



Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América
Facultad de Ingeniería Electrónica y Eléctrica
Escuela Profesional de Ingeniería de Telecomunicaciones

**Implementación de infraestructura virtual local
gestionada en nube para garantizar la continuidad
operativa para una clínica privada**

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de Ingeniero de
Telecomunicaciones

AUTOR

Franz Kenneth LOZANO TORRES

ASESOR

Dr. Williams Fernando ACOSTA SOLORZANO

Lima, Perú

2026



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

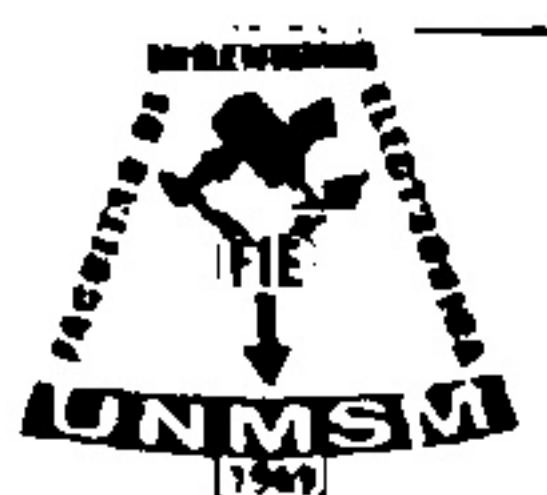
Referencia bibliográfica

Lozano, F. (2026). *Implementación de infraestructura virtual local gestionada en nube para garantizar la continuidad operativa para una clínica privada*. [Trabajo de suficiencia profesional de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería Electrónica y Eléctrica, Escuela Profesional de Ingeniería de Telecomunicaciones]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Franz Kenneth Lozano Torres
Tipo de documento de identidad	DNI
Número de documento de identidad	76219513
URL de ORCID	No Aplica
Datos de asesor	
Nombres y apellidos	Williams Fernando Acosta Solorzano
Tipo de documento de identidad	DNI
Número de documento de identidad	06434186
URL de ORCID	https://orcid.org/0000-0002-2473-4581/
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Teresa Esther Nuñez Zuñiga
Tipo de documento	DNI
Número de documento de identidad	08006778
Miembro del jurado 1	
Nombres y apellidos	Wilbert Chavez Irazabal
Tipo de documento	DNI
Número de documento de identidad	08121733
Miembro del jurado 2	
Nombres y apellidos	Jean Carlos Malca Fernández
Tipo de documento	DNI
Número de documento de identidad	45535181
Datos de investigación	
Línea de investigación	C.0.3.28. Comunicaciones/redes y sistemas distribuidos
Grupo de investigación	No Aplica
Agencia de financiamiento	No Aplica

Ubicación geográfica de la investigación	Edificio: Vistacorp País: Perú Departamento: Lima Provincia: Lima Distrito: Santiago de Surco Calle: Jr. Monterrey Latitud: -12.1127801 Longitud: -76.9894897
Año o rango de años en que se realizó la investigación	Mayo 2025 - Agosto 2025
URL de disciplinas OCDE	Ingeniería de sistemas y comunicaciones https://purl.org/pe-repo/ocde/ford#2.02.04 Telecomunicaciones https://purl.org/pe-repo/ocde/ford#2.02.05 Hardware, Arquitectura de computadoras https://purl.org/pe-repo/ocde/ford#2.02.06



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
(Universidad del Perú, DECANA DE AMÉRICA)
FACULTAD DE INGENIERÍA ELECTRÓNICA Y ELÉCTRICA
Teléfono 619-7000 Anexo 4226
Calle Germán Amezaga 375 – Lima 1 – Perú



ACTA DE SUSTENTACIÓN
TRABAJO DE
SUFICIENCIA PROFESIONAL
ACTA N°39/FIEE-PPP/2026

Los suscritos Miembros del Jurado, docentes permanentes de las Escuelas Profesionales de la Facultad de Ingeniería Electrónica y Eléctrica, reunidos en la fecha 19 de Junio del 2026, como presidente de Jurado la **DRA. TERESA ESTHER NUÑEZ ZUÑIGA**, integrado por el Miembro de Jurado el **MG. WILBERT CHAVEZ IRAZABAL**, el Miembro de Jurado el **MG. JEAN CARLOS MALCA FERNÁNDEZ** y Miembro Asesor el **DR. WILLIAMS FERNANDO ACOSTA SOLORZANO**.

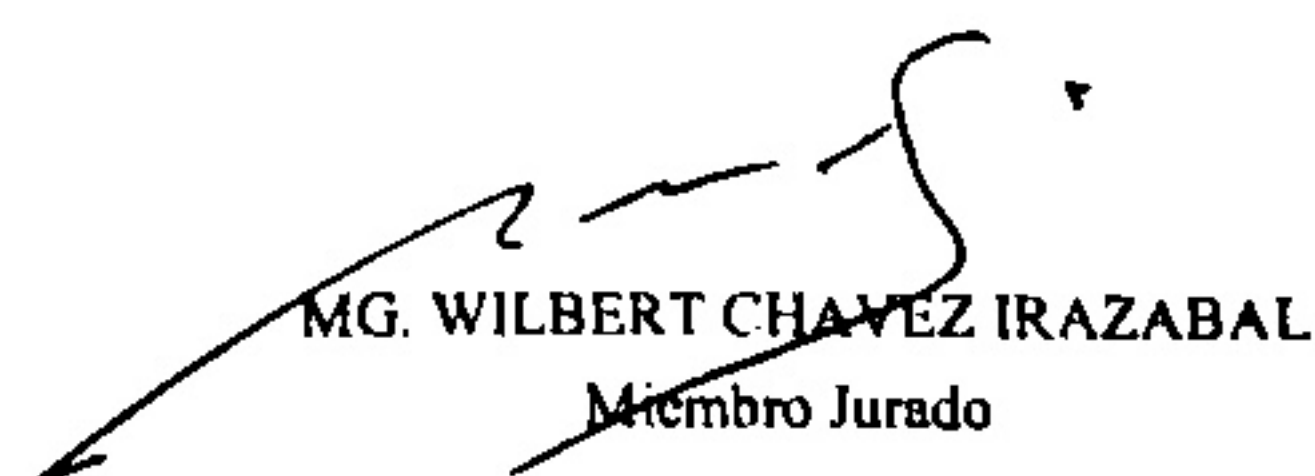
Después de escuchar la Sustentación Presencial del Trabajo de Suficiencia Profesional del Bachiller **FRANZ KENNETH LOZANO TORRES** con código 15190258 que para optar el Título Profesional de Ingeniero de Telecomunicaciones sustentó el Trabajo de Suficiencia Profesional titulado **IMPLEMENTACIÓN DE INFRAESTRUCTURA VIRTUAL LOCAL GESTIONADA EN NUBE PARA GARANTIZAR LA CONTINUIDAD OPERATIVA PARA UNA CLÍNICA PRIVADA**.

El jurado examinador procedió a formular las preguntas reglamentarias y, luego de una deliberación en privado, decidió otorgarle el calificativo de 15 (Quince).

Ciudad Universitaria, 19 de junio del 2026



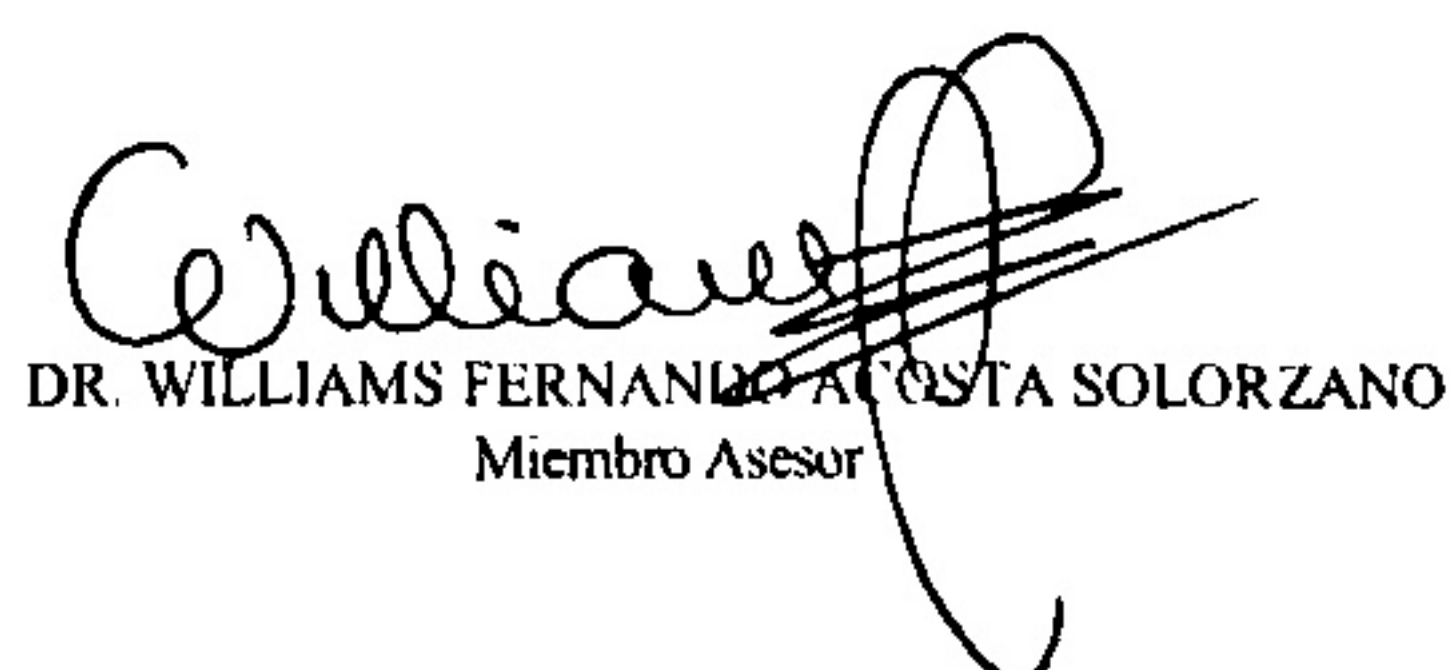
DRA. TERESA ESTHER NUÑEZ ZUÑIGA
Presidente Jurado



MG. WILBERT CHAVEZ IRAZABAL
Miembro Jurado



MG. JEAN CARLOS MALCA FERNÁNDEZ
Miembro Jurado



DR. WILLIAMS FERNANDO ACOSTA SOLORZANO
Miembro Asesor



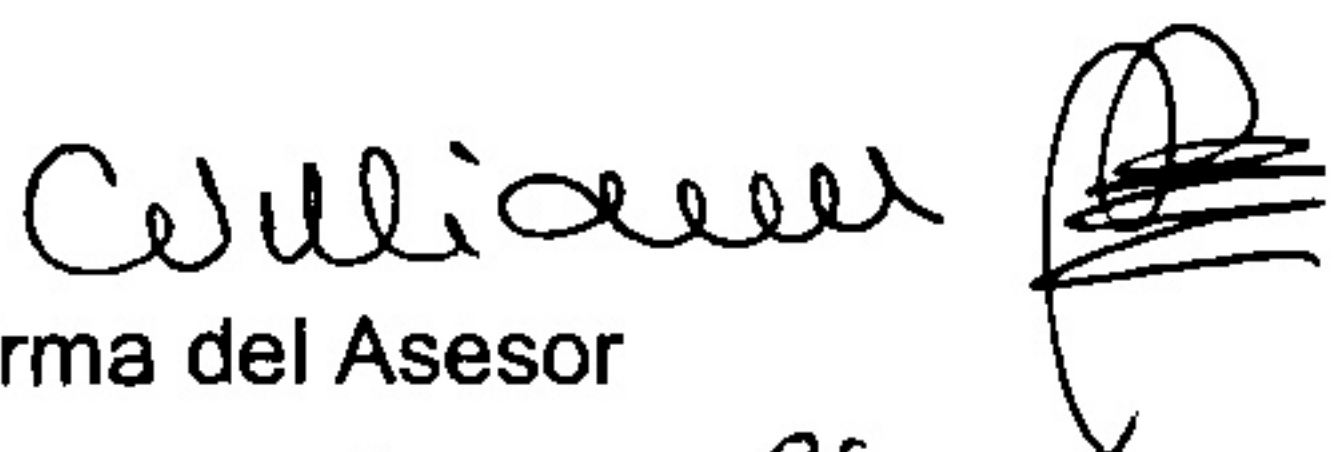
UNIVERSIDAD NACIONAL MAYOR DE
SAN MARCOS
Universidad del Perú, Decana de América

CERTIFICADO DE SIMILITUD

Yo , **WILLIAMS FERNANDO ACOSTA SOLORZANO** en mi condición de asesor acreditado con el Dictamen N°41/FIEE-PPP/2026 del Trabajo de Suficiencia Profesional titulado **IMPLEMENTACIÓN DE INFRAESTRUCTURA VIRTUAL LOCAL GESTIONADA EN NUBE PARA GARANTIZAR LA CONTINUIDAD OPERATIVA PARA UNA CLÍNICA PRIVADA**, presentado por el bachiller **FRANZ KENNETH LOZANO TORRES**, para optar el título profesional de Ingeniero de Telecomunicaciones. CERTIFICO que se ha cumplido con lo establecido en la Directiva de Originalidad y de Similitud de Trabajos Académicos, de Investigación y Producción Intelectual. Según la revisión, análisis y evaluación mediante la plataforma PIDS, el documento evaluado cuenta con el 3% de similitud, nivel PERMITIDO para continuar con los trámites correspondientes y para su publicación en el repositorio institucional.

Se emite el presente certificado en cumplimiento de lo establecido en las normas vigentes, como uno de los requisitos para la obtención del título profesional de Ingeniero de Telecomunicaciones.

Lima, 19 de Junio del 2026


Firma del Asesor

DNI: 06434186

Nombres y apellidos del asesor:

WILLIAMS FERNANDO ACOSTA SOLORZANO

DEDICATORIA

Este trabajo está dedicado a mis padres: a mi madre, Ines Torres, por ser siempre mi ejemplo de esfuerzo y constancia; y a la memoria de mi padre, Galo Lozano, cuyo legado de integridad me acompaña siempre. De igual manera, dedico este trabajo a la memoria de Mauro Lozano, por su invaluable compañía y por haber sido mi guía y mentor desde mis primeros pasos como estudiante.

AGRADECIMIENTOS

A mi madre por su incondicional apoyo y consejos de vida que me sirven para mejorar como persona y profesional.

A mi equipo de trabajo por el profesionalismo y el alto nivel de exigencia.

RESUMEN

El objetivo del presente trabajo es elaborar el diseño a bajo nivel (LLD) e implementar un clúster de servidores ESXi sobre la plataforma Cisco UCS Serie X en una clínica privada, para asegurar la continuidad operativa de sus aplicaciones críticas. El método utilizado integró la metodología de ciclo de vida PPDIOO de Cisco y los procesos de dirección de proyectos del PMBOK 6, abarcando desde el levantamiento de información hasta la configuración de protocolos de redundancia vPC, HSRP y *Multipathing*. Los resultados muestran una integración exitosa con los sistemas de almacenamiento heredados y una migración de cargas de trabajo sin interrupciones en los servicios hospitalarios, superando retos de incompatibilidad de *firmware* mediante enlaces ISL. Se concluye que el diseño implementado y la gestión centralizada mediante Cisco Intersight optimizaron el rendimiento de la infraestructura, dotando a la institución de un entorno de alta disponibilidad, escalable y sin puntos únicos de falla.

Palabras clave: Cisco UCS, centro de datos, diseño LLD, alta disponibilidad, virtualización

ABSTRACT

The objective of this work is to develop the low-level design (LLD) and implement an ESXi server cluster on the Cisco UCS X-Series platform in a private clinic, to ensure the operational continuity of its critical applications. The method used integrated Cisco's PPDIOO lifecycle methodology and PMBOK 6 project management processes, ranging from information gathering to the configuration of vPC, HSRP, and Multipathing redundancy protocols. The results show a successful integration with legacy storage systems and a seamless workload migration of hospital services, overcoming firmware incompatibility challenges through ISL links. It is concluded that the implemented design and centralized management through Cisco Intersight optimized the infrastructure performance, providing the institution with a high-availability, scalable environment with no single points of failure.

Keywords: Cisco UCS, data center, LLD design, high availability, virtualization

ÍNDICE GENERAL

CARÁTULA	i
RESUMEN	iv
ABSTRACT	v
ÍNDICE GENERAL	vi
LISTA DE FIGURAS	ix
LISTA DE TABLAS	xi
CAPITULO I: INTRODUCCIÓN	13
1.1 Objetivos del informe	13
1.2 Estructura de informe	13
CAPITULO II: INFORMACIÓN DEL LUGAR DONDE SE DESARROLLÓ LA ACTIVIDAD	14
2.1 Institución – Actividad que desarrolla	14
2.2 Periodo de duración de la actividad	14
2.3 Finalidad y objetivos de la entidad	14
2.4 Razón social	14
2.5 Dirección postal	14
2.6 Nombre y correo electrónico del profesional a cargo	14
CAPITULO III: DESCRIPCIÓN DE LA ACTIVIDAD	15
3.1 Organización de la actividad	15
3.2 Finalidad y objetivos de la Actividad	15
3.2.1 Finalidad	15
3.2.2 Objetivos	16
3.2.2.1 Objetivo General	16
3.2.2.2 Objetivos Específicos	16
3.3 Problemática	16
3.3.1 Problema General	17

3.3.2	Problemas Específicos	18
3.3.3	Justificación e importancia de la investigación	18
3.4	Metodología	19
3.4.1	Bases teóricas	19
3.4.2	Marco conceptual	21
3.4.2.1	Metodología PPDIOO de Cisco	21
3.4.2.2	Estándar PMBOK 6	22
3.4.2.3	LAN	23
3.4.2.4	SAN	27
3.4.2.5	Capa 1: Interfaces, SFPs y QSFPs	34
3.4.2.6	Servidores y Computación Unificada	35
3.4.2.7	Virtualización	37
3.5	Procedimiento	39
3.5.1	Elección de la Tecnología	39
3.5.1.1	HPE - Synergy 480 Gen11	40
3.5.1.2	Dell Technologies - PowerEdge MX7000	40
3.5.1.3	Cisco Systems - Solución implementada	41
3.5.1.4	Definición de solución propuesta	41
3.5.2	Metodología de Implementación	42
3.5.3	Diseño a Alto Nivel (HLD)	44
3.5.4	Diseño a Bajo Nivel (LLD)	52
3.5.4.1	Port mapping	53
3.5.4.2	Storage y SAN	55
3.5.4.3	LAN	62
3.5.4.4	Cisco UCS	65
3.5.4.5	Gestión	74
3.5.4.6	Virtualización	76
3.5.4.7	Software y licenciamiento	78

	viii
3.5.5 Implementación	79
3.5.5.1 Configuración de almacenamiento	80
3.5.5.2 Despliegue de redes LAN y SAN	80
3.5.5.3 Migración de redes LAN y SAN	81
3.5.5.4 Configuración de solución Cisco UCS	82
3.5.5.5 Configuración de solución VMware vSphere 8.0	84
3.5.5.6 Migración de máquinas virtuales	84
3.6 Resultado de la actividad	85
CAPITULO IV: DISCUSIÓN DE RESULTADOS	94
4.1 Descripción de la implementación	94
4.1.1 Desarrollo de LLD para integración con equipos existentes	94
4.1.2 Redundancia de las redes LAN y SAN	94
4.1.3 Migración y ventanas de mantenimiento	95
4.1.4 Optimización mediante Intersight	95
4.2 Evaluación Económica	95
CAPITULO V: CONCLUSIONES	98
CAPITULO VI: RECOMENDACIONES	99
CAPITULO VII: REFERENCIAS BIBLIOGRÁFICAS	100
CAPITULO VIII: ANEXOS	104

LISTA DE FIGURAS

Figura 1 Organigrama de Noovus Technology.	15
Figura 2 Fases del ciclo de vida de redes PPDIOO.	22
Figura 3 Grupos de Procesos de la Gestión de Proyectos según PMBOK 6.	23
Figura 4 Diseño de Core Colapsado.	25
Figura 5 Topología de una red SAN.	28
Figura 6 Vistas frontal y posterior del chasis modular Cisco UCS X9508.	46
Figura 7 Vista frontal de servidores blade Cisco X210c M7.	46
Figura 8 Vista frontal de un Cisco UCS FI 6454.	46
Figura 9 Vista frontal de un switch LAN Cisco Nexus N9K-C93180YC-FX3.	47
Figura 10. Vista frontal de un switch SAN Cisco MDS DS-C9132T-MEK9.	47
Figura 11 Topología actual de la red DC de la clínica.	48
Figura 12 Topología propuesta para la red DC de la clínica.	49
Figura 13 Cabinet Layout de los nuevos equipos de la clínica.	51
Figura 14 Topología física definida para la red DC de la clínica.	52
Figura 15 Función multipathing de VMware con Fibre Channel.	55
Figura 16 Topología lógica definida para red SAN.	56
Figura 17 Topología lógica definida para red LAN.	63
Figura 18 Conexiones lógicas definidas para gestión.	75
Figura 19 Configuración de Device Connector en FIs.	83
Figura 20 Servidores UCS-X en Intersight.	86
Figura 21 Chasis UCS-X en Intersight.	86
Figura 22 Fuentes de energía del chasis UCS-X operativas.	87
Figura 23 Fabric Interconnects en Intersight.	87
Figura 24 Fuentes de energía redundantes en Fabric Interconnect A.	88
Figura 25 Fuentes de energía redundantes en Fabric Interconnect B.	88
Figura 26 Estado final del dominio vPC en el switch Core 1.	89
Figura 27 Estado final del dominio vPC en el switch Core 2.	90
Figura 28 Estado final del protocolo HSRP en el switch Core 1.	90
Figura 29 Estado final del protocolo HSRP en el switch Core 2.	90
Figura 30 Estado final de los enlaces port-channel en ambos switches MDS.	91

Figura 31 Estado final de los nodos registrados en el switch MDS A.	91
Figura 32 Estado final de los nodos registrados en el switch MDS B.	91
Figura 33 Estado de redundancia SAN de hosts ESXi nuevos.	92
Figura 34 Verificación de multipath en host ESXi nuevo.	92
Figura 35 Verificación de máquinas virtuales migradas a nuevo cluster.	93

LISTA DE TABLAS

Tabla 1 Relación de equipos a desplegar en el proyecto	50
Tabla 2 Port mapping propuesto	53
Tabla 3 Enlaces Port Channel en red SAN	57
Tabla 4 Listado de direcciones pWWN y Alias	59
Tabla 5 Listado de zonas	60
Tabla 6 Listado de targets	60
Tabla 7 Configuración de Switches Nexus	64
Tabla 8 UCS Domain Profile	65
Tabla 9 UCS Chassis Profile	65
Tabla 10 UCS Server Profile Template	66
Tabla 11 UCS Server Profiles	66
Tabla 12 Port Policy FI-A	67
Tabla 13 Port Policy FI-B	67
Tabla 14 VLAN Policy	67
Tabla 15 VSAN Policy FI-A	68
Tabla 16 VSAN Policy FI-B	68
Tabla 17 NTP Policy	69
Tabla 18 Network Connectivity Policy	69
Tabla 19 Switch Control Policy	69
Tabla 20 IMC Access Policy para chasis	70
Tabla 21 IP Pool para acceso vKVM	70
Tabla 22 Power Policy para chasis	70
Tabla 23 Thermal Policy	71
Tabla 24 Boot Order Policy	71
Tabla 25 Virtual Media Policy	71
Tabla 26 Local User Policy	72
Tabla 27 Virtual KVM Policy	72
Tabla 28 LAN Connectivity Policy	72
Tabla 29 Ethernet Network Group Policy	73
Tabla 30 MAC Address Pools	73

Tabla 31 SAN Connectivity Policy	73
Tabla 32 WWNN Address Pool	74
Tabla 33 WWPN Address Pools	74
Tabla 34 FC Network Policies	74
Tabla 35 Parámetros comunes	75
Tabla 36 Direccionamiento de gestión definido	76
Tabla 37 Inventario de hosts en vCenter	77
Tabla 38 Configuración de VMkernel de gestión	77
Tabla 39 Configuración de VMkernel de vMotion	77
Tabla 40 Configuración de vSwitches	77
Tabla 41 Versiones de software	78
Tabla 42 Modos de licenciamiento	78
Tabla 43 Flujo de Caja proyectado en soles	97
Tabla 44 Resultados de la evaluación económica	97

CAPITULO I: INTRODUCCIÓN

1.1 Objetivos del informe

El presente informe expone de manera clara y precisa el desarrollo de un diseño a bajo nivel (LLD) y la estrategia planificada para la implementación de un *clúster* de servidores virtuales sobre el hardware Cisco UCS Serie X gestionado en nube para incrementar la continuidad operativa en una clínica privada.

1.2 Estructura de informe

Para una mejor comprensión, el documento se ha organizado en ocho capítulos.

El Capítulo I define formalmente los objetivos principales y la estructura general del presente documento, mientras que el Capítulo II detalla el entorno de la institución donde se realizaron las actividades y su periodo de ejecución. Por su parte, el Capítulo III aborda a fondo la problemática identificada, el marco conceptual referencial y el procedimiento técnico de ingeniería, incluyendo la metodología y el diseño detallado (LLD) que guiaron la implementación.

El Capítulo IV analiza detalladamente los resultados obtenidos y realiza una evaluación económica cualitativa del impacto del proyecto. Finalmente, las conclusiones técnico-profesionales se exponen en el Capítulo V, seguidas de las recomendaciones clave en el Capítulo VI, dejando el Capítulo VII para compilar el sustento bibliográfico utilizado y el Capítulo VIII para los anexos, donde se incluyó el cronograma del proyecto con los tiempos correctos, pero con fechas editadas por confidencialidad.

CAPITULO II: INFORMACIÓN DEL LUGAR DONDE SE DESARROLLÓ LA ACTIVIDAD

2.1 Institución – Actividad que desarrolla

La compañía en la cual se desarrolló el Trabajo de Suficiencia Profesional es una clínica privada. Las actividades fueron realizadas por la empresa Noovus Technology Business Unit S.A.C.

