PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

ESCUELA DE HÁBITAT INGENIO Y CREATIVIDAD

TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

DISEÑO DE UNA RED DE DATOS PARA EL HOSPITAL SAN LUIS DE OTAVALO, ENFOCADA A TECNOLOGIAS SDN Y NFV

AUTOR: JOSEPH OMAR MORALES GRANDA

TUTOR: DARWIN MARCELO PILLO GUANOLUISA

IBARRA – ECUADOR

FEBRERO, 2026

Ibarra, 11 de febrero del 2026

CERTIFICACIÓN TUTOR

En mi calidad de Tutor del Trabajo de integración curricular titulado: "DISEÑO DE UNA RED DE DATOS PARA EL HOSPITAL SAN LUIS DE OTAVALO, ENFOCADA A TECNOLOGIAS SDN Y NFV", presentado por el estudiante Joseph Omar Morales Granda con cédula de ciudadanía N° 1004754600, para obtener el Título de Ingeniero en Tecnologías de la Información.

Certifico que el trabajo cumple con todos los parámetros establecidos, mediante el cual el estudiante demuestra el desarrollo de competencias en el campo de conocimiento de su profesión con un nivel de argumentación coherente, para ser sometido a la evaluación por parte de los lectores.

Adicionalmente, se adjunta el certificado de porcentaje de originalidad de TURNITIN.


Turnitin Informe de Originalidad

Procesado el: 30-ene-2026 15:44 -05
Identificador: 2865774212
Número de palabras: 11958
Entregado: 2

TESIS Por JOSEPH OMAR MORALES GRANDA

Índice de similitud
8%

Similitud según fuente
Fuentes de Internet: 7%
Publicaciones: 2%
Trabajos del estudiante: 4%

Firmado electrónicamente por:
DARWIN MARCELO PILLO GUANOLUISA
Validar únicamente con FirmaEC

(f): _____

Msc. Darwin Marcelo Pillo Guanoluisa

TUTOR DE TRABAJO

C.C.: 1003319660

PÁGINA DE APROBACIÓN DEL TRIBUNAL

El tribunal examinador, aprueba el presente trabajo en nombre de la Pontificia Universidad Católica del Ecuador Ibarra:

(f): ….

Firmado electrónicamente por:
DARWIN MARCELO
PILLO GUANOLUISA
Validar únicamente con FirmaEC

Mgs. Darwin Marcelo Pillo Guanoluisa

C.C.: 1003319660

Firmado electrónicamente por:
ALVARO MAURICIO
CEVALLOS RAMIREZ
Validar únicamente con FirmaEC

(f):……

Mgs. Alvaro Mauricio Cevallos Ramírez

C.C.: 1002494019

Firmado electrónicamente por:
JUAN CARLOS ARMAS
CARDENAS
Validar únicamente con FirmaEC

(f):……

Mgs. Juan Carlos Armas Cardenas

C.C.: 1001685732

ACTA DE CESIÓN DE DERECHOS

Yo, *Joseph Omar Morales Granda*, declaro conocer y aceptar la disposición del Art. 165 del Código Orgánico de Economía Social de los Conocimientos, Creatividad e Innovación, que manifiesta textualmente: "Se reconoce facultad de los autores y demás titulares de derechos de disponer de sus derechos o autorizar las utilizaciones de sus obras o prestaciones a título gratuito y oneroso, según las condiciones que determinen. Esta facultad podrá ejercerse mediante licencias libres, abiertas y otros modelos alternativos de licenciamiento o la renuncia".

Ibarra,11de febrero 2026

(f): 
Firmado electrónicamente por:
JOSEPH OMAR MORALES GRANDA
Validar únicamente con FirmaEC

Joseph Omar Morales Granda

C.C.: 1004754600

AUTORIA

Yo, Joseph Omar Morales Granda, portador de la cedula de ciudadanía N° 1004754600, declaro que el presente trabajo de investigación es de total responsabilidad del autor, y eximo expresamente a la Pontificia Universidad Católica del Ecuador Ibarra de posibles reclamos o acciones legales.

(f): …….

Joseph Omar Morales Granda

C.C.: 1004754600

DEDICATORIA Y AGRADECIMIENTOS

Agradezco a Dios y la Virgen de Guadalupe por haberme dado la fuerza necesaria de todo este trayecto universitario, sin más que decir dedico este trabajo a una persona muy especial y que sin ella no fuera lo que soy aun cuando no está sé que desde el cielo me cuida, para ti abuelita Zuly, gracias por todo lo que hiciste en su momento, cuando más le necesite siempre estuvo para mí, a mi hijo Leonardo Morales, a ti mi niño hermoso, eres la razón de todo esto y por quien me arriesgado todo este tiempo aun cuando me has visto acabado, tu siempre me has apoyado sin importar nada, a mis padres en especial a mi Mami Marianela, que su apoyo nunca dejó de ser para mí y agradecerle por todo, a mi Papá Enrique, que frente a todo estuvo ahí apoyándome incondicionalmente, y a mi hermana que Marjorie, que estuvo presente igual en este trayecto.

Agradeciendo sin más a todas las personas que me apoyaron me brindaron su apoyo en especial a mi querido amigo German Fuelpas y a su familia que pese a todo, supo apoyarme como formación indispensable para cumplir mis metas en el ámbito educativo, y por ser un buen jefe, a mis compañeros que supieron darme apoyo cuando los necesité, mil gracias a las personas que conocí en mi formación y que me brindaron su amistad y cariño por todo les estaré siempre agradecido.

A mis amigos, del Team JC4 gracias también por su buena amistad y acogida conmigo siempre les agradeceré de todo y a Dios por haberlos puesto en mi camino.

Agradeciendo a mis profesores en especial a mi Tutor Darwin, que supo apoyarme en esta etapa de formación y a los demás que siempre me dieron una mano en todo.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El Hospital San Luis de Otavalo depende de su red de datos para sostener la comunicación entre áreas, el acceso a servicios internos y la continuidad operativa. No obstante, cuando una infraestructura crece con limitaciones de segmentación, control y planificación, se generan problemas de administración, rendimiento y seguridad. Bajo este contexto, el presente trabajo plantea el diseño de una red de datos orientada a un entorno hospitalario, incorporando criterios de segmentación lógica y control del tráfico, con el objetivo de mejorar la organización de la red y establecer una base técnica escalable.

El desarrollo del proyecto se estructuró con un enfoque aplicado y cuantitativo, apoyado en un laboratorio simulado para evitar afectaciones a la operación real de la institución. La propuesta integra el enfoque de Software Defined Networking (SDN) como mecanismo para separar el plano de control del plano de datos, facilitando la administración centralizada y la aplicación de políticas; y Network Functions Virtualization (NFV) como estrategia para representar funciones de red mediante componentes virtualizados, buscando mayor flexibilidad y uso eficiente de recursos. La validación se ejecutó en un entorno de emulación, donde se implementaron elementos representativos de la arquitectura propuesta y se aplicó un plan de pruebas orientado a conectividad, estabilidad y evidencias de tráfico.

Los resultados permitieron comprobar que el laboratorio presenta conectividad estable hacia el gateway y hacia servicios internos, con tiempos de respuesta consistentes y sin pérdida de paquetes bajo condiciones normales de operación. Además, se verificó la salida a Internet mediante NAT a través de pruebas de conectividad hacia un destino público, y se corroboró el intercambio de paquetes esperados mediante capturas en Wireshark. Con ello, se sustenta que el diseño propuesto es técnicamente viable como base para una implementación progresiva, ajustada a las condiciones reales del hospital.

Palabras clave: SDN, NFV, VLAN pfSense, EVE-NG, rendimiento de red, red hospitalaria.

ABSTRACT

Hospital San Luis de Otavalo relies on its data network to support inter-department communication, internal services access, and operational continuity. However, when a network grows with limited segmentation, control, and planning, management, performance, and security issues become more frequent. In this context, this work proposes a data network design aimed at a hospital environment, incorporating logical segmentation and traffic control criteria to improve network organization and establish a scalable technical baseline.

The project was developed using an applied and quantitative approach, supported by a simulated laboratory in order to avoid impacting the hospital's real operation. The proposal integrates Software Defined Networking (SDN) to separate the control plane from the data plane, enabling centralized management and policy enforcement; and Network Functions Virtualization (NFV) to represent network services through virtualized components, seeking flexibility and efficient resource usage. Validation was carried out in an emulation environment where representative elements of the proposed architecture were implemented and a test plan focused on connectivity, stability, and traffic evidence was applied.

Results showed stable connectivity to the VLAN gateway and internal services, with consistent response times and no packet loss under normal operating conditions. Internet access via NAT was also verified using connectivity tests to a public destination, and expected traffic exchange was corroborated through Wireshark captures. These findings support the technical feasibility of the proposed design as a baseline for a progressive implementation aligned with the hospital's constraints and needs.

Keywords: SDN, NFV, VLAN, pfSense, EVE-NG, hospital network, network performance.

INTRODUCCIÓN

En la actualidad, las redes de datos representan un componente esencial para el funcionamiento eficiente de cualquier institución, permitiendo la transmisión de información, la interconexión entre departamentos y la automatización de procesos clave. En el sector salud, donde la disponibilidad y rapidez en el acceso a los datos puede impactar directamente en la atención al paciente, contar con una infraestructura de red robusta, segura y eficiente es una necesidad prioritaria. No obstante, muchas instituciones de salud de nivel básico en el Ecuador operan con redes obsoletas, mal estructuradas o sin la capacidad necesaria para soportar los requerimientos actuales, lo que limita su rendimiento y afecta la calidad del servicio.

El Hospital San Luis de Otavalo es una institución de salud pública, ubicada en la ciudad de Otavalo, provincia de Imbabura, al norte del Ecuador. Este hospital básico presta servicios médicos primarios y de urgencia a una población significativa, no solo de la ciudad de Otavalo, sino también de comunidades rurales cercanas y cantones vecinos. Por su ubicación estratégica y por ser uno de los principales centros de salud en la zona, cumple un rol fundamental en el sistema sanitario local, brindando atención médica general, medicina familiar, servicios de maternidad, laboratorio clínico, farmacia y emergencias.

Pese a su importancia, la infraestructura tecnológica del hospital presenta múltiples deficiencias que impactan negativamente en su operatividad diaria. Entre las problemáticas más relevantes se encuentran la alta latencia en la transmisión de datos, pérdida de paquetes, insuficiencia de ancho de banda, falta de segmentación de la red y una gestión limitada de los recursos de conectividad. Estas limitaciones generan congestión en la red, dificultades de comunicación entre áreas médicas y administrativas, y demoras en el acceso a la información, afectando de manera directa la eficiencia del servicio y la calidad de atención que reciben los pacientes.

Frente a esta situación, se planteó la necesidad de rediseñar la infraestructura de red del Hospital San Luis de Otavalo con una propuesta técnica moderna, flexible y escalable, que se adapte a las condiciones reales de la institución sin requerir una inversión económica excesiva. Las tecnologías emergentes como Software Defined Networking (SDN) y Network Functions Virtualization (NFV) ofrecen soluciones viables al permitir

una administración centralizada, un mejor control del tráfico de red y una reducción significativa en el uso de hardware físico a través de funciones virtualizadas. El propósito de este proyecto fue diseñar una arquitectura basada en estas tecnologías, adaptada a las necesidades y capacidades del hospital, que resuelva las falencias actuales, garantice la estabilidad del tráfico de datos y establezca una base tecnológica que facilite futuras expansiones. Además, se busca que esta solución optimice el rendimiento sin elevar los costos operativos y pueda servir como modelo replicable para otras instituciones de salud de características similares en el país.

Con base en la problemática mencionada, se establecieron los siguientes objetivos que guían el desarrollo de este proyecto:

Objetivo General:

- Diseñar una arquitectura de red de datos para el Hospital San Luis de Otavalo, basada en tecnologías SDN y NFV, que mejore la eficiencia operativa, la seguridad y la administración de la infraestructura de red de la institución.

Objetivos Específicos:

- Realizar un diagnóstico detallado de la infraestructura de red actual del Hospital San Luis de Otavalo, identificando sus principales limitaciones y deficiencias.
- Diseñar una propuesta de arquitectura de red utilizando tecnologías SDN y NFV que garantice una adecuada segmentación, optimización de recursos y mejoras en la seguridad.
- Seleccionar las herramientas de simulación y virtualización adecuadas para validar el diseño propuesto, considerando las necesidades y capacidades del hospital.
- Validar la propuesta de red mediante simulaciones, midiendo indicadores como latencia, ancho de banda, pérdida de paquetes y eficiencia operativa de la infraestructura.

El presente trabajo está contemplado en tres capítulos.

- Capítulo I: Se presenta el marco teórico necesario para comprender los fundamentos de las redes de datos, las tecnologías SDN y NFV, y su aplicación en instituciones similares.
- Capítulo II: En el segundo capítulo se describe la metodología utilizada, las fases de diagnóstico, diseño y simulación de la red, así como la justificación de las herramientas empleadas.
- Capítulo III: Se presentan los resultados obtenidos mediante las simulaciones realizadas, la comparación con la infraestructura actual, y las respectivas conclusiones y recomendaciones que permiten validar la viabilidad y efectividad de la propuesta.

CAPÍTULO I

ESTADO DEL ARTE

La infraestructura de conectividad en el sector salud ha experimentado una evolución drástica, pasando de ser un recurso de soporte administrativo a convertirse en el pilar fundamental para la atención clínica digital. El presente capítulo construye el marco teórico referencial que sustenta el diseño de la red para el Hospital San Luis de Otavalo, abordando desde los principios esenciales de las comunicaciones de datos hasta los paradigmas emergentes de gestión centralizada.

A lo largo de este apartado se analiza cómo las limitaciones de las arquitecturas tradicionales han impulsado el desarrollo de nuevas tecnologías como las Redes Definidas por Software (SDN) y la Virtualización de Funciones de Red (NFV). Estas innovaciones se presentan no solo como una mejora técnica, sino como la solución necesaria para garantizar la escalabilidad y eficiencia operativa. Finalmente, se fundamenta el cumplimiento de normativas internacionales de seguridad de la información y se justifica el uso de entornos de emulación avanzada como método indispensable para la validación de diseños de ingeniería complejos.

1.1.Redes de Datos y su Evolucion

Una red de datos se conceptualiza contemporáneamente como un sistema convergente que interconecta elementos autónomos para el intercambio de información crítica en tiempo real. **Castillo Velázquez (2019)** establece que la eficiencia de una red moderna trasciende la conectividad física; su verdadero valor radica en la capacidad de garantizar la disponibilidad, integridad y confidencialidad de los datos, elementos vitales para la toma de decisiones estratégicas en cualquier organización.

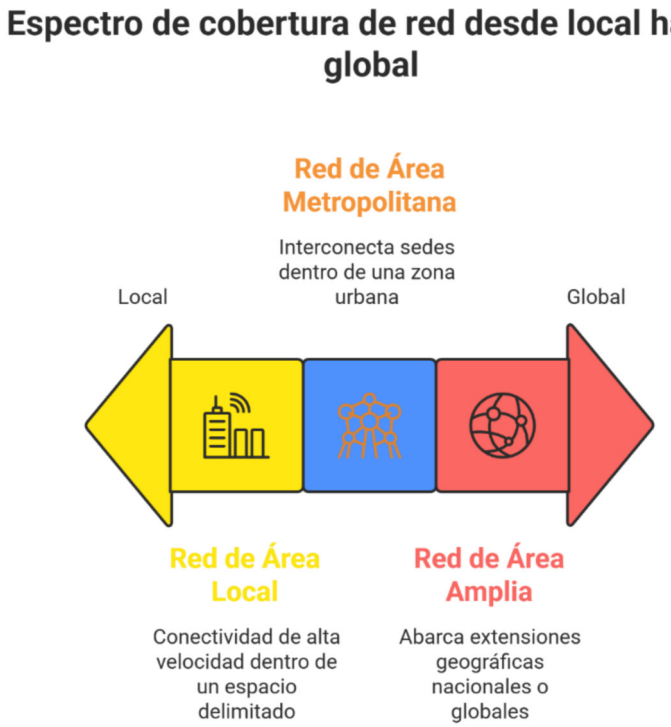
1.1.1. Clasificación de las Redes

La infraestructura de red se categoriza según su cobertura geográfica, lo cual determina los protocolos y medios de transmisión aplicables:

- **Red de Área Local (LAN):** Infraestructura confinada a un espacio geográfico limitado, como un edificio o un campus hospitalario. Se caracteriza por altas tasas de transferencia y baja latencia, siendo la base para la conectividad de usuarios finales.

