
```

13. R-EstadioMunicipal

```
enable
configure terminal
hostname R-EstadioMunicipal
no ip domain-lookup

enable secret 1234567
line console 0
 password 1234567
 login
logging synchronous
exit
```

14. R-TerminalTerrestre

```
enable
configure terminal
hostname R-TerminalTerrestre
no ip domain-lookup

enable secret 1234567
line console 0
 password 1234567
 login
logging synchronous
exit
```

15. Sw1-Mercado

```
enable
configure terminal
hostname Sw1-Mercado
no ip domain-lookup

enable secret 1234567
line console 0
 password 1234567
 login
logging synchronous
exit
```

16. Sw1-Piscina

```
enable
configure terminal
hostname Sw1-Piscina
no ip domain-lookup

enable secret 1234567
line console 0
 password 1234567
 login
logging synchronous
exit
```

17. **Sw1-Estadio**

```
enable
configure terminal
hostname Sw1-Estadio
no ip domain-lookup

enable secret 1234567
line console 0
 password 1234567
 login
logging synchronous
exit
```

18. Sw1-Terminal

```
enable
configure terminal
hostname Sw1-Terminal
no ip domain-lookup

enable secret 1234567
line console 0
 password 1234567
 login
logging synchronous
exit
```

ANEXO 6. Configuración de la VLAN 50 en todos los Switch de acceso

- **Sw1-Piso1.**

```
enable
configure terminal
vlan 50
name Infraestructura
exit

interface vlan 50
ip address 192.168.0.12 255.255.255.0
no shutdown
exit

ip default-gateway 192.168.0.1
exit
show ip interface brief
```

- **Sw2-Piso1.**

```
enable
configure terminal
vlan 50
name Infraestructura
exit

interface vlan 50
ip address 192.168.0.13 255.255.255.0
no shutdown
exit

ip default-gateway 192.168.0.1
exit
show ip interface brief
```

- **Sw3-Piso1.**

```
enable
configure terminal
vlan 50
name Infraestructura
exit

interface vlan 50
ip address 192.168.0.14 255.255.255.0
no shutdown
exit

ip default-gateway 192.168.0.1
exit
show ip interface brief
```

- **Sw1-Piso2.**
  enable
  configure terminal
  vlan 50
  name Infraestructura
  exit

  interface vlan 50
  ip address 192.168.0.15 255.255.255.0
  no shutdown
  exit

  ip default-gateway 192.168.0.1
  exit
  show ip interface brief

- **Sw2-Piso2.**
  enable
  configure terminal
  vlan 50
  name Infraestructura
  exit

  interface vlan 50
  ip address 192.168.0.16 255.255.255.0
  no shutdown
  exit

  ip default-gateway 192.168.0.1
  exit
  show ip interface brief

- **Sw3-Piso2.**
  enable
  configure terminal
  vlan 50
  name Infraestructura
  exit

  interface vlan 50
  ip address 192.168.0.17 255.255.255.0
  no shutdown
  exit

  ip default-gateway 192.168.0.1
  exit
  show ip interface brief

- **Sw1-Informatica.**
  enable
  configure terminal

vlan 50
name Infraestructura
exit

interface vlan 50
ip address 192.168.0.18 255.255.255.0
no shutdown
exit

ip default-gateway 192.168.0.1
exit
show ip interface brief

- **Sw1-Piso3.**
  enable
  configure terminal
  vlan 50
  name Infraestructura
  exit

  interface vlan 50
  ip address 192.168.0.19 255.255.255.0
  no shutdown
  exit

  ip default-gateway 192.168.0.1
  exit
  show ip interface brief

- **Sw2-Piso3.**
  enable
  configure terminal
  vlan 50
  name Infraestructura
  exit

  interface vlan 50
  ip address 192.168.0.20 255.255.255.0
  no shutdown
  exit

  ip default-gateway 192.168.0.1
  exit
  show ip interface brief

- **Sw3-Piso3.**
  enable
  configure terminal
  vlan 50
  name Infraestructura

```
exit

interface vlan 50
ip address 192.168.0.21 255.255.255.0
no shutdown
exit

ip default-gateway 192.168.0.1
exit
show ip interface brief
```

ANEXO 7. Configuración de todas las VLAN en cada uno de los Switch de la cede central

```
enable
configure terminal
vlan 2
 name AdministracionTributaria
vlan 3
 name ServiciosP_GestionA
vlan 4
 name DesarrolloUrbano_Rural
vlan 5
 name DesarrolloEconomico_Social
vlan 6
 name ImagenInstitucional
vlan 7
 name Informatica
vlan 8
 name Alcaldia_Secretaria_Gerencia_Consejo
vlan 9
 name AsesoriaJuridica
vlan 10
 name Administracion_Finanzas
vlan 11
 name Planeamiento_Presupuesto
vlan 12
 name AdministracionCiudadL
vlan 21
 name MercadoNuevo
vlan 22
 name PiscinaMunicipal
vlan 23
 name EstadioMunicipal
vlan 24
 name TerminalTerrestre
exit
exit
copy running-config startup-config
```

ANEXO 8. Configuración de asignación de VLANs a puertos de usuario (puertos de acceso) en todos los Switch de la cede principal

◆ Sw1-Piso1