2.2 Periodo de duración de la actividad

La implementación del proyecto se dio entre los meses de mayo y agosto de 2025.

2.3 Finalidad y objetivos de la entidad

Noovus Technology Business Unit S.A.C. (en adelante Noovus) es una empresa integradora de soluciones de TI, informática, redes, seguridad, Data Center y presencia en Perú, Chile y EE.UU.

2.4 Razón social

Noovus Technology Business Unit S.A.C.

2.5 Dirección postal

Jr. Monterrey Nro. 405 Int. 403, Santiago de Surco, Lima, Perú.

2.6 Nombre y correo electrónico del profesional a cargo

Nombres y Apellidos: Luis Miranda Salvador

Correo Electrónico: lmiranda@noovus.tech

CAPITULO III: DESCRIPCIÓN DE LA ACTIVIDAD

3.1 Organización de la actividad

En la Figura 1 se muestra la estructura organizativa de la empresa Noovus Technology de forma resumida, acotada al área de Ingeniería Postventa y las áreas involucradas en la implementación de proyectos.

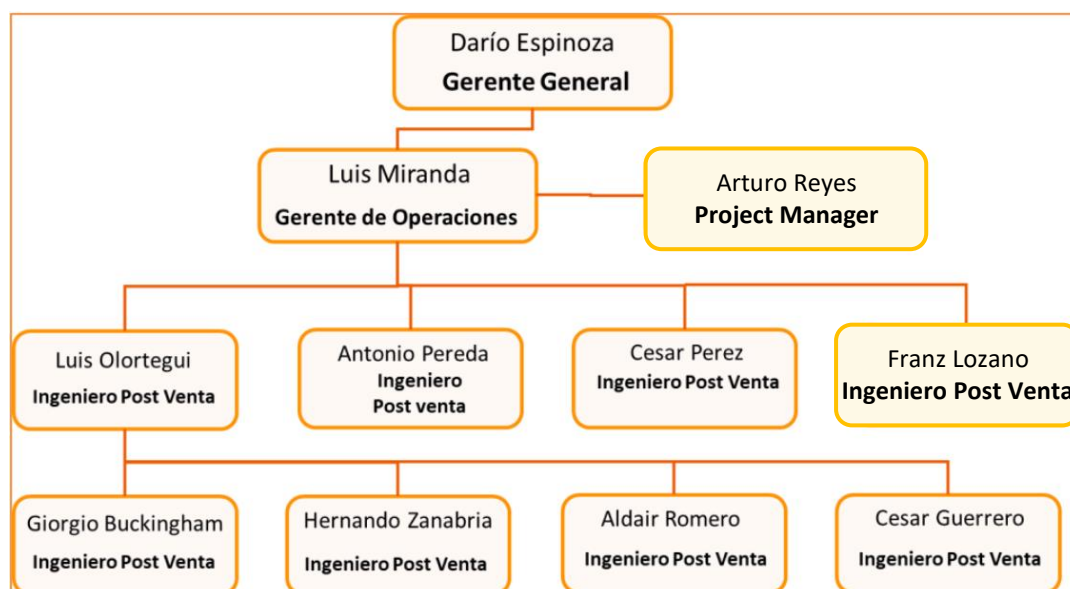


Figura 1 Organigrama de Noovus Technology. Fuente. Elaboración propia.

3.2 Finalidad y objetivos de la Actividad

3.2.1 Finalidad

El presente documento tiene como finalidad detallar la elaboración del diseño a bajo nivel (LLD) y la implementación de un sistema de cómputo de gran capacidad con funciones avanzadas de gestión en nube y con un alto nivel de resiliencia requerido por una clínica privada, asegurando una transición segura desde su infraestructura legada.

3.2.2 Objetivos

3.2.2.1 Objetivo General

Elaborar el diseño a bajo nivel (LLD) e implementar un clúster de servidores ESXi haciendo uso del hardware Cisco UCS serie X en la sede de una clínica privada, con el fin de integrar las nuevas capacidades de cómputo y mejorar la continuidad operativa de las aplicaciones de dicha entidad ante diversos escenarios de falla física y lógica.

3.2.2.2 Objetivos Específicos

- Desarrollar el diseño a bajo nivel (LLD) aplicando las buenas prácticas recomendadas por el fabricante y los criterios técnicos del implementador, con la finalidad de aprovechar al máximo las capacidades tecnológicas del nuevo equipamiento y garantizar su correcta interoperabilidad con la infraestructura existente.
- Configurar los protocolos de red LAN (vPC, HSRP) y SAN (Multipath, Zonificación) en los nuevos switches Nexus y MDS para que las aplicaciones de la clínica no se vean afectadas ante fallas de red.
- Ejecutar la migración de los enlaces de red y las cargas de trabajo virtualizadas hacia la nueva infraestructura con el menor impacto posible sobre los servicios médicos y administrativos.
- Implementar la gestión centralizada del hardware de cómputo mediante la plataforma en nube Cisco Intersight.

3.3 Problemática

Los centros de datos son un elemento crucial en las operaciones de cada institución. Es de gran importancia que la infraestructura y las aplicaciones

mantengan una continuidad en su operación diaria, y que el entorno sea lo suficientemente resiliente ante diversos riesgos que pueden impactar de forma grave en el desarrollo y funcionamiento del negocio. Estos riesgos son altos en el día a día, ya que siempre existe la posibilidad de que ocurran fallas a nivel físico en los cables de fibras ópticas, a nivel eléctrico en los sistemas de respaldo y fuentes de energía, o a nivel de hardware en los componentes de los equipos principales.

Una de las bases fundamentales de una infraestructura sólida es contar con un diseño redundante bien estructurado que permita soportar múltiples escenarios de falla, asegurando en todo momento el menor impacto posible a las aplicaciones que operan en los servidores locales (on-premise) de la institución.

Las instituciones privadas de salud, a medida que incrementan su capacidad de atención y amplían los servicios médicos que ofrecen a los usuarios, aumentan también la cantidad de operaciones realizadas por sus diversas aplicaciones clínicas y administrativas, y la cantidad de datos que necesitan ser procesados y almacenados de forma segura. Esto se traduce en la necesidad de adquirir nuevo equipamiento tecnológico para aumentar las capacidades de cómputo, almacenamiento y ancho de banda de la red. Sin embargo, el reto técnico principal radica en cómo insertar, configurar y migrar estos nuevos equipos de misión crítica dentro de una red hospitalaria en constante funcionamiento, sin generar interrupciones inesperadas ni caídas del sistema que afecten directamente la continuidad en la atención a los pacientes.

3.3.1 Problema General

¿De qué manera la elaboración de un diseño a bajo nivel (LLD) y la implementación de la solución Cisco UCS Serie X permiten renovar la infraestructura de servidores virtuales de una clínica privada, asegurando la continuidad operativa y minimizando el impacto durante la migración de sus aplicaciones críticas?

3.3.2 Problemas Específicos

- ¿De qué manera el diseño a bajo nivel (LLD) permite la integración eficiente de la nueva solución Cisco (UCS Serie X, Nexus y MDS) con los sistemas de almacenamiento existentes, maximizando el rendimiento de la infraestructura en el entorno clínico?
- ¿Qué configuraciones y protocolos de redundancia en las redes LAN y SAN son necesarios para soportar múltiples escenarios de falla en la nueva infraestructura?
- ¿Qué estrategia de implementación y migración garantizan una migración segura de la red y las aplicaciones, minimizando el impacto en la operatividad de la clínica?
- ¿De qué forma la plataforma de gestión en nube mejora y optimiza la administración de una solución de cómputo local?

3.3.3 Justificación e importancia de la investigación

El presente trabajo se justifica en la necesidad técnica de ejecutar una transición estructurada, gradual y segura hacia una infraestructura virtualizada de mayor capacidad en sus componentes principales de cómputo, almacenamiento y ancho de banda en las redes Ethernet y Fiber Channel (FC). De esta manera, se busca mejorar directamente la continuidad operativa y la disponibilidad de las aplicaciones críticas de una clínica privada.

Además, el diseño detallado y la implementación documentada en este proyecto habilitan la escalabilidad del centro de datos ante un potencial incremento de las cargas de trabajo cotidianas. Esto asegura que la infraestructura base no solo responda a las exigencias actuales, sino que también soporte el crecimiento continuo de las operaciones, el resguardo de la información y los servicios médicos brindados por la clínica a largo plazo.

3.4 Metodología

3.4.1 Bases teóricas

Tello Coello (2014), en su tesis acerca de la implementación de una solución Cisco UCS, tiene como objetivo integrar una solución Cisco UCS a su red para hacer uso de su infraestructura de almacenamiento y correr aplicaciones de la empresa PuntoNet en Ecuador. El autor concluye que la implementación del chasis Cisco UCS en el proyecto cumplió con los principios de escalabilidad y gestión unificada, integrando recursos de cómputo en un dominio común y simplificando la configuración gracias a la intuitiva interfaz propia de la plataforma UCS. También resaltó la incorporación de switches Cisco Nexus 5000, junto con la conectividad LAN y de servidores a 10 Gbps y la adopción de Fibre Channel over Ethernet, que permitieron unificar interfaces y optimizar la infraestructura del centro de datos. Los Fabric Interconnect, combinados con los servidores UCS, favorecieron la consolidación de recursos, logrando una operación estable y eficiente. Entre los beneficios obtenidos destacan la administración simplificada, facilidad de actualización, excelente rendimiento, mejoras ambientales, optimización de costos y flexibilidad de uso para incrementar la productividad organizacional. (Tello Coello, 2014)

Tello Illescas (2024), en su tesis acerca del diseño de una arquitectura de cómputo y almacenamiento para una escuela en la Universidad Politécnica Salesiana en Quito, tiene como objetivo estudiar las diversas opciones del mercado de cómputo y almacenamiento para proponer la arquitectura idónea que cubra las expectativas de modernización, rendimiento y crecimiento de capacidad de su infraestructura. Las conclusiones resultantes de la investigación fueron la elección de HPE como la marca con la solución mejor calificada en cuanto a rendimiento, modernización, integración, escalabilidad y soporte técnico por los rankings de sitios web como Statista y Gartner. Además, la propuesta desarrollada en su tesis fue dimensionada para cubrir los requerimientos de crecimiento de capacidad de CPU, memoria y almacenamiento necesarios para las aplicaciones que la institución educativa

exige debido al incremento de sus actividades académicas y administrativas; y al avance del estado del arte en las tecnologías que los educandos requieren ser capacitados y que demandan más recursos de cómputo y almacenamiento en la institución.

Guevara y Lopez (2020), en su trabajo de titulación acerca de la implementación de un sistema de administración de un Cisco UCS mediante comandos de voz, tuvieron como objetivo desarrollar una solución que permitiera automatizar las funciones básicas de gestión de un UCS utilizando Cisco DevNet, Amazon Web Services y el asistente virtual Amazon Alexa en el centro de datos académico de la Universidad de las Américas. Los autores concluyen que la integración de estas tecnologías permitió simplificar la administración del entorno UCS mediante el uso de comandos de voz, ejecutados a través de dispositivos Amazon Echo y procesados mediante funciones en AWS Lambda desarrolladas en Python. Esta arquitectura posibilitó la interacción entre el usuario y el UCS Manager para realizar consultas y configuraciones básicas, facilitando la gestión remota de la infraestructura. Asimismo, resaltan que la propuesta no solo contribuye a la automatización de tareas administrativas en el centro de datos, sino que también promueve nuevas formas de interacción con los sistemas informáticos, destacando su potencial aplicación para mejorar la accesibilidad de personas con discapacidad y fomentar el desarrollo de soluciones innovadoras basadas en tecnologías de automatización y servicios en la nube.

Ayuso (2019), en su trabajo de titulación orientado al diseño e implementación de una infraestructura virtual basada en servidores Cisco UCS y software de virtualización VMware, tuvo como objetivo desarrollar un entorno virtualizado que permitiera optimizar el uso de recursos físicos mediante la creación y gestión de máquinas virtuales en un clúster de servidores. El autor concluye que la implementación del hipervisor ESXi junto con la plataforma de administración vCenter permitió consolidar múltiples sistemas operativos en un mismo servidor, logrando una administración centralizada, mayor escalabilidad y eficiencia en el uso del hardware. Asimismo, destaca que la virtualización facilitó la reducción de costos operativos, la flexibilidad para

desplegar servicios como servidores proxy y de respaldo, y la posibilidad de ampliar la infraestructura en función de nuevas necesidades. Finalmente, resalta que el proyecto permitió adquirir una comprensión integral del diseño e implementación de entornos virtualizados, constituyendo una base sólida para el desarrollo de soluciones innovadoras en el ámbito de redes y centros de datos.

3.4.2 Marco conceptual

3.4.2.1 Metodología PPDIOO de Cisco

La gestión del ciclo de vida de las redes de telecomunicaciones requiere un enfoque estructurado para asegurar que la infraestructura sea viable y escalable. El modelo metodológico PPDIOO de Cisco Systems es un estándar en la industria para el despliegue de redes empresariales. Este marco define un ciclo continuo de seis fases orientado a reducir los costos operativos, mejorar la disponibilidad de los servicios y agilizar la integración de nuevas tecnologías (Purwanto y Soewito, 2021; Swari y Agussalim, 2023).

Las seis fases de este ciclo de vida se ilustran en la Figura 2 y se describen en las siguientes líneas:

1. Prepare (Preparar): Se establecen los requerimientos del negocio y la justificación financiera para adoptar la nueva tecnología.
2. Plan (Planificar): Se evalúa el estado de la red actual para determinar el plan de implementación, definiendo el alcance inicial del proyecto.
3. Design (Diseñar): Se elaboran los diseños técnicos detallados, que garantizan el cumplimiento de los requisitos técnicos.
4. Implement (Implementar): Se realiza la instalación física y la configuración lógica de los equipos en la red, buscando el menor impacto posible en los servicios activos.

5. Operate (Operar): Consiste en el mantenimiento diario y el monitoreo del rendimiento de la red una vez que los equipos entran en producción.
6. Optimize (Optimizar): Se analiza el desempeño de la red para identificar áreas de mejora o planificar futuras expansiones.

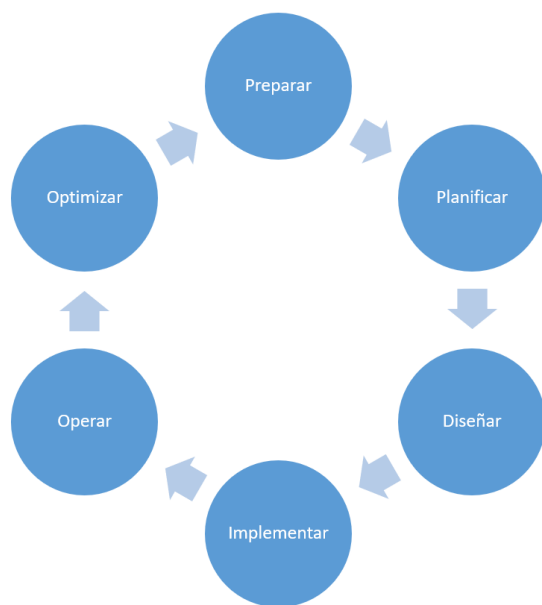


Figura 2 Fases del ciclo de vida de redes PPDIOO. Fuente. Elaboración propia basada en la metodología de implementación de redes de Cisco Systems.

3.4.2.2 Estándar PMBOK 6

El PMBOK (Project Management Body of Knowledge) en su sexta edición es una guía de buenas prácticas desarrollada por el Project Management Institute (PMI). En proyectos de infraestructura, este estándar organiza las tareas en fases claras para asegurar que la instalación de hardware y software cumpla con el tiempo, el alcance técnico y la calidad esperada (Project Management Institute, 2017; Pribadi et al., 2022).

La Figura 3 ilustra la división del proyecto en cinco grupos de procesos.

1. Initiating (Inicio): Es la etapa donde se define el objetivo del proyecto y se obtienen las autorizaciones para comenzar.

2. Planning (Planificación): Se organiza el modo de trabajo y se elaboran los documentos de diseño técnico definitivos.
3. Executing (Ejecución): Es la etapa técnica donde se instalan los equipos físicos y se aplican las configuraciones lógicas.
4. Monitoring and Controlling (Monitoreo y Control): Se supervisa el avance para asegurar el cumplimiento del plan y se realizan ajustes ante imprevistos técnicos en campo.
5. Closing (Cierre): Consiste en la entrega oficial del proyecto operando correctamente, junto con la firma de actas e informes finales.

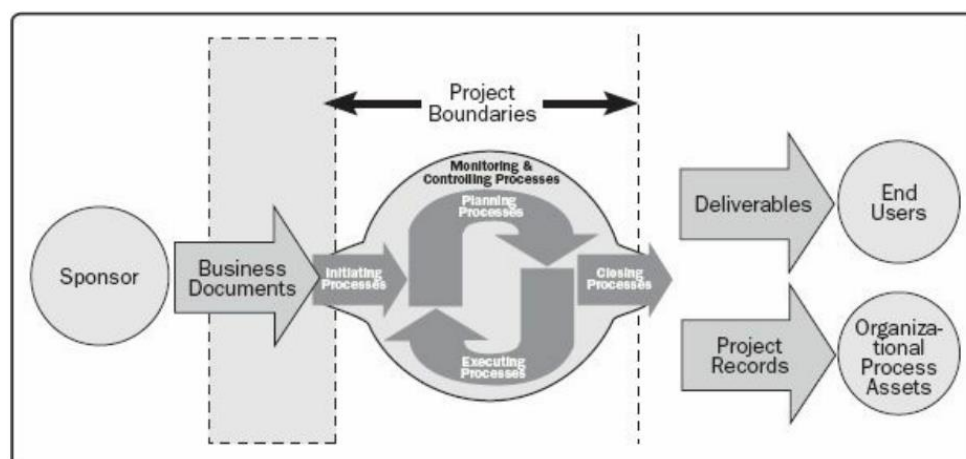


Figura 3 Grupos de Procesos de la Gestión de Proyectos según PMBOK 6.
Fuente. Datos tomados de Project Management Institute (2017).

3.4.2.3 LAN

La red de área local (LAN) en un centro de datos representa la infraestructura de conectividad que permite el intercambio de información entre los servidores, los usuarios y las aplicaciones. A diferencia de una red doméstica, la LAN de grado empresarial requiere de equipos de alta capacidad que soporten grandes volúmenes de tráfico de datos con una latencia mínima. En este proyecto, la red LAN se encarga de gestionar la comunicación de los servicios de la clínica, asegurando que los sistemas administrativos y médicos

estén disponibles de forma permanente a través de mecanismos de redundancia en hardware y enlaces físicos.

Topologías de Red en Entornos Corporativos y Centros de Datos

La topología define la forma en que se interconectan los dispositivos de red. Históricamente, las redes se han diseñado bajo un modelo jerárquico tradicional de tres capas (Acceso, Distribución y Core) para segmentar las funciones de conectividad y separar el tráfico de los usuarios finales del tráfico de los servidores. Sin embargo, en los centros de datos modernos se utiliza frecuentemente la arquitectura Leaf-Spine o de red plana. Este diseño de dos capas permite que cualquier servidor se comuniquen con otro de forma directa y rápida, optimizando el tráfico de datos en sentido horizontal (este-oeste) y reduciendo notablemente los tiempos de latencia dentro del entorno virtualizado. Según estudios sobre infraestructuras críticas, la elección de la topología impacta directamente en la facilidad para diagnosticar fallas y en la capacidad de crecimiento futuro de la red sin afectar los servicios activos (Jiménez y Torres, 2021).

Arquitectura de Core Colapsado (Modelo de dos capas)

El diseño de Core colapsado es una variante simplificada en dos capas del modelo jerárquico tradicional de tres niveles. En esta estructura, las funciones de la capa de distribución y del núcleo de la red se integran en un solo bloque funcional, utilizando un par de switches de alta capacidad. Este enfoque es ideal para entornos donde se busca optimizar el rendimiento y la disponibilidad sin la complejidad de una capa intermedia separada, lo que permite reducir la cantidad de hardware, el consumo de energía y el esfuerzo administrativo. Para el caso de la clínica, este modelo garantiza una conexión directa y de alta velocidad entre el centro de datos y la red de campus, suprimiendo saltos innecesarios y minimizando la latencia en el acceso a los servicios de salud (Bruno y Jordan, 2024).

La Figura 4 ejemplifica este tipo de arquitectura de red LAN.

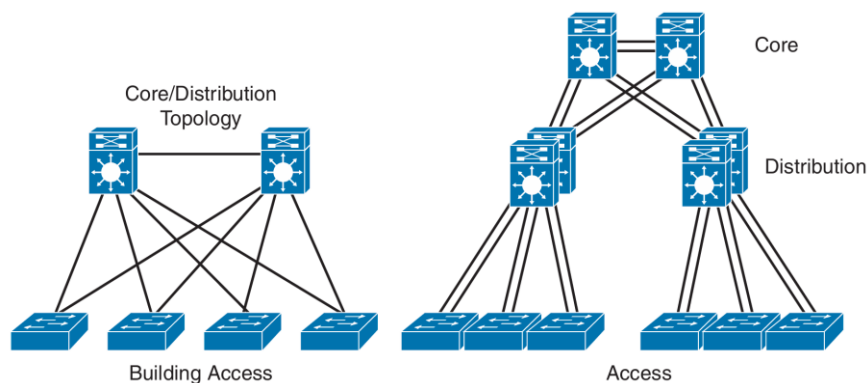


Figura 4 Diseño de Core Colapsado. Fuente. Datos tomados de Bruno y Jordan (2024).

Redes de Área Local (LAN) en la Capa de Core

El Core de la red es el punto central donde se concentra todo el tráfico. En esta capa, los switches Nexus operan como el núcleo de la red LAN, encargándose de decidir la ruta más rápida para los paquetes de datos que viajan entre diferentes sedes o departamentos. Su función principal es el enrutamiento de alta velocidad, asegurando que no existan cuellos de botella cuando muchos usuarios acceden a los sistemas de la clínica.

Protocolo Ethernet

Ethernet es el estándar de capa de enlace utilizado para la red LAN de la clínica. Su función práctica es organizar la información en tramas para su envío a través de los medios físicos. En este diseño, Ethernet no solo transporta el tráfico de los usuarios, sino que facilita funciones de redundancia mediante la agregación de enlaces (*Port-Channel*). La robustez de Ethernet en centros de datos modernos reside en su capacidad para manejar velocidades crecientes manteniendo la compatibilidad con tecnologías anteriores (Tanenbaum y Wetherall, 2021).

Protocolo IP

El protocolo de Internet (IP) es el responsable del direccionamiento y enrutamiento de los paquetes. En la práctica, permite que cada servidor y

switch de la clínica tenga una dirección única para comunicarse entre diferentes subredes. Mientras Ethernet mueve los datos dentro de un mismo segmento físico, el protocolo IP permite que los switches Nexus en capa de Core realicen el envío de información hacia otras sedes o Internet, basándose en tablas de enrutamiento para asegurar que cada paquete llegue a su destino final (Kurose y Ross, 2022).

LAN Virtual (VLAN)

Una VLAN es una tecnología que permite segmentar de forma lógica una red física en múltiples redes independientes. En el entorno de un centro de datos hospitalario, el uso de VLANs es fundamental por motivos de seguridad y rendimiento. Permite separar el tráfico de administración de los equipos, el tráfico de datos de los pacientes y el tráfico de los invitados; garantizando que un problema de saturación o seguridad en un segmento no afecte la operatividad de los demás, todo compartiendo los mismos switches físicos y enlaces Nexus (Odom, 2024).

Virtual Port Channel (vPC)

vPC es una tecnología que permite agrupar puertos físicos de dos switches diferentes para que funcionen como si fueran un solo enlace lógico. Esto es fundamental para la alta disponibilidad, ya que si uno de los switches de la red LAN falla, el tráfico continúa fluyendo por el segundo switch sin interrupciones. A diferencia de otros métodos como Spanning Tree, vPC permite utilizar el 100% del ancho de banda disponible en ambos switches de forma simultánea, optimizando el rendimiento de la red.

Protocolo de Enrutamiento de Standby en Caliente (HSRP)

El protocolo HSRP (Hot Standby Router Protocol) es una tecnología de Cisco diseñada para proporcionar alta disponibilidad en el gateway predeterminado de una red. Funciona mediante la agrupación de dos switches de capa 3 en un grupo que comparte una dirección IP y una dirección MAC virtuales. En

este esquema, un equipo asume el rol "Active" para procesar el tráfico, mientras que el segundo permanece en modo "Standby". Si el switch activo falla, el secundario asume inmediatamente las funciones de enrutamiento de forma transparente para los usuarios, asegurando la continuidad operativa de los servicios críticos sin necesidad de reconfigurar los hosts finales (Edgeworth y Lacoste, 2023).

Port Channel Ethernet

El Port Channel permite combinar varios cables de red físicos en una sola conexión lógica. Esto sirve para aumentar la velocidad de transferencia (por ejemplo, combinando dos enlaces de 10 Gbps para obtener 20 Gbps) y para proporcionar seguridad, ya que, si un cable se rompe, la conexión no se pierde, sino que continúa funcionando a través de los cables restantes del grupo.

3.4.2.4 SAN

En la arquitectura de servidores, el almacenamiento puede presentarse de distintas formas. El almacenamiento local o Direct-Attached Storage (DAS) se refiere a los discos duros instalados físicamente dentro del servidor. Si bien es rápido, no puede ser compartido fácilmente con otros equipos. Por otro lado, el almacenamiento SAN-Attached externaliza los discos hacia una red dedicada, permitiendo que múltiples servidores accedan de forma simultánea y centralizada a los mismos datos, lo cual es un requisito indispensable para tecnologías de alta disponibilidad como los clústeres de VMware.

La red de área de almacenamiento (SAN) es una red independiente dedicada exclusivamente a conectar los servidores con los arreglos de almacenamiento, tal como se muestra en la Figura 5. A diferencia de la red LAN, donde viaja tráfico IP, en la SAN solo viaja información de lectura y escritura de archivos y máquinas virtuales. Esta separación es crucial para garantizar que el acceso a los datos sea extremadamente rápido y que no se pierda ninguna transacción debido a la congestión de la red de usuarios.