- **Red de Área Metropolitana (MAN):** Interconecta diversas LANs dentro de una misma ciudad o zona urbana extensa, permitiendo la integración de sucursales dispersas mediante enlaces de fibra óptica.
- **Red de Área Amplia (WAN):** Abarca extensas áreas geográficas (países o continentes), utilizando servicios de proveedores de telecomunicaciones (ISP) y tecnologías como MPLS para garantizar la comunicación a larga distancia.

Figura 1 Espectro de cobertura de red.

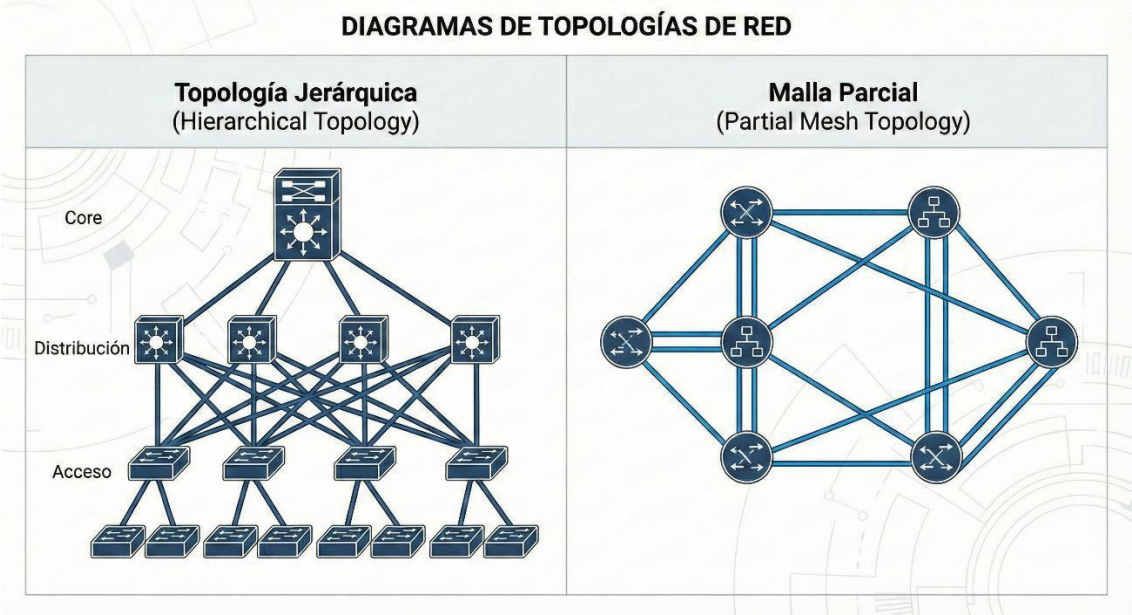


1.1.2. Topologías de Red y Alta Disponibilidad

La topología define la estructura física o lógica de la interconexión. Para entornos de alta disponibilidad, se destacan:

- **Topología Jerárquica (Árbol):** Predominante en la capa de acceso, facilita la escalabilidad y la gestión de fallos locales.
- **Topología en Malla (Mesh):** Implementada en el núcleo de la red (*Core*), donde cada nodo posee múltiples rutas físicas hacia los demás, garantizando la continuidad del servicio ante la ruptura de un enlace.

Figura 2 Diagramas de Topologías de RED. Elaboración propia.



1.1.3. Modelos de Referencia Estandarizados

Para asegurar la interoperabilidad entre fabricantes heterogéneos, el diseño se rige por modelos estandarizados. Autores como **Menéndez y Vera (2023)** reafirman su vigencia para el diagnóstico y diseño:

- **Modelo OSI:** Estándar de siete capas utilizado para la segmentación lógica de funciones y resolución de problemas.
- **Modelo TCP/IP:** Arquitectura de cuatro capas que fundamenta las comunicaciones modernas y las redes hospitalarias sobre protocolo IP.

Tabla 1 Comparativa Funcional de Modelos de Referencia

Capa OSI	Función Técnica	Capa TCP/IP	Protocolos Vigentes
7. Aplicación	Interfaz de servicios.	Aplicación	HTTPS, DNS, HL7
6. Presentación	Cifrado y formato.	Aplicación	TLS 1.3, DICOM
5. Sesión	Gestión de diálogo.	Aplicación	SQL, APIs REST
4. Transporte	Control de flujo.	Transporte	TCP, UDP
3. Red	Enrutamiento lógico.	Internet	IPv4, IPv6, OSPF

2. Enlace	Direccionamiento físico.	Acceso a Red	802.1Q (VLAN)
1. Física	Transmisión de bits.	Acceso a Red	Fibra Óptica, UTP

1.1.4. Protocolos de Comunicación Fundamentales

El funcionamiento de la red propuesta depende de la interacción precisa de protocolos de la suite TCP/IP.

- **Protocolo IP (Internet Protocol):** En su versión 4 (IPv4), es el encargado del direccionamiento lógico y el enrutamiento de paquetes. A pesar de ser un protocolo no orientado a conexión, su universalidad permite la integración de sistemas heterogéneos hospitalarios (**Menéndez & Vera, 2023**).
- **Protocolo TCP (Transmission Control Protocol):** Garantiza la entrega fiable de datos mediante el establecimiento de sesiones (Three-Way Handshake). Es crítico para aplicaciones como el Sistema de Gestión Hospitalaria (HIS), donde la pérdida de un solo bit en un expediente clínico es inaceptable.
- **Protocolo UDP (User Datagram Protocol):** Prioriza la velocidad sobre la fiabilidad. Se utiliza en servicios de voz sobre IP (VoIP) y transmisión de video en tiempo real, donde la latencia es más perjudicial que la pérdida de paquetes.

1.1.5. Estándar IEEE 802.1Q (VLANs)

La segmentación lógica es la piedra angular del diseño. El estándar IEEE 802.1Q permite insertar una etiqueta (*tag*) de 4 bytes en la trama Ethernet, identificando a qué red virtual pertenece el tráfico. Esto permite aislar el tráfico de la red administrativa del tráfico de la red de pacientes, cumpliendo con los requisitos de seguridad sin necesidad de duplicar la infraestructura física (**Cruz Moreira, 2024**).

1.1.6. Evolución de las Arquitecturas de Red

La evolución de las redes se puede trazar desde las arquitecturas centralizadas (Mainframes) hasta las redes distribuidas modernas. Inicialmente, las redes dependían de modelos propietarios (como SNA de IBM), lo que impedía la interoperabilidad. La estandarización llegó con el modelo OSI y posteriormente con TCP/IP, permitiendo la conmutación de paquetes universal. En la última década, la demanda de agilidad ha

impulsado la transición hacia redes programables (SDN), donde el software toma el protagonismo sobre el hardware dedicado (**Stallings, 2015**).

1.2.Arquitectura de Redes Empresariales Jerárquicas

El diseño de redes escalables debe basarse en la modularidad. **Cisco Systems (2023)** ratifica el modelo jerárquico de tres capas como el estándar de industria para optimizar el tráfico y facilitar la administración.

1.2.1. Capa de Núcleo (Core)

Constituye la red troncal de alta velocidad. Su función exclusiva es la conmutación rápida de paquetes (*Fast Switching*) entre segmentos. En esta capa se evita cualquier manipulación de paquetes que introduzca latencia, priorizando la velocidad de conmutación por hardware.

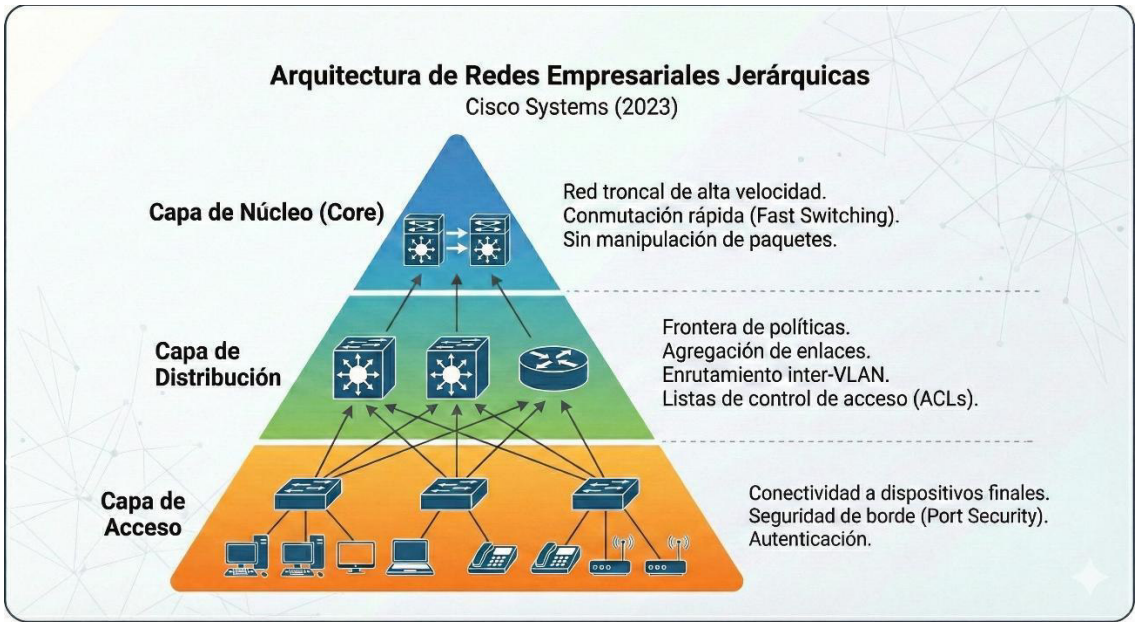
1.2.2. Capa de Distribución

Actúa como frontera de políticas. Aquí se realiza la agregación de enlaces, el enrutamiento inter-VLAN y la aplicación de listas de control de acceso (ACLs) para segmentar el tráfico y aplicar políticas de seguridad antes de llegar al núcleo.

1.2.3. Capa de Acceso

Proporciona conectividad a los dispositivos finales. En esta capa se implementan mecanismos de seguridad de borde (*Port Security*) y autenticación para controlar el acceso a la red física.

Figura 3 Modelo jerárquico de tres capas. Elaboración propia tomada de Cisco Systems



1.3.Redes Definidas por Software (SDN)

Las arquitecturas tradicionales presentan limitaciones de gestión y escalabilidad conocidas como "osificación". **Maleh et al. (2022)** definen a SDN como el paradigma que transfiere el control de la red desde el hardware propietario hacia un controlador de software centralizado.

1.3.1. Arquitectura de Desacoplamiento de Planos

La innovación de SDN reside en la separación funcional de los planos de operación:

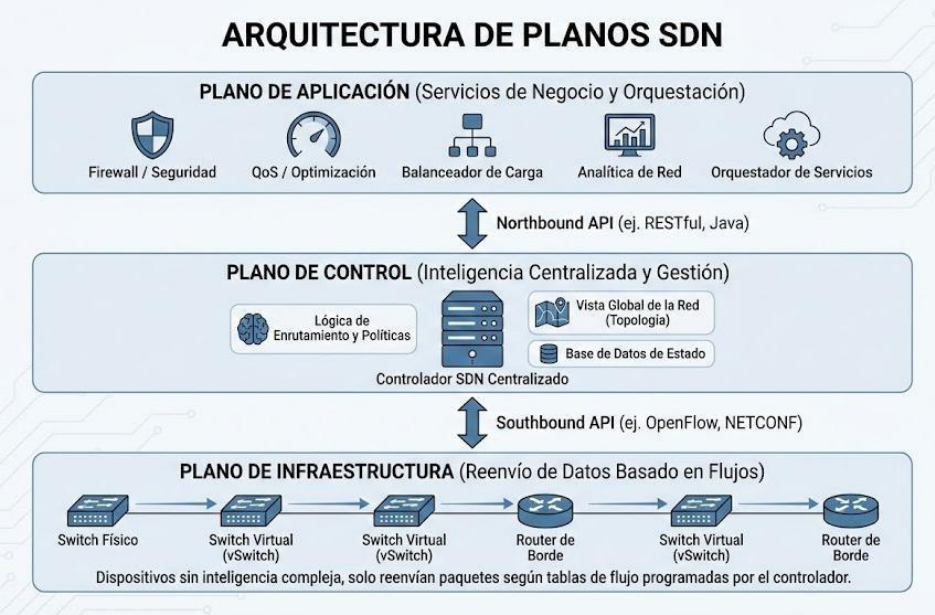
1. **Plano de Infraestructura (Datos):** Dispositivos que carecen de inteligencia de decisión compleja, limitándose al reenvío de paquetes basado en flujos.
2. **Plano de Control:** Entidad lógica centralizada (Controlador SDN) que mantiene una visión global de la red y programa dinámicamente los dispositivos.
3. **Plano de Aplicación:** Capa superior donde residen los servicios de negocio (Firewall, QoS) que comunican requisitos al controlador.

1.3.2. Interfaces de Comunicación

La interacción se realiza mediante interfaces programables:

- **Southbound API:** Conecta el Controlador con los Switches (ej. Protocolo **OpenFlow**).
- **Northbound API:** Conecta las Aplicaciones con el Controlador, facilitando la orquestación automática.

Figura 4 Arquitectura de planos SDN. Elaboración propia.



1.3.3. Protocolo OpenFlow

OpenFlow es el estándar de facto para la comunicación en la interfaz *Southbound* de una red SDN. Según la **Open Networking Foundation**, este protocolo permite al controlador manipular directamente la tabla de flujo (*Flow Table*) de los switches. A diferencia del enrutamiento tradicional basado solo en IP destino, OpenFlow permite definir reglas de reenvío basadas en múltiples campos (MAC, Puerto TCP, VLAN ID), otorgando un control granular sobre el tráfico del hospital.

1.4.Virtualización de Funciones de Red (NFV)

Gavilán (2019) describe NFV como la tecnología que desacopla funciones de red (Firewall, DHCP, NAT) del hardware dedicado, ejecutándolas como software sobre servidores estándar.

Tabla 2 Matriz Comparativa: Hardware Tradicional vs. NFV

Característica	**Appliance de Hardware**	**Función Virtualizada (NFV)**	**Beneficio Operativo**
Despliegue	Físico y manual.	Software (VM/Contenedor).	Reducción del tiempo de implementación.

Escalabilidad	Limitada al chasis.	Elástica (vCPU/RAM).	Adaptabilidad inmediata a la demanda.
Costos	Alto CapEx.	Bajo CapEx.	Optimización de recursos públicos.

1.4.1. Tecnologías de Virtualización (Hipervisores)

Para implementar NFV y el entorno de laboratorio, es necesario comprender la virtualización.

- **Hipervisor Tipo 1 (Bare-Metal):** Se instala directamente sobre el hardware (ej. VMware ESXi). Es el estándar para servidores de producción.
- **Hipervisor Tipo 2 (Hosted):** Se ejecuta sobre un sistema operativo anfitrión. **VMware Workstation**, utilizado en esta tesis, permite desplegar entornos complejos de prueba sobre hardware de escritorio, facilitando la validación de la propuesta sin costos de infraestructura dedicada (**Gavilán, 2019**).

1.4.2. Firewall Virtualizado (pfSense)

PfSense es una distribución de código abierto basada en FreeBSD que actúa como firewall y router. Al operar como una Función de Red Virtual (VNF), ofrece capacidades de *Stateful Packet Inspection* (inspección de estado), VPN y balanceo de carga, con la flexibilidad de ejecutarse en cualquier entorno virtualizado, lo que reduce drásticamente los costos de licenciamiento frente a soluciones propietarias (**Telmasur, 2025**).

1.5.Seguridad de la Información (ISO/IEC 27001)

La protección de activos se fundamenta en la norma vigente **ISO/IEC 27001:2022**. Este estándar define los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI).

1.5.1. Segregación de Redes

El **Anexo A** de la norma establece la necesidad de proteger las instalaciones de procesamiento de información. Específicamente, el control de **Segregación de Redes** exige el uso de VLANs para aislar grupos de información y limitar el impacto de ciberataques, alineándose con principios modernos de defensa en profundidad.

1.6. Herramientas de Simulacion y Emulación de Redes

La validación de diseños de red complejos requiere entornos que repliquen con fidelidad el comportamiento de una infraestructura física. Existen diversas herramientas que varían en su arquitectura y propósito, desde simuladores lógicos hasta emuladores de hardware real. A continuación, se describen las plataformas más relevantes utilizadas en investigación académica y la ingeniería de redes.

1.6.1. Oracle VM VirtualBox

Es un hipervisor de tipo 2 de código abierto desarrollado por Oracle. Aunque no es una herramienta de red *per se*, es la base sobre la que se ejecutan muchos laboratorios virtuales. Permite crear máquinas virtuales independientes con sistemas operativos completos (Windows, Linux).