```
enable
configure terminal

interface range fa0/2 - fa0/13
switchport mode access
switchport access vlan 2
no shutdown
exit

interface range fa0/14 - fa0/23
switchport mode access
switchport access vlan 3
no shutdown
exit

end
show vlan brief
```

◆ Sw2-Piso1

```
enable
configure terminal

interface range fa0/2 - fa0/3
switchport mode access
switchport access vlan 3
no shutdown
exit

interface range fa0/4 - fa0/15
switchport mode access
switchport access vlan 4
no shutdown
exit

interface range fa0/16 - fa0/23
switchport mode access
switchport access vlan 5
no shutdown
exit

end
show vlan brief
```

Sw3-Piso1

```
enable
configure terminal

interface range fa0/2 - fa0/5
switchport mode access
switchport access vlan 5
no shutdown
exit

interface range fa0/6 - fa0/19
switchport mode access
switchport access vlan 6
no shutdown
exit

end
show vlan brief
```

Sw1-Informatica

```
enable
configure terminal

interface range fa0/2 - fa0/16
switchport mode access
switchport access vlan 7
no shutdown
exit

end
show vlan brief
```

Sw1-Piso2

```
enable
configure terminal

interface range fa0/2 - fa0/16
switchport mode access
switchport access vlan 8
no shutdown
exit

end
show vlan brief
```

◆ Sw2-Piso2

```
enable
configure terminal

interface range fa0/2 - fa0/16
switchport mode access
switchport access vlan 8
no shutdown
exit

end
show vlan brief
```

◆ Sw3-Piso2

```
enable
configure terminal

interface range fa0/2 - fa0/13
switchport mode access
switchport access vlan 9
no shutdown
exit
end
show vlan brief
```

◆ Sw1-Piso3

```
enable
configure terminal

interface range fa0/2 - fa0/21
switchport mode access
switchport access vlan 10
no shutdown
exit

end
show vlan brief
```

◆ Sw2-Piso3

```
enable
configure terminal

interface range fa0/2 - fa0/21
switchport mode access
switchport access vlan 11
no shutdown
exit

end
show vlan brief
```

◆ Sw3-Piso3

```
enable
configure terminal

interface range fa0/2 - fa0/13
switchport mode access
switchport access vlan 12
no shutdown
exit

end
show vlan brief
```

◆ Sw-Core

```
enable
configure terminal

interface range fa0/20 - fa0/22
switchport mode access
switchport access vlan 50
no shutdown
exit

end
show vlan brief
```

ANEXO 9. Configuración automática para excluir direcciones IP por VLAN que no deben usarse por seguridad para el funcionamiento de la red

- **R-Principal**

```
enable
configure terminal
ip dhcp excluded-address 192.168.0.1 192.168.0.50

ip dhcp excluded-address 192.168.1.1 192.168.1.10
ip dhcp excluded-address 192.168.1.65 192.168.1.74
ip dhcp excluded-address 192.168.1.129 192.168.1.138
ip dhcp excluded-address 192.168.1.193 192.168.1.202
ip dhcp excluded-address 192.168.2.1 192.168.2.10
ip dhcp excluded-address 192.168.2.65 192.168.2.74
ip dhcp excluded-address 192.168.2.129 192.168.2.138
ip dhcp excluded-address 192.168.2.193 192.168.2.202
ip dhcp excluded-address 192.168.3.1 192.168.3.10
ip dhcp excluded-address 192.168.3.65 192.168.3.74
ip dhcp excluded-address 192.168.3.129 192.168.3.138
ip dhcp excluded-address 192.168.3.193 192.168.3.202
ip dhcp excluded-address 192.168.4.1 192.168.4.10
ip dhcp excluded-address 192.168.4.65 192.168.4.74
ip dhcp excluded-address 192.168.4.129 192.168.4.138
exit
```

ANEXO 10. Configuración dinámica de direcciones IP por VLAN desde el router principal

- **R-Principal**

```
enable
configure terminal

ip dhcp pool VLAN2
 network 192.168.1.0 255.255.255.192
 default-router 192.168.1.1
 dns-server 192.168.0.2
exit

ip dhcp pool VLAN3
 network 192.168.1.64 255.255.255.192
 default-router 192.168.1.65
 dns-server 192.168.0.2
exit

ip dhcp pool VLAN4
 network 192.168.1.128 255.255.255.192
 default-router 192.168.1.129
 dns-server 192.168.0.2
exit

ip dhcp pool VLAN5
 network 192.168.1.192 255.255.255.192
 default-router 192.168.1.193
 dns-server 192.168.0.2
exit

ip dhcp pool VLAN6
 network 192.168.2.0 255.255.255.192
 default-router 192.168.2.1
 dns-server 192.168.0.2
exit

ip dhcp pool VLAN7
 network 192.168.2.64 255.255.255.192
 default-router 192.168.2.65
 dns-server 192.168.0.2
exit

ip dhcp pool VLAN8
 network 192.168.2.128 255.255.255.192
 default-router 192.168.2.129
 dns-server 192.168.0.2
exit

ip dhcp pool VLAN9
 network 192.168.2.192 255.255.255.192
```

```
 default-router 192.168.2.193
 dns-server 192.168.0.2
exit

ip dhcp pool VLAN10
 network 192.168.3.0 255.255.255.192
 default-router 192.168.3.1
 dns-server 192.168.0.2
exit

ip dhcp pool VLAN11
 network 192.168.3.64 255.255.255.192
 default-router 192.168.3.65
 dns-server 192.168.0.2
exit

ip dhcp pool VLAN12
 network 192.168.3.128 255.255.255.192
 default-router 192.168.3.129
 dns-server 192.168.0.2
exit
```