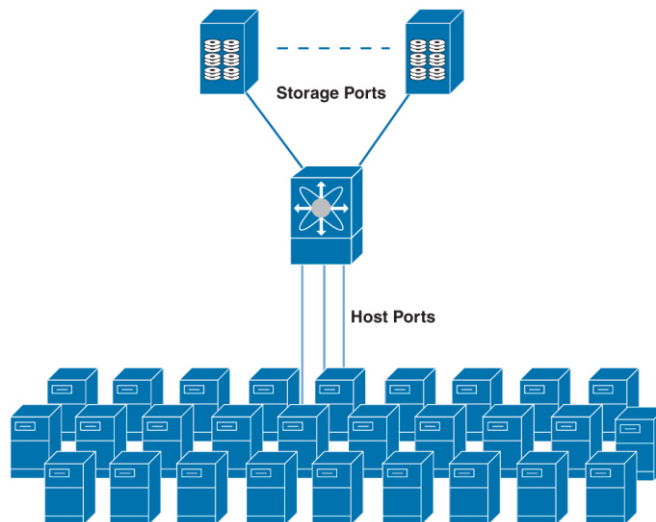


Figura 5 Topología de una red SAN. Fuente. Datos tomados de Maloo et al. (2023).

Controlador de Almacenamiento

En la arquitectura de almacenamiento, ya sea interno en un servidor o en un arreglo externo de discos, el controlador es el cerebro del sistema. Es el componente de hardware equipado con procesadores y memoria caché que recibe las peticiones de lectura y escritura. En un entorno de almacenamiento local (DAS), se presenta generalmente como una tarjeta controladora RAID dentro del servidor. Por su parte, en las topologías SAN, son módulos de alto rendimiento que además de leer y escribir en los discos, gestionan la protección avanzada de datos y la entrega de información a múltiples servidores simultáneamente a gran velocidad (Hwang et al., 2021).

Protocolos de Comunicación de Almacenamiento: SCSI, NVMe, SAS e iSCSI

Para que un servidor pueda interactuar con un disco, necesita hablar un lenguaje o protocolo de comandos:

- **SCSI (Small Computer System Interface):** Es el conjunto de comandos base e histórico que utilizan los sistemas operativos para solicitar bloques de información a los discos.

- NVMe (Non-Volatile Memory Express): A diferencia de SCSI, que fue concebido en la era de los discos mecánicos, NVMe es un protocolo moderno diseñado desde cero para memorias de estado sólido (SSD). Al conectar el almacenamiento directamente al bus PCIe del servidor, elimina los cuellos de botella lógicos y ofrece tiempos de respuesta casi instantáneos.
- SAS (Serial Attached SCSI): Es la evolución del SCSI tradicional, utilizado principalmente para conectar discos de estado sólido y mecánicos empresariales de forma directa dentro del servidor (DAS).
- iSCSI (Internet SCSI): Es un protocolo que encapsula los comandos SCSI dentro de paquetes de red estándar TCP/IP, permitiendo acceder a arreglos de almacenamiento a través de la red LAN convencional (Ethernet) en lugar de utilizar una red de fibra dedicada.

Número de Unidad Lógica (LUN)

Una LUN (Logical Unit Number) es una porción lógica de espacio de almacenamiento creada dentro del arreglo de discos que se presenta a un servidor específico. Para el sistema operativo del servidor, la LUN aparece como si fuera un disco duro físico local recién instalado, listo para ser formateado y utilizado para alojar bases de datos o máquinas virtuales.

Fibre Channel (FC)

Fibre Channel es el protocolo especializado para redes SAN. Su principal ventaja es que está diseñado para no perder paquetes de datos (*loss/less*). Mientras que en Ethernet es común que algunos datos se retransmitan si hay congestión, en FC existen mecanismos de control por hardware denominado *Buffer-to-Buffer Credits* (BB_Credits). Este mecanismo impide que un dispositivo transmisor envíe tramas si el receptor no tiene espacio libre en sus

búferes, garantizando la integridad de las lecturas y escrituras de información de almacenamiento.

Modos de Puerto Fibre Channel (F y E)

Los puertos de un switch SAN MDS cambian su comportamiento según lo que tengan conectado:

- Puerto modo N (Node): Es el puerto que reside físicamente en el dispositivo final, como la tarjeta adaptadora (HBA) de un servidor o la interfaz de un arreglo de discos. Es el punto exacto donde se inician o terminan las comunicaciones de almacenamiento, y siempre se enlaza mediante fibra óptica hacia un puerto modo F.
- Puerto modo F (Fabric): Es el puerto de acceso en el switch SAN, como los equipos de la serie MDS, diseñado para recibir la conexión directa de los dispositivos finales (puertos N). Su función principal es servir como puerta de entrada para que los servidores y los sistemas de almacenamiento se integren de forma segura a la matriz de la red.
- Puerto modo E (Expansion): Se usa exclusivamente para conectar un switch SAN con otro, permitiendo que la red de almacenamiento se extienda entre diferentes salas o sedes.

NPV y NPIV

Estas tecnologías permiten virtualizar las conexiones en la SAN para hacerlas más eficientes. El modo NPV se activa en el equipo que conecta los servidores (Fabric Interconnect) para que este se comporte como un puente y no complique la gestión del switch principal. Por su parte, NPIV permite que una sola conexión física transporte las identidades de múltiples máquinas virtuales, asignando a cada una su propia dirección dentro de la red SAN.

Redes de Almacenamiento Virtuales (VSAN)

Al igual que las VLANs en la red de datos, una VSAN permite dividir lógicamente un switch de red de almacenamiento físico en múltiples switches virtuales aislados. Esto proporciona un alto nivel de seguridad y estabilidad, ya que permite separar el tráfico de almacenamiento de diferentes entornos dentro de la misma infraestructura física MDS (Cisco Systems, 2026a).

Direccionamiento en la red SAN: WWN, FCID y FCNS

A diferencia de la red LAN que usa direcciones MAC e IP, la red SAN utiliza sus propios identificadores:

1. WWN (World Wide Name): Es el identificador único y permanente grabado de fábrica en cada tarjeta Fibre Channel, similar a la dirección MAC. Existen el Node WWN (nWWN) que identifica al equipo físico, y el Port WWN (pWWN) que identifica al puerto específico.
2. FCID (Fibre Channel ID): Es una dirección de enrutamiento dinámica de 24 bits, comparable a la dirección IP, que el switch SAN asigna temporalmente a un puerto cuando este se conecta, permitiendo que los datos viajen por la red de forma eficiente.
3. FCNS (Fibre Channel Name Server): Es un servicio interno del switch SAN que funciona como un directorio; registra todos los WWNs y FCIDs conectados a la red para que los servidores y los discos puedan encontrarse entre sí.

Procesos de Inicio de Sesión: FLOGI, PLOGI y PRLI

Para que la comunicación exista en una red SAN, los equipos deben pasar por un proceso de registro estricto:

- FLOGI (Fabric Login): Es el primer paso. El servidor se conecta al

switch SAN, presenta su WWN y solicita su dirección de red temporal (FCID) para registrarse en el FCNS.

- PLOGI (Port Login): Es el segundo paso. Una vez que el servidor está en la red, realiza un PLOGI para establecer una sesión de comunicación de extremo a extremo directamente con el puerto del sistema de almacenamiento con el que desea intercambiar datos.
- PRLI (Process Login): Es el tercer y último paso. Tras establecer la conexión de extremo a extremo, los equipos usan el PRLI para negociar los parámetros del protocolo de capa superior, generalmente SCSI sobre Fibre Channel (FCP). En esta etapa se definen los roles operativos, confirmando formalmente quién actuará como iniciador y quién como *target*, dejando el canal completamente listo para la lectura y escritura de bloques de datos.

Fibre Channel Multipath (MPIO)

El Multipathing es una tecnología de alta disponibilidad configurada en el hipervisor. Permite que el servidor utilice simultáneamente varias conexiones físicas Fibre Channel para acceder a la misma LUN en el almacenamiento. Si un cable, un switch o un puerto falla, el software desvía el tráfico por otro camino sin que las aplicaciones pierdan conexión (Broadcom, 2026).

FSPF (Fabric Shortest Path First)

FSPF es el “OSPF” de la red SAN. Es el protocolo encargado de calcular cuál es el camino más corto y eficiente para que los datos viajen entre switches. En este proyecto, FSPF es el responsable de gestionar la conexión entre los switches MDS de la sede clínica y los de la sede central.

Zonificación (Zoning)

La zonificación es una medida de seguridad fundamental en las redes de

almacenamiento que define qué servidor tiene permiso para comunicarse con qué disco o arreglo de almacenamiento. Funciona de manera similar a una lista de control de acceso, asegurando un aislamiento lógico para evitar que un servidor acceda por error a la información de otro. Técnicamente, este proceso se realiza mediante el agrupamiento de las direcciones pWWN de los iniciadores, que representan a los servidores, y los *targets*, que corresponden a los puertos del arreglo de almacenamiento, permitiendo que la comunicación y visibilidad de los datos ocurra únicamente entre los miembros autorizados dentro de la zona (Cisco Systems, 2026a).

Licenciamiento en Switches SAN

Los switches MDS utilizan un modelo de licencias basado en el uso. El equipo viene con una cantidad de puertos físicos, pero solo se activan mediante software aquellos que el cliente necesita. Esto permite que la clínica empiece con una inversión menor y vaya activando más puertos conforme crezca su necesidad de almacenamiento sin cambiar el equipo físico.

Port Channel FC

Al igual que en la red LAN, el Port Channel en la red SAN agrupa varios enlaces de fibra óptica para que funcionen como uno solo de mayor velocidad. Esto es muy común en los enlaces entre switches (ISL) para asegurar que el flujo de datos entre servidores y discos no tenga restricciones de velocidad.

Device-alias

El *device-alias* es una función de los switches MDS que permite asignar nombres legibles (como "Storage1-P1-N1") a las direcciones físicas (pWWN) de los dispositivos conectados a la SAN. Existen dos modos de operación: el modo básico y el modo *enhanced*. En el modo básico, los nombres se traducen a sus valores hexadecimales al momento de configurar la zona, mientras que en el modo *enhanced* el nombre se mantiene como una identidad lógica en toda la base de datos del *fabric*. Esta herramienta es

fundamental en la administración de redes SAN de centros de datos, ya que reduce significativamente el riesgo de errores humanos al momento de identificar servidores o arreglos de almacenamiento durante tareas de mantenimiento o expansión (Cisco Systems, 2026a).

Modos de Zonificación y Seguridad (Enhanced Zoning)

La zonificación en redes Fibre Channel se puede implementar en modo básico o mejorado (*enhanced zoning*). El modo *enhanced* proporciona una capa adicional de seguridad y consistencia al implementar un mecanismo de bloqueo de sesión. Esto garantiza que solo un administrador pueda realizar cambios en la base de datos de zonas a la vez, evitando que configuraciones simultáneas generen conflictos o inconsistencias en la matriz. Además, este modo asegura que todos los switches de la red SAN tengan una copia idéntica y validada de la política de seguridad activa, lo cual es crítico en entornos hospitalarios donde la disponibilidad de la data es prioritaria (Cisco Systems, 2026a).

Distribución de Zonas

Cuando se interconectan dos switches SAN, estos deben fusionar sus bases de datos de zonas. La función `zone merge-control restrict` es una directiva de seguridad que instruye al switch a detener el proceso de unión si se detectan discrepancias entre las zonas de ambos equipos. Por otro lado, la función `zone distribute` utiliza el protocolo Cisco Fabric Services (CFS) para replicar automáticamente cualquier cambio en la zonificación a través de todos los switches interconectados. Estas funciones aseguran que la red extendida entre diferentes sedes mantenga una política de acceso uniforme y protegida ante errores de configuración durante la fusión de redes (Cisco Systems, 2026a).

3.4.2.5 Capa 1: Interfaces, SFPs y QSFPs

La capa física comprende los medios de transmisión y los transceptores

ópticos utilizados tanto en la red LAN como en la SAN. En este proyecto se emplean principalmente dos factores de forma:

- SFP (Small Form-factor Pluggable): Son módulos compactos utilizados para conexiones de 10/25 Gbps en Ethernet y hasta 32 Gbps en Fibre Channel. Se seleccionan transceptores de corto alcance (SR) para fibras multimodo dentro del mismo centro de datos.
- QSFP (Quad SFP): Se utilizan en los enlaces de alta densidad, como la conexión entre el chasis UCS y los FI, permitiendo velocidades de 40 Gbps y 100 Gbps mediante la agregación de cuatro canales internos.

3.4.2.6 Servidores y Computación Unificada

El modelo de infraestructura on-premise consiste en el despliegue, gestión y mantenimiento de los servidores y equipos de red directamente dentro de las instalaciones físicas de la propia organización. Aunque los modelos de computación en la nube pública (Cloud) ofrecen una alta flexibilidad, muchas instituciones, particularmente en sectores críticos como el de la salud, optan por mantener arquitecturas on-premise por estrictos motivos de seguridad y cumplimiento normativo. Este enfoque garantiza que el procesamiento y almacenamiento de datos altamente sensibles, como los historiales médicos de los pacientes, se mantenga confinado dentro de la red privada local. Al evitar enviar este tráfico crítico a través de Internet, la clínica mitiga las vulnerabilidades de exposición externa, reduce problemas de latencia y retiene el control absoluto sobre el ciclo de vida de su información y hardware (Hwang et al., 2021).

La computación unificada es un concepto que busca integrar el procesamiento de los servidores con la conectividad de la red en un solo sistema gestionado centralmente. En lugar de tener servidores independientes con muchos cables cada uno, se utiliza un sistema modular que reduce el cableado y permite

administrar todo el hardware desde una única consola. Este enfoque mejora la agilidad del área de TI, permitiendo desplegar nuevos servicios en cuestión de minutos en lugar de días.

Cisco UCS Serie X

La Serie X de Cisco es la plataforma de servidores de última generación instalada en este proyecto. Consiste en un chasis modular que alberga servidores de tipo *blade*. Su diseño innovador permite una mejor refrigeración y está preparado para futuras tecnologías de procesamiento, asegurando que la inversión de la clínica tenga una larga vida útil (Cisco Systems, 2025d).

Virtualización de Interfaces: vNIC y vHBA

Una de las ventajas de la arquitectura de Cisco UCS es la abstracción del hardware. En lugar de instalar múltiples tarjetas físicas en cada servidor, el sistema utiliza tarjetas de red convergentes (VIC) que permiten crear interfaces virtuales. Las vNICs (Virtual Network Interface Cards) son tarjetas de red virtuales presentadas al sistema operativo para el tráfico LAN, mientras que los vHBAs (Virtual Host Bus Adapters) son interfaces virtuales dedicadas al tráfico de almacenamiento SAN. El ingeniero puede definir por software cuántas de estas tarjetas necesita cada servidor, su velocidad y su redundancia, simplificando radicalmente el diseño físico (Maloo et al., 2023).

Fabric Interconnect (FI) Serie 6400

El Fabric Interconnect es el cerebro del sistema de servidores. Es el equipo donde se conectan físicamente los chasis de servidores y donde se definen todas las reglas de red. Unifica todo el tráfico de las redes LAN y SAN, actuando como el único punto de gestión para todos los servidores UCS.

Cisco Intersight

Cisco Intersight es una plataforma de gestión basada en la nube. A través de

Intersight, el personal de ingeniería puede monitorear la salud de los servidores, actualizar el software y recibir alertas preventivas de posibles fallas desde cualquier lugar. Esto representa un cambio frente a los sistemas antiguos que requerían estar físicamente en el centro de datos para realizar tareas de mantenimiento.

Conexión IFM 9108 - FI 6454

La conectividad interna del chasis UCS X9508 se gestiona a través de los módulos IFM 9108 (Intelligent Fabric Modules). Estos componentes eliminan la necesidad de un panel de conexiones interno rígido, proporcionando enlaces de alta velocidad de 25 Gbps hacia cada nodo de cómputo (blade). La conexión física desde el IFM hacia los Fabric Interconnect 6454 se realiza mediante puertos de 100 Gbps. Esta estructura asegura que el chasis cuente con el ancho de banda necesario para manejar el tráfico de las aplicaciones sin generar saturación en los enlaces de subida (Cisco Systems, 2025d).

3.4.2.7 Virtualización

La virtualización es una tecnología que permite dividir un único servidor físico en múltiples "servidores virtuales" independientes. Esto permite un uso mucho más eficiente del hardware, ya que una sola máquina potente puede ejecutar simultáneamente varios sistemas operativos y aplicaciones, ahorrando espacio, energía y costos de mantenimiento. En este entorno, el software encargado de repartir los recursos del equipo físico es el hipervisor.

Hipervisores

El hipervisor es la capa de software que gestiona las máquinas virtuales. Existen dos tipos principales:

- Tipo 1 (Nativo o Bare-Metal): Se instala directamente sobre el hardware del servidor. Es el más eficiente y seguro, por lo que es el estándar para centros de datos empresariales como el de

la clínica.

- Tipo 2 (Hosted): Se instala sobre un sistema operativo ya existente (como Windows). Es común para uso personal o pruebas, pero no para servicios críticos debido a su menor rendimiento (Castro y López, 2023).

VMware ESXi 8.0

ESXi es el hipervisor de Tipo 1 utilizado en este proyecto. Se instala en los servidores Cisco UCS para crear el entorno donde funcionarán las máquinas virtuales. La versión 8.0 ofrece mejoras en el rendimiento de los procesadores modernos y mayor seguridad para proteger los datos médicos contra ataques.

Redes Virtuales: Port Group y VMkernel

Dentro del hipervisor ESXi, la red física se virtualiza utilizando switches virtuales. Para gestionar el tráfico en estos switches se utilizan dos componentes clave:

- Port Group: Es una agrupación lógica de puertos virtuales que comparten la misma configuración, como el identificador de la VLAN o las políticas de seguridad. Las máquinas virtuales se conectan a estos Port Groups para tener acceso a la red de la clínica.
- VMkernel: Es una interfaz de red especializada y exclusiva para el uso interno del propio hipervisor ESXi. Se utiliza para cursar tráfico crítico de la infraestructura, como la conexión al almacenamiento de red, el tráfico de administración del servidor y el movimiento de máquinas virtuales entre nodos físicos.

vSphere vCenter 8.0

vCenter es la consola de administración central para todo el entorno virtual de

VMware. Permite que el equipo de TI gestione todos los servidores ESXi desde un solo lugar, facilitando tareas como mover una máquina virtual de un servidor a otro sin que el servicio se detenga (vMotion) o reiniciar automáticamente las máquinas en otro servidor si uno físico falla (High Availability).

vMotion

vMotion es una de las tecnologías más críticas de VMware vSphere. Permite trasladar una máquina virtual en funcionamiento desde un servidor físico hacia otro, transfiriendo su estado activo en la memoria RAM y sus conexiones de red sin interrumpir el servicio ni causar tiempo de inactividad perceptible. Esta función es vital para mantener la operatividad de los sistemas médicos cuando se requiere apagar un servidor para realizar mantenimiento al hardware (Broadcom, 2026).

3.5 Procedimiento

Por motivos de seguridad y confidencialidad, a petición de la clínica, se han ocultado o modificado los datos sensibles en las evidencias de este documento. Esto incluye la razón social de la clínica, nombres de los equipos, números de serie, fechas exactas, direcciones IP, MAC, WWN y otros identificadores lógicos. Tomar esta medida protege la red del cliente, pero no afecta en nada la validez técnica de las configuraciones y los resultados mostrados.

3.5.1 Elección de la Tecnología

En la fase de preventa (julio de 2025), el área de ingeniería evaluó las principales alternativas del mercado de centros de datos de última generación para reemplazar la plataforma obsoleta de la clínica. El objetivo era encontrar una solución que integrara alta densidad de cómputo, redes LAN de alta velocidad y conectividad SAN tolerante a fallas, garantizando un ciclo de vida mínimo de 5 años.

Se analizaron tres propuestas técnicas de los principales fabricantes del rubro de infraestructura de servidores y redes, calculando el Costo Total de Propiedad (TCO) a 5 años, el cual incluye la adquisición del hardware (CAPEX) y los servicios de soporte y licenciamiento que cada fabricante brinda a su propia tecnología (OPEX).

3.5.1.1 HPE - Synergy 480 Gen11

- *Descripción:* Arquitectura componible basada en chasis modulares Frame 12000.
- *Costo Estimado a 5 años (TCO):* Aproximadamente US\$ 225,000 (CAPEX referencial de US\$ 160,000 + OPEX de US\$ 65,000). El costo se eleva debido a los módulos de interconexión propietarios (Virtual Connect) y al licenciamiento avanzado de HPE OneView.
- *Ventajas:* Excelente granularidad en la asignación dinámica de recursos de almacenamiento local y cómputo.

3.5.1.2 Dell Technologies - PowerEdge MX7000

- *Descripción:* Plataforma modular de 7U orientada a centros de datos empresariales con soporte para procesadores Intel Xeon de 5ta generación.
- *Costo Estimado a 5 años (TCO):* Aproximadamente US\$ 192,000 (CAPEX referencial de US\$ 142,000 + OPEX de US\$ 50,000). Presenta el costo de adquisición más agresivo del mercado.
- *Ventajas:* Chasis robusto sin plano posterior (*midplaneless*), lo que facilita futuras actualizaciones directas de bus sin cambiar la estructura.

3.5.1.3 Cisco Systems - Solución implementada

- *Descripción:* Arquitectura de cómputo unificado modular gestionada nativamente en la nube (Cisco Systems, 2025d).
- *Costo a 5 años (TCO):* US\$ 209,996 (CAPEX de US\$ 151,796 + OPEX de US\$ 58,200 por SaaS y soporte CX Level 1 24x7).
- *Ventajas:* Integración total del ecosistema de cómputo, red LAN y almacenamiento SAN bajo una sola consola de administración en nube (Cisco Intersight).

3.5.1.4 Definición de solución propuesta

A pesar de la competitividad de Dell y HPE, la preventa seleccionó la solución unificada de Cisco debido a los siguientes criterios de ingeniería y negocio:

- Un factor decisivo en la optimización del presupuesto fue el nivel de relación comercial de Noovus con Cisco. Esto permitió acceder a descuentos exclusivos por especialización de canal, logrando optimizar el TCO para la clínica y, al mismo tiempo, maximizando los márgenes del integrador durante la licitación.
- La clínica ya contaba en su infraestructura antigua con servidores blade de la plataforma Cisco UCS Serie B. Al mantener la misma línea de fabricante, el personal de TI del cliente ya estaba familiarizado con el aprovisionamiento basado en plantillas e identidades lógicas. El paso a la Serie X no requirió gastos adicionales en costosos cursos de certificación o capacitación desde cero para los administradores, reduciendo el riesgo operativo por error humano y garantizando un pase a operación inmediato (Cisco Systems, 2025d).
- Traslada el plano de gestión a la nube con el servicio Cisco

Intersight. Evita instalar servidores locales de gestión dentro del chasis, centralizando firmwares y políticas sin infraestructura de cómputo ni almacenamiento dedicada a gestores.

- En la LAN (Fabric Interconnects 6454), el modo End-Host evita activar Spanning Tree hacia el Core de la clínica, anulando el riesgo de bucles lógicos. En la SAN, el modo End-Host activa la virtualización de puertos NPV/NPIV con los switches MDS 9132T, consolidando múltiples WWNs de VMware ESXi 8.0 en un solo puerto físico. Esto simplifica la carga administrativa de red en la solución Cisco UCS Serie X.
- Mediante los módulos IFM 9108, todo el tráfico LAN/SAN de los blades viaja unificado hacia los Fabric Interconnects en enlaces 25G, reduciendo el cableado físico e incrementando la escalabilidad ante futuras ampliaciones de capacidad.

Durante la preventa, el equipo de ingenieros preventa recibe los requerimientos del cliente para elaborar una propuesta de solución. Esta propuesta abarca el equipamiento nuevo elegido por el integrador, la arquitectura física y lógica propuesta para la solución, funciones y protocolos de red a alto nivel a utilizar, el alcance de los servicios de la empresa integradora y una propuesta económica, los cuales deben ser lo suficientemente competitivos a nivel técnico y económico frente a los demás postores para poder recibir la buena pro de la empresa solicitante.

3.5.2 Metodología de Implementación

Al adjudicarse un proyecto a Noovus, el área de preventa debe transferirle al área de Ingeniería Postventa toda la información del proyecto que forma parte de las propuestas Técnica y Económica, lo cual comprende: diseño propuesto, equipamiento comprado, alcance de los servicios de Noovus y plazos. Con esta información, el área de postventa asigna los recursos necesarios y los roles de cada uno para la ejecución del proyecto.

El proyecto inicia con la celebración del Kick Off, donde las partes interesadas del proyecto se reúnen en forma presencial o telepresencial para repasar los objetivos y alcances del proyecto, y realizar coordinaciones iniciales entre los equipos de ingeniería del lado cliente, implementación del lado proveedor y logísticos de ambos lados. Esto inicia la etapa de “Diseño y planificación” del proyecto.

El equipo de ingeniería postventa sostiene reuniones técnicas con el cliente para realizar el levantamiento de información detallado de la solución actual (AS IS). Si bien en la etapa de preventa ya se propuso una arquitectura, en este levantamiento se pueden identificar detalles de la solución actual que requieran nuevas consideraciones en el diseño propuesto. Con este levantamiento de información se puede confirmar el diseño a alto nivel (High Level Design o HLD) de la solución que se implementará en el proyecto (TO BE); y se puede elaborar el cronograma del proyecto, el cual va actualizando sus fechas a medida que se avanza el diseño, los planes de trabajo, migración y surgen nuevas consideraciones, restricciones o cambios a lo largo de la ejecución del proyecto.

Para el despliegue de la nueva infraestructura en la clínica, se utilizó la metodología PPDIOO de Cisco, adaptando sus etapas a la operatividad de los proyectos de integración. Las fases iniciales de Preparación y Planificación (PP) fueron ejecutadas por el área de preventa durante la elaboración de la propuesta comercial.