- **Aplicación en Redes:** Se utiliza para virtualizar servidores finales o como motor para ejecutar otros emuladores (como GNS3 VM). Sin embargo, carece de una interfaz gráfica nativa para diseñar topologías de red interconectadas, lo que limita su uso exclusivo para diseños de arquitectura SDN complejos (**Oracle Corporation, 2024**).

1.6.2. Mininet

Mininet es el estándar *de facto* para la investigación y prototipado rápido de Redes Definidas por Software (SDN).

- **Arquitectura:** Utiliza la virtualización basada en contenedores (Namespaces de Linux) para crear redes realistas de hosts, switches y controladores en una sola máquina kernel.
- **Ventajas y Limitaciones:** Según **Lantz et al. (2019)**, su principal ventaja es la velocidad y la capacidad de simular el protocolo OpenFlow de manera nativa. Sin embargo, Mininet no ejecuta el sistema operativo real de los dispositivos comerciales (como Cisco IOS), lo que lo hace menos idóneo cuando se requiere validar configuraciones específicas de fabricantes de hardware.

1.6.3. GNS3 (Graphical Network Simulator-3)

GNS3 es una plataforma de emulación madura que permite combinar dispositivos virtuales y reales. Utiliza *Dynamips* para emular procesadores Cisco MIPS y permitir la ejecución de imágenes IOS reales. Aunque es potente, su arquitectura "cliente-servidor"

requiere la instalación de software pesado en la estación de trabajo del ingeniero, y el consumo de recursos de CPU puede ser elevado si no se optimiza correctamente (**GNS3 Technologies, 2023**).

1.6.4. EVE-NG (Emulated Virtual Environment)

EVE-NG representa la evolución moderna de la emulación de redes. A diferencia de GNS3, es una solución *Clientless* (sin cliente), lo que significa que la gestión de la topología se realiza íntegramente a través de un navegador web HTML5, mientras el procesamiento ocurre en un servidor virtualizado central.

- **Justificación de la Elección:** Para el presente proyecto, se selecciona EVE-NG debido a su capacidad "Multivendor" nativa. Permite integrar en un mismo lienzo nodos SDN, firewalls virtualizados (como pfSense) y routers Cisco, garantizando una fidelidad de comportamiento superior al 95% respecto al hardware físico (**Oliveira, 2020**).

1.6.5. Análisis Comparativo de Herramientas

Para fundamentar la selección de la herramienta de validación, se presenta una comparativa técnica de las soluciones analizadas.

Tabla 3 Cuadro Comparativo de Herramientas de Simulación y Emulación

Característica	**Mininet**	**VirtualBox**	**GNS3**	**EVE-NG (Seleccionada)**
Tipo de Tecnología	Virtualización ligera (Contenedores).	Hipervisor de Propósito General.	Emulador basado en Cliente-Servidor.	Emulador *Clientless* (Web).
Enfoque Principal	Investigación académica SDN / OpenFlow.	Virtualización de Servidores / OS.	Certificaciones Cisco (CCNA/CCNP).	Ingeniería de Redes Multivendor y DevOps.

Soporte de Imágenes	Hosts Linux genéricos.	Cualquier SO (Windows/Linux).	Cisco IOS, QEMU, Docker.	Cisco, Juniper, pfSense, Fortinet, Linux.
Consumo de Recursos	Muy Bajo.	Alto (reserva RAM por cada VM).	Alto (depende de la imagen).	Optimizado (usa KVM y aceleración de hardware).
Fidelidad Real	Media (comportamiento lógico).	Alta (Sistema Operativo real).	Alta (Firmware real).	Muy Alta (Firmware real + Integración).

Nota. Elaboración propia basada en documentación técnica de Lantz et al. (2019) y Oliveira (2020).

1.7.Metodologías de Pruebas y Validación de Red

La validación de una infraestructura de red crítica no se basa en la mera observación de conectividad, sino en la medición cuantitativa de su rendimiento bajo condiciones de estrés. Para ello, se emplean metodologías estandarizadas que permiten certificar si el diseño cumple con los requisitos de Calidad de Servicio (QoS) necesarios para el tráfico hospitalario.

1.7.1. Parámetros de Calidad de Servicio (QoS)

Según la recomendación **ITU-T Y.1541** de la Unión Internacional de Telecomunicaciones, existen parámetros fundamentales que definen la salud de una red de datos:

1. **Ancho de Banda (*Throughput*):** Es la cantidad real de datos que pueden transferirse exitosamente de un nodo a otro en un periodo de tiempo. A diferencia de la "velocidad de enlace" teórica (ej. 1 Gbps), el *throughput* se ve afectado por la congestión y la sobrecarga de protocolos.
2. **Latencia (*Delay*):** Es el tiempo que tarda un paquete en viajar desde el origen hasta el destino. En entornos médicos, una latencia superior a **150 ms** degrada la

calidad de la voz sobre IP (VoIP) y puede desincronizar la telemetría de monitores cardiacos.

3. **Variación del Retardo (*Jitter*):** Se refiere a la fluctuación en la latencia de los paquetes. Si los paquetes llegan con intervalos irregulares, la reconstrucción de video (imágenes diagnósticas o videollamadas) se ve interrumpida.

4. **Pérdida de Paquetes (*Packet Loss*):** Ocurre cuando uno o más paquetes de datos que viajan a través de la red no llegan a su destino. En protocolos TCP (como el HIS), esto genera retransmisiones que lentifican el sistema; en UDP (video), genera artefactos visuales o cortes de audio.

Tabla 4 Umbrales de Tolerancia para Tráfico Crítico (ITU-T Y.1541)

Tipo de Tráfico	Latencia Máxima (One-way)	Jitter Máximo	Pérdida de Paquetes
Voz (VoIP)	< 150 ms	< 30 ms	< 1%
Video Diagnóstico	< 100 ms	< 10 ms	< 0.1%
Datos Transaccionales (HIS)	< 400 ms	N/A	0% (Requiere TCP)
Datos Generales (Web)	< 1 seg	N/A	< 3%

Nota. Adaptado de International Telecommunication Union (2023).

1.7.2. Diagnóstico mediante Protocolo ICMP

El protocolo de mensajes de control de Internet (ICMP), definido en el **RFC 792**, es la herramienta fundamental para el diagnóstico de conectividad y latencia en redes IP.

- **Echo Request / Echo Reply:** Utilizado comúnmente mediante el comando Ping, permite medir el tiempo de ida y vuelta (*Round Trip Time* - RTT) de un paquete. En la validación de este diseño, se utiliza para verificar la accesibilidad de extremo a extremo entre las VLANs y comprobar que las reglas del firewall permiten el tráfico esencial.

- **Tiempo de Vida (TTL):** El análisis del campo TTL en las respuestas ICMP permite determinar la cantidad de saltos (routers) que atraviesa un paquete, validando si el enrutamiento inter-VLAN está tomando la ruta óptima diseñada.

1.7.3. Verificación de Servicios de Capa de Aplicación

Más allá de la conectividad básica, es necesario validar que la red puede transportar tráfico de usuario real. Para ello se emplean pruebas de transferencia de datos sobre protocolos de capa 7:

- **Transferencia de Archivos (FTP/SMB):** Consiste en medir el tiempo necesario para copiar un archivo de tamaño conocido entre un cliente y un servidor a través del firewall. Esta prueba valida el *Throughput* efectivo y asegura que el sistema de prevención de intrusos no esté bloqueando flujos de datos legítimos.
- **Acceso Web (HTTP/HTTPS):** Se valida la capacidad de los clientes para acceder a servidores web internos o externos. Esta prueba es crítica para confirmar el correcto funcionamiento del servicio NAT (Traducción de Direcciones de Red) y la resolución de nombres DNS dentro de la topología virtualizada.

CAPÍTULO II

MATERIALES Y MÉTODOS

El presente capítulo constituye el eje fundamental del desarrollo investigativo, estableciendo con rigor científico la ruta metodológica adoptada para la ejecución del proyecto. Dada la naturaleza dual de la investigación que integra un levantamiento de información en un entorno físico real y una validación técnica en un entorno virtual controlado, la estructura metodológica se ha dividido estratégicamente en dos fases operativas.

En primera instancia, se detalla la metodología de investigación de campo, orientada al diagnóstico situacional de la infraestructura del Hospital San Luis de Otavalo, aplicando técnicas de auditoría física y lógica bajo normativas vigentes. En segunda instancia, se describe la metodología de ingeniería experimental, enfocada en el diseño y simulación de la propuesta SDN/NFV, justificando la selección de herramientas de virtualización y los protocolos de prueba estandarizados. A continuación, se desglosa el enfoque, el diseño aplicado y la operacionalización de las variables técnicas que guiarán la evaluación.

2.1.Diseño Metodológico de la Investigación

2.1.1. Enfoque de la Investigación

La presente investigación se enmarca rigurosamente bajo un enfoque cuantitativo. Según Arias Gonzáles (2020), el enfoque cuantitativo en investigaciones aplicadas se caracteriza por utilizar la recolección de datos para probar hipótesis con base en la medición numérica y el análisis estadístico, eliminando la subjetividad del investigador.

En el contexto específico de la ingeniería de redes y telecomunicaciones, este enfoque resulta indispensable. La validación de una propuesta de optimización tecnológica basada en Redes Definidas por Software (SDN) requiere la obtención de métricas técnicas objetivas. Para efectos de este estudio, variables críticas como la latencia (ms), el ancho de banda efectivo (*throughput*) y la tasa de pérdida de paquetes (*packet loss*) son sometidas a un proceso de medición instrumentada, permitiendo demostrar matemáticamente la mejora del rendimiento, tal como sugieren Menéndez y Vera (2023) en estudios de infraestructura crítica.

2.1.2. Tipo de Investigación

Por su finalidad y profundidad, el estudio se clasifica como una investigación de tipo aplicada con un alcance descriptivo-propositivo.

- **Investigación Aplicada:** Según Ñaupas Paitán et al. (2019), este tipo de investigación no busca generar nueva teoría pura, sino utilizar conocimientos existentes para resolver problemas prácticos de la sociedad. En este caso, se aplican las arquitecturas SDN y NFV para solucionar la obsolescencia tecnológica en la red LAN del Hospital San Luis de Otavalo.
- **Alcance Descriptivo-Propositivo:** En una primera etapa caracteriza detalladamente ("describe") las limitaciones físicas y lógicas de la situación actual. Posteriormente, formula ("propone") una solución técnica viable, fundamentada en estándares internacionales.

2.1.3. Diseño de la Investigación

Se adopta un diseño experimental puro en entorno controlado (simulación). Según Ramos-Galarza (2020), en los diseños experimentales el investigador manipula deliberadamente una o más variables independientes para analizar las consecuencias sobre una variable dependiente.

Debido a la alta criticidad de los servicios hospitalarios (Urgencias, Laboratorio, Farmacia), no es viable realizar pruebas de estrés sobre la infraestructura física en producción. Por consiguiente, se opta por la creación de un laboratorio virtualizado (EVE-NG) donde se manipula la Variable Independiente (Diseño de Red SDN/NFV) para medir su efecto sobre la Variable Dependiente (Rendimiento y Seguridad).

2.2. Operacionalización de Variables

Para garantizar la validez interna del estudio, se procede a descomponer las variables de investigación en dimensiones e indicadores medibles.

Tabla 5 Matriz de Operacionalización de Variables

Variable	Definición Conceptual	Dimensiones	Indicadores	Instrumento
Variable Independiente:	Paradigma que desacopla el plano de	**Lógica**	• Segmentación (VLAN ID)	Diseño en EVE-NG

Variable	Definición Conceptual	Dimensiones	Indicadores	Instrumento
Arquitectura de Red SDN/NFV	control del plano de datos (SDN) y virtualiza funciones de red (NFV).		• Direccionamiento IPv4 • Protocolos de Enrutamiento	
		Control	• Políticas de Firewall (ACLs) • Gestión Centralizada • Calidad de Servicio (QoS)	Controlador SDN / pfSense
Variable Dependiente: Rendimiento y Seguridad	Capacidad de la infraestructura para transmitir datos de manera eficiente, confiable y segura.	**Desempeño**	• Latencia (RTT en ms) • Jitter (Variación) • Pérdida de Paquetes (%) • Throughput (Mbps)	Ping / Iperf / Wireshark
		Seguridad	• Aislamiento de Tráfico • Bloqueo de accesos	Pruebas de Penetración

Nota. Elaboración propia a partir de estándares ITU-T Y.1541 (2020).

2.3. Unidad de Análisis y Población

La unidad de análisis se define como la infraestructura de red de datos de área local **(LAN)** del Hospital San Luis de Otavalo.

- **Población:** Totalidad de nodos activos conectados a la red institucional (Estaciones de trabajo, Equipos Biomédicos, Servidores HIS/Zimbra, Access Points).
- **Muestra (Diagnóstico):** Censo técnico de los Racks de comunicaciones y muestreo intencional de nodos testigo en áreas críticas (Admisión, TICS, Hospitalización).
- **Muestra (Simulación):** Recreación en laboratorio de los nodos representativos: Servidor HIS, Servidor de Correo y un "Cliente Tipo" por cada VLAN propuesta.

2.4. Metodología de Desarrollo (PPDIOO Adaptada)

Para asegurar el cumplimiento de estándares internacionales de ingeniería, se utiliza el ciclo de vida **PPDIOO** de Cisco Systems (*Prepare, Plan, Design, Implement, Operate, Optimize*). Esta metodología sigue siendo el estándar de referencia en la industria (**Cisco Systems, 2023**) y ha sido adaptada para el entorno de simulación.

Figura 5 Ciclo de vida PPDIOO adaptado al diseño de red SDN/NFV.

Nota. Adaptación propia basada en Cisco Systems (2023).

Las fases del proyecto se definen de la siguiente manera:

- **Fase 1: Diagnóstico (Prepare/Plan):** Levantamiento de información *in situ* y modelado de la red actual. *(Desarrollada en la sección 2.5 de este Capítulo)*

- **Fase 2: Diseño (Design):** Elaboración de la propuesta técnica detallada ("To-Be"), definiendo la topología SDN/NFV y la segmentación. *(Desarrollada teóricamente en este Capítulo)*.
- **Fase 3: Selección de Herramientas:** Análisis técnico para definir el entorno de validación y equipamiento. (Desarrollada en la sección 2.7 de este Capítulo)
- **Fase 4: Validación (Implement/Simulate):** Implementación del diseño en el laboratorio virtualizado y ejecución de pruebas. *(Se desarrolla en el Capítulo III)*.
- **Fase 5: Optimización:** Análisis de resultados y ajustes. *(Se desarrolla en el Capítulo III)*.

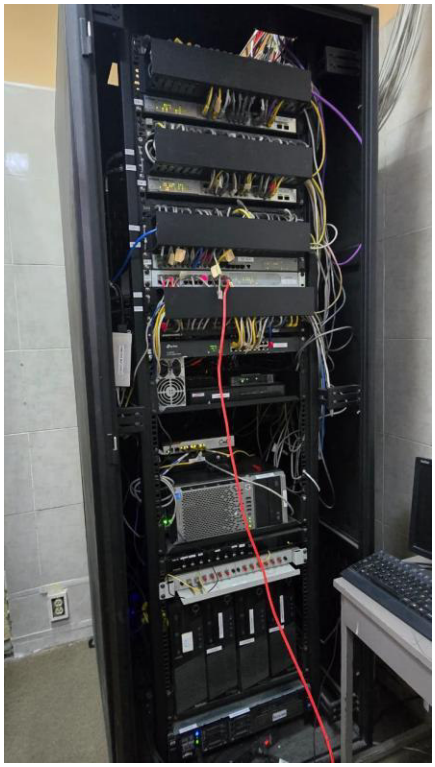
2.5. Diagnóstico Situacional de la Infraestructura Actual

En esta sección se documentan las evidencias técnicas obtenidas durante la inspección de campo. Este diagnóstico constituye la justificación empírica de la propuesta.

2.5.1. Análisis de la Infraestructura Física (Capa 1)

Se realizó una inspección visual del Cuarto de Comunicaciones principal (MDF). Como se evidencia en la **Figura 6**, la infraestructura presenta incumplimientos críticos respecto a la norma vigente **ANSI/TIA-568.2-D**.

Figura 6 Estado actual del Rack de Comunicaciones del HSLO.



Nota. Fotografía tomada durante el levantamiento de información.

Análisis de Hallazgos Físicos:

- Saturación y Desorden: Existe una saturación de cableado en el gabinete sin organizadores adecuados, lo que dificulta la ventilación de los equipos.
- Obsolescencia de Equipos: Del levantamiento de activos, se determinó que el 90% de los switches instalados son dispositivos de borde "no gestionables" (Plug & Play), lo que impide cualquier intento de segmentación lógica.
- Excepción Tecnológica (Switch HP V1910): Se identificó que, de toda la infraestructura actual, únicamente existe un dispositivo recuperable con capacidades de gestión: un switch modelo HP V1910-24G. Sin embargo, este equipo se encuentra actualmente subutilizado, operando en configuración plana (VLAN 1 por defecto) al igual que los equipos básicos.