La fase de Diseño (Design) funcionó como una etapa de transición; se inició con la arquitectura conceptual de preventa y concluyó con la intervención del área de ingeniería postventa para realizar el levantamiento de información de la red actual (AS-IS) y elaborar los diseños a bajo nivel (LLD) definitivos. Las fases de Operación y Optimización (OO) serán responsabilidad del cliente tras la entrega de la solución.

El alcance del presente trabajo abarca el cierre de la fase de diseño y la totalidad de la fase de implementación (Implement). Para mantener un orden

técnico y administrativo, se organizaron las tareas mediante los cinco grupos de procesos del PMBOK 6 (Project Management Institute, 2017):

1. Inicio (Initiating): Se realizó la reunión de Kick Off y las coordinaciones iniciales con los líderes de la clínica para alinear los objetivos, definir los canales de comunicación y establecer las ventanas de trabajo que no afectaran la operación hospitalaria.
2. Planificación (Planning): Se ejecutó el levantamiento de información de la arquitectura existente. Con estos datos, se elaboraron los documentos HLD y LLD, definiendo los direccionamientos y puertos de los equipos Cisco UCS, Nexus y MDS.
3. Ejecución (Executing): Comprendió el trabajo físico en los gabinetes y la configuración lógica. Se realizaron las ventanas de migración, trasladando las conexiones LAN en frío y la conectividad SAN en caliente hacia los equipos nuevos.
4. Monitoreo y Control (Monitoring and Controlling): Se supervisó el avance para resolver incidentes. En esta fase se determinó el uso de una topología de convivencia (enlaces ISL) entre los switches MDS nuevos y antiguos para solucionar la incompatibilidad detectada en el chasis legado UCS B.
5. Cierre (Closing): La implementación finalizó con la estabilización de los servicios, la entrega del Informe Técnico final por parte del implementador a la clínica y la firma de las actas de conformidad de la solución por parte del cliente.

3.5.3 Diseño a Alto Nivel (HLD)

La solución está basada en un diseño validado por Cisco, garantizando la compatibilidad entre todos los componentes de la topología, combinando buenas prácticas en las configuraciones de red LAN, SAN y servidores. Este

diseño implementa la serie X de UCS, y permitirá ampliar la infraestructura virtualizada que tiene la clínica, además de contar con una poderosa plataforma de gestión y monitoreo en nube, como lo es Cisco Intersight.

En los siguientes párrafos se describe el equipamiento de cómputo y red que incluye la ampliación.

Para la capa de cómputo, se implementa un chasis modular Cisco UCS X9508 poblado con tres nodos de cómputo Cisco UCS X210c M7 que incluyen dos CPU Intel Platinum I8562Y+ con 32 núcleos cada uno, 512 GB de RAM y dos unidades de almacenamiento SSD M.2 SATA local de 400 GB. La Figura 6 ilustra cómo se ve un chasis Cisco UCS X9508 por delante y detrás, lo que nos da una idea de la flexibilidad del chasis para cubrir diversos requerimientos de un cliente, permitiendo brindarle una solución a la medida. Mientras tanto, la Figura 7 muestra dos configuraciones de hardware distintas de servidores blade Cisco UCS X210c M7, cuya configuración es realizada por el área de manufactura de Cisco, donde insertan los componentes de CPU, memoria, GPU, tarjetas de red, entre otros tipos, según las capacidades que los servidores requieran. Estos blades serán habilitados para su uso como hipervisores con el sistema operativo VMware ESXi 8.0, donde albergarán las máquinas virtuales encargadas de ejecutar las distintas aplicaciones y servicios de la clínica (Cisco Systems, 2025d).

El control del tráfico unificado y la gestión centralizada se logran a través de dos Cisco Fabric Interconnect 6454 con puertos de servidor de hasta 25 Gbps, Ethernet de hasta 100 Gbps y FC de hasta 32 Gbps. Incluye licencias para 18 puertos Ethernet/FC de 10/25/8/16/32 Gbps y dos puertos Ethernet de 40/100 Gbps en cada FI. Esta nueva serie de servidores y switches de tráfico unificado tiene la novedad de permitir la gestión en nube a través del servicio SaaS Cisco Intersight, el cual reemplaza al antiguo software de gestión local (*on-premise*) UCS Manager de la serie B de Cisco UCS. La Figura 8 muestra el panel frontal de un Fabric Interconnect 6454, que ilustra la gran capacidad de puertos para conexiones a múltiples equipos de red LAN, SAN y Chasis Cisco UCS X9508 de forma escalable (Cisco Systems, 2021).

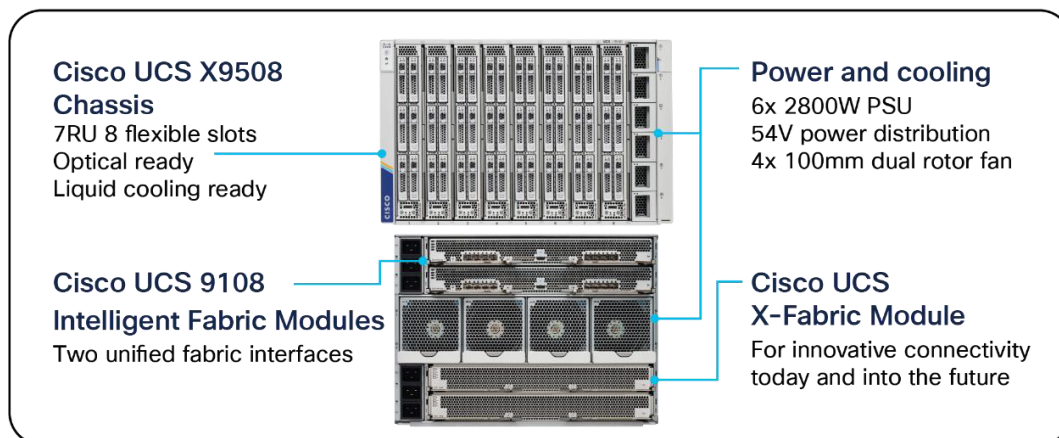


Figura 6 Vistas frontal y posterior del chasis modular Cisco UCS X9508. Fuente. Datos tomados de Cisco Systems (2025d).

Front View with Drives



Front View with Drives and GPU



Figura 7 Vista frontal de servidores blade Cisco X210c M7. Fuente. Datos tomados de Cisco Systems (2025c).



Figura 8 Vista frontal de un Cisco UCS FI 6454. Fuente. Datos tomados de Cisco Systems (2021).

En cuanto a la conectividad LAN, el diseño incluye dos Switches LAN Cisco

Nexus N9K-C93180YC-FX3 de 48 puertos SFP+ de hasta 25 Gbps y seis puertos QSFP de hasta 100 Gbps. Estos switches cuentan con la funcionalidad vPC para la agregación de enlaces multi-chasis, con lo cual se alcanza la máxima redundancia de red LAN. La Figura 9 muestra un switch Nexus 93180YC-FX3 visto desde la parte frontal (Cisco Systems, 2025b).



Figura 9 Vista frontal de un switch LAN Cisco Nexus N9K-C93180YC-FX3. Fuente. Datos tomados de Cisco Systems (2025b).

Para la red de almacenamiento, se despliegan dos Switches SAN Cisco MDS DS-C9132T-MEK9 de 16 puertos SFP+ de hasta 32 Gbps. Cada uno de estos switches SAN se conectan de forma independiente a los nodos iniciadores (servidores) y objetivos (almacenamiento), sin interconectar ambos switches nuevos SAN, formando dos redes independientes SAN. De esta forma, los problemas en la red A no impactan en absoluto a la red B, y viceversa. La Figura 10 muestra un switch Cisco MDS 9132T visto desde la parte frontal (Cisco Systems, 2023).



Figura 10. Vista frontal de un switch SAN Cisco MDS DS-C9132T-MEK9. Fuente. Datos tomados de Cisco Systems (2023).

Con la información obtenida de la solución antigua, se elaboró el diagrama *as is* de la solución, el cual se ilustra en la Figura 11. Este diagrama tiene la intención de graficar la situación actual de los equipos involucrados en la renovación y mostrar a alto nivel la arquitectura que se planea optimizar con los nuevos equipos y las actividades de migración del proyecto.

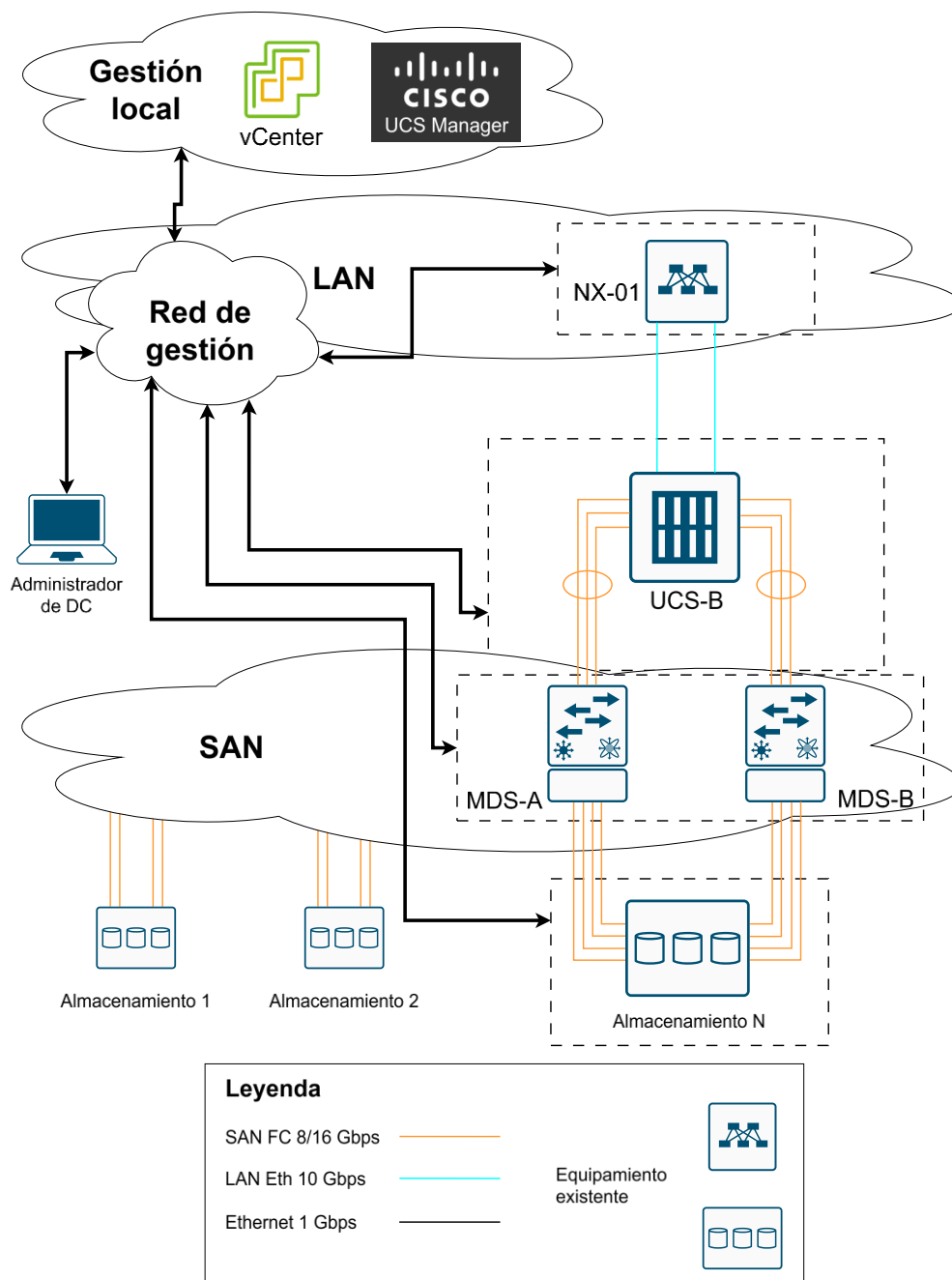


Figura 11 Topología actual de la red DC de la clínica. Fuente. Elaboración propia. Los íconos y logotipos son propiedad de Cisco Systems, Inc. y Broadcom Inc.; estos se incluyen con el fin de ilustrar el diseño.

El diseño a alto nivel definido en la etapa de diseño y planificación del proyecto se plasma en un diagrama *to be*, como se muestra en la Figura 12. En este diagrama se integran los equipos de la solución antigua y el equipamiento nuevo adquirido en el proyecto, evidenciando las diferencias con respecto a la situación actual y sirviendo como guía para planificar las actividades de implementación y migración a lo largo del proyecto.

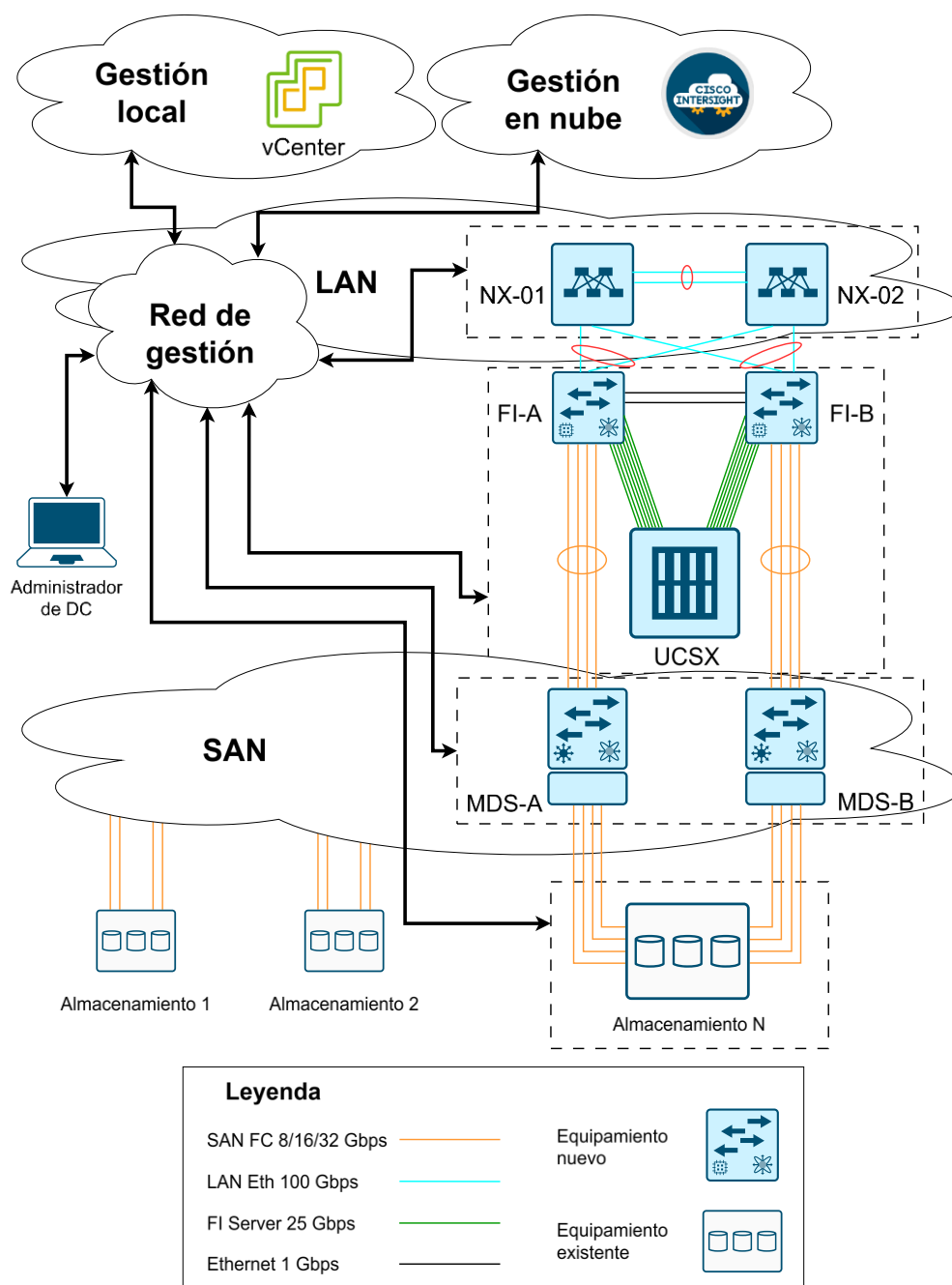


Figura 12 Topología propuesta para la red DC de la clínica. Fuente. Elaboración propia. Los íconos y logotipos son propiedad de Cisco Systems, Inc. y Broadcom Inc.; estos se incluyen con el fin de ilustrar el diseño.

En la Tabla 1, se resume el equipamiento adquirido en el proyecto y se definen los nombres de cada uno y la ubicación donde se instalarán.

La distribución de los equipos en los gabinetes es plasmada en un diagrama conocido como *cabinet layout*. La Figura 13 muestra el *cabinet layout* de los equipos nuevos del proyecto.

Tabla 1 Relación de equipos a desplegar en el proyecto

Hostname	Tipo	Fabricante	Ubicación	Gabinete	Unidad de Rack	Modelo Hardware
ucsclinica1-1-1	Servidor de cómputo	Cisco	DC	1	RU 14-20	UCS X210c M7
ucsclinica1-1-2	Servidor de cómputo	Cisco	DC	1	RU 14-20	UCS X210c M7
ucsclinica1-1-3	Servidor de cómputo	Cisco	DC	1	RU 14-20	UCS X210c M7
clinicaesxi01	Host ESXi	VMware	DC	1	RU 14-20	Sistema Operativo
clinicaesxi02	Host ESXi	VMware	DC	1	RU 14-20	Sistema Operativo
clinicaesxi03	Host ESXi	VMware	DC	1	RU 14-20	Sistema Operativo
ucsclinica1-A	Fabric Interconnect	Cisco	DC	1	RU 25	UCS FI 6454
ucsclinica1-B	Fabric Interconnect	Cisco	DC	1	RU 24	UCS FI 6454
ucsclinica1-1	Chásis	Cisco	DC	1	RU 14-20	UCS X9508
SW-CORE-Clinica1	Switch LAN	Cisco	DC	2	RU 26	N9K-C93180YC-FX3
SW-CORE-Clinica2	Switch LAN	Cisco	DC	2	RU 24	N9K-C93180YC-FX3
MDS-Clinica-A	Switch SAN	Cisco	DC	1	RU 23	DS-C9132T
MDS-Clinica-B	Switch SAN	Cisco	DC	1	RU 22	DS-C9132T

Fuente. Elaboración propia.

Una vez desarrollado el HLD, se realizan los requerimientos físicos y lógicos al cliente para la instalación y la configuración de la solución. En estos requerimientos lógicos se incluye lo siguiente:

- Asignación de direccionamiento IP para equipamiento de la solución nueva.
- Definición de nomenclatura y hostnames para equipamiento nuevo.
- Parámetros comunes de servicios y funciones de red, como servidores DNS, NTP y nombre de dominio.
- El cliente también puede solicitar algunas configuraciones especiales. Todas las demás configuraciones serán sugeridas por el implementador basándose en sus buenas prácticas, en la medida de lo posible.

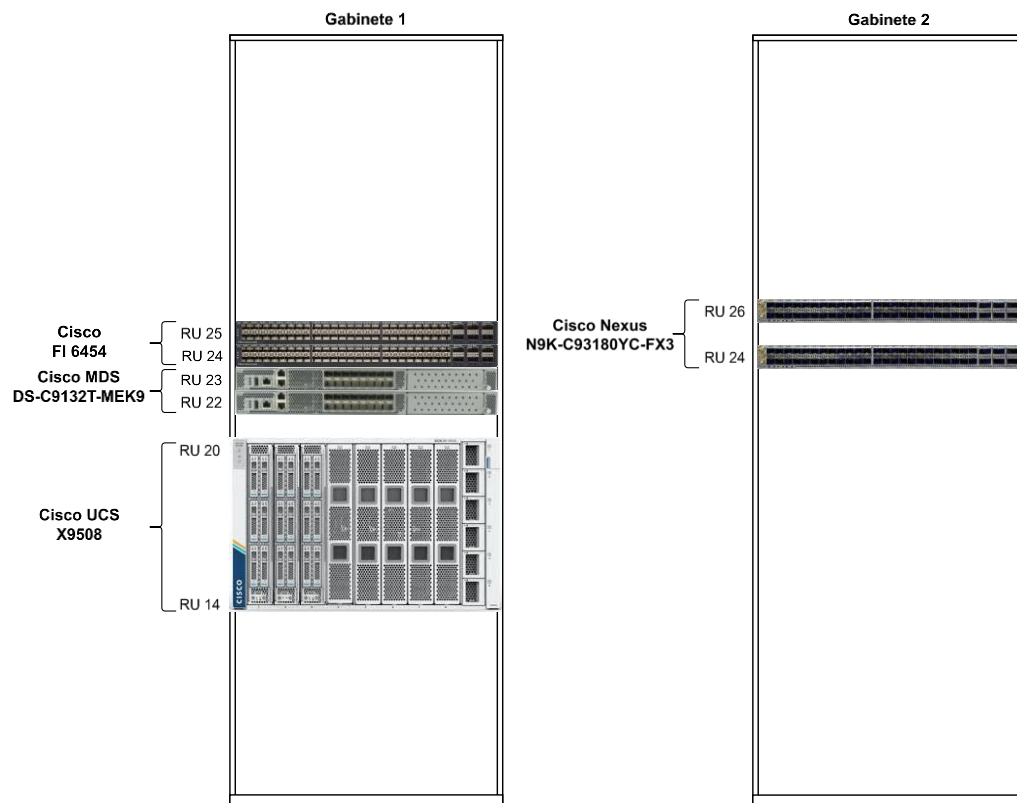


Figura 13 Cabinet Layout de los nuevos equipos de la clínica. Fuente. Elaboración propia. Las imágenes frontales de los equipos son propiedad de Cisco Systems, Inc.; estas se incluyen con el fin de ilustrar el diseño.

Entre los requerimientos físicos se incluye lo siguiente:

- Asignación de coordenadas (sala, gabinete y número de rack) que cumplan con las dimensiones y condiciones ambientales requeridas para la instalación física del equipamiento nuevo. Para esto es necesario compartirle las especificaciones técnicas de los equipos al cliente.
- Asignación de puertos de red y equipos de red para conexiones nuevas de gestión.
- Asignación de tomas de energía en gabinetes con suficiente potencia disponible para la conexión de fuentes redundantes de energía mediante alimentaciones eléctricas independientes, distribuidas a través de PDUs A y B (Unidades de Distribución de Energía).

Con estas definiciones entregadas por el cliente, se completa el diseño a bajo nivel (Low Level Design o LLD), el cual incluye el máximo detalle del diseño técnico de la solución.

3.5.4 Diseño a Bajo Nivel (LLD)

Al culminar las definiciones físicas y lógicas, se puede elaborar un diseño más detallado, lo cual se conoce como Low Level Design (LLD). La Figura 14 muestra la topología resultante en el diseño a bajo nivel.

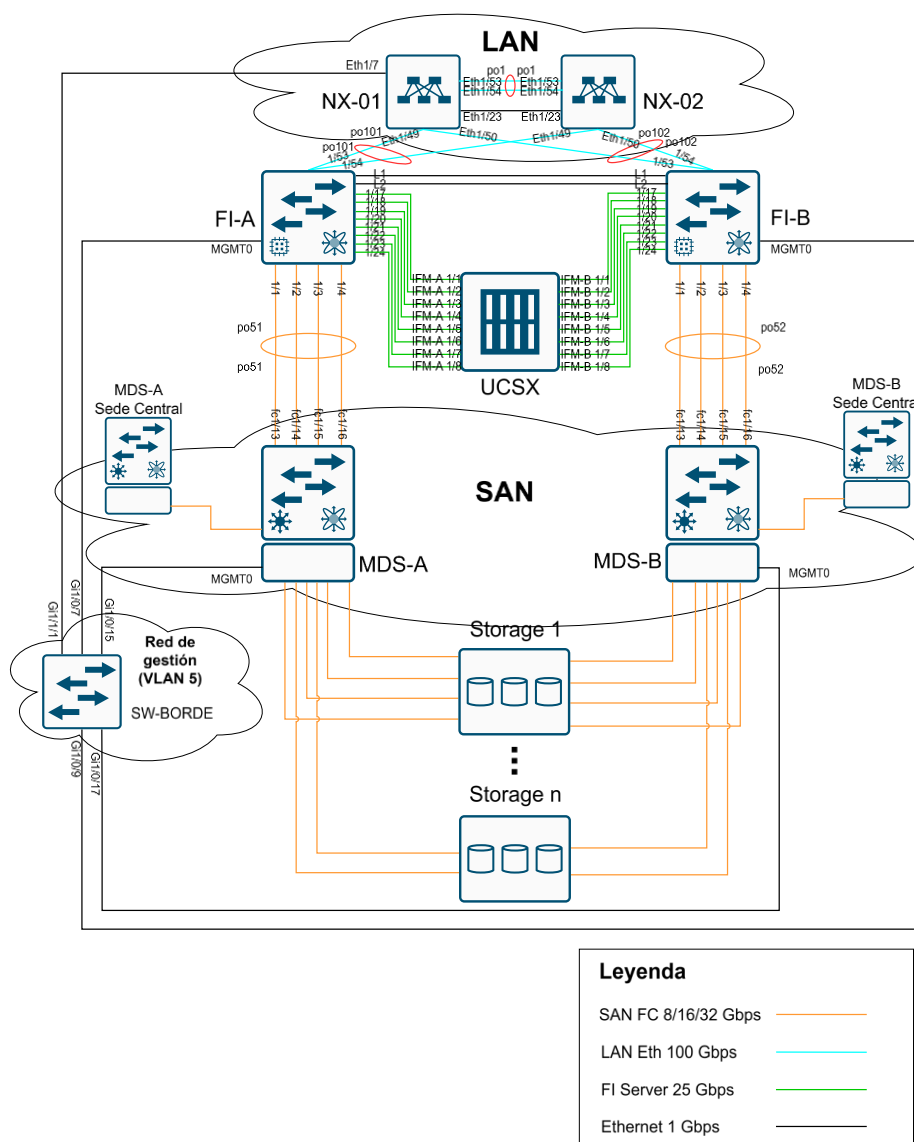


Figura 14 Topología física definida para la red DC de la clínica. Fuente. Elaboración propia. Los íconos y logotipos son propiedad de Cisco Systems, Inc.; estos se incluyen con el fin de ilustrar el diseño.

En las siguientes secciones se detallan las conexiones, funciones y configuraciones definidas para la configuración de la solución.

3.5.4.1 Port mapping

La Tabla 2 lista todas las conexiones definidas para la infraestructura de DC en la clínica, lo cual se conoce como el port mapping del proyecto. El port mapping servirá como guía para realizar todas las conexiones de fibra y cobre.

Tabla 2 Port mapping propuesto

Equipo Origen	Puerto Origen	Tipo enlace	Tipo Puerto	Función	Velocidad	Puerto destino	Equipo destino
UCS-X Chassis	IFM-A 1/1	Fibra Óptica	SFP28	Server	25 Gbps	1/17	Fabric Interconnect A
	IFM-A 1/2				25 Gbps	1/18	
	IFM-A 1/3				25 Gbps	1/19	
	IFM-A 1/4				25 Gbps	1/20	
	IFM-A 1/5				25 Gbps	1/21	
	IFM-A 1/6				25 Gbps	1/22	
	IFM-A 1/7				25 Gbps	1/23	
	IFM-A 1/8				25 Gbps	1/24	
	IFM-B 1/1	Fibra Óptica	SFP28	Server	25 Gbps	1/17	Fabric Interconnect B
	IFM-B 1/2				25 Gbps	1/18	
	IFM-B 1/3				25 Gbps	1/19	
	IFM-B 1/4				25 Gbps	1/20	
	IFM-B 1/5				25 Gbps	1/21	
	IFM-B 1/6				25 Gbps	1/22	
	IFM-B 1/7				25 Gbps	1/23	
	IFM-B 1/8				25 Gbps	1/24	
Fabric Interconnect A	FC 1/1	Fibra Óptica	SFP+	SAN	32 Gbps	fc1/13	MDS A
	FC 1/2				32 Gbps	fc1/14	
	FC 1/3				32 Gbps	fc1/15	
	FC 1/4				32 Gbps	fc1/16	
	Eth1/53	Fibra	QSFP28	LAN	100 Gbps	Eth1/49	NX1
	Eth1/54	Óptica			100 Gbps	Eth1/50	NX2
	MGMT0	Cobre	RJ45	MGMT	1 Gbps	Gi1/0/7	Sw OOB MGMT
Fabric Interconnect B	FC 1/1	Fibra Óptica	SFP+	SAN	32 Gbps	fc1/13	MDS B
	FC 1/2				32 Gbps	fc1/14	
	FC 1/3				32 Gbps	fc1/15	
	FC 1/4				32 Gbps	fc1/16	
	Eth1/53	Fibra	QSFP28	LAN	100 Gbps	Eth1/49	NX1
	Eth1/54	Óptica			100 Gbps	Eth1/50	NX2
	MGMT0	Cobre	RJ45	MGMT	1 Gbps	Gi1/0/9	Sw OOB MGMT

MDS A	fc1/2	Fibra Óptica	SFP+	SAN	32 Gbps	P1	Storage 1
	fc1/3				32 Gbps	P2	Storage 1
	fc1/4				32 Gbps	P5	Storage 1
	fc1/5				16 Gbps	P1	Storage 2
	fc1/6				8 Gbps	fc1/6	MDS-A2 (Sede Central)
	fc1/7				16 Gbps	P1	Storage 3
	fc1/8				16 Gbps	P3	Storage 3
	fc1/9				32 Gbps	P6	Storage 1
	fc1/10				32 Gbps	Libre	Libre
	fc1/11				32 Gbps	Libre	Libre
	fc1/12				32 Gbps	Libre	Libre
	fc1/13				16 Gbps	1/1	UCS9108 A
	fc1/14				16 Gbps	1/2	UCS9108 A
	fc1/15				16 Gbps	1/3	UCS9108 A
	fc1/16				16 Gbps	1/4	UCS9108 A
	MGMT0	Cobre	RJ45	MGMT	1 Gbps	Gi1/0/15	Sw OOB MGMT
MDS B	fc1/1	Fibra Óptica	SFP+	SAN	32 Gbps	P3	Storage 1
	fc1/3				32 Gbps	P4	Storage 1
	fc1/4				32 Gbps	P7	Storage 1
	fc1/5				16 Gbps	P2	Storage 2
	fc1/6				8 Gbps	fc1/6	MDS-B2 (Sede Central)
	fc1/7				16 Gbps	P2	Storage 3
	fc1/8				16 Gbps	P4	Storage 3
	fc1/9				32 Gbps	P8	Storage 1
	fc1/10				32 Gbps	Libre	Libre
	fc1/11				32 Gbps	Libre	Libre
	fc1/12				32 Gbps	Libre	Libre
	fc1/13				16 Gbps	1/1	UCS9108 B
	fc1/14				16 Gbps	1/2	UCS9108 B
	fc1/15				16 Gbps	1/3	UCS9108 B
	fc1/16				16 Gbps	1/4	UCS9108 B
	MGMT0	Cobre	RJ45	MGMT	1 Gbps	Gi1/0/17	Sw OOB MGMT
NX1	Eth1/53	Fibra Óptica	QSFP28	vPC Peer Link	100 Gbps	Eth1/53	NX2
	Eth1/54				100 Gbps	Eth1/54	
	Eth1/23	Cobre	SFP+	vPC Keepalive Link	10 Gbps	Eth1/23	

Fuente. Elaboración propia.

El cuadro detalla en cada conexión los nombres y puertos de los equipos origen y destino entre los cuales se realiza la conexión física, el tipo de medio utilizado, transceiver y velocidad. También detalla la función del enlace, sea para conexión LAN, SAN, gestión (MGMT) o de dominio vPC.

3.5.4.2 Storage y SAN

El diseño contempla la expansión de la infraestructura de cómputo, gracias al despliegue de tres servidores tipo Blade Cisco UCS X210c M7 que también serán conectados con los equipos de almacenamiento existentes a través de la infraestructura SAN Fibre Channel habilitada por los switches MDS nuevos, la cual ahora comunica los HBA de los servidores UCS con los storages de la clínica. El diseño garantiza la redundancia de la conectividad SAN gracias a la capacidad de multipathing de VMware que hace uso de las dos SAN, las cuales existen en dos switches MDS separados, y hace uso de todos los path de ambas SAN para balancear la carga de operaciones I/O. La Figura 15 ilustra el diseño de conexión SAN que habilita la función de *multipathing*.

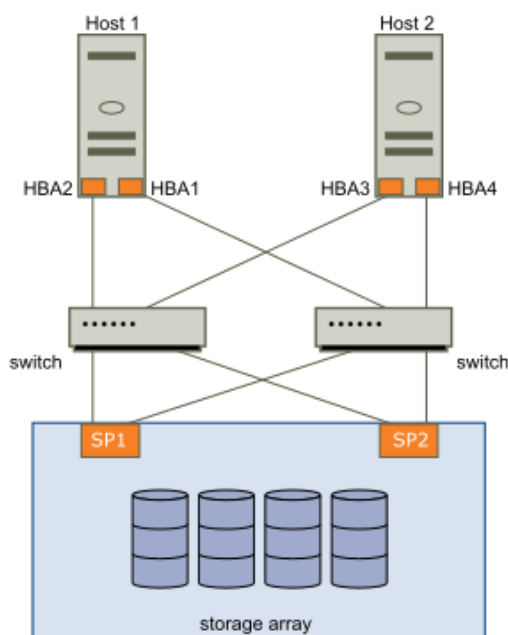


Figura 15 Función multipathing de VMware con Fibre Channel. Fuente. Datos tomados de Broadcom (2026).

Los volúmenes creados en los storage de la solución existente serán utilizados como datastores para los hosts VMware ESXi nuevos, donde se podrán almacenar imágenes de sistemas operativos, discos de máquinas virtuales y snapshots.

La Figura 16 muestra las conexiones y equipos involucrados en la red SAN del DC de la clínica.

utilizarán para las conexiones a los Fabric Interconnect (en dirección a los hosts UCS) y las conexiones a los arreglos de almacenamiento existentes.

Para la interconexión Fibre Channel entre los Fabric Interconnect (FI) y los switches MDS de la clínica, se hará uso de enlaces agregados y virtualización de puertos. La comunicación se establece mediante la configuración de Port Channel de Fibre Channel entre cada FI y su respectivo switch MDS, utilizando interfaces de 16 Gbps para garantizar la alta disponibilidad y el rendimiento requerido por las aplicaciones de salud.

La Tabla 3 resume las conexiones de Port Channel en los Switches MDS.

Tabla 3 Enlaces Port Channel en red SAN

Equipo Origen	Port Channel Origen	Puerto origen	Puerto destino	Port Channel Destino	Equipo destino
Fabric Interconnect A	Port Channel 51	FC 1/1	fc1/13	Port Channel 51	MDS A
		FC 1/2	fc1/14		
		FC 1/3	fc1/15		
		FC 1/4	fc1/16		
Fabric Interconnect B	Port Channel 52	FC 1/1	fc1/13	Port Channel 52	MDS B
		FC 1/2	fc1/14		
		FC 1/3	fc1/15		
		FC 1/4	fc1/16		

Fuente. Elaboración propia.

A nivel lógico, la configuración SAN de los Fabric Interconnect en modo End Host define la forma de operación. Bajo este esquema, los FI actúan como intermediarios que registran los puertos vHBA de los servidores en la red SAN principal, delegando la gestión de los identificadores lógicos (pWWN, nWWN y FCID) a los switches MDS A y B, sin necesidad de configurar la zonificación en los FI. Al habilitar el modo SAN End Host en los FI, se configura el mecanismo NPV en sus interfaces FC Port Channel, mientras que en los switches MDS es necesario habilitar la función NPIV (Cisco Systems, 2026b).

Por otro lado, las conexiones entre los Fabric Interconnect y los distintos arreglos de almacenamiento no utilizan la funcionalidad de FC Port Channel, sino que confían en el mecanismo de multipathing de los servidores. Los

almacenamientos registran sus puertos de forma independiente en la SAN, lo cual permite que los servidores reconozcan varios caminos (paths) hacia un mismo volumen de datos, asegurando que se mantenga la redundancia y facilitando el balanceo de tráfico entre los enlaces activos (Broadcom, 2026).

Una vez definidos los puertos a utilizar para las conexiones a UCS y arreglos de almacenamiento, debemos configurar el tipo de puerto F a todos estos puertos. La configuración de trunking no es necesaria (en la red solo se usa 1 vSAN por cada SAN A o B), pero el puerto debe tener habilitada al menos la vSAN 100 para el caso del MDS-A y 200 para el MDS-B.

Para extender la conectividad hacia la sede alterna, se implementaron enlaces troncales directos de fibra óptica a 8 Gbps a través de los puertos fc1/6 configurados en modo E. La comunicación opera de forma exclusiva sobre la vSAN 100 para el caso del MDS-A y 200 para el MDS-B, manteniendo el trunking habilitado por si en el futuro se desean utilizar VSAN adicionales. El tráfico de replicación de los arreglos FlashSystem 7300 existentes en la clínica y en la sede central es controlado por su función HyperSwap y se enruta entre sedes mediante el protocolo FSPF, utilizando identificadores de dominio que fueron asignados de forma dinámica por el fabric. De esta manera, para la SAN A se obtuvieron los dominios 117 (local) y 21 (remoto), mientras que en la SAN B se asignaron los dominios 25 (local) y 77 (remoto). Esta arquitectura extendida se apoya en la distribución automática de zonas, device-alias y el servicio FCNS, permitiendo que los nodos de la sede clínica reconozcan a los nodos en el sitio remoto y así se logre la comunicación entre sistemas de almacenamiento necesaria para la replicación (Cisco Systems, 2026a).

Alias, direccionamiento FCID y zonificación

Se asignaron nombres de alias a los pWWN de los HBA (initiators y targets) para facilitar su identificación durante un eventual *troubleshooting*, al nombrarlos haciendo referencia al equipo y puerto que pertenecen. La Tabla 4 muestra los nombres de alias asignados a cada dirección pWWN.

Tabla 4 Listado de direcciones pWWN y Alias

Equipo	SAN	Puerto	pWWN	Alias
Storage 1	A	P1	52:c7:38:20:a9:13:3e:88	Storage1-P1-N1
			52:c7:38:20:a9:17:3e:88	Storage1-P1-N2
			52:c7:38:20:a9:1b:3e:88	Storage1-P1-N3
		P2	52:c7:38:20:a9:11:3e:74	Storage1-P2-N1
			52:c7:38:20:a9:15:3e:74	Storage1-P2-N2
			52:c7:38:20:a9:19:3e:74	Storage1-P2-N3
		P5	52:c7:38:20:a9:13:3e:74	Storage1-P5-N1
			52:c7:38:20:a9:17:3e:74	Storage1-P5-N2
			52:c7:38:20:a9:1b:3e:74	Storage1-P5-N3
	B	P6	52:c7:38:20:a9:11:3e:88	Storage1-P6-N1
			52:c7:38:20:a9:15:3e:88	Storage1-P6-N2
			52:c7:38:20:a9:19:3e:88	Storage1-P6-N3
		P3	52:c7:38:20:10:12:3e:88	Storage1-P3-N1
			52:c7:38:20:10:16:3e:88	Storage1-P3-N2
			52:c7:38:20:10:1a:3e:88	Storage1-P3-N2
		P4	52:c7:38:20:10:12:3e:74	Storage1-P4-N1
			52:c7:38:20:10:16:3e:74	Storage1-P4-N2
			52:c7:38:20:10:1a:3e:74	Storage1-P4-N3
		P7	52:c7:38:20:10:14:3e:74	Storage1-P7-N1
			52:c7:38:20:10:18:3e:74	Storage1-P7-N2
			52:c7:38:20:10:1c:3e:74	Storage1-P7-N3
		P8	52:c7:38:20:10:14:3e:88	Storage1-P8-N1
			52:c7:38:20:10:18:3e:88	Storage1-P8-N2
			52:c7:38:20:10:1c:3e:88	Storage1-P8-N3
Storage 2	A	P1	24:3f:58:d3:9c:20:43:00	Storage2-P1-N1
	B	P2	24:3f:58:d3:9c:20:43:10	Storage2-P2-N1
Storage 3	A	P1	52:c7:38:20:0d:06:9a:90	Storage3-P1-N1
			52:c7:38:20:0d:76:9a:90	Storage3-P1-N2
		P3	52:c7:38:20:0d:06:9a:91	Storage3-P3-N1
			52:c7:38:20:0d:76:9a:91	Storage3-P3-N2
	B	P2	52:c7:38:20:0d:0a:9a:90	Storage3-P2-N1
			52:c7:38:20:0d:7a:9a:90	Storage3-P2-N2
		P4	52:c7:38:20:0d:0a:9a:91	Storage3-P4-N1
			52:c7:38:20:0d:7a:9a:91	Storage3-P4-N2
Servidor 1	A	vHBA0	24:d7:ac:73:d2:22:a0:00	CHASSIS1-BLADE1-vHBA0-A
		vHBA1	24:d7:ac:73:d2:22:a0:01	CHASSIS1-BLADE1-vHBA1-A
Servidor 2	A	vHBA0	24:d7:ac:73:d2:22:a0:02	CHASSIS1-BLADE2-vHBA0-A
		vHBA1	24:d7:ac:73:d2:22:a0:03	CHASSIS1-BLADE2-vHBA1-A
Servidor 3	A	vHBA0	24:d7:ac:73:d2:22:a0:04	CHASSIS1-BLADE3-vHBA0-A
		vHBA1	24:d7:ac:73:d2:22:a0:05	CHASSIS1-BLADE3-vHBA1-A
Servidor 1	B	vHBA2	24:d7:ac:73:d2:22:b0:00	CHASSIS1-BLADE1-vHBA2-B
		vHBA3	24:d7:ac:73:d2:22:b0:01	CHASSIS1-BLADE1-vHBA3-B
Servidor 2	B	vHBA2	24:d7:ac:73:d2:22:b0:02	CHASSIS1-BLADE2-vHBA2-B
		vHBA3	24:d7:ac:73:d2:22:b0:03	CHASSIS1-BLADE2-vHBA3-B

Servidor 3	B	vHBA2	24:d7:ac:73:d2:22:b0:04	CHASSIS1-BLADE3-vHBA2-B
		vHBA3	24:d7:ac:73:d2:22:b0:05	CHASSIS1-BLADE3-vHBA3-B

Fuente. Elaboración propia.

El direccionamiento FCID se asigna de forma dinámica a todos los host y puertos de array que se conectan a la vSAN (100 o 200), y siempre compartirán el mismo Domain ID en el mismo Switch.

Finalmente, se requiere agregar nuevos pWWN target a la zonificación existente y crear nuevas zonas que incluyan a los nuevos pWWN initiator y a los pWWN target antiguos y nuevos.

La Tabla 5 lista los nombres de las zonas a crear para los nuevos hosts.

Tabla 5 Listado de zonas

Zoneset	VSAN	Zona
MDS_A	100	ZONE_CHASSIS1-BLADE1-vHBA0-A
		ZONE_CHASSIS1-BLADE1-vHBA1-A
		ZONE_CHASSIS1-BLADE2-vHBA0-A
		ZONE_CHASSIS1-BLADE2-vHBA1-A
		ZONE_CHASSIS1-BLADE3-vHBA0-A
		ZONE_CHASSIS1-BLADE3-vHBA1-A
MDS_B	200	ZONE_CHASSIS1-BLADE1-vHBA2-B
		ZONE_CHASSIS1-BLADE1-vHBA3-B
		ZONE_CHASSIS1-BLADE2-vHBA2-B
		ZONE_CHASSIS1-BLADE2-vHBA3-B
		ZONE_CHASSIS1-BLADE3-vHBA2-B
		ZONE_CHASSIS1-BLADE3-vHBA3-B

Fuente. Elaboración propia.

Finalmente, la Tabla 6 lista todos los miembros target existentes que deben tener las zonas existentes y nuevas. Tener en cuenta que cada zona también deberá tener registrado el pWWN del vHBA initiator respectivo, ya que se crea una zona para cada iniciador.

Tabla 6 Listado de targets

Zoneset	pWWN	Alias
MDS_A	52:c7:38:20:a9:13:3e:88	Storage1-P1-N1
	52:c7:38:20:a9:17:3e:88	Storage1-P1-N2

MDS_A	52:c7:38:20:a9:1b:3e:88	Storage1-P1-N3
	52:c7:38:20:a9:11:3e:74	Storage1-P2-N1
	52:c7:38:20:a9:15:3e:74	Storage1-P2-N2
	52:c7:38:20:a9:19:3e:74	Storage1-P2-N3
	52:c7:38:20:a9:13:3e:74	Storage1-P5-N1
	52:c7:38:20:a9:17:3e:74	Storage1-P5-N2
	52:c7:38:20:a9:1b:3e:74	Storage1-P5-N3
	52:c7:38:20:a9:11:3e:88	Storage1-P6-N1
	52:c7:38:20:a9:15:3e:88	Storage1-P6-N2
	52:c7:38:20:a9:19:3e:88	Storage1-P6-N3
	24:3f:58:d3:9c:20:43:00	Storage2-P1-N1
	52:c7:38:20:0d:06:9a:90	Storage3-P1-N1
	52:c7:38:20:0d:76:9a:90	Storage3-P1-N2
	52:c7:38:20:0d:06:9a:91	Storage3-P3-N1
	52:c7:38:20:0d:76:9a:91	Storage3-P3-N2
MDS_B	52:c7:38:20:10:12:3e:88	Storage1-P3-N1
	52:c7:38:20:10:16:3e:88	Storage1-P3-N2
	52:c7:38:20:10:1a:3e:88	Storage1-P3-N2
	52:c7:38:20:10:12:3e:74	Storage1-P4-N1
	52:c7:38:20:10:16:3e:74	Storage1-P4-N2
	52:c7:38:20:10:1a:3e:74	Storage1-P4-N3
	52:c7:38:20:10:14:3e:74	Storage1-P7-N1
	52:c7:38:20:10:18:3e:74	Storage1-P7-N2
	52:c7:38:20:10:1c:3e:74	Storage1-P7-N3
	52:c7:38:20:10:14:3e:88	Storage1-P8-N1
	52:c7:38:20:10:18:3e:88	Storage1-P8-N2
	52:c7:38:20:10:1c:3e:88	Storage1-P8-N3
	24:3f:58:d3:9c:20:43:10	Storage2-P2-N1
	52:c7:38:20:0d:0a:9a:90	Storage3-P2-N1
	52:c7:38:20:0d:7a:9a:90	Storage3-P2-N2
	52:c7:38:20:0d:0a:9a:91	Storage3-P4-N1
	52:c7:38:20:0d:7a:9a:91	Storage3-P4-N2

Fuente. Elaboración propia.

Para la administración y seguridad de la red SAN, se definieron configuraciones adicionales orientadas a la estabilidad del fabric. Se utilizó device-alias en modo básico para una identificación simplificada de los equipos y se activó el zone mode enhanced en las VSAN de producción y

replicación para prevenir conflictos por cambios simultáneos. En los enlaces inter-sede, se configuró zone merge-control restrict como medida de protección ante discrepancias de configuración durante la unión de los switches, complementado con zone distribute para garantizar que las reglas de acceso se repliquen automáticamente en toda la infraestructura de la clínica (Cisco Systems, 2026a).

3.5.4.3 LAN

La conectividad LAN a los servicios del DC y todos los usuarios del edificio hace uso de la red LAN habilitada por los nuevos Switches Core Nexus. A través de esta red fluye el tráfico de las Máquinas Virtuales de los nuevos servidores del DC; el tráfico proveniente de todos los pisos del edificio; tráfico de gestión en banda de los host ESXi hacia los dispositivos administradores y hacia vCenter; y migraciones de VMs con vMotion. La Figura 17 muestra los flujos de tráfico LAN en la nueva arquitectura.

Para la interconexión de la red de datos (LAN) entre los Fabric Interconnect (FI) y los switches Nexus de Core (NX1 y NX2) de la clínica, se implementó una topología de alta disponibilidad activo-activo basada en vPC (Virtual Port-Channel). Desde el FI-A se configuró el Port Channel 101 utilizando las interfaces Eth1/53 y Eth1/54, las cuales se conectan a los puertos Eth1/49 del NX1 y Eth1/50 del NX2 respectivamente, operando a una velocidad de 100 Gbps mediante transceptores QSFP28 en el vPC 101. De manera homóloga, el FI-B establece su conectividad a través del Port Channel 102 hacia los mismos equipos de Core en el vPC 102. Este diseño proporciona un ancho de banda agregado de 200 Gbps por cada Fabric Interconnect hacia la red principal, asegurando el rendimiento necesario para el tráfico del entorno VMware.

A nivel lógico, ambos Fabric Interconnect se configuraron en modo LAN End Host. Bajo este esquema, los equipos FI no participan en el dominio del Spanning Tree Protocol (STP) hacia el Core, presentándose como hosts finales con múltiples enlaces de subida (uplinks). Esta configuración elimina

el riesgo de bucles en capa dos y utiliza un mecanismo de anclaje dinámico (*dynamic pinning*) para distribuir el tráfico de las interfaces virtuales de los servidores (vNICs) a través de los enlaces de 100 Gbps, garantizando un *switching* eficiente sin descartes de paquetes (Cisco Systems, 2026c).

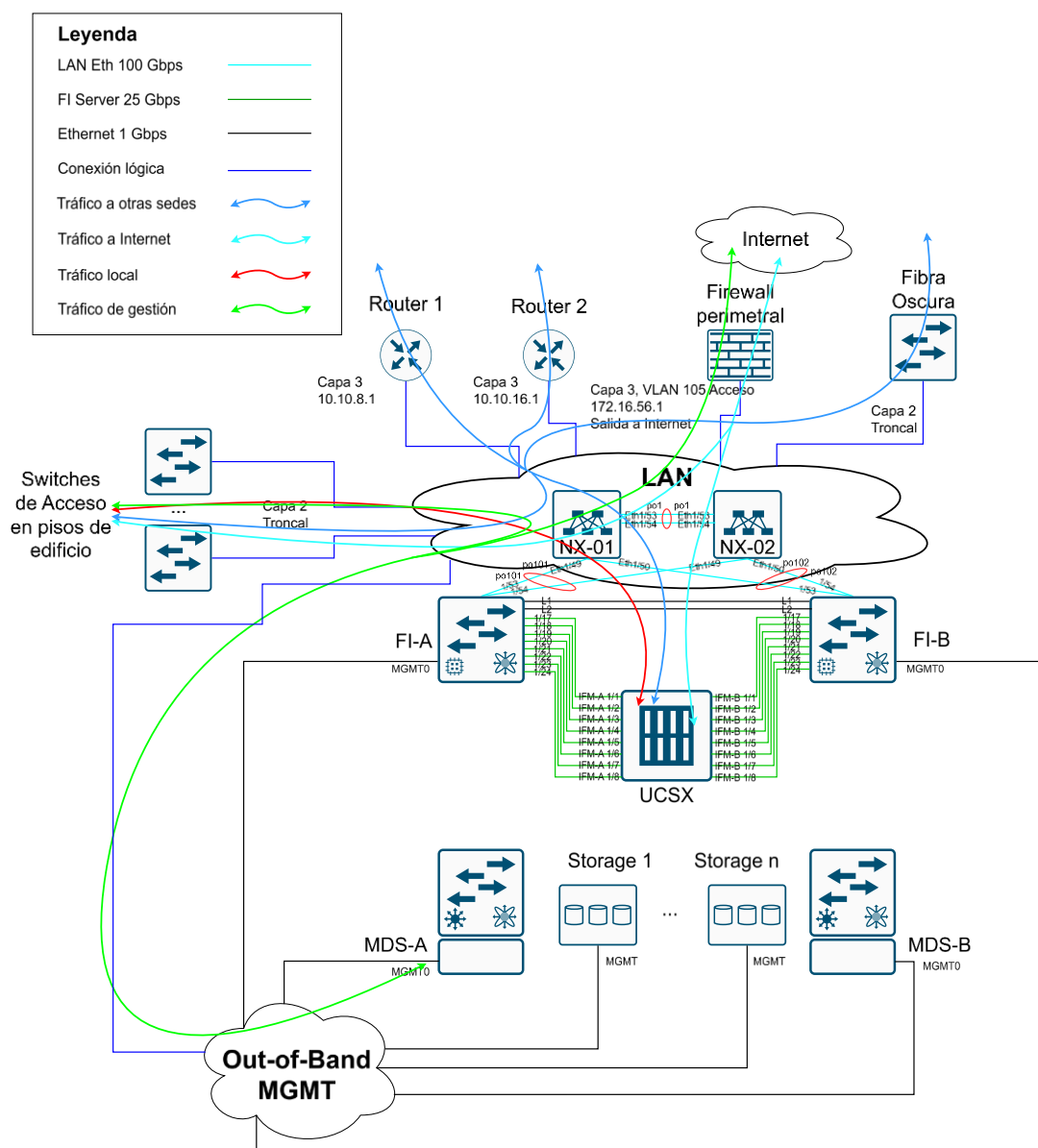


Figura 17 Topología lógica definida para red LAN. Fuente. Elaboración propia. Los íconos y logotipos son propiedad de Cisco Systems, Inc.; estos se incluyen con el fin de ilustrar el diseño.