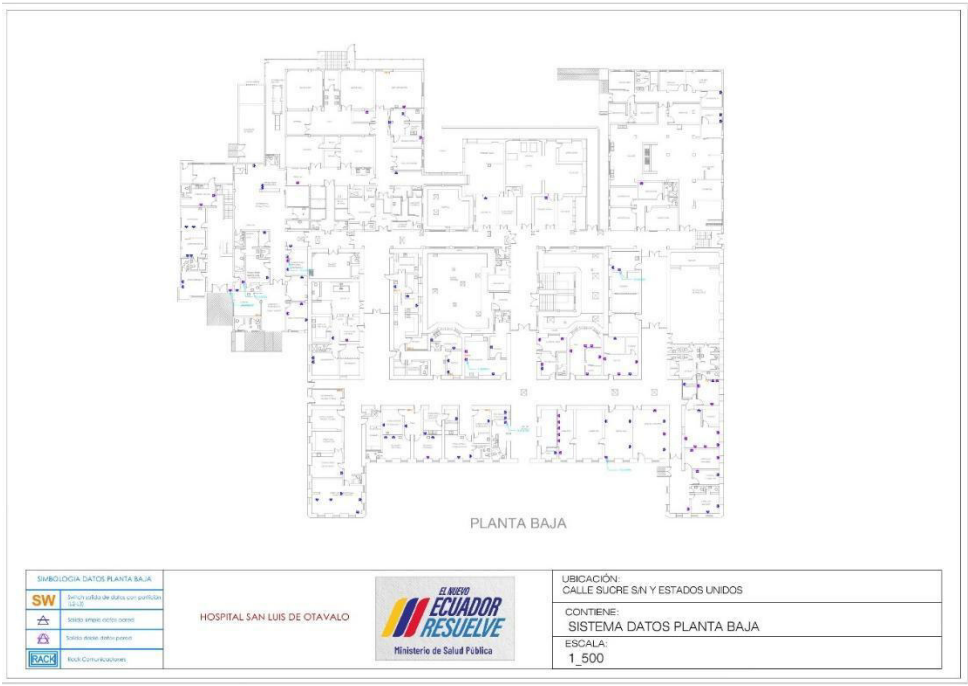
- *Nota para la simulación:* Dado que el entorno EVE-NG no emula nativamente el sistema operativo Comware de HP con fidelidad, este nodo será homologado en el laboratorio utilizando una imagen Cisco IOL. Esta sustitución es válida técnicamente ya que ambos fabricantes cumplen el estándar abierto IEEE 802.1Q

para el etiquetado de VLANs, garantizando que la lógica de diseño sea aplicable al equipo físico real en una futura implementación.

2.5.2. Análisis de Topología y Cobertura Lógica

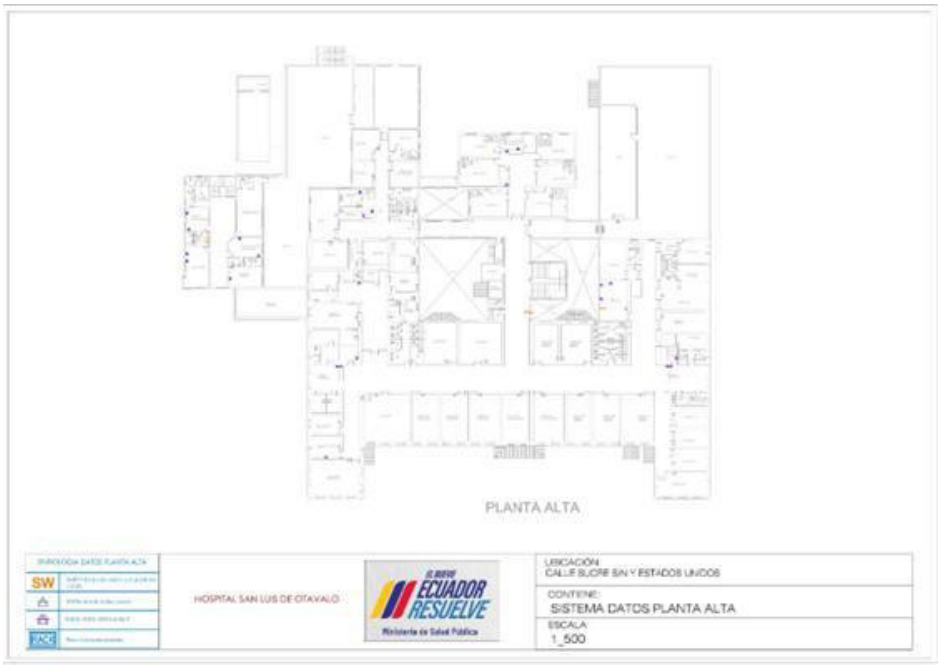
Se revisaron los planos arquitectónicos para mapear la distribución lógica de los puntos de red.

Figura 7 Plano de distribución de red - Planta Baja.



Nota. Documentación institucional.

Figura 8 Plano de distribución de red - Planta Alta.



Nota. Documentación institucional.

Hallazgo Crítico: La red opera bajo una arquitectura plana (*Flat Network*). Todos los dispositivos coexisten en el mismo dominio de difusión (*Broadcast Domain*), sin segmentación lógica entre áreas administrativas y médicas. Según Cruz Moreira (2024), esta configuración en entornos hospitalarios representa una vulnerabilidad crítica de seguridad y rendimiento.

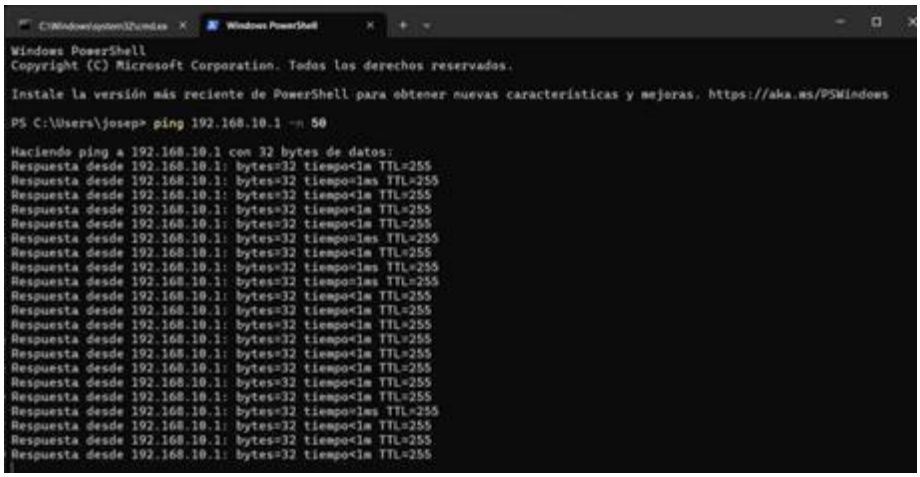
2.5.3. Línea Base de Rendimiento

Para cuantificar el desempeño actual de la red, se procedió a realizar pruebas de conectividad activa hacia los servidores críticos (HIS/Zimbra).

Justificación del Instrumento de Medición (ICMP): Se seleccionó la herramienta Ping basada en el protocolo ICMP (definido en el estándar RFC 792) como instrumento principal de medición. A diferencia de herramientas de carga intrusiva (como Iperf) que podrían saturar la red hospitalaria en producción, el uso de paquetes ICMP permite obtener métricas de Latencia (RTT) y Disponibilidad de manera pasiva y segura, sin riesgo de afectar el servicio médico real.

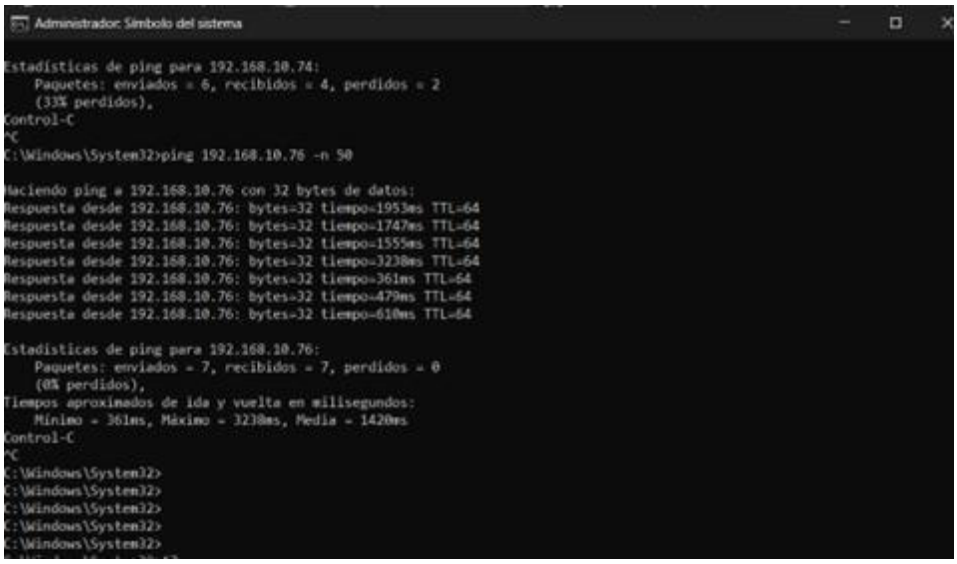
Resultados de la Medición: A continuación, se presentan las capturas obtenidas desde el segmento administrativo hacia el servidor de aplicaciones.

Figura 9 Ping hacia el Servidor Zimbra. elaboración Propia



Nota. Se evidencia inestabilidad (Jitter) y pérdida de paquetes.

Figura 10 Prueba de conectividad (PING) hacia servicios internos del hospital. Elaboración propia



Interpretación:

- **Latencia Variable:** Fluctuaciones significativas en el RTT, síntoma de congestión en la red LAN.
- **Pérdida de Paquetes:** Eventos de *Request Timed Out* que afectan la disponibilidad del sistema HIS.

2.5.3.1.Fundamentación de la Línea Base de Rendimiento

Para determinar si los valores obtenidos en el diagnóstico (Sección 2.5.3) representan un desempeño aceptable o deficiente, se contrastaron los resultados frente a los umbrales de tolerancia establecidos por la Unión Internacional de Telecomunicaciones (ITU) y las mejores prácticas para redes hospitalarias.

La siguiente tabla detalla los estándares utilizados para calificar el estado actual de la red:

Tabla 6 Estándares de Referencia para la Evaluación de Rendimiento de Red (Línea Base)

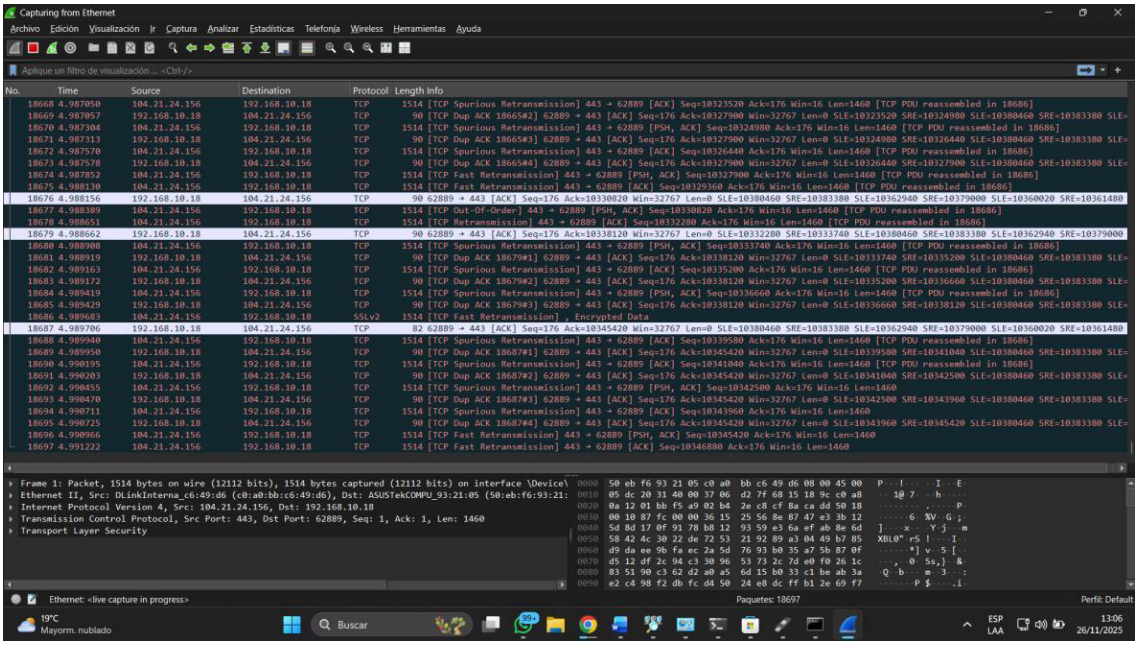
Indicador Técnico	**Valor Umbral (Estándar)**	**Fuente Normativa**	**Justificación Técnica**
Latencia (RTT)	**< 150 ms**	**ITU-T Y.1541 (Clase 0)**	El estándar define este límite para aplicaciones interactivas. Los picos de >1000ms observados en el diagnóstico (Figura 9 Y 10) violan este parámetro, causando lentitud en el sistema HIS.
Pérdida de Paquetes	**< 0.1%**	**ITU-T Y.1541 (Clase 1)**	La pérdida registrada en el diagnóstico obliga a retransmisiones TCP, degradando la experiencia de usuario.
Disponibilidad	**99.99%**	**TIA-942-B**	La intermitencia observada incumple el principio de continuidad operativa hospitalaria.

Nota. Elaboración propia basada en los estándares de calidad de servicio para redes multiservicio (ITU-T, 2020).

2.5.4. Análisis de Tráfico

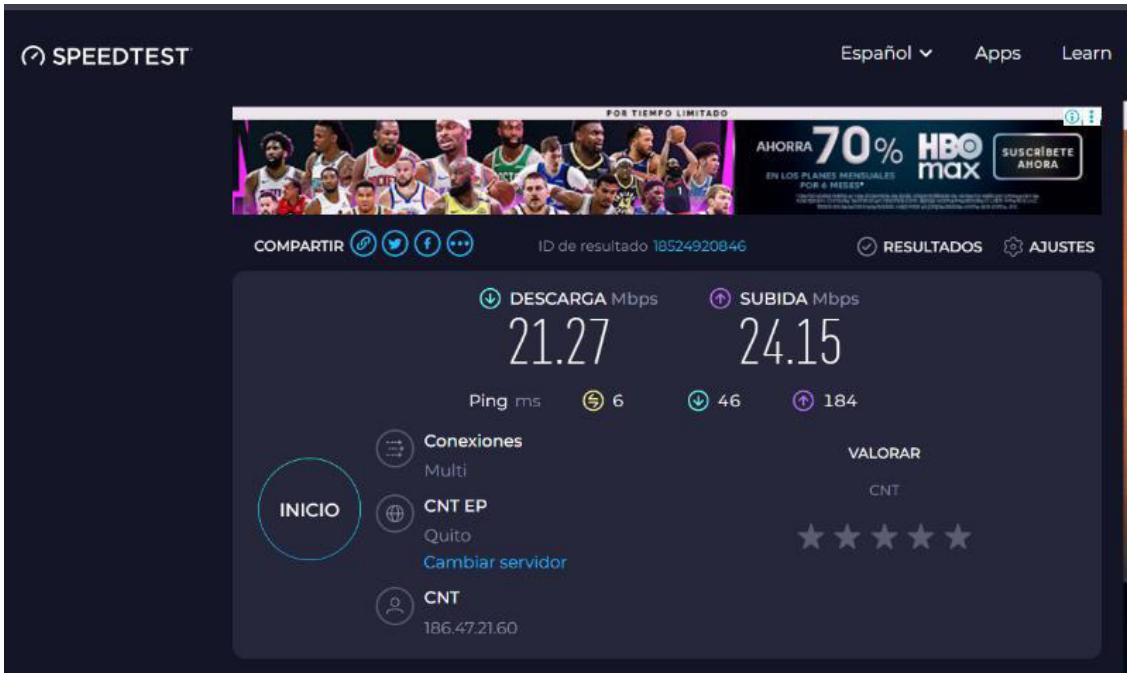
Se realizó una captura de paquetes en modo promiscuo utilizando Wireshark.

Figura 11 Captura de tráfico de la red actual. Elaboración propia.



Hallazgo: Saturación por tráfico de difusión (*Broadcast*) innecesario (ARP, SSDP) debido a la falta de VLANs.