Para sostener la robustez de la arquitectura vPC en la capa de Core, la sincronización de las tablas de direcciones MAC y protocolos de control entre los switches NX1 y NX2 se realiza mediante un *vPC Peer Link* configurado en

el Port Channel 1, agrupando dos interfaces de 100 Gbps (Eth1/53 y Eth1/54). Como mecanismo de protección adicional para evitar escenarios de Split Brain, se estableció un enlace *vPC Peer Keepalive* dedicado de 10 Gbps a través de los puertos Eth1/23, encargado de monitorear el estado del chasis de forma independiente (heartbeat). Este diseño asegura que, ante la falla de un enlace físico o la caída de un switch de Core, el tráfico hospitalario conmute de forma transparente en milisegundos. En la Tabla 7 se resumen los enlaces agregados que forman *Port-Channels* y *vPCs* (Cisco Systems, 2025a).

Tabla 7 Configuración de Switches Nexus

Equipo Origen	Port Channel Origen	Puerto origen	Puerto destino	Port Channel Destino	vPC	Equipo destino
Fabric Interconnect A	Port Channel 101	Eth1/53	Eth1/51	Port Channel 101	101	NX1
		Eth1/54	Eth1/51			NX2
Fabric Interconnect B	Port Channel 102	Eth1/53	Eth1/52	Port Channel 102	102	NX1
		Eth1/54	Eth1/52			NX2
NX1	Port Channel 1	Eth1/49	Eth1/49	Port Channel 1	-	NX2
		Eth1/50	Eth1/50		-	

Fuente. Elaboración propia.

La función de Core en capa tres se centraliza en el par de switches Nexus NX1 y NX2, los cuales operan como el gateway predeterminado de las diversas VLANs de la clínica mediante el protocolo HSRP. Se configuraron interfaces virtuales de switch (SVI) con una dirección IP virtual para cada segmento de red, asignando al NX1 la prioridad 105 para actuar como el nodo activo principal, complementado con la función preempt para asegurar que retome su rol automáticamente tras cualquier reinicio. Para garantizar la conectividad en capa dos hacia los gabinetes de comunicaciones ubicados en los diversos pisos, se desplegaron Port-Channels vPC hacia los switches de acceso. Este diseño permite que cada piso cuente con enlaces redundantes distribuidos físicamente entre ambos equipos Nexus, duplicando el ancho de banda disponible y eliminando los tiempos de convergencia tradicionales al mantener todas las rutas activas de forma simultánea.

Los *switches* Core también tienen conectividad en capa tres hacia otras sedes

por medio de rutas que apuntan a algunos *routers* existentes y fibras oscuras y a Internet a través del Firewall perimetral.

3.5.4.4 Cisco UCS

La nueva solución UCS adquirida en el proyecto incluye un nuevo modo de administración llamado *Intersight Managed Mode* (IMM), con el cual se puede realizar el monitoreo, configuración, administración y *troubleshooting* de la solución desde la nube utilizando el servicio *Intersight Infrastructure Service*.

Profiles y Templates

Para la configuración del chasis de la clínica se definió un UCS Server Profile Template para derivar los UCS Server Profiles que serán aplicados a cada servidor blade. También se crearon un UCS Domain Profile para configurar el par de Fabric Interconnects (UCS Domain) y un UCS Chassis Profile para la configuración del chasis UCS.

En las Tablas 8 y 9, se muestra cómo se configuraron los *profiles* aplicados al par de FIs y chasis.

Tabla 8 UCS Domain Profile

UCS Domain Profile	ucsclinica1
Descripción	Perfil para FI
Port Policy A	Clinica_Plc_FIPort_A
Port Policy B	Clinica_Plc_FIPort_B
VLAN Policy	Clinica_Plc_VLAN
VSAN Policy A	Clinica_Plc_VSAN_A
VSAN Policy B	Clinica_Plc_VSAN_B
NTP Policy	Clinica_Plc_NTP
Network Connectivity Policy	Clinica_Plc_NetworkConnectivity
Switch Control	Clinica_Plc_SwitchEndHost

Fuente. Elaboración propia.

Tabla 9 UCS Chassis Profile

UCS Chassis Profile	ucsclinica1_Chassis_1
Descripción	Perfil para chasis
IMC Access Policy	Clinica_Plc_IMCAccess

Power Policy	Clinica_Plc_PowerPolicy
Thermal Policy	Clinica_Plc_ThermalPolicy

Fuente. Elaboración propia.

En la Tabla 10 se muestra la configuración del UCS Server Profile Template que servirá como plantilla para todos los blades nuevos y futuros del chasis adquirido.

Tabla 10 UCS Server Profile Template

UCS Server Profile Template	ucsclinica1_X210c_1_LocalDisk	
Descripción	Plantilla de perfil de servidores UCS X210c M7 del Chassis 1 con 6 vNICs y 4 vHBAs	
Compute	UUID Pool	Clinica_Pool_UUIDPool
	BIOS Policy	Clinica_Plc_BIOS
	Boot Order Policy	Clinica_Plc_BootOrder_LocalDisk
	Virtual Media Policy	Clinica_Plc_VirtualMedia
Management	IMC Access Policy	Clinica_Plc_IMCAccess
	Local User Policy	Clinica_Plc_LocalUser
	Virtual KVM Policy	Clinica_Plc_vKVM
Network	LAN Connectivity Policy	Clinica_Plc_LANConn
	SAN Connectivity Policy	Clinica_Plc_SANConn

Fuente. Elaboración propia.

La Tabla 11 muestra los UCS Server Profiles a ser derivados a partir del UCS Server Profile Template ucsclinica1_X210c_1_LocalDisk.

Tabla 11 UCS Server Profiles

UCS Server Profiles
Clinica_Pr_f_ucsclinica111
Clinica_Pr_f_ucsclinica112
Clinica_Pr_f_ucsclinica113

Fuente. Elaboración propia.

Policies y Pools

En la etapa de diseño LLD también se definieron los Policies y Pools que integran los perfiles de la solución UCS, los cuales definen los parámetros, identificadores lógicos y configuraciones que serán aplicados a los servidores, chasis y Fabric Interconnects a través de la plataforma Cisco Intersight.

A continuación, se detallan las configuraciones definidas para los UCS Domain Policies.

Los dos Port Policy A y B definen los roles de los puertos de los Fabric Interconnect, además de crear los Port Channel de Ethernet y FC necesarios para la conectividad a los Uplink LAN (hacia los Nexus) y FC (hacia los MDS). Estos Port Policy se detallan en las Tablas 12 y 13.

Tabla 12 Port Policy FI-A

Nombre	Clinica_Plc_FIPort_A
Descripción	Política de puertos FI A
Puertos FC	1-16
Puertos Eth	53-54
Puertos Server	17-28
Eth Port Channel	51
Eth Port Channel Admin Speed	100 Gbps
Eth Port Channel Link Aggregation Policy	Clinica_Plc_LinkAggregation
Eth Port Channel Link Control Policy	Clinica_Plc_LinkControl
Eth Port Channel Members	53-54
FC UL Port Channel	101
FC UL Port Channel Admin Speed	32 Gbps
FC UL Port Channel VSAN ID	100
FC UL Port Channel Members	1-4

Fuente. Elaboración propia.

Tabla 13 Port Policy FI-B

Nombre	Clinica_Plc_FIPort_B
Descripción	Política de puertos FI B
Puertos FC	1-16
Puertos Eth	53-54
Puertos Server	17-28
Eth Port Channel	52
Eth Port Channel Admin Speed	100 Mbps
Eth Port Channel Link Aggregation Policy	Clinica_Plc_LinkAggregation
Eth Port Channel Link Control Policy	Clinica_Plc_LinkControl
Eth Port Channel Members	53-54
FC UL Port Channel	102
FC UL Port Channel Admin Speed	32 Gbps
FC UL Port Channel VSAN ID	200
FC UL Port Channel Members	1-4

Fuente. Elaboración propia.

La VLAN Policy mostrada en la Tabla 14 define el listado de VLANs habilitadas en los Fabric Interconnect, además de indicar la VLAN Nativa.

Tabla 14 VLAN Policy

Nombre	Clinica_Plc_VLAN
---------------	------------------

Descripción	Política de uplinks LAN			
VLAN Nativa	1			
Nombre de VLAN	Descripción	VLAN	Auto Allow on Uplinks	Multicast Policy
vlan1	Nativa	1	Enabled	Clinica_Plc_Multicast
Vlan2	Tráfico VM #0	2	Enabled	Clinica_Plc_Multicast
Vlan101	Tráfico VM #1	101	Enabled	Clinica_Plc_Multicast
vlan102	Tráfico VM #2	102	Enabled	Clinica_Plc_Multicast
vlan103	Tráfico VM #3	103	Enabled	Clinica_Plc_Multicast
vlan104	Tráfico VM #4	104	Enabled	Clinica_Plc_Multicast

Fuente. Elaboración propia.

Las dos VSAN Policy A y B mostradas en las Tablas 15 y 16 definen las VSAN permitidas y su alcance, el cual en este caso se limita al Uplink debido a que el extremo opuesto se conecta un switch MDS y no un arreglo de almacenamiento directamente. En este caso, se definieron las VSAN 100 y 200 para los Fabric Interconnect A y B, respectivamente.

Tabla 15 VSAN Policy FI-A

Nombre	Clinica_Plc_VSAN_A
Descripción	Política de VSAN A
Uplink Trunking	Enabled
Nombre de VSAN	Clinica_VSAN_A
Descripción	VSAN A
VSAN Scope	Uplink
VSAN	100
FCoE VLAN ID	100

Fuente. Elaboración propia.

Tabla 16 VSAN Policy FI-B

Nombre	Clinica_Plc_VSAN_B
Descripción	Política de VSAN B
Uplink Trunking	Enabled
Nombre de VSAN	Clinica_VSAN_B
Descripción	VSAN A
VSAN Scope	Uplink
VSAN	200
FCoE VLAN ID	200

Fuente. Elaboración propia.

La *NTP Policy* detallada en la Tabla 17 configura los servidores NTP que utilizan los *Fabric Interconnect*.

Tabla 17 NTP Policy

Nombre	Clinica_Plc_NTTPolicy
Enable NTP	Enabled
NTP Server 1	172.16.50.100
NTP Server 2	172.16.51.101
Timezone	America/Lima

Fuente. Elaboración propia.

La *Network Connectivity Policy* mostrada en la Tabla 18 configura los servidores DNS que utilizan los *Fabric Interconnect*.

Tabla 18 Network Connectivity Policy

Nombre	Clinica_Plc_NetworkConfigPolicy
DNS Server 1	172.16.50.10
DNS Server 2	172.16.51.11
Enable IPv6	Disabled

Fuente. Elaboración propia.

La Tabla 19 muestra la *Switch Control Policy* que configura al *Fabric Interconnect* en modo End Host para el tráfico Ethernet y FC debido a que la infraestructura cuenta con dispositivos Ethernet (Switches Nexus) y FC (Switches MDS) intermedios para la conmutación del tráfico y zonificación. En el caso del tráfico Ethernet, deshabilita la intervención de los *Fabric Interconnects* en Spanning-Tree Protocol (STP) y para el tráfico FC activa el modo NPV para reutilizar los FC Domain de los *switches* MDS y deshabilita la zonificación en los FIs.

Tabla 19 Switch Control Policy

Nombre	Clinica_Plc_SwitchEndHost
Ethernet Switching Mode	End Host
FC Switching Mode	End Host

Fuente. Elaboración propia.

En los siguientes cuadros se detallan las configuraciones aplicadas en los UCS Chassis Policies.

La IMC Access Policy mostrada en la Tabla 20 define la interfaz de acceso

para la gestión vKVM de los servidores que se instalan en este chasis, además de indicar el pool que asigna las IP KVM a los servidores, el cual se detalla en la Tabla 21.

Tabla 20 IMC Access Policy para chasis

Nombre	Clinica_Plc_IMC_Access
Descripción	Política de acceso IMC (KVM)
In-Band Configuration	Disabled
Out-of-Band Configuration	Enabled
IP Pool Name	IPPool

Fuente. Elaboración propia.

Tabla 21 IP Pool para acceso vKVM

Nombre	Clinica_Pool_IPPool
Descripción	Pool de IP para vKVM
Netmask	255.255.255.0
Gateway	172.16.24.254
Primary DNS	172.16.50.10
Secondary DNS	172.16.51.11
From	172.16.24.111
Size	8

Fuente. Elaboración propia.

La *Power Policy* para chasis mostrada en la Tabla 22 habilita el modo *Grid* que permite habilitar el doble de fuentes de energía requeridas, siendo el segundo grupo redundante en caso el primer grupo de 3 fuentes sufra alguna pérdida de alimentación en su PDU.

Tabla 22 Power Policy para chasis

Nombre	Clinica_Plc_PowerPolicy
Descripción	Política de energía de chasis
Redundancy Mode	Grid (N+N o 3+3)

Fuente. Elaboración propia.

La *Thermal Policy* mostrada en la Tabla 23 selecciona el modo *Balanced* para los ventiladores del chasis, con el cual varía automáticamente la velocidad según la temperatura de los componentes internos del chasis, asegurando un consumo eficiente de energía y mejorando la performance bajo demanda.

Tabla 23 Thermal Policy

Nombre	Clinica_Plc_ThermalPolicy
Descripción	Política de ventilación
Fan Control Mode	Balanced

Fuente. Elaboración propia.

En los siguientes cuadros se detallan las configuraciones aplicadas en los UCS Server Policies.

La *Boot Order Policy* mostrada en la Tabla 24 define los dispositivos de almacenamiento que se utilizarán como dispositivos de arranque del sistema, además del orden en que serán elegidos por el servidor durante el arranque hasta encontrar un sistema operativo.

Tabla 24 Boot Order Policy

Nombre	Clinica_Plc_BootOrder-BootFromLocalDisk	
Descripción	Política de orden de booteo	
Configured Boot Mode	UEFI	
Enable Secure Boot	Enabled	
1. Local Disk1	Device Name	LocalDisk1
	Slot	1
2. Virtual Media (ISO)	Device Name	kvmDVD
	Sub-Type	KVM MAPPED DVD

Fuente. Elaboración propia.

La vMedia Policy mostrada en la Tabla 25 habilita los medios virtuales para insertar a través de la interfaz vKVM, con lo cual se podrán conectar imágenes de sistemas operativos a los blades para su instalación.

Tabla 25 Virtual Media Policy

Nombre	Clinica_Plc_vMedia
Descripción	Política de dispositivos virtuales en KVM
Enable Virtual Media	Enabled
Enable Virtual Media Encryption	Enabled
Enable Low Power USB	Enabled

Fuente. Elaboración propia.

La *Local User Policy* mostrada en la Tabla 26 define el usuario de administración de vKVM. Tener en cuenta que se ha ocultado la contraseña configurada por motivos de confidencialidad.

Tabla 26 Local User Policy

Nombre	Clinica_Plc_LocalUser
Descripción	Política de usuarios locales para acceso vKVM
Enforce Strong Password	Disabled
Enable Password Expiry	Disabled
Password History	5
Always Send User Password	Disabled
Username	admin
New User	Enabled
Role	admin
Password	#####

Fuente. Elaboración propia.

La vKVM Policy mostrada en la Tabla 27 habilita la interfaz Virtual KVM y define el puerto TCP a utilizar para la comunicación con dicha interfaz (adicional al puerto TCP/2068 que siempre se utiliza para la validación de certificados SSL).

Tabla 27 Virtual KVM Policy

Nombre	Clinica_Plc_kvm
Descripción	Política de interfaz vKVM
Enable Virtual KVM	Enabled
Max Sessions (1-4)	4
Remote Port	2068
Enable Video Encryption	Enabled
Enable Local Server Video	Enabled
Allow Tunneled vKVM	Enabled

Fuente. Elaboración propia.

La LAN Connectivity Policy mostrada en la Tabla 28 define la cantidad de vNICs Ethernet que se utilizan en el servidor, indicar el Fabric Interconnect A o B de cada vNIC, seleccionar el MAC Address Pool del cual se asignan las MAC a cada vNIC del fabric A o B, y configurar las VLAN permitidas (deben estar permitidas en los Fabric Interconnect también). En este caso, se crearon seis vNICs para el servidor. Cabe resaltar que se ha habilitado el Failover para todas las vNICs. Además, la Tabla 29 muestra la configuración de VLANs para cada vNIC, y la Tabla 30 muestra los Pools de direcciones MAC.

Tabla 28 LAN Connectivity Policy

Nombre	Clinica_Plc_LANConn
Descripción	Política de LAN

vNIC Configuration	Manual	
vNICs	0, 2 y 4	1, 3 y 5
MAC Pool	Clinica_Pool_MACAddrPool_A	Clinica_Pool_MACAddrPool_B
Failover	Enabled	Enabled
Slot ID	MLOM	MLOM
Switch ID	A	B
Ethernet Network Group Policy	Clinica_Plc_LanVlans	Clinica_Plc_LanVlans

Fuente. Elaboración propia.

Tabla 29 Ethernet Network Group Policy

Nombre	Clinica_Plc_LanVlans
Descripción	Política de asignación de VLANs
VLAN Nativa	1
VLANs permitidas	1,2,101-104

Fuente. Elaboración propia.

Tabla 30 MAC Address Pools

Nombre	Clinica_Pool_MACAddrPool_A	Clinica_Pool_MACAddrPool_B
Descripción	Pool de MACs para vNICs en Fabric A	Pool de MACs para vNICs en Fabric B
MAC Address Inicial	00:25:B5:37:A0:00	00:25:B5:37:B0:00
Size	64	64
Switch ID	A	B

Fuente. Elaboración propia.

La *SAN Connectivity Policy* detallada en la Tabla 31 crea las vHBA que utiliza el servidor para la comunicación SAN, así como los pWWN y nWWN Pools asignados a los vHBAs y servidores, el modo iniciador para los HBA, el fabric A o B al que pertenecen y la vSAN 100 o 200 a la que se asocia el tráfico de cada vHBA (con las FC Network Policies). Cabe mencionar que, al estar configurada la red SAN en modo End Host, no hace falta utilizar una *FC Zone Policy* pues son los *switches* MDS quienes se encargan de la zonificación. Las *Pools* y *Policies* que componen la *SAN Connectivity Policy* se detallan en las Tablas 32, 33 y 34.

Tabla 31 SAN Connectivity Policy

Nombre	Clinica_Plc_SANConn	
Descripción	Política de SAN	
WWNN Pool	Clinica_Pool_WWNNAddrPool	
vHBA Placement	Manual	
vHBA	0 y 1	2 y 3
vHBA Type	fc-initiator	fc-initiator
WWPN Pool	Clinica_Pool_WWPNAddrPool_A	Clinica_Pool_WWPNAddrPool_B

Slot ID	MLOM	MLOM
Switch ID	A	B
FC Network Policy	vSANID_A	vSANID_B
FC Zone Policy	-	-

Fuente. Elaboración propia.

Tabla 32 WWNN Address Pool

Nombre	WWNNAddrPool
Descripción	Pool de WWNNs para UCS
Starting WWNN	24:d7:ac:73:d2:22:00:00
Size	256

Fuente. Elaboración propia.

Tabla 33 WWPN Address Pools

Nombre	WWPNAddrPool_A	WWPNAddrPool_B
Descripción	Pool de WWPNS para vHBA en Fabric A	Pool de WWPNS para vHBA en Fabric B
Starting WWNN	24:d7:ac:73:d2:22:a0:00	24:d7:ac:73:d2:22:b0:00
Size	256	256
Switch ID	A	B

Fuente. Elaboración propia.

Tabla 34 FC Network Policies

Nombre	vSANID_A	vSANID_B
Descripción	Política de asignación de VSAN en vHBA-A	Política de asignación de VSAN en vHBA-B
VSAN	100	200

Fuente. Elaboración propia.

3.5.4.5 Gestión

Se hace uso de la red existente de Gestión (MGMT) para los flujos que son graficados en la Figura 18, los cuales se describen a continuación.

- Gestión de los Switches LAN y SAN nuevos.
- Acceso vía HTTPS a la interfaz vKVM (TCP/2068 y TCP/443) de los blades.
- Gestión en nube del chasis y los blades vía Cisco Intersight.
- Gestión on-premise de la infraestructura vSphere vía vCenter.

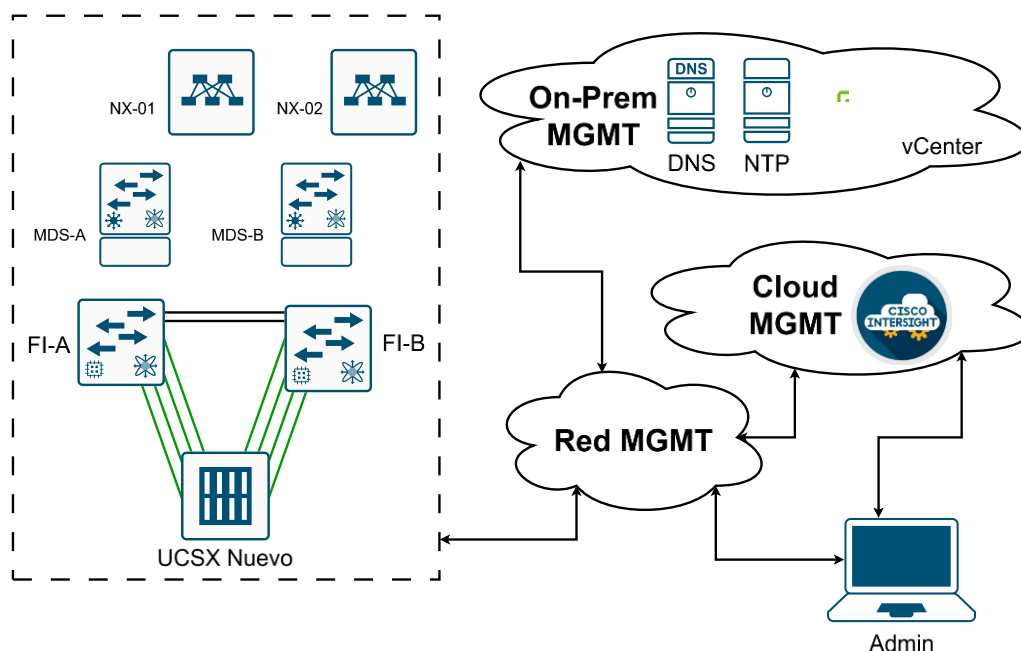


Figura 18 Conexiones lógicas definidas para gestión. Fuente. Elaboración propia. Los íconos y logotipos son propiedad de Cisco Systems, Inc. y Broadcom Inc.; estos se incluyen con el fin de ilustrar el diseño.

Además, la clínica cuenta con servidores DNS para asegurar la resolución de nombres de dominio de servicios en nube y servidores NTP para mantener sincronizada la hora de los equipos y sea posible la correcta correlación de eventos entre diversos equipos haciendo uso de los timestamps. Es necesario configurar los switches LAN, SAN y servidores nuevos con estos mismos servidores, lo cual se denomina parámetros comunes. Los parámetros comunes para este proyecto se detallan en la Tabla 35.

Tabla 35 Parámetros comunes

Dominio	clinica.com.pe
Servidor DNS primario	172.16.50.10
Servidor DNS secundario	172.16.51.11
Servidor NTP primario	172.16.50.100
Servidor NTP primario	172.16.51.101

Fuente. Elaboración propia.

Se utilizó la VLAN 101 de Gestión para el direccionamiento de los Switches LAN, SAN, los FI, las interfaces vKVM de los servidores Blade UCS-X (los cuales se comunican a través de las interfaces MGMT de los FI) y los vmkernel de gestión y vMotion de los nuevos hosts ESXi. La Tabla 36 detalla el direccionamiento de gestión asignado en el proyecto.

Tabla 36 Direccionamiento de gestión definido

Equipo	Interfaz	IP	Mascara	Gateway	VLAN
ucsclinica1-1-1	vKVM	172.16.24.111	255.255.255.0	172.16.24.254	101
ucsclinica1-1-2	vKVM	172.16.24.112			
ucsclinica1-1-3	vKVM	172.16.24.113			
clinicaesxi01.clinica.com.pe	vmk0 (mgmt+vmotion)	172.16.24.101			
clinicaesxi02.clinica.com.pe	vmk0 (mgmt+vmotion)	172.16.24.102			
clinicaesxi03.clinica.com.pe	vmk0 (mgmt+vmotion)	172.16.24.103			
ucsclinica1-A	mgmt0	172.16.24.109			
ucsclinica1-B	mgmt0	172.16.24.110			
SW-CORE-Clinica1	Vlan5	172.16.24.252			
SW-CORE-Clinica2	Vlan5	172.16.24.253			
SW-CORE-Clinica1 y SW-CORE-Clinica2	VIP HSRP	172.16.24.254			
MDS-Clinica-A	mgmt0	172.16.24.201			
MDS-Clinica-B	mgmt0	172.16.24.202			
clinicavcenter.clinica.com.pe	vCenter	172.16.24.100			

Fuente. Elaboración propia.