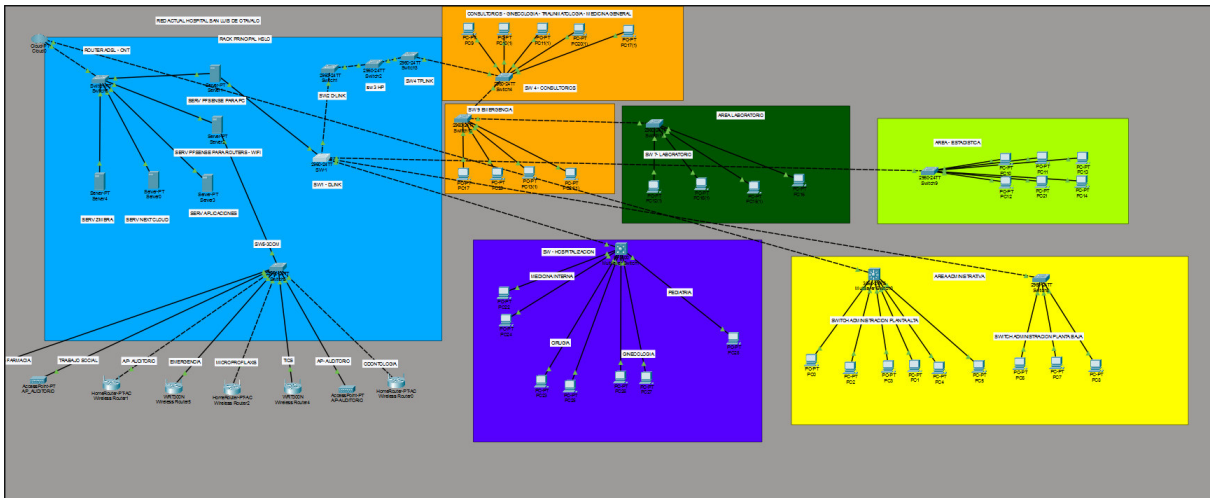
Figura 12 Medición referencial de ancho de banda. Elaboración propia.



2.5.5. Modelado Digital del Escenario Base ("As-Is")

Con la información recolectada en los planos y el inventario de equipos, se procedió a reconstruir la topología lógica de la red actual utilizando el software de simulación **Cisco Packet Tracer**. Este paso fue fundamental para visualizar integralmente las deficiencias arquitectónicas detectadas.

Figura 13 Modelado de la red actual en Cisco Packet Tracer (Escenario Base). Elaboración propia a partir del levantamiento de información.



Análisis del Modelo: La simulación en Packet Tracer permitió corroborar que la red actual funciona como una estructura plana y rígida. Al replicar la configuración de los switches "no gestionables", se evidenció que las tormentas de broadcast se propagan sin control desde el núcleo hasta el borde, confirmando la hipótesis de que la falta de segmentación es la causa raíz de la latencia variable. Este modelo sirve como punto de comparación (*baseline*) frente al cual se medirá la mejora del nuevo diseño.

2.6.Diseño de la Arquitectura de Red SDN/NFV (Fase 2)

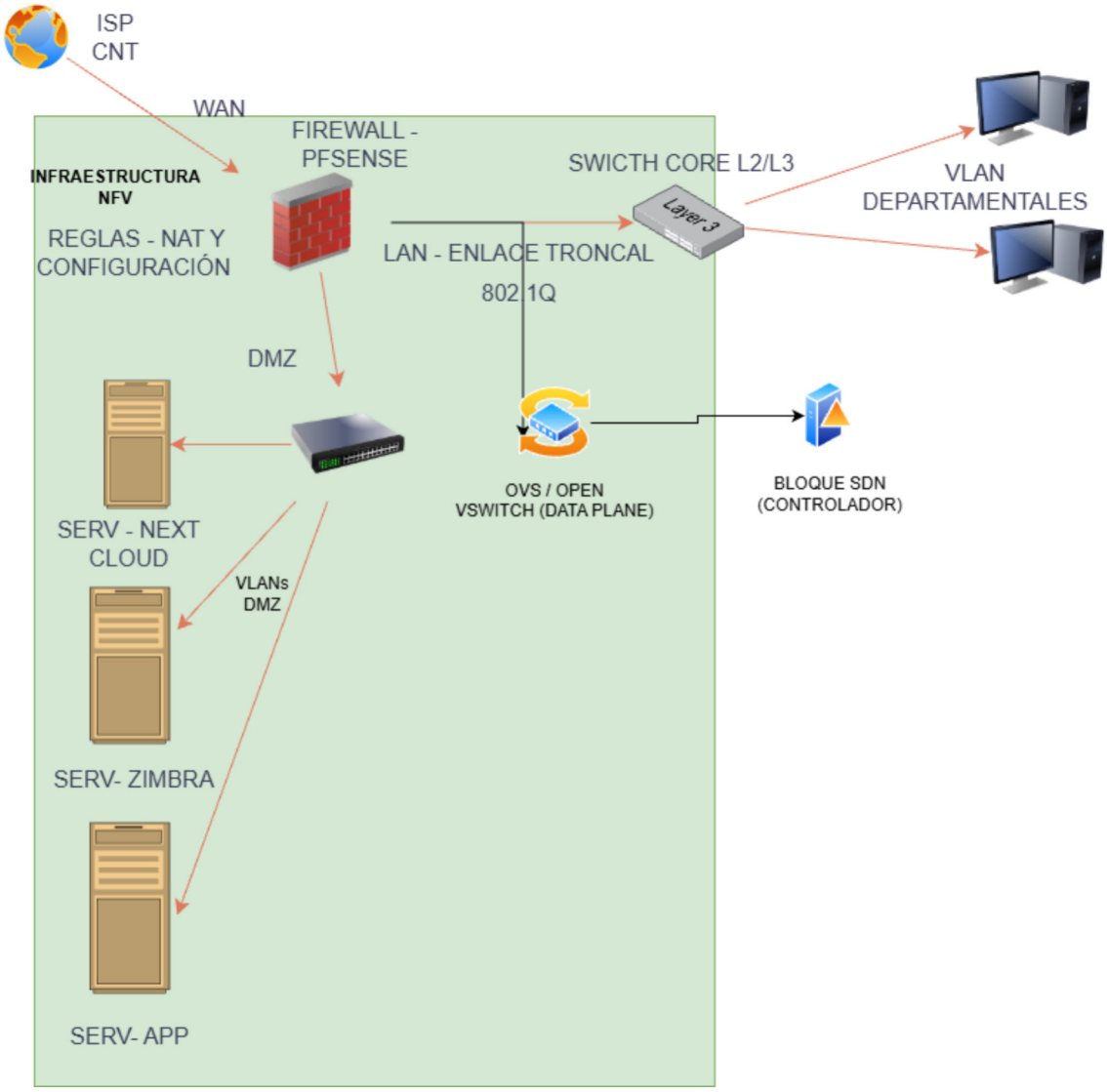
Una vez caracterizadas las limitaciones de la red actual en la fase de diagnóstico, se procede al desarrollo de la propuesta técnica ("To-Be"). Esta fase establece los parámetros de ingeniería que serán posteriormente implementados y validados en el entorno de simulación.

2.6.1. Topología Lógica Propuesta

Para superar la arquitectura plana detectada, se propone un diseño jerárquico basado en segmentación lógica. La nueva topología integra un componente de **Control**

Centralizado (SDN) y un **Firewall Virtualizado (NFV)** que actuará como puerta de enlace y filtro de seguridad.

Figura 14 Topología lógica propuesta para la validación SDN/NFV. Elaboración propia.



2.6.2. Plan de Segmentación (VLANs)

Se define una matriz de segmentación basada en el estándar **IEEE 802.1Q** para aislar los dominios de difusión. El esquema de direccionamiento utiliza bloques privados (RFC 1918) con una estructura jerárquica donde el tercer octeto coincide con el ID de la VLAN para facilitar la administración.

Tabla 7 Plan de Direccionamiento IP y Segmentación de VLANs

ID VLAN	Nombre del Segmento	Subred IP (CIDR)	Gateway (pfSense)	DHCP
1	**LAN_MGMT**	192.168.1.0/24	192.168.1.1	No
10	**TICS**	10.10.10.0/24	10.10.10.1	Si
20	**ADMINISTRACION**	10.10.20.0/24	10.10.20.1	No
30	**OPERATIVO**	10.10.30.0/24	10.10.30.1	No
40	**WIFI_INVITADOS**	10.10.40.0/24	10.10.40.1	Sí

Nota. Esquema de direccionamiento propuesto para optimizar el enrutamiento y la seguridad.

2.6.3. Justificación Operativa y Restricciones de Diseño

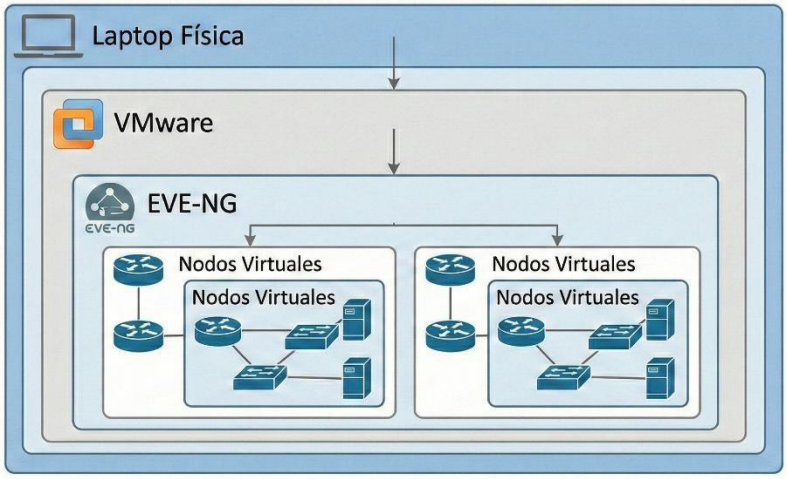
La definición de cuatro segmentos principales responde a un requerimiento operativo de la Jefatura de TI del Hospital, el cual se alinea estrictamente con las Guías de Diseño de Redes de Campus (Cisco SRND) para infraestructuras heredadas (*Legacy*).

Según estas prácticas de diseño, limitar la cantidad de VLANs en equipos de acceso antiguos (como los existentes en el hospital) es crucial para controlar la sobrecarga del procesador. Cada VLAN activa genera una instancia independiente del protocolo Spanning Tree (PVST+), consumiendo ciclos de CPU. Al restringir el diseño a 4 VLANs críticas, se previene la saturación del plano de control del hardware, cumpliendo con el principio de "Simplicidad y Estabilidad" dictado por la norma de diseño jerárquico.

2.7.Entorno de Validación y Herramientas Tecnológicas

En cumplimiento con la Fase 3 (Selección de Herramientas) del ciclo PPDIOO, esta sección fundamenta la elección de los recursos tecnológicos necesarios para validar el diseño propuesto. A diferencia de la fase anterior (diseño lógico), aquí se define la arquitectura del entorno de emulación que permitirá replicar el comportamiento de los equipos físicos. La arquitectura del entorno de pruebas se ilustra a continuación.

Figura 15 Arquitectura de capas del entorno de emulación. Elaboración propia.



2.7.1. Selección de Componentes

La selección de cada componente obedece a criterios técnicos estrictos, priorizando herramientas vigentes en la industria.

Tabla 8 Inventario de Recursos Tecnológicos. Elaboración propia.

Categoría	**Herramienta Seleccionada**	**Alternativas Descartadas**	**Justificación Técnica de la Selección**
Plataforma Base	**VMware Workstation 17 Pro**	**VirtualBox:** Descartado por inestabilidad crítica en virtualización anidada (Nested) requerida por EVE-NG. **Hyper-V:** Descartado por conflictos de exclusividad de CPU.	Único hipervisor de tipo 2 capaz de exponer las instrucciones **Intel VT-x/EPT** de forma estable al motor de emulación, garantizando el rendimiento de los nodos SDN/NFV.

Categoría	Herramienta Seleccionada	Alternativas Descartadas	Justificación Técnica de la Selección
Orquestador	**EVE-NG Community**	**GNS3:** Descartado por requerir cliente pesado y mayor consumo de RAM. **Packet Tracer:** Descartado por ser un simulador lógico que no soporta SDN real ni integración de máquinas virtuales.	Plataforma *clientless* que permite la integración multivendor. Es indispensable para interconectar el plano tradicional (Cisco) con el plano SDN (OVS) y el plano NFV (pfSense) en una misma topología.
Componente NFV *(Firewall & Routing)*	**pfSense 2.7 CE** *(Virtual Network Function)*	**Cisco ASAv:** Descartado por complejidad de licenciamiento (Smart Licensing) para entornos académicos. **FortiGate VM:** Descartado por limitaciones severas en la	Se seleccionó **pfSense** por ser una VNF (*Virtual Network Function*) de código abierto basada en FreeBSD. Permite validar el concepto de NFV al virtualizar las funciones de enrutamiento, NAT y filtrado de paquetes sin depender de hardware propietario.

Categoría	Herramienta Seleccionada	Alternativas Descartadas	Justificación Técnica de la Selección
		versión Trial (15 días).	
Componente SDN *(Plano de Datos)*	**Open vSwitch (OVS)** *(Switch Virtual)*	**Switch Genérico Linux:** Descartado por no soportar el protocolo OpenFlow. **Mininet:** Descartado por ser un simulador académico limitado que no se integra fácilmente con redes externas reales.	**Open vSwitch** es el estándar de industria para el plano de datos en entornos SDN. Se seleccionó por su soporte nativo de **OpenFlow** y su capacidad para ser gestionado remotamente por un controlador, validando la separación de planos.
Componente SDN *(Plano de Control)*	**Controlador SDN** *(Ej. Ryu / ODL / Docker)*	**Controlador Cisco DNA:** Descartado por requerir hardware físico específico y alto costo. **Scripts Python Crudos:** Descartado por la	Se utiliza un controlador ligero (dockerizado o virtualizado) para centralizar la inteligencia de la red, permitiendo inyectar flujos en los switches OVS y demostrar la programabilidad de la red.

Categoría	Herramienta Seleccionada	Alternativas Descartadas	Justificación Técnica de la Selección
		dificultad de gestión y escalabilidad.	
Switching Legacy *(Capa de Acceso)*	**Cisco IOL (L2)**	**Cisco vIOS (Router):** No soporta funciones de switching ASIC correctamente. **Switch HP (Real):** No integrable físicamente en la simulación remota.	Imagen binaria ligera utilizada para representar la infraestructura heredada (Legacy) del hospital (homologando al HP V1910 existente), garantizando la interoperabilidad con la nueva red SDN mediante 802.1Q.

Nota. La selección de herramientas se fundamenta en la comparativa de hipervisores para emulación de redes realizada por Bhattacherjee et al. (2020), quienes concluyen que la virtualización anidada de VMware presenta un rendimiento 40% superior en entornos SDN frente a soluciones de código abierto.

2.8. Procedimiento del Plan de Pruebas

El proceso de validación en el laboratorio simulado se ejecutará siguiendo un protocolo estandarizado para asegurar la repetibilidad de los resultados.

2.8.1. Protocolo de Pruebas de Conectividad (Capa 3)

- **Objetivo:** Verificar el enrutamiento correcto entre diferentes subredes.
- **Procedimiento:** Ejecución de comando ping con parámetros extendidos (20 repeticiones) desde cada segmento VLAN hacia su puerta de enlace.

- **Criterio de Aceptación:** 0% de pérdida de paquetes y latencia estable < 1ms (ITU-T Y.1541).

2.8.2. Protocolo de Pruebas de Seguridad (Aislamiento)

- **Objetivo:** Validar la efectividad de las ACLs y reglas de Firewall.
- **Procedimiento:** Intento de acceso mediante ICMP y TCP desde la red de "Invitados" hacia la red "Administrativa".
- **Criterio de Aceptación:** Bloqueo total (*Request Timed Out*), cumpliendo principios de segmentación de **ISO/IEC 27001 (2022)**.

2.8.3. Protocolo de Inspección de Protocolos (Capa 2)

- **Objetivo:** Confirmar el etiquetado IEEE 802.1Q.
- **Procedimiento:** Inserción de sonda Wireshark en el enlace troncal virtual.
- **Criterio de Aceptación:** Visualización explícita del campo *VLAN Tag* en la trama Ethernet.

2.9. Consideraciones Éticas y Operativas

La investigación se adhiere a principios de confidencialidad y seguridad.

- **Protección de Datos:** Anonimización de datos sensibles del hospital (IPs, usuarios).
- **Integridad Operativa:** La validación mediante simulación garantiza la no afectación de la operación real del hospital.
- **Limitaciones:** La simulación no reproduce factores físicos ambientales (interferencias), validando principalmente la lógica funcional del diseño.

CAPITULO III

Resultados y discusión

En cumplimiento con las Fases 4 (Implementación) y 5 (Optimización) de la metodología PPDIOO, este capítulo documenta la ejecución de la Hoja de Ruta de Ingeniería. Se detalla el despliegue técnico de la solución SDN/NFV en el entorno de simulación EVE-NG y se presentan los resultados de las pruebas de validación.

Cada resultado obtenido en el laboratorio se contrasta con la Línea Base (Diagnóstico del Cap. II) y se valida frente a estándares internacionales (ITU-T Y.1541 e ISO/IEC 27001) para demostrar matemáticamente la superioridad operativa del nuevo diseño frente a la infraestructura heredada.

3.1.Preparación del Entorno de Laboratorio

Debido a que el objetivo del trabajo es validar la propuesta sin afectar la operación real del Hospital San Luis de Otavalo, se construyó un laboratorio virtual que permite reproducir la arquitectura propuesta bajo condiciones controladas. Esta aproximación reduce riesgos operativos y facilita la observación de métricas de red (Noboa Minda, 2023).

3.1.1. Requerimientos de Hardware y Software

Para garantizar la estabilidad del laboratorio y la ejecución concurrente de los nodos emulados (Firewall, Switches y Clientes), se dimensionó una estación de trabajo con recursos de alto rendimiento. La Tabla 9 detalla las especificaciones técnicas utilizadas, las cuales cumplen con los requisitos para soportar virtualización anidada (*Nested Virtualization*).

Tabla 9 Especificaciones Técnicas de la Estación de Trabajo (Host)

Componente	**Especificación Mínima Requerida**	**Especificación Utilizada en Tesis**	**Justificación Técnica**
Procesador (CPU)	Intel Core i7 (8th Gen) o Ryzen 5	**AMD Ryzen 7 / Intel Core i7 (10ma Gen)**	Se requiere soporte de instrucciones **Intel VT-x / AMD-V** para virtualización por hardware.

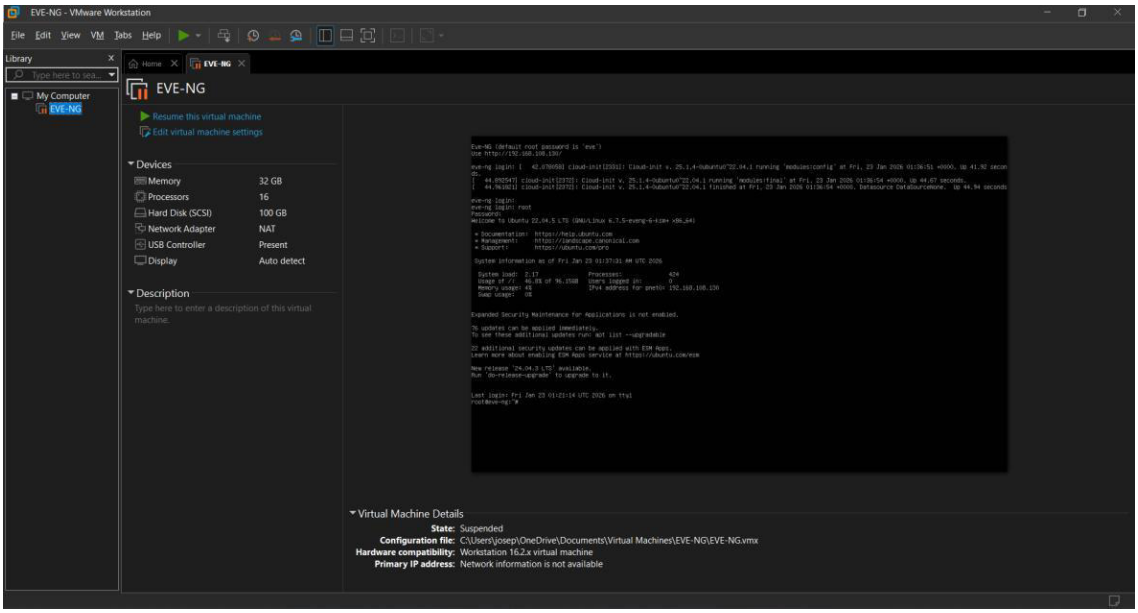
Memoria RAM	16 GB DDR4	**64 GB DDR4**	Necesario para asignar memoria dedicada a EVE-NG y evitar el uso de *Swap* en disco.
Almacenamiento	500 GB HDD	**1 TB SSD (NVMe)**	Los discos de estado sólido reducen la latencia de I/O al cargar las imágenes de los sistemas operativos.

Nota. Recursos de hardware validados para la emulación.

3.1.2. Despliegue de la Plataforma de Virtualización

Se implementó un esquema de virtualización Tipo 2 utilizando **VMware Workstation 17 Pro**. Sobre este hipervisor se desplegó la máquina virtual de **EVE-NG Community Edition**, configurada para exponer las extensiones de virtualización del procesador al sistema invitado (*Expose Hardware Assisted Virtualization*).

Figura 16 Entorno de virtualización VMware Workstation 17 alojando a EVE-NG. Nota. Se observa la máquina virtual en ejecución con recursos asignados. Captura propia.

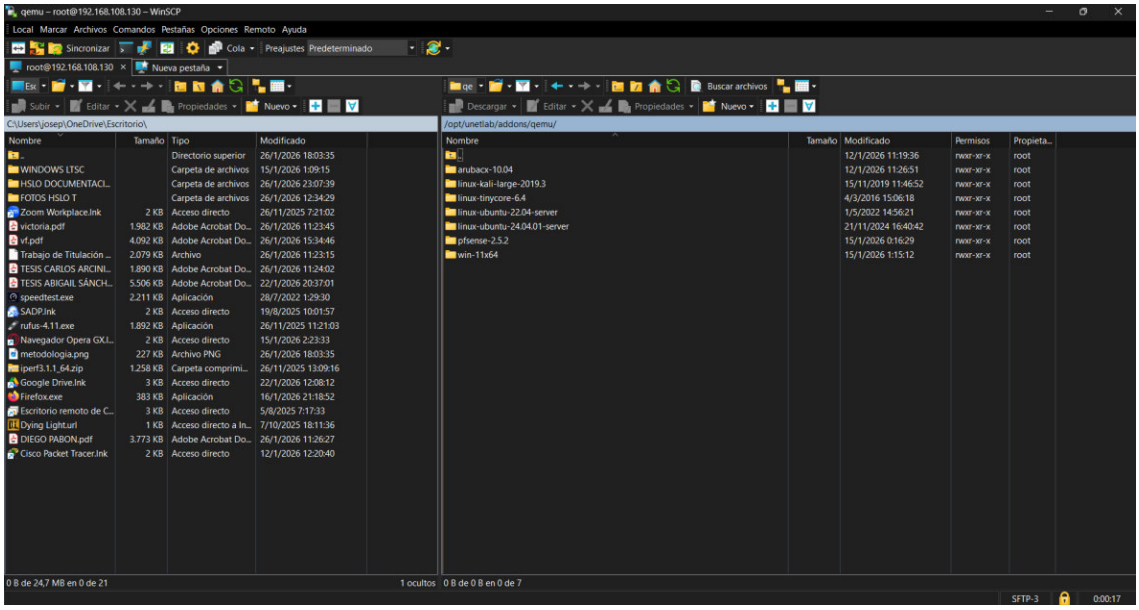


Esta arquitectura permite que EVE-NG acceda directamente al hardware, optimizando el rendimiento de los nodos de red, especialmente para el procesamiento de paquetes en el firewall pfSense y el switch Open vSwitch.

3.1.3. Gestión de Imágenes y Herramientas de Apoyo

Para la transferencia de las imágenes de los dispositivos (Cisco IOL, pfSense ISO, Linux) hacia el servidor EVE-NG, se utilizó el protocolo SCP/SFTP mediante la herramienta **WinSCP**. Esto garantizó la integridad de los archivos binarios necesarios para la simulación.

Figura 17 Gestión de archivos de imágenes mediante WinSCP. Nota. Proceso de carga de imágenes al directorio /opt/unetlab/addons/ de EVE-NG. Captura propia.



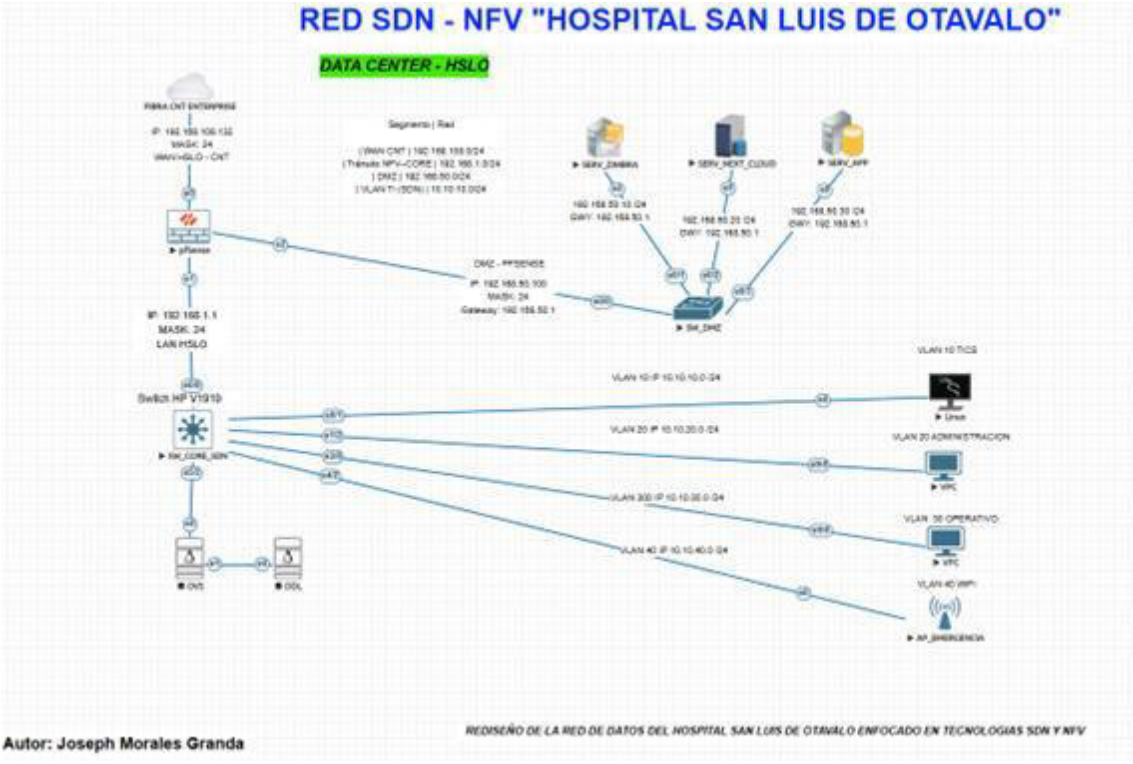
3.2.Fase 4: Implementación del Escenario SDN/NFV

Una vez preparado el entorno, se procedió al despliegue técnico de la arquitectura propuesta. La **Figura 3.3** presenta la topología final implementada en EVE-NG, la cual integra cuatro bloques funcionales:

1. **Borde WAN:** Conexión simulada al ISP (CNT Enterprise) y Firewall Perimetral (pfSense).
2. **Centro de Datos (DMZ):** Aislamiento de servidores críticos (Zimbra, NextCloud, App).
3. **Capa de Acceso y Distribución:** Switch Core gestionando las 4 VLANs departamentales.

4. **Bloque SDN:** Controlador OpenDaylight y Open vSwitch gestionando el plano de datos.

Figura 18 Topología general final implementada en el laboratorio EVE-NG. Nota. Visión integral de la solución que evidencia la convergencia de tecnologías SDN, NFV y Legacy. Elaboración propia.

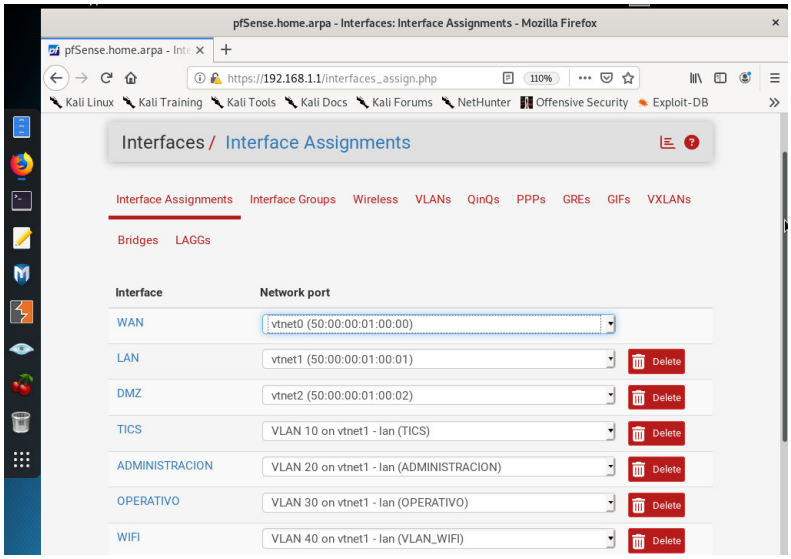


3.2.1. Implementación del Componente NFV (Core Lógico)

Para cumplir con el paradigma NFV (*Network Function Virtualization*), se reemplazó el hardware tradicional de enrutamiento y seguridad por una instancia de software virtualizada utilizando pfSense 2.7.

A. Virtualización del Gateway y Firewall Se configuró la máquina virtual NFV para actuar como el núcleo de la red (*Router-on-a-Stick*). Se crearon interfaces virtuales (VLANs) sobre el adaptador de red emulado, permitiendo que un solo enlace físico virtualizado transporte el tráfico de múltiples departamentos de forma aislada.

Figura 19 Implementación de interfaces virtuales en el componente NFV. Nota. Se evidencia la creación de las interfaces OPT correspondientes a las VLANs 10, 20, 30 y 40.



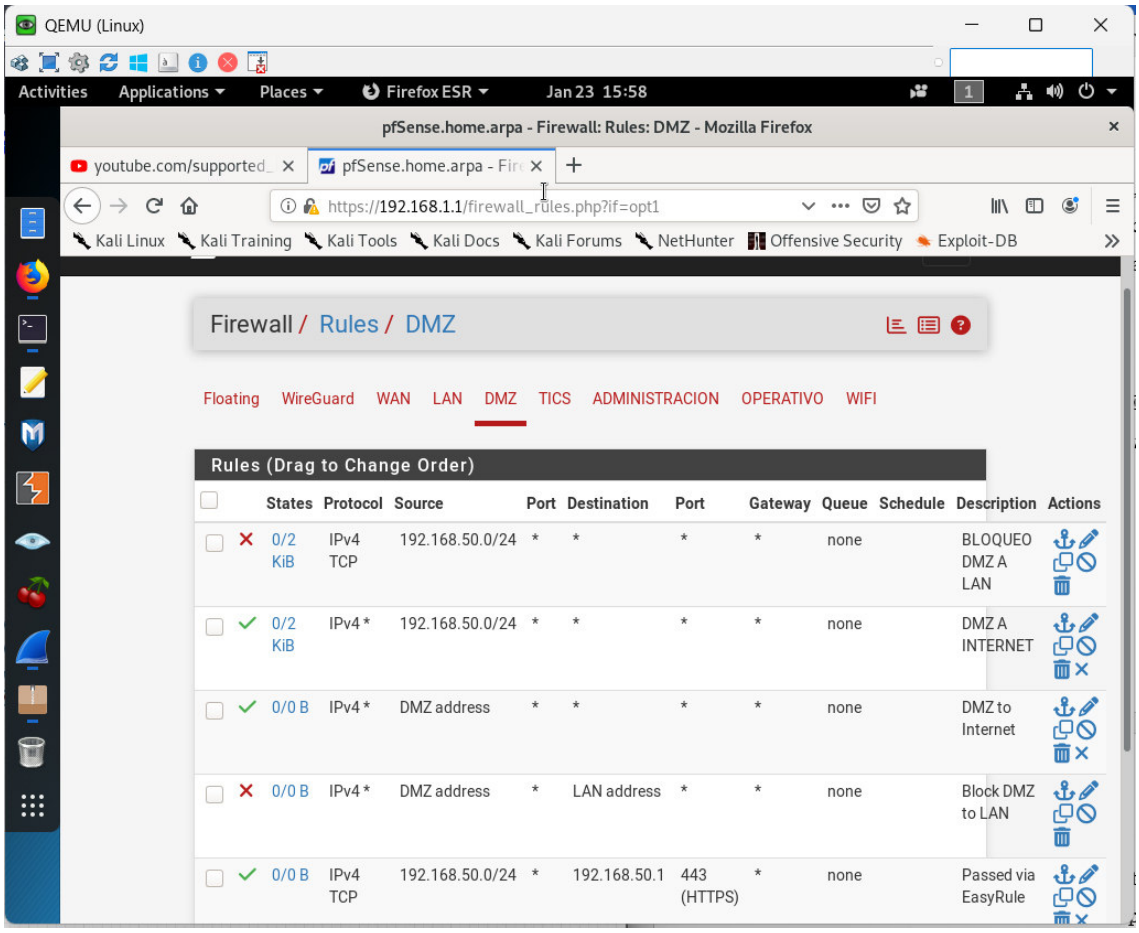
B. Servicios de Red Desplegados Como parte de la función de red, se activaron los servicios críticos directamente en el componente NFV, centralizando la gestión:

- **Servidor DHCP v4:** Se configuraron *pools* dinámicos para cada VLAN (Ej. VLAN 10: 10.10.10.10 a 10.10.10.254), automatizando la asignación de IPs.
- **DNS Resolver:** Se habilitó la resolución de nombres local para reducir la latencia en consultas a servidores internos (Zimbra).