La red de gestión es desplegada físicamente a través del switch SW-BORDE, el cual tiene configurados los puertos de acceso en VLAN 101 para las interfaces de gestión de los equipos nuevos de la solución (FI, Nexus y MDS).

3.5.4.6 Virtualización

La finalidad del despliegue de los servidores UCS-X es poder ampliar la infraestructura virtualizada, añadiendo tres nuevos hosts ESXi al inventario.

El vCenter designado para administrar esta nueva infraestructura es el servidor existente clinicavcenter.clinica.com.pe. En la Tabla 37 se muestra la distribución de los hosts en el inventario del vCenter.

Cada host cuenta con dos puertos VMkernel: uno para Management y el otro para vMotion. En la Tabla 38 se indica el direccionamiento de gestión de ESXi.

La Tabla 39 muestra el direccionamiento de los puertos VMkernel vMotion, los cuales se utilizarán para la migración en caliente de máquinas virtuales.

Tabla 37 Inventario de hosts en vCenter

Host	Cluster	Data Center	vCenter	IP vCenter	Dominio
clinicaesxi01					
clinicaesxi02	Cluster_Clinica	DC_Clinica	clinicavcenter.clinica.com.pe	172.16.24.100	clinica.com.pe
clinicaesxi03					

Fuente. Elaboración propia.

Tabla 38 Configuración de VMkernel de gestión

Host	VLAN Gestión	IP Gestión/máscara	Gateway
clinicaesxi01.clinica.com.pe	101 (Tagged)	172.16.24.101/24	172.16.24.254
clinicaesxi02.clinica.com.pe		172.16.24.102/24	
clinicaesxi03.clinica.com.pe		172.16.24.103/24	

Fuente. Elaboración propia.

Tabla 39 Configuración de VMkernel de vMotion

Host	VLAN vMotion	IP vMotion/máscara	Gateway
clinicaesxi01.clinica.com.pe	101 (Tagged)	172.16.24.101/24	172.16.24.254
clinicaesxi02.clinica.com.pe		172.16.24.102/24	
clinicaesxi03.clinica.com.pe		172.16.24.103/24	

Fuente. Elaboración propia.

Además, cada host cuenta con dos vSwitches estándar, siendo el primero para tráfico de gestión y de máquinas virtuales, y el segundo para tráfico de vMotion. Cada vSwitch cuenta con dos Uplinks que pertenecen al Fabric Ethernet A y B. La configuración de vSwitches, Port Groups y VMKernels se muestran en la Tabla 40.

Tabla 40 Configuración de vSwitches

Standard vSwitch	Uplinks	Port Groups	VLAN de Port Group	VMkernels en Port Group
vSwitch0	vmnic0 (Fabric A) vmnic1 (Fabric B)	VLAN1	1	Nativa
		VLAN2	2	Tráfico VM #0
		VLAN101	101	vmk0 (MGMT)
		VLAN102	102	Tráfico VM #2
		VLAN103	103	Tráfico VM #3
		VLAN104	104	Tráfico VM #4
		VLAN105	105	Tráfico VM #5
vSwitch1	vmnic2 (Fabric A) vmnic3 (Fabric B)	vMotion	101	vmk1 (vMotion)

Fuente. Elaboración propia.

Además, se habilitó el modo High Performance en la Power Policy de los tres hosts, el cual deshabilita las funciones de ahorro de energía para priorizar el rendimiento de los servidores.

3.5.4.7 Software y licenciamiento

En el diseño LLD se definen las versiones de software que se instalarán en todos los equipos a configurar. Para esto es necesario revisar cuáles son las versiones estables de cada sistema, y verificar la compatibilidad de cada componente de la solución y sus versiones de software en las matrices de compatibilidad de cada fabricante que, generalmente, se encuentran publicadas en sus sitios web.

El equipamiento en este proyecto utilizó las versiones de software listadas en la Tabla 41.

Tabla 41 Versiones de software

Equipo	Versión
UCS X210c M7	5.2(2.240074)
UCS FI 6454	4.3(5.240032)
VMware ESXi	8.0.3c 24414501
VMware vCenter	8.0.3d 24322831
Cisco Nexus	10.3(5)
Cisco MDS	9.2(1a)

Fuente. Elaboración propia.

En el diseño LLD también se documenta el licenciamiento adquirido para los equipos del proyecto, el cual se resume en la Tabla 42.

Tabla 42 Modos de licenciamiento

Equipo	Nivel de licenciamiento
UCS X210c M7	Essentials por 5 años

UCS FI 6454	Licenciamiento embebido de 18 puertos Ethernet/FC de 10/25/8/16/32 Gbps y dos puertos Ethernet de 40/100 Gbps en cada FI.
Cisco MDS 9132T	Licenciamiento embebido de 8 puertos FC y licencia adicional de 8 puertos FC para cada switch. Con esto se logra licenciar el uso de los 16 puertos FC de cada switch MDS.
VMware ESXi	Licenciado por el cliente.

Fuente. Elaboración propia.

3.5.5 Implementación

Para implementar esta solución, es necesario analizar la arquitectura existente para determinar el procedimiento óptimo para poner en producción los nuevos equipos, teniendo como criterios causar el menor impacto posible al tráfico y cargas de trabajo de la empresa; y optimizar los tiempos de implementación, evitando el retrabajo y reduciendo las ventanas de mantenimiento.

La solución Cisco UCS necesita integrarse a la red LAN y SAN nueva, ya que integrarla a los switches antiguos habría implicado un esfuerzo técnico innecesario para lograr la compatibilidad entre equipos nuevos y antiguos, lo cual debe evitarse en la medida de lo posible. Con esta premisa, se acordó realizar la configuración y reemplazo de switches Nexus (LAN) y MDS (SAN) antes de conectar el chasis y los FI a las redes LAN y SAN, seguido de la configuración de los sistemas de almacenamiento, servidores, los sistemas operativos, y preparar la migración de las máquinas virtuales.

3.5.5.1 Configuración de almacenamiento

La clínica contaba con arreglos de almacenamiento como parte de su infraestructura existente, la cual se iba a mantener en la nueva solución para ser conectados a los nuevos switches y servidores.

Teniendo como insumo los nombres de los servidores y los valores de identificadores WWPN definidos en la etapa de LLD, se realizó la creación de los objetos de hosts en los almacenamientos para que se puedan conectar a las LUN que contienen a los datastores de la solución actual de VMware vSphere.

3.5.5.2 Despliegue de redes LAN y SAN

Los switches Cisco Nexus y Cisco MDS nuevos de este proyecto fueron configurados desde cero. Esto incluye el upgrade del firmware NX-OS de estos switches SAN y LAN, el cual fue definido en la etapa de diseño.

Posterior a esto, se realiza la configuración de enlaces y conexiones existentes en la solución antigua, y se agregan las configuraciones de enlaces a equipos nuevos. También se agregan las configuraciones adicionales definidas en la etapa de diseño.

Se aprovechó el espacio de trabajo para preconfigurar también el nuevo cluster Fabric Interconnect vía consola. Se configuraron el nombre del dominio UCS, direcciones IP y credenciales de administración y el modo Intersight para gestionar la solución UCS por la interfaz de gestión en nube.

Una vez preconfigurados los switches SAN, LAN y los FI, se agenda una ventana de mantenimiento para instalar los switches nuevos. En el caso de la red LAN, no se incluyó la adquisición de nuevos cableados de cobre ni fibra para enlaces existentes, siendo necesaria la instalación de los switches nuevos en una posición cercana a los switches antiguos para realizar la migración reutilizando los cables existentes sin problemas. Los enlaces

nuevos de la solución sí requirieron nuevos cables Twinax de 100 Gbps de Cisco, los cuales funcionan como uplinks LAN de la solución UCS y enlace Peer Link para ambos switches Nexus nuevos. Estos cables fueron conectados entre los switches Nexus nuevos y los nuevos FI, según el port mapping mostrado en este documento.

Por otro lado, en la red SAN sí se adquirieron nuevas fibras ópticas multimodo para realizar la conexión de los nuevos switches SAN a los sistemas de almacenamiento existentes y los FI nuevos. Las fibras ópticas monomodo que conectaban los switches MDS antiguos de la clínica con los switches MDS de la sede central sí tuvieron que ser reutilizados, ya que no se consideraron nuevas fibras de este tipo en el proyecto. Para aprovechar el espacio libre del gabinete de servidores, se optó por instalar los nuevos switches SAN en este gabinete junto a los FI nuevos. Las 2 fibras ópticas monomodo se trasladaron sin problemas de un gabinete a otro, y las nuevas fibras ópticas multimodo se tendieron desde la ubicación de los nuevos switches SAN hacia los racks de los sistemas de almacenamiento y se conectaron a los FI nuevos.

3.5.5.3 Migración de redes LAN y SAN

El proceso de reemplazo de switches tuvo estrategias diferentes para las redes LAN y SAN.

Para la red LAN, la migración se tuvo que realizar "en frío" mediante una ventana de mantenimiento disruptiva coordinada con la clínica. Esto se debió a que la totalidad de las conexiones de red se concentraban en un único switch Nexus antiguo, por lo que no existía redundancia para mover el tráfico gradualmente. Todos los enlaces se desconectaron del equipo legado y se reconectaron distribuidos entre el nuevo par de switches Nexus A y B.

Por otro lado, la migración de la red SAN sí se realizó de forma no disruptiva ("en caliente"), gracias a la configuración de redundancia en los servidores y arreglos de almacenamiento, se procedió a migrar primero todas las conexiones de la SAN A hacia el nuevo MDS, y una vez estabilizado el tráfico

en la SAN A, se repitió el proceso con la SAN B. De esta forma, se logró migrar todos los storage existentes a los nuevos switches MDS.

Sin embargo, durante esta etapa se presentó un inconveniente: un catálogo de compatibilidad en el chasis UCS antiguo no incluía al modelo de switch MDS nuevo, debido a la antigüedad de la versión de firmware del chasis antiguo. Al ser un equipo sin contrato de soporte activo con Cisco, se descartó realizarle una actualización de versión. Para evitar un impacto en los servidores antiguos, se optó por una topología de convivencia temporal. Se mantuvieron los switches MDS antiguos operativos y el chasis UCS B se dejó conectado a ellos. Luego, se configuraron enlaces troncales (ISL) entre los MDS antiguos y los nuevos. De esta manera, los almacenamientos y los nuevos nuevos Fabric Interconnect se conectaron directamente a los nuevos switches SAN, garantizando que los servidores antiguos del UCS B pudieran seguir accediendo a sus discos a través de los enlaces ISL sin interrumpir la operación.

Finalmente, se conectaron los puertos de gestión de los switches MDS y los FI a los puertos de acceso definidos en el switch de gestión SW-BORDE, para poder tener gestión remota de los nuevos switches instalados y los FI puedan conectarse a Internet para alcanzar la plataforma de gestión en nube.

3.5.5.4 Configuración de solución Cisco UCS

Para realizar la configuración de la solución Cisco UCS, es necesario crear una cuenta para la clínica en la plataforma Cisco Intersight, la cual luego puede dar los permisos a otros usuarios Cisco para su acceso a la organización creada en Cisco Intersight.

En esta organización, es necesario registrar los Fabric Interconnects utilizando sus identificadores y código de registro que se muestra en su interfaz Web Local. Para lograr la administración y control completa que necesitamos, es necesario validar que los FI tengan configurado el modo “Allow control” en el Device Connector, tal como se muestra en la Figura 19.

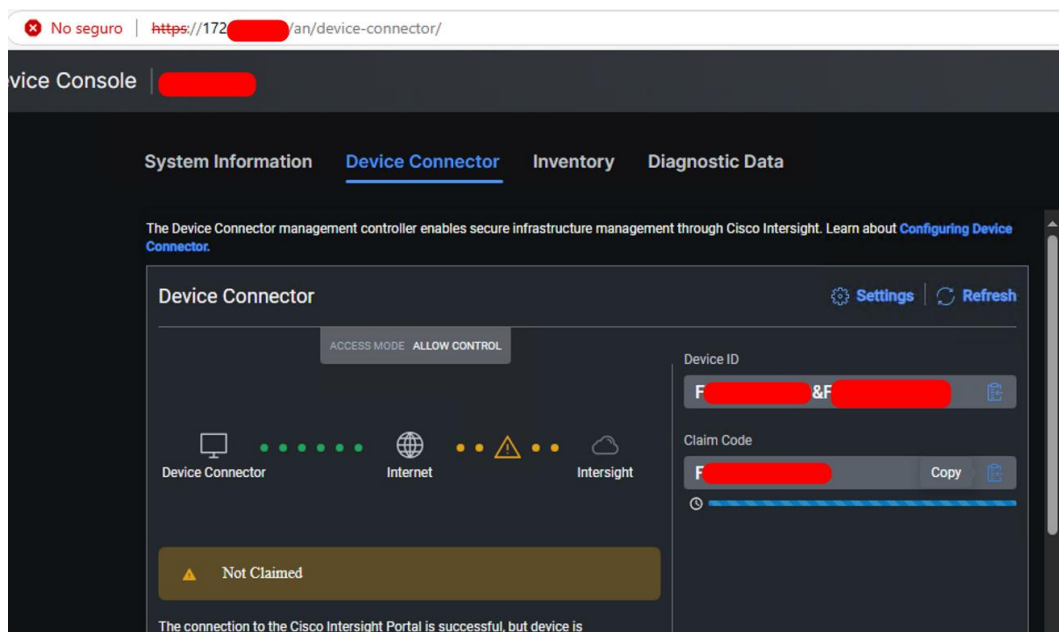


Figura 19 Configuración de Device Connector en Fls. Fuente. Captura de pantalla del portal Cisco Intersight del cliente, mostrando el estado operativo de los servidores desplegados.

Luego de registrar los FI en Cisco Intersight, podremos aplicar la configuración de los FI utilizando los UCS Domain Policies y UCS Domain Profile según se definió en el LLD. Al desplegar estos perfiles en los FI y realizar las conexiones entre los FI y las tarjetas IFM del chasis nuevo y los switches LAN y SAN, se logrará crear el dominio UCS (Cluster FI), se descubrirá el chasis y los nuevos blades en Cisco Intersight, y se tendrá el nuevo chasis integrado a las redes LAN y SAN. También se tendrá disponible la función de upgrade de dominio UCS, con lo cual se puede actualizar los FI a la versión de firmware definida en el LLD. Tras su descubrimiento, se validó que los servidores Cisco UCS ya tenían instalada la versión de firmware recomendada hasta ese momento (la misma versión que se definió en el LLD).

Con el descubrimiento del chasis y los servidores, se puede aplicar la configuración de servidores y chasis definidas en los UCS Server Profile Templates y UCS Chassis Profile. El despliegue de los UCS Server Profiles habilita los servidores para poder ser gestionados localmente vía IP de vKVM, despliega las interfaces de red vNIC y vHBA con sus identificadores lógicos; además de aplicar otras configuraciones a los servidores según se definió en el LLD.

3.5.5.5 Configuración de solución VMware vSphere 8.0

Haciendo uso de la interfaz web vKVM de los servidores Cisco UCS y el archivo de instalación de sistema operativo VMware ESXi 8.0 en formato .iso, se realiza la instalación en el almacenamiento local de cada servidor.

Luego de instalar los sistemas operativos en los servidores Cisco UCS, se realiza la configuración básica de gestión de host ESXi, con lo cual se les habilita la conectividad de gestión necesaria para ser integrados a la solución vSphere existente.

El vCenter existente se encontraba en una versión antigua de software, la cual no soportaba el registro de los nuevos hosts ESXi en versión 8.0.3, para lo cual se realizó el upgrade del vCenter a la versión 8.0.3d 24322831 definida en el LLD.

Luego de esto, se registran los nuevos hosts ESXi en el vCenter existente para poder finalizar las configuraciones de cluster, licenciamiento, port groups y vmkernel para vMotion de forma centralizada desde el gestor vCenter.

El vCenter también permite visualizar de forma simplificada las LUNs y paths descubiertos por los hosts a través de la red SAN, identificando las interfaces vHBA desde la que se descubre cada path. De esta forma se puede verificar rápidamente la redundancia de conexión SAN de cada host ESXi. En caso no se logre visualizar alguna de las LUN de los arreglos de almacenamiento existentes o algún datastore, se puede realizar el escaneo de los adaptadores de almacenamiento (vmhba) para descubrir las LUN y montar los datastores VMFS.

3.5.5.6 Migración de máquinas virtuales

Hasta este punto, se tiene la infraestructura de Data Center lista para correr las cargas de trabajo productivas de la solución antigua, y solo falta realizar la migración de las máquinas virtuales del antiguo chasis UCS serie B al nuevo

chasis UCS serie X (entre hosts, sin cambiar de storage).

Esta migración se realiza de forma no disruptiva gracias a la función vMotion que el vCenter habilita en los hosts registrados, lo cual permite transferir en caliente el procesamiento de una máquina virtual a otro host ESXi ubicado en otro chasis, a través de la red LAN. No es necesario realizar ninguna transferencia de datos de almacenamiento, ya que en este escenario se hace uso de un arreglo de almacenamiento compartido, al cual ambos hosts antiguo y nuevo tienen conectividad vía SAN.

Dependiendo del tamaño de la memoria en ejecución de la máquina virtual migrada, el tiempo de cada migración puede variar entre los 15 segundos a los cinco minutos, mientras que las máquinas virtuales apagadas se migran instantáneamente.

3.6 Resultado de la actividad

Debido a la criticidad de los servicios médicos y administrativos de la clínica que operan las 24 horas del día, los 7 días de la semana, la ventana de mantenimiento no contempló la ejecución de pruebas destructivas de *failover* (como la desconexión física de enlaces o apagado de equipos) para evitar riesgos sobre las aplicaciones en producción. En su lugar, la validación de la alta disponibilidad y continuidad operativa se realizó verificando el estado lógico y físico de la redundancia en las plataformas de gestión de cada componente, confirmando que la arquitectura base se encontraba operando sin puntos únicos de falla.

La plataforma en la nube Cisco Intersight permite monitorear el estado de los componentes UCS (Fabric Interconnects, chasis y servidores), sus elementos internos, recursos, configuración, alertas y versión de firmware. Además, proporciona la capacidad de ejecutar acciones de administración que tradicionalmente se realizaban desde el gestor local UCS Manager en la antigua serie B de chasis y servidores Cisco UCS.

En la sección *Infrastructure > Operate > Servers* mostrada en la Figura 20, se evidencia el estado *Healthy* de los cuatro servidores instalados, lo cual indica la ausencia de alertas operativas en los equipos tras la implementación.

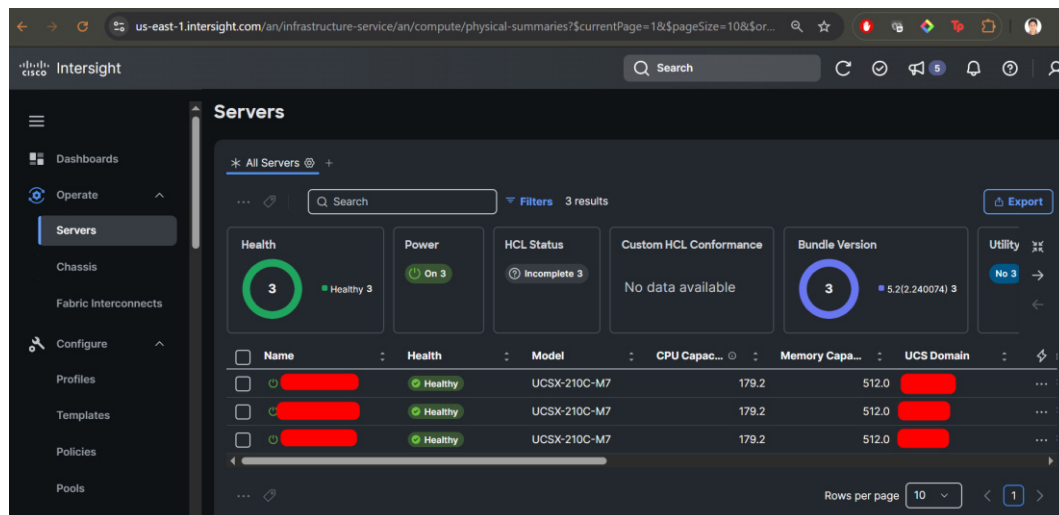


Figura 20 Servidores UCS-X en Intersight. Fuente. Captura de pantalla del portal Cisco Intersight del cliente, mostrando el estado operativo de los servidores desplegados.

Asimismo, la Figura 21 presenta la sección *Infrastructure > Operate > Chassis* muestra el estado *Healthy* del chasis UCS-X9508 desplegado en la solución.

Para un análisis más detallado del hardware, dentro de la sección *Inventory > Power > PSUs* correspondiente al chasis, mostrada en la Figura 22, se verifica el estado de operación normal de las seis fuentes de alimentación.

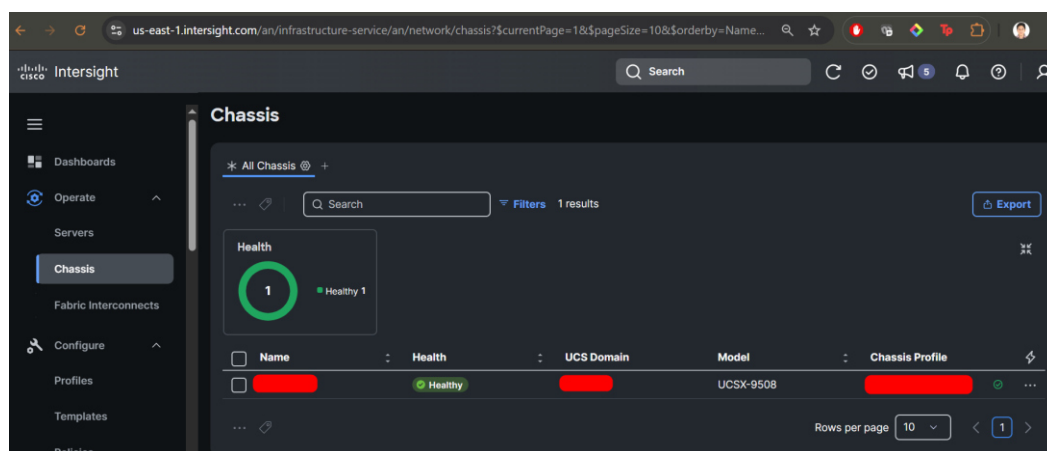


Figura 21 Chasis UCS-X en Intersight. Fuente. Captura de pantalla del portal Cisco Intersight del cliente, evidenciando el estado general del chasis.

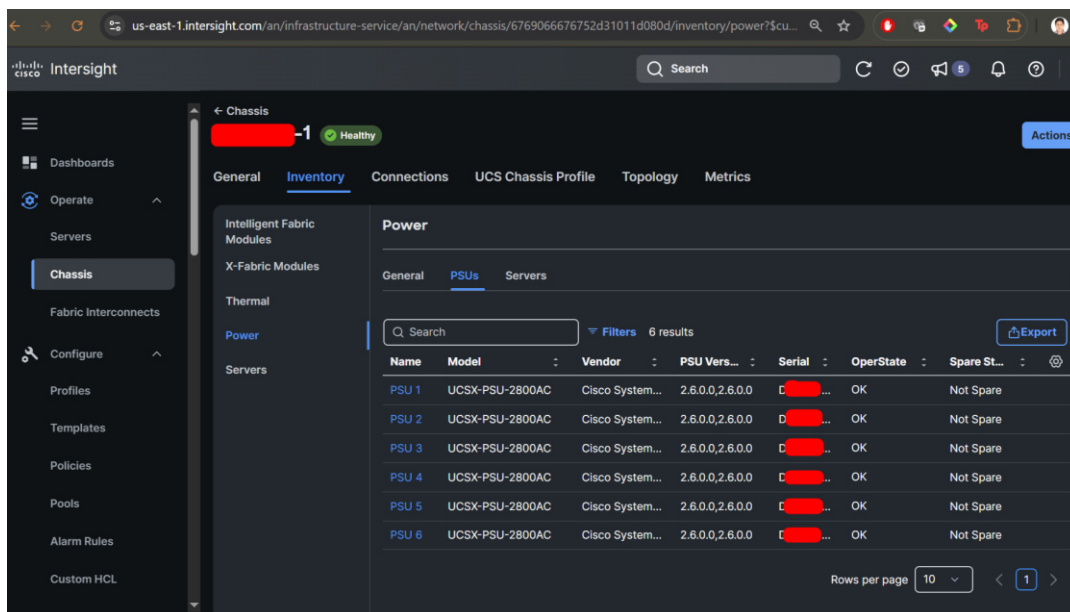


Figura 22 Fuentes de energía del chasis UCS-X operativas. Fuente. Captura de pantalla de la plataforma de gestión que confirma la redundancia eléctrica del equipo.

En cuanto a los componentes de red, la sección *Infrastructure > Operate > Fabric Interconnects* detalla el estado funcional de los dos equipos Fabric Interconnect integrados en el proyecto y algunos detalles resumidos como el modelo, firmware y uso de puertos, lo cual se muestra en la Figura 23.

Finalmente, al explorar la ruta *Inventory > PSUs* de los Fabric Interconnects mostradas en las Figuras 24 y 25, se confirma el estado operativo de sus dos fuentes de alimentación.