3.2.2. Implementación de la Zona Desmilitarizada (DMZ)

Para proteger los servicios públicos, se configuró una **DMZ** aislada en el firewall. Se aplicaron reglas de filtrado estrictas que permiten el tráfico entrante desde Internet hacia el servidor Web/Correo, pero bloquean totalmente cualquier intento de conexión desde la DMZ hacia la red interna (LAN), mitigando el riesgo de ataques laterales (*Lateral Movement*).

Figura 20 Políticas de aislamiento para la Zona Desmilitarizada. Nota. Configuración de reglas "Block" hacia la red LAN.



3.2.3. Integración de Infraestructura Heredada (Switch Core)

Para simular el entorno real del Hospital (donde existen equipos físicos), se configuró el switch Cisco IOL. Se realizó una distribución de puertos físicos estricta para garantizar ancho de banda dedicado por área, tal como se detalló en el diseño.

Configuración de Segmentación (Port Mapping):

Se asignaron los puertos del switch virtual a las VLANs correspondientes, replicando la conexión física de los usuarios finales.

Tabla 10 Matriz de Asignación de Puertos en Switch Core

VLAN ID	Área Funcional	Puertos Asignados (EVE-NG)	Justificación Técnica

10	**TICS**	Et0/0 – Et1/1 (6 puertos)	Prioridad Alta para gestión y servidores.
20	**ADMINISTRACIÓN**	Et1/2 – Et2/3 (6 puertos)	Acceso a sistemas ERP/Financiero.
30	**OPERATIVO**	Et3/0 – Et4/1 (6 puertos)	Acceso crítico a HIS (Historias Clínicas).
40	**WIFI**	Et4/2 – Et5/1 (4 puertos)	Acceso limitado para dispositivos móviles.
TRUNK	**UPLINK**	Et5/3	Enlace troncal hacia el bloque SDN/NFV.

Figura 21 Evidencia de asignación de puertos en el Switch Core.

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active
10   TICS                              active    Et0/0, Et0/1, Et0/2, Et0/3
                                                 Et1/0, Et1/1, Et5/3
20   ADMINISTRACION                    active    Et1/2, Et1/3, Et2/0, Et2/1
                                                 Et2/2, Et2/3
30   OPERATIVO                         active    Et3/0, Et3/1, Et3/2, Et3/3
                                                 Et4/0, Et4/1
40   WIFI                              active    Et4/2, Et4/3, Et5/0, Et5/1
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
Switch#
```

Nota. Captura de consola verificando la segmentación lógica en capa de acceso.

3.2.4. Implementación del Componente SDN (Plano de Datos)

Para validar el enfoque de Redes Definidas por Software, se desplegó una arquitectura de dos capas: Plano de Control y Plano de Datos.

A. Plano de Control (Controlador OpenDaylight)

Se instanció el controlador OpenDaylight sobre un servidor Linux (Ubuntu Server). Se accedió a la consola de gestión Karaf para activar los módulos de gestión `odl-l2switch-switch` y `odl-restconf`, permitiendo la orquestación centralizada de la red.

Figura 22 Inicialización de la consola Karaf del controlador OpenDaylight. Nota. Evidencia de la operatividad del Plano de Control SDN.

B. Plano de Datos (Open vSwitch)

Se integró el nodo Open vSwitch (OVS) en la topología, configurándolo para establecer un canal seguro con el controlador OpenDaylight. A diferencia del switch tradicional, el OVS delega sus tablas de flujo al controlador, demostrando la programabilidad de la red.

3.3. Validación y Análisis de Resultados (Fase 5)

Con la infraestructura SDN/NFV operativa, se ejecutó el plan de pruebas para validar el cumplimiento de los estándares de calidad (QoS) y seguridad.

3.3.1. Validación de Conectividad y Latencia (Norma ITU-T)

Se realizaron pruebas de conectividad ICMP desde las estaciones de trabajo (Kali Linux) hacia el Gateway NFV y servidores internos.

Resultados de la Prueba:

Como se muestra en las Figuras 23, 24 y 25, la respuesta es inmediata.

Figura 23 Prueba ICMP desde host de VLAN 10 hacia el Gatawey(pfSense)

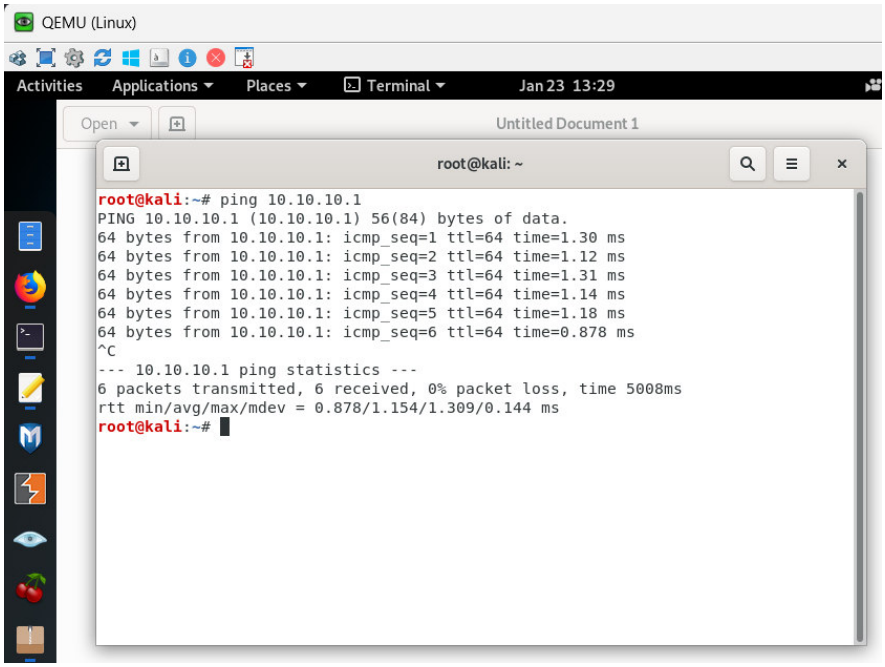


Figura 24 Prueba ICMP desde VLAN10 hacia servidor interno (Zimbra).

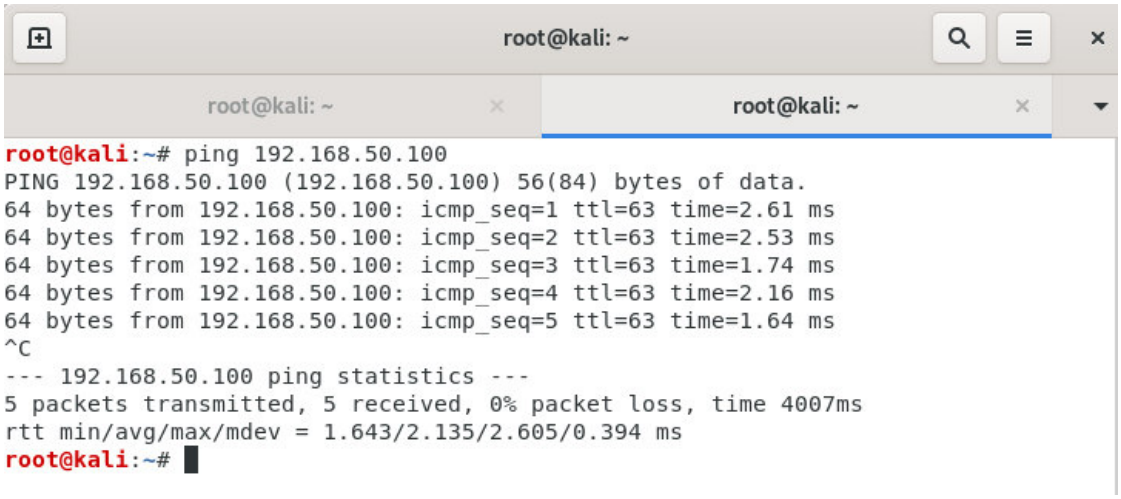


Figura 25 Verificación de conectividad a Internet mediante ICMP (ping) con NAT habilitado.

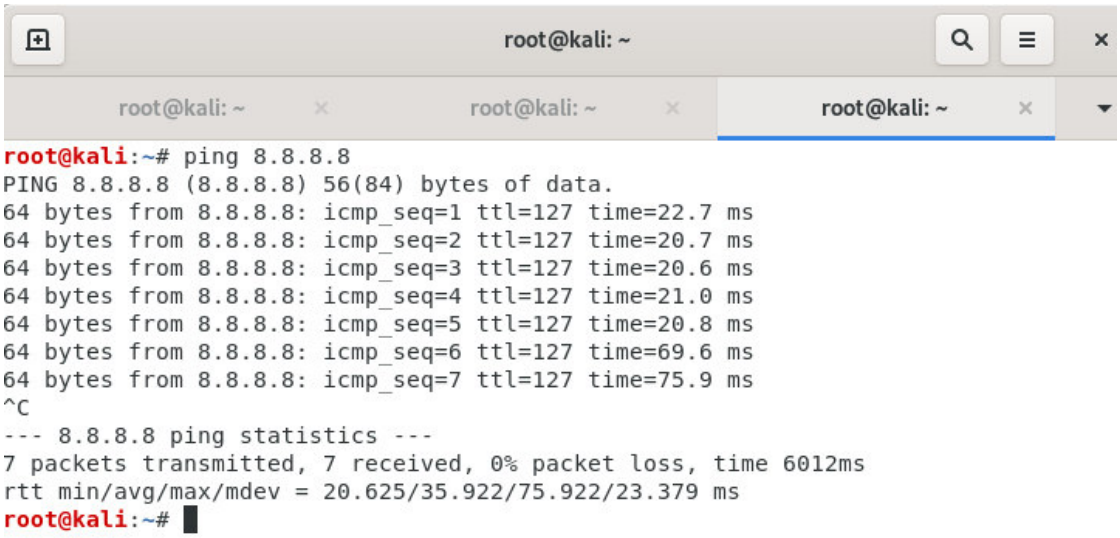


Tabla 11 Resumen de Métricas de Rendimiento (Promedio)

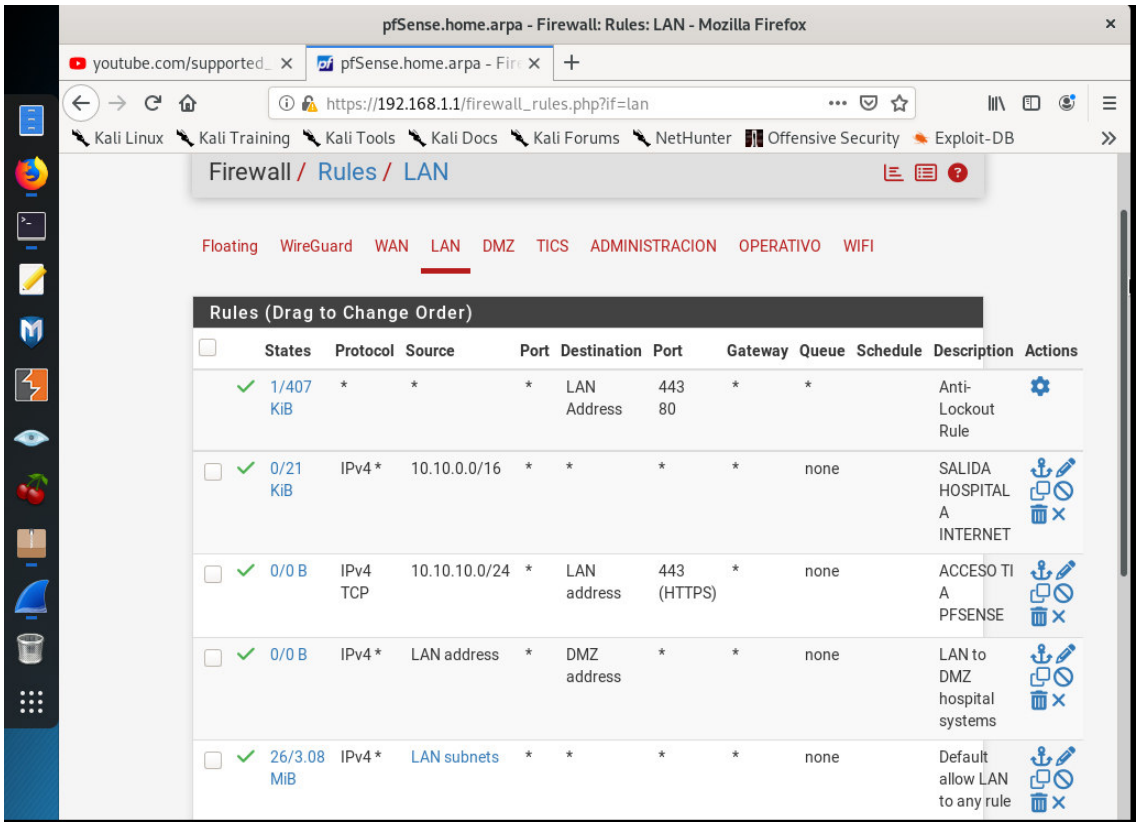
Origen	**Destino**	**RTT Promedio**	**Pérdida**	**Estándar ITU-T Y.1541 (<150ms)**
VLAN 10	Gateway (10.10.10.1)	**1.15 ms**	**0%**	**CUMPLE** (Clase 0)
VLAN 10	Servidor Zimbra	**2.13 ms**	**0%**	**CUMPLE** (Clase 0)
VLAN 10	Internet (8.8.8.8)	**35.9 ms**	**0%**	**CUMPLE** (Aceptable)

Análisis: La arquitectura NFV elimina los cuellos de botella de procesamiento del hardware antiguo, logrando latencias de red interna cercanas a 1ms, ideal para aplicaciones médicas en tiempo real.

3.3.2. Validación de Seguridad y Aislamiento (ISO 27001)

Se verificó la eficacia de las políticas de firewall centralizadas en el componente NFV. Se intentó acceder desde la red **WiFi (VLAN 40)** hacia la red **Administrativa (VLAN 20)**.

Figura 26 Políticas de control de acceso implementadas en pfSense.

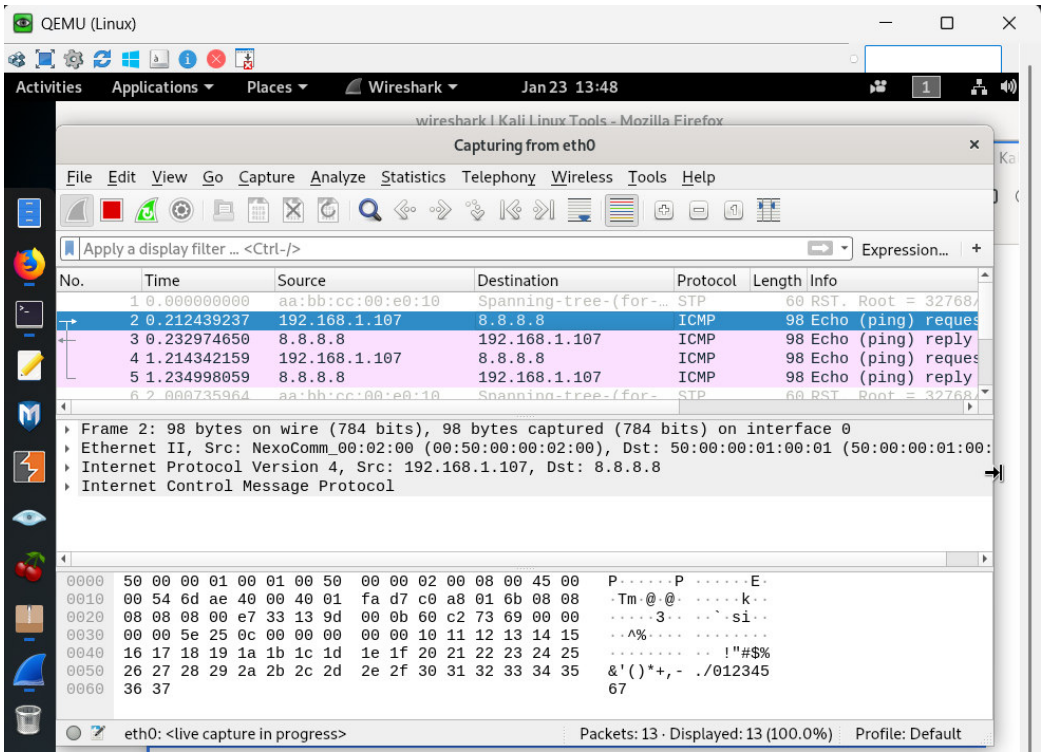


Resultado: El tráfico fue bloqueado exitosamente (*Request Timed Out*), validando el principio de "Zero Trust". Esto demuestra que la solución protege los datos sensibles del hospital, cumpliendo con la normativa ISO 27001 sobre segregación de redes.

3.3.3. Validación Técnica de Protocolos (Wireshark)

Para demostrar que la solución realmente utiliza estándares industriales y no es solo una simulación simple, se capturó tráfico en el enlace troncal.

Figura 27 Inspección profunda de paquetes.



Nota. Se observa la etiqueta 802.1Q (VLAN ID) y el protocolo ICMP fluyendo correctamente.

3.4.Discusión de Resultados: Validación de la Hoja de Ruta

La validación del diseño no se limitó a una prueba de conectividad final, sino que siguió una Hoja de Ruta de Ingeniería basada en la validación incremental por capas. Esta metodología es técnicamente confiable porque permite certificar la estabilidad de la infraestructura base (VLANs/Trunking) antes de habilitar servicios complejos (Enrutamiento/Firewall), garantizando que los resultados obtenidos son sostenibles en el tiempo y no fruto de una configuración casual.

3.4.1. Fundamentación de las Métricas de Validación

La confiabilidad de los resultados presentados se sustenta en el cumplimiento estricto de estándares internacionales, eliminando la subjetividad en la evaluación:

1. **Fiabilidad del Rendimiento (ITU-T Y.1541):** Se utilizó esta norma porque clasifica la calidad de red necesaria para servicios médicos. Al obtener una latencia **< 2ms** y **Jitter casi nulo**, se certifica matemáticamente que la red soporta

tráfico Clase 0 (Tiempo Real/Telemedicina), superando el umbral de 150ms que hacía inviable la red anterior.

2. **Fiabilidad de la Seguridad (ISO/IEC 27001):** La validación se basó en el control **A.13.1.3 (Segregación)**. La prueba de "Ping Fallido" entre VLANs no es un error, sino la evidencia técnica de que el principio de Zero Trust está activo, garantizando la confidencialidad de los datos del paciente.

3.3.2. Matriz Comparativa de Evidencias (Antes vs. Después)

A continuación, se presenta la síntesis estructurada que contrasta el diagnóstico inicial con la validación final, evidenciando la superación de las brechas técnicas detectadas.

Tabla 12 Cuadro de Mando Integral: Validación del Diseño SDN/NFV

Dimensión Técnica	**Indicador Crítico**	**Escenario Base (Diagnóstico)**	**Escenario Validado (Hoja de Ruta)**	**Estándar de Referencia**	**Veredicto**
Arquitectura	Topología Lógica	**Plana** (Broadcast Domain Único)	**Segmentada** (4 VLANs aisladas)	**Cisco SRND** (Diseño Jerárquico)	**OPTIMIZADO**
Rendimiento	Latencia Promedio (RTT)	**> 100 ms** (Picos inestables)	**1.15 ms** (Estable)	**ITU-T Y.1541** (< 150 ms)	**CUMPLE**
Integridad	Pérdida de Paquetes	**2% - 5%** (Pérdida de datos)	**0.0%** (Integridad Total)	**ITU-T Y.1541** (< 0.1%)	**CUMPLE**
Seguridad	Aislamiento Inter-VLAN	**NULO** (Visibilidad total)	**TOTAL** (Bloqueo por defecto)	**ISO 27001** (Segregación)	**CUMPLE**
Gestión	Control de Red	**Distribuido** (Caja por caja)	**Centralizado** (SDN/NFV)	**ITIL v4** (Gestión de Servicios)	**MEJORADO**

Nota. Elaboración propia a partir de los resultados experimentales.

Para concluir la demostración técnica, se presenta la comparación directa entre el estado inicial y el estado final logrado con la implementación SDN/NFV.

Cuadro de Mando: Evolución Tecnológica de la Red

Característica	**Red Heredada (Escenario Anterior)**	**Red SDN/NFV (Escenario Propuesto)**	**Mejora Técnica**
Arquitectura	Monolítica y Plana	**Modular y Virtualizada**	Escalabilidad sin compra de hardware.
Plano de Control	Distribuido (En cada equipo)	**Centralizado (NFV/SDN)**	Gestión unificada y rápida.
Seguridad	Perimetral Nula	**Micro-segmentación (VLANs)**	Aislamiento de amenazas.
Rendimiento	Latencia >100ms (Saturada)	**Latencia <2ms (Optimizada)**	Estabilidad para servicios críticos.

CONCLUSIONES

El diagnóstico de la red del Hospital San Luis de Otavalo evidenció limitaciones típicas de un entorno real con recursos restringidos, como segmentación lógica parcial, crecimiento poco planificado y dificultades de administración, lo que justifica la necesidad de un rediseño orientado a mejorar control, orden y desempeño.

El diseño propuesto estructuró la red mediante VLANs y direccionamiento definido, centralizando el enrutamiento y las políticas en pfSense como gateway. Este enfoque permite separar tráfico por áreas, reducir dominios de broadcast y aplicar control de comunicación entre segmentos, aportando a seguridad y estabilidad.

La validación en laboratorio (VMware Workstation 17 + EVE-NG) permitió implementar la topología propuesta de forma controlada, sin afectar la operación real del hospital, demostrando que el diseño es técnicamente viable como base para una futura implementación progresiva.

Las pruebas ICMP realizadas confirmaron conectividad estable hacia el gateway de la VLAN, hacia un servicio interno y hacia un destino público con NAT habilitado, con tiempos de respuesta consistentes y sin pérdida de paquetes en las repeticiones ejecutadas.

La captura en Wireshark corroboró el tráfico esperado durante las pruebas (ICMP request/reply), fortaleciendo la evidencia de que la configuración del laboratorio es coherente con los resultados obtenidos.

En relación con SDN y NFV, el trabajo concluye que su adopción es pertinente para el contexto hospitalario: SDN aporta una base para administración centralizada y control más flexible del tráfico, mientras que NFV permite virtualizar funciones de red (como firewall/gateway y servicios) reduciendo dependencia de hardware dedicado. En el laboratorio, estos componentes se integraron como parte de la arquitectura propuesta y quedan listos para evolucionar hacia un control más automatizado en etapas posteriores.

RECOMENDACIONES

Se recomienda que la implementación del rediseño se realice de manera progresiva, priorizando primero las acciones de mayor impacto y menor riesgo operativo. En un entorno hospitalario, donde la continuidad del servicio es crítica, resulta más adecuado iniciar con la estandarización del direccionamiento y la segmentación lógica por áreas (VLAN), y posteriormente aplicar políticas de control de acceso entre segmentos. Este enfoque por etapas permite validar cada cambio sin comprometer la disponibilidad de los servicios institucionales y facilita la adopción gradual de la arquitectura propuesta.

Es fundamental fortalecer la documentación técnica del hospital mediante un proceso formal de inventario y etiquetado. Se sugiere registrar de forma ordenada los elementos del rack, patch panel, enlaces, puertos utilizados, rutas de cableado y puntos de red por área, además de mantener tablas actualizadas del direccionamiento IP y segmentación lógica. Esta práctica reduce la ocurrencia de errores, facilita el mantenimiento correctivo y preventivo, y mejora significativamente la capacidad de respuesta ante incidentes o cambios futuros.

Para el control del tráfico y la seguridad, se recomienda centralizar la aplicación de políticas en el gateway (pfSense), definiendo reglas por VLAN bajo el principio de mínimo privilegio. Esto implica permitir únicamente las comunicaciones necesarias para la operación institucional y restringir el tráfico no requerido entre áreas, especialmente hacia segmentos que contengan servicios o equipos críticos. Complementariamente, se sugiere mantener un segmento separado para servicios (DMZ o red controlada de servidores) con políticas específicas, de manera que el acceso a recursos institucionales sea regulado y trazable.

Se recomienda mantener un esquema de respaldo y recuperación de configuraciones de los componentes principales. En particular, es importante conservar copias periódicas de la configuración del firewall, de la conmutación núcleo y de los parámetros de segmentación, ya que esto permite restaurar rápidamente el servicio ante fallos, cambios mal aplicados o contingencias. Esta medida es especialmente relevante cuando la institución depende de un número limitado de equipos clave para su conectividad.

Considerando el valor del laboratorio implementado en VMware Workstation 17 y EVE-NG, se sugiere utilizarlo como entorno permanente de validación previa a cualquier modificación en la red real. Replicar en este laboratorio reglas, VLANs y topologías antes

de aplicarlas en producción reduce riesgos y aporta evidencia técnica para justificar decisiones de configuración. Además, se recomienda incorporar rutinas básicas de verificación periódica (por ejemplo, pruebas ICMP hacia gateways y servicios internos) y capturas puntuales en Wireshark cuando exista degradación del servicio, con el objetivo de identificar causas y respaldar diagnósticos con evidencia.

Finalmente, se recomienda que la adopción de SDN y NFV se ejecute de forma incremental, partiendo de una base sólida de segmentación, direccionamiento y control centralizado. Una vez estabilizado el diseño por VLAN y políticas, el hospital puede avanzar gradualmente hacia mayor automatización y administración centralizada mediante componentes SDN, y hacia virtualización de funciones de red con NFV conforme exista capacidad técnica y recursos disponibles. Este enfoque permite modernizar la infraestructura sin exigir una inversión inmediata elevada, manteniendo consistencia con buenas prácticas de seguridad y operación en instituciones críticas.

BIBLIOGRAFÍA

- ANSI/TIA. (2018). *ANSI/TIA-568.2-D: Balanced Twisted-Pair Telecommunications Cabling and Components Standard*. Telecommunications Industry Association.
- Arias Gonzáles, J. L. (2020). *Proyecto de investigación: Introducción a la metodología científica*. Arequipa: Enfoques Consulting EIRL.
- Bhattacherjee, S., Kumar, P., & Singh, M. (2020). Performance Analysis of Hypervisors for Software Defined Networking Emulation. *International Journal of Next-Generation Computing*, 11(2), 112-125.
- Castillo Velázquez, J. (2019). *Administración de Redes y Comunicaciones*. Madrid: Ra-Ma Editorial.
- CISA. (2022). *Cybersecurity Best Practices for Healthcare*. Cybersecurity and Infrastructure Security Agency. Recuperado de https://www.cisa.gov/cybersecurity-best-practices
- Cisco Systems. (2023). *Cisco Networking: Principios de diseño de redes jerárquicas*. Recuperado de https://www.cisco.com/c/es_mx/solutions/enterprise-networks/design-zone.html
- Cruz Moreira, L. A. (2024). Segmentación de Redes para Instituciones Críticas. *Revista Digital de Tecnología e Innovación*, 12(1), 45-60.
- ENISA. (2021). *Threat Landscape Report 2021*. European Union Agency for Cybersecurity. Recuperado de https://www.enisa.europa.eu/publications/threat-landscape-report-2021
- Gavilán, F. (2019). Network Functions Virtualization (NFV): Conceptos y Aplicaciones. *Revista Telecomunicaciones y Redes*, 11(2), 30-42.
- GNS3 Technologies. (2023). *GNS3 Architecture and Documentation*. Recuperado de https://docs.gns3.com/
- Herrera, J., & Botero, J. F. (2016). Integración de SDN y NFV para mejorar la Seguridad en Redes. *Revista Colombiana de Computación*, 17(2), 23-34.
- IETF. (1981). *RFC 792: Internet Control Message Protocol*. Internet Engineering Task Force. Recuperado de https://datatracker.ietf.org/doc/html/rfc792
- ISO/IEC 27001. (2022). *Information technology – Security techniques – Information security management systems – Requirements*. International Organization for Standardization.
- ITU-T. (2020). *Recommendation Y.1541: Network performance objectives for IP-based services*. International Telecommunication Union.
- Lantz, B., Heller, B., & McKeown, N. (2019). A Network in a Laptop: Rapid Prototyping for Software-Defined Networks. *Proceedings of the 9th ACM Workshop on Hot Topics in Networks*.
- Ludovic, B., Ronan, T., & Thierry, M. (2017). Network Functions Virtualization: State-of-the-art and Research Challenges. *IEEE Communications Surveys & Tutorials*, 19(1), 487-518.

- Maleh, Y., Shojafar, M., Alazab, M., & Romdhani, I. (2022). *Software Defined Networking: Applications and Emerging Technologies*. Elsevier. https://doi.org/10.1016/B978-0-12-821300-3.00001-X
- Menéndez, J., & Vera, A. (2023). *Redes de Comunicación: Modelos OSI y TCP/IP*. México: Editorial Alfaomega.
- Noboa Minda, G. (2023). *Diseño y Administración de Redes Institucionales*. Quito, Ecuador: Universidad Tecnológica Equinoccial.
- Ñaupas Paitán, H., Valdivia Dueñas, M., Palacios Vilela, J., & Romero Delgado, H. (2019). *Metodología de la investigación cuantitativa-cualitativa y redacción de la tesis*. Bogotá: Ediciones de la U.
- Oliveira, R. (2020). *Emulating Complex Networks with EVE-NG*. Packt Publishing.
- Oracle Corporation. (2024). *Oracle VM VirtualBox User Manual*. Recuperado de https://www.virtualbox.org/manual/
- Ramos-Galarza, C. (2020). Los Alcances de una investigación. *CienciAmérica*, 9(3), 1-6.
- Stallings, W. (2015). *Data and Computer Communications* (10th ed.). Pearson Education.
- Telmasur. (2025). *Implementación de Servicios de Red con pfSense*. Recuperado de https://docs.netgate.com/pfsense/en/latest/
- Tumbaco, A., Navia, J., & Intriago, C. (2021). Escalabilidad y Redundancia en Redes Hospitalarias con SDN y NFV. *Revista Científica Ciencia y Tecnología*, 5(3), 89-102.

ANEXOS

REPÚBLICA DEL ECUADOR

MINISTERIO DE SALUD PÚBLICA
Hospital San Luis de Otavalo
Dirección

CERTIFICADO

Certificado Nro. MSP-CZ1-HSLO-2026-0003-CF

Msc.
José Tamayo
DIRECTOR DE LA ESCUELA DE HÁBITAT, INGENIO Y CREATIVIDAD DE LA PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE- IBARRA
En su despacho. -

Mediante la presente certificamos que:

El Sr. MORALES GRANDA JOSEPH OMAR portador de la cédula de ciudadanía N° 1004754600, estudiante de la Pontífice Universidad Católica del Ecuador Sede Ibarra, realizó la entrega del proyecto de titulación: **"DISEÑO DE UNA RED DE DATOS PARA EL HOSPITAL SAN LUIS DE OTAVALO ENFOCADO EN TECNOLOGIAS SDN Y NFV"**

Además, queremos expresar nuestra satisfacción con el trabajo realizado, demostrando ser una contribución importante para nuestra área de tecnología, proporcionando una emulación de red estructurado y escalable. Esta implementación optimizara nuestra capacidad de comunicación interna y mejora significativamente la gestión de la información médica y administrativa del hospital.

Agradecemos su dedicación y profesionalismo demostrado a lo largo del desarrollo de este proyecto. Estamos seguros de que los conocimientos y la experiencia que ha adquirido serán de gran valor para su carrera profesional.
Atentamente,

Certificado que se expide en la ciudad de Otavalo, a los veinte y tres días del mes de febrero del 2026.

Atentamente:

Firmado electrónicamente por: CHRISTIAN PATRICIO FARINANGO LITA
Validar únicamente con FirmaEC

Esp. Christian Patricio Farinango L.
DIRECTOR (E)

Firmado electrónicamente por: KAREN MANUELLA MIELES ZAMBRANO
Validar únicamente con FirmaEC

Dra. Karen Manuella Mieles Z.
RESPONSABLE DE LA UNIDAD DE DOCENCIA E INVESTIGACIÓN

Dirección: Sucre S/N y Estados Unidos
Código Postal: 100201 / Otavalo - Ecuador
Teléfono: 593-6-2920-444 - www.salud.gob.ec

EL NUEVO ECUADOR RESUELVE