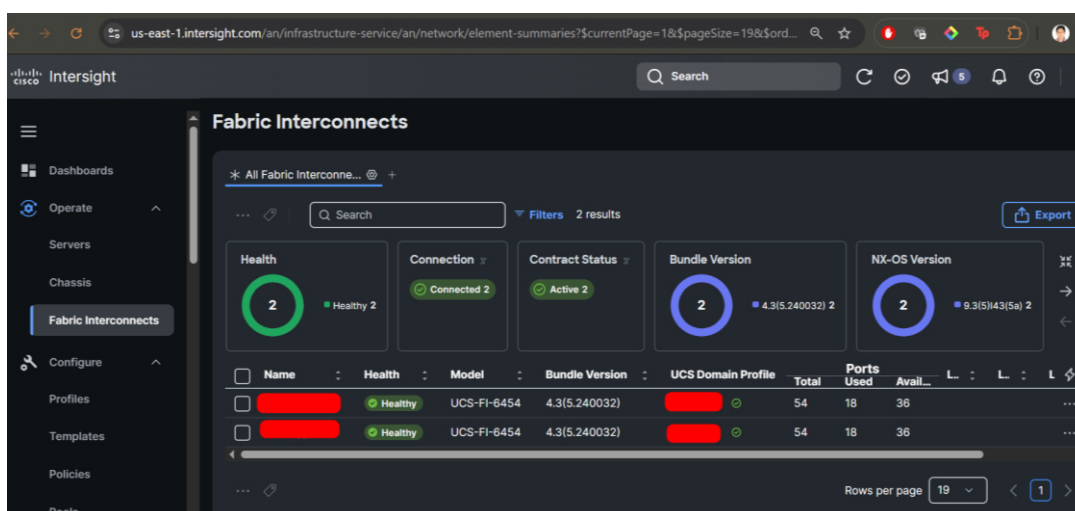


Figura 23 Fabric Interconnects en Intersight. Fuente. Captura de pantalla del portal Cisco Intersight mostrando los módulos de interconexión.

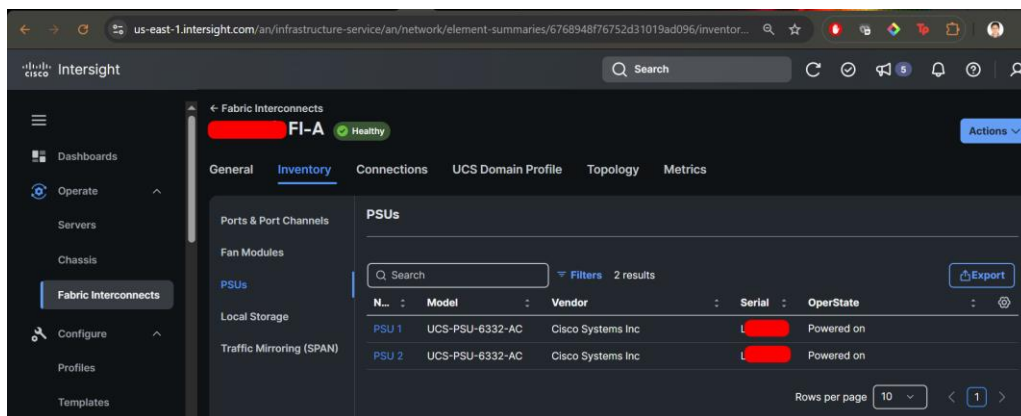


Figura 24 Fuentes de energía redundantes en Fabric Interconnect A. Fuente. Captura de pantalla que evidencia el funcionamiento de las fuentes de poder del primer Fabric Interconnect.

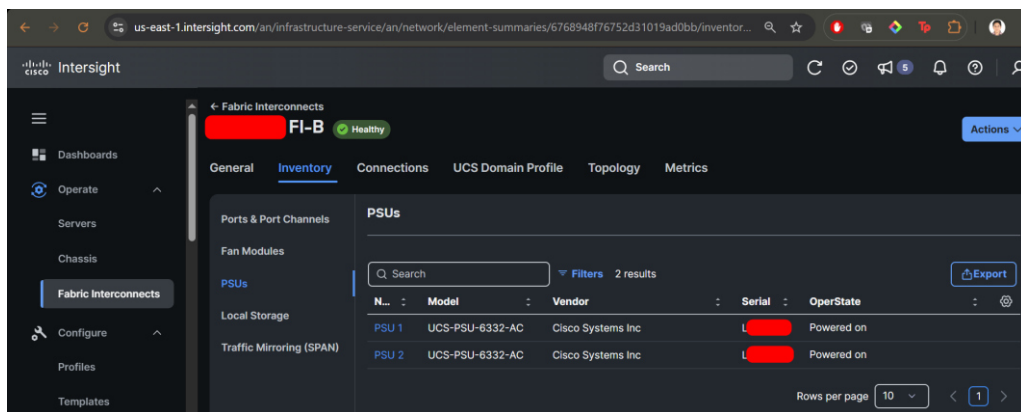


Figura 25 Fuentes de energía redundantes en Fabric Interconnect B. Fuente. Captura de pantalla que evidencia el funcionamiento de las fuentes de poder del segundo Fabric Interconnect.

En la red LAN, la combinación de los protocolos vPC y HSRP logran obtener una infraestructura sumamente resiliente que soporta la caída de un enlace individual o de un switch Core. Tras la implementación, esto se puede validar ejecutando los comandos “show vpc” y “show hsrp brief”. Las Figuras 26 y 27 muestran el estado correcto de la vecindad vPC entre ambos switches; el estado *alive* del enlace vPC *keep-alive* que permitirá que se eviten conflictos de plano de control duplicado en caso de perder el enlace vPC *peer-link* principal; el rol primario y secundario de cada switch; el estado del enlace vPC *peer-link* que sirve para la sincronización de tráfico de control entre ambos switches y el tráfico de interfaces huérfanas; las VLAN permitidas en el enlace vPC *peer-link* y el estado de los enlaces vPC agregados, incluyendo los vPC 101 y 102 formados entre los switches core y los FI.

Las Figuras 28 y 29 muestran el estado de redundancia HSRP de los switches en cada VLAN, confirmando que ambos switches core están listos para enrutar tráfico en todas las VLAN.

Los *switches* de la red SAN alcanzan la redundancia por medio del mecanismo de *port-channel*, el cual permite que el tráfico entre los servidores y los arreglos de almacenamiento no se vea afectado hasta que se caigan los 4 miembros de cada *port-channel* en simultáneo; y la independencia de redes SAN A y B que evita la interrupción del tráfico ante la caída de una red SAN o de un switch MDS. La Figura 30 muestra el estado activo de los 4 puertos miembros de cada *port-channel*, mientras que las Figuras 31 y 32 muestran el listado de nodos iniciadores y *target* que se descubren en cada red SAN, donde se observan presentes los mismos servidores y arreglos de almacenamiento, pero con diferentes puertos e identificadores WWN y FCID.

```
SW 1# show vpc
Legend:
(*) - local vPC is down, forwarding via vPC peer-link

vPC domain id          : 1
Peer status             : peer adjacency formed ok
vPC keep-alive status   : peer is alive
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 consistency status : success
vPC role                : primary
Number of vPCs configured : 5
Peer Gateway            : Enabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status    : Disabled
Delay-restore status    : Timer is off.(timeout = 30s)
Delay-restore SVI status : Timer is off.(timeout = 10s)
Delay-restore Orphan-port status : Timer is off.(timeout = 0s)
Operational Layer3 Peer-router : Disabled
Virtual-peerlink mode   : Disabled

vPC Peer-link status
-----
id   Port   Status Active vlans
--   -
1    Po1    up     1,2,101-105

vPC status
-----
Id   Port   Status Consistency Reason      Active vlans
--   -
10   Po10    up     success  success  1,101-104
20   Po20    up     success  success  1,101-104
30   Po30    up     success  success  1,101-104
101  Po101    up     success  success  1,2,101-104
102  Po102    up     success  success  1,2,101-104
```

Figura 26 Estado final del dominio vPC en el switch Core 1. Fuente. Captura de pantalla del switch Core 1 tras la implementación.

```

SW 2# show vpc
Legend:
(*) - local vPC is down, forwarding via vPC peer-link

vPC domain id          : 1
Peer status             : peer adjacency formed ok
vPC keep-alive status   : peer is alive
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 consistency status : success
vPC role                : secondary
Number of vPCs configured : 5
Peer Gateway            : Enabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status    : Disabled
Delay-restore status    : Timer is off.(timeout = 30s)
Delay-restore SVI status : Timer is off.(timeout = 10s)
Delay-restore Orphan-port status : Timer is off.(timeout = 0s)
Operational Layer3 Peer-router : Disabled
Virtual-peerlink mode   : Disabled

vPC Peer-link status
-----
id   Port   Status Active vlans
--   --
1    Po1    up    1,2,101-105

vPC status
-----
Id   Port   Status Consistency Reason      Active vlans
--   --
10   Po10    up    success  success  1,101-104
20   Po20    up    success  success  1,101-104
30   Po30    up    success  success  1,101-104
101  Po101    up    success  success  1,2,101-104
102  Po102    up    success  success  1,2,101-104

```

Figura 27 Estado final del dominio vPC en el switch Core 2. Fuente. Captura de pantalla del switch Core 2 tras la implementación.

```

SW 1# show hsrp brief
*:IPv6 group #:group belongs to a bundle
              P indicates configured to preempt.
Interface  Grp  Prio P State Active addr Standby addr Group addr
Vlan1      1   105 P Active local      172.16.8.253 172.16.8.254 (conf)
Vlan2      2   105 P Active local      172.16.16.253 172.16.16.254 (conf)
Vlan101    101 105 P Active local      172.16.24.253 172.16.24.254 (conf)
Vlan102    102 105 P Active local      172.16.32.253 172.16.32.254 (conf)
Vlan103    103 105 P Active local      172.16.40.253 172.16.40.254 (conf)
Vlan104    104 105 P Active local      172.16.48.253 172.16.48.254 (conf)
Vlan105    105 105 P Active local      172.16.56.253 172.16.56.254 (conf)

```

Figura 28 Estado final del protocolo HSRP en el switch Core 1. Fuente. Captura de pantalla del switch Core 1 tras la implementación.

```

SW 2# show hsrp brief
*:IPv6 group #:group belongs to a bundle
              P indicates configured to preempt.
Interface  Grp  Prio P State Active addr Standby addr Group addr
Vlan1      1   100 P Standby 172.16.8.252 local      172.16.8.254 (conf)
Vlan2      2   100 P Standby 172.16.16.252 local      172.16.16.254 (conf)
Vlan101    101 100 P Standby 172.16.24.252 local      172.16.24.254 (conf)
Vlan102    102 100 P Standby 172.16.32.252 local      172.16.32.254 (conf)
Vlan103    103 100 P Standby 172.16.40.252 local      172.16.40.254 (conf)
Vlan104    104 100 P Standby 172.16.48.252 local      172.16.48.254 (conf)
Vlan105    105 100 P Standby 172.16.56.252 local      172.16.56.254 (conf)

```

Figura 29 Estado final del protocolo HSRP en el switch Core 2. Fuente. Captura de pantalla del switch Core 2 tras la implementación.

```

MDS A# show port-channel database
port-channel51
  Administrative channel mode is active
  Last membership update succeeded
  First operational port is fc1/14
  4 ports in total, 4 ports up
  Ports:  fc1/13  [up]
          fc1/14  [up] *
          fc1/15  [up]
          fc1/16  [up]

MDS B# show port-channel database
port-channel52
  Administrative channel mode is active
  Last membership update succeeded
  First operational port is fc1/13
  4 ports in total, 4 ports up
  Ports:  fc1/13  [up] *
          fc1/14  [up]
          fc1/15  [up]
          fc1/16  [up]

```

Figura 30 Estado final de los enlaces port-channel en ambos switches MDS.
Fuente. Captura de pantalla de los switches MDS A y B tras la implementación.

```

fc1/4      100  0x7500c2  52:c7:38:20:a9:1b:3e:74 52:c7:38:20:a9:00:3e:74
           [Storage1-P5-N3]
fc1/5      100  0x750000  24:3f:58:d3:9c:20:43:00 24:3f:58:d3:9c:20:43:00
           [Storage2-P1-N1]
fc1/7      100  0x750020  52:c7:38:20:0d:06:9a:90 52:c7:38:20:0d:02:9a:90
           [Storage3-P1-N1]
fc1/7      100  0x750021  52:c7:38:20:0d:76:9a:90 52:c7:38:20:0d:02:9a:90
           [Storage3-P1-N2]
fc1/8      100  0x750040  52:c7:38:20:0d:06:9a:91 52:c7:38:20:0d:02:9a:91
           [Storage3-P3-N1]
fc1/8      100  0x750041  52:c7:38:20:0d:76:9a:91 52:c7:38:20:0d:02:9a:91
           [Storage3-P3-N2]
fc1/9      100  0x750100  52:c7:38:20:a9:11:3e:88 52:c7:38:20:a9:00:3e:88
           [Storage1-P6-N1]
fc1/9      100  0x750101  52:c7:38:20:a9:15:3e:88 52:c7:38:20:a9:00:3e:88
           [Storage1-P6-N2]
fc1/9      100  0x750102  52:c7:38:20:a9:19:3e:88 52:c7:38:20:a9:00:3e:88
           [Storage1-P6-N3]
port-channel31 100 0x750060 28:e4:29:b2:91:84:3b:c0 22:58:29:b2:91:84:3b:c1
port-channel31 100 0x750061 24:d7:ac:73:d2:22:a0:00 24:d7:ac:73:d2:22:00:00
           [CHASSIS1-BLADE1-vHBA0-A]
port-channel31 100 0x750062 24:d7:ac:73:d2:22:a0:01 24:d7:ac:73:d2:22:00:00
           [CHASSIS1-BLADE1-vHBA1-A]
port-channel31 100 0x750063 24:d7:ac:73:d2:22:a0:02 24:d7:ac:73:d2:22:00:01
           [CHASSIS1-BLADE2-vHBA0-A]
port-channel31 100 0x750064 24:d7:ac:73:d2:22:a0:03 24:d7:ac:73:d2:22:00:01
           [CHASSIS1-BLADE2-vHBA1-A]
port-channel31 100 0x750065 24:d7:ac:73:d2:22:a0:04 24:d7:ac:73:d2:22:00:02
           [CHASSIS1-BLADE3-vHBA0-A]
port-channel31 100 0x750066 24:d7:ac:73:d2:22:a0:05 24:d7:ac:73:d2:22:00:02
           [CHASSIS1-BLADE3-vHBA1-A]

Total number of flogi = 24.

MDS A#

```

Figura 31 Estado final de los nodos registrados en el switch MDS A. Fuente.
Captura de pantalla del switch MDS A tras la implementación.

```

fc1/4      200  0x290085  52:c7:38:20:10:1c:3e:74 52:c7:38:20:10:00:3e:74
           [Storage1-P7-N3]
fc1/5      200  0x290000  24:3f:58:d3:9c:20:43:10 24:3f:58:d3:9c:20:43:10
           [Storage2-P2-N1]
fc1/7      200  0x290020  52:c7:38:20:0d:0a:9a:90 52:c7:38:20:0d:02:9a:90
           [Storage3-P2-N1]
fc1/7      200  0x290021  52:c7:38:20:0d:7a:9a:90 52:c7:38:20:0d:02:9a:90
           [Storage3-P2-N2]
fc1/8      200  0x290040  52:c7:38:20:0d:0a:9a:91 52:c7:38:20:0d:02:9a:91
           [Storage3-P4-N1]
fc1/8      200  0x290041  52:c7:38:20:0d:7a:9a:91 52:c7:38:20:0d:02:9a:91
           [Storage3-P4-N2]
fc1/9      200  0x2900c0  52:c7:38:20:10:14:3e:88 52:c7:38:20:10:00:3e:88
           [Storage1-P8-N1]
fc1/9      200  0x2900c1  52:c7:38:20:10:18:3e:88 52:c7:38:20:10:00:3e:88
           [Storage1-P8-N2]
fc1/9      200  0x2900c2  52:c7:38:20:10:1c:3e:88 52:c7:38:20:10:00:3e:88
           [Storage1-P8-N3]
port-channel32 200 0x290100 28:e5:29:b2:91:89:3b:a0 22:58:29:b2:91:89:3b:a1
port-channel32 200 0x290101 24:d7:ac:73:d2:22:b0:00 24:d7:ac:73:d2:22:00:00
           [CHASSIS1-BLADE1-vHBA2-B]
port-channel32 200 0x290102 24:d7:ac:73:d2:22:b0:01 24:d7:ac:73:d2:22:00:00
           [CHASSIS1-BLADE1-vHBA3-B]
port-channel32 200 0x290103 24:d7:ac:73:d2:22:b0:02 24:d7:ac:73:d2:22:00:01
           [CHASSIS1-BLADE2-vHBA2-B]
port-channel32 200 0x290104 24:d7:ac:73:d2:22:b0:03 24:d7:ac:73:d2:22:00:01
           [CHASSIS1-BLADE2-vHBA3-B]
port-channel32 200 0x290105 24:d7:ac:73:d2:22:b0:04 24:d7:ac:73:d2:22:00:02
           [CHASSIS1-BLADE3-vHBA2-B]
port-channel32 200 0x290106 24:d7:ac:73:d2:22:b0:05 24:d7:ac:73:d2:22:00:02
           [CHASSIS1-BLADE3-vHBA3-B]

Total number of flogi = 24.

MDS B#

```

Figura 32 Estado final de los nodos registrados en el switch MDS B. Fuente.
Captura de pantalla del switch MDS B tras la implementación.

Por otro lado, los sistemas de almacenamiento pueden verificar la redundancia de conectividad a cada host, como se muestra en la Figura 33.

Host	# WWN	# IQN	# NQN	Paths	CT0	CT1
ESXi001	2	0	0	Redundant	1	1
ESXi002	2	0	0	Redundant	1	1
ESXi003	2	0	0	Redundant	1	1
ESXi004	2	0	0	Redundant	1	1
ESXi005	2	0	0	Redundant	1	1
[Redacted]	4	0	0	Redundant	2	2
[Redacted]	4	0	0	Redundant	2	2
[Redacted]	4	0	0	Redundant	2	2

Figura 33 Estado de redundancia SAN de hosts ESXi nuevos. Fuente. Captura de pantalla de la interfaz web del almacenamiento FlashArray donde se valida el estado redundante de los HBA de los nuevos servidores.

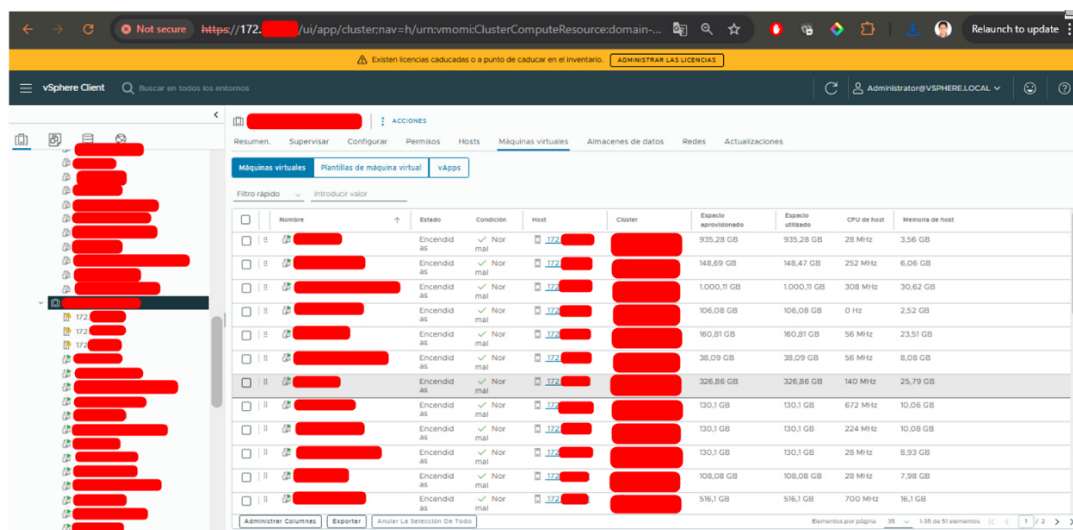
El gestor vCenter permite visualizar los múltiples caminos de forma redundante hacia una misma LUN, como se muestra en la Figura 34.

Nombre	LUN	Tip	Capacidad	Almacenamiento de datos	Estado operativo	Acceleración de hardware	Tip de unidad	Transporte
IBM Fibre Channel Disk (sas)	4	disco	7,70 TB	P17300	Asociado	Compatible	HDD	Canal c
IBM Fibre Channel Disk (sas)	1	disco	4,00 TB	P17300	Asociado	Compatible	HDD	Canal c
Local NVMe Disk (RD-NVMe_Moron_7450)	0	disco	372,61 GB	asociado	Asociado	Compatible	Flash	PCIe
IBM Fibre Channel Disk (sas)	0	disco	2,00 TB	P17300	Asociado	Compatible	HDD	Canal c
IBM Fibre Channel Disk (sas)	1	disco	10,50 TB	P17300	Asociado	Compatible	HDD	Canal c
PURE Fibre Channel Disk (sas)	252	disco	15,00 TB	P17300	Asociado	Compatible	Flash	Canal c
IBM Fibre Channel Disk (sas)	3	disco	10,00 TB	P17300	Asociado	Compatible	HDD	Canal c

Figura 34 Verificación de multipath en host ESXi nuevo. Fuente. Captura de pantalla de vCenter donde se identifica la lista de rutas de acceso redundantes a una LUN del almacenamiento FlashSystem 7300 desde uno de los hosts nuevos.

Finalmente, se verifica que no reste ninguna máquina virtual productiva en el *cluster* antiguo, y todas las máquinas virtuales se encuentren funcionando

correctamente en el cluster nuevo, como se muestra en la Figura 35.



Nombre	Estado	Condición	Host	Cluster	Espacio provisionado	Espacio utilizado	CPU de host	Memoria de host
[Redacted]	Encendido	✓ Nor mal	[Redacted]	[Redacted]	935,28 GB	935,28 GB	28 MHz	3,56 GB
[Redacted]	Encendido	✓ Nor mal	[Redacted]	[Redacted]	143,69 GB	143,47 GB	252 MHz	6,06 GB
[Redacted]	Encendido	✓ Nor mal	[Redacted]	[Redacted]	1,000,11 GB	1,000,11 GB	308 MHz	30,62 GB
[Redacted]	Encendido	✓ Nor mal	[Redacted]	[Redacted]	106,08 GB	106,08 GB	0 Hz	2,52 GB
[Redacted]	Encendido	✓ Nor mal	[Redacted]	[Redacted]	160,81 GB	160,81 GB	56 MHz	23,51 GB
[Redacted]	Encendido	✓ Nor mal	[Redacted]	[Redacted]	38,09 GB	38,09 GB	56 MHz	8,08 GB
[Redacted]	Encendido	✓ Nor mal	[Redacted]	[Redacted]	326,86 GB	326,86 GB	140 MHz	25,79 GB
[Redacted]	Encendido	✓ Nor mal	[Redacted]	[Redacted]	130,1 GB	130,1 GB	672 MHz	10,06 GB
[Redacted]	Encendido	✓ Nor mal	[Redacted]	[Redacted]	130,1 GB	130,1 GB	224 MHz	10,08 GB
[Redacted]	Encendido	✓ Nor mal	[Redacted]	[Redacted]	130,1 GB	130,1 GB	28 MHz	8,93 GB
[Redacted]	Encendido	✓ Nor mal	[Redacted]	[Redacted]	108,08 GB	108,08 GB	28 MHz	7,98 GB
[Redacted]	Encendido	✓ Nor mal	[Redacted]	[Redacted]	516,1 GB	516,1 GB	700 MHz	16,1 GB

Figura 35 Verificación de máquinas virtuales migradas a nuevo cluster. Fuente. Captura de pantalla de vCenter donde se identifican VMs operando en el nuevo cluster, sin VMs prendidas en el antiguo cluster.

En este punto, los servicios y el tráfico de red están fluyendo a través del nuevo equipamiento adquirido en el proyecto. La solución ha sido implementada siguiendo cada pauta definida en el diseño de bajo nivel, el cual sirvió como el plano para configurar cada componente de los cinco frentes de tecnologías: red LAN, red SAN, cómputo, almacenamiento y virtualización.

Las validaciones realizadas a nivel lógico en los equipos de red y almacenamiento confirman el alto nivel de resiliencia alcanzado en esta arquitectura, lo cual asegura que la clínica goce de una continuidad operativa sin precedentes, gracias a la redundancia habilitada en sus redes LAN y SAN.

La puesta en producción fue planificada de forma estratégica, para causar el menor impacto posible en las cargas de trabajo y la menor cantidad de ventanas de mantenimiento, ya que, al tratarse de un entorno hospitalario, la operación no se detiene nunca.

Finalmente, se verifican las funciones avanzadas de monitoreo y administración de la solución Cisco UCS desde el servicio Intersight en nube, lo cual facilitará la operación.

CAPITULO IV: DISCUSIÓN DE RESULTADOS

4.1 Descripción de la implementación

El desarrollo y los resultados del proyecto confirman que el diseño a bajo nivel propuesto fue el adecuado. A continuación, se discuten los resultados obtenidos en base a los problemas específicos planteados:

4.1.1 Desarrollo de LLD para integración con equipos existentes

Acerca de la integración de la nueva solución Cisco con los sistemas de almacenamiento actuales de la clínica, el levantamiento de información y el documento LLD fueron claves. La configuración del modo End Host en los Fabric Interconnects, junto con los Port Mappings y la correcta asignación de WWPNs y FCIDs, permitió que los equipos nuevos se comuniquen correctamente con los equipos legados sin generar problemas lógicos en la red. Esto demuestra que aplicar un buen diseño ayuda a aprovechar las capacidades de los equipos nuevos dentro de una red en producción.

4.1.2 Redundancia de las redes LAN y SAN

Sobre las configuraciones de redundancia, aunque no se realizaron pruebas apagando equipos por restricciones del cliente, la verificación de los estados en las consolas confirmó que la implementación de vPC y HSRP en la red LAN logró una topología activo-activo real. De igual forma, la zonificación y el protocolo FSPF en la SAN permitieron el uso de Multipathing en VMware. Esto confirma que la infraestructura no tiene puntos únicos de falla y asegura la continuidad operativa de las aplicaciones de la clínica si ocurre la caída de algún enlace.

4.1.3 Migración y ventanas de mantenimiento

Respecto a las estrategias de migración, fue un acierto separar los trabajos en una migración "en frío" para la red LAN y una "en caliente" para la red SAN. El mayor reto en campo fue la incompatibilidad del firmware del chasis UCS antiguo con los nuevos switches MDS. Para solucionar esto y no afectar las operaciones médicas, se implementó una topología de convivencia temporal conectando los MDS antiguos y nuevos mediante enlaces ISL. Esta decisión técnica permitió migrar la red de almacenamiento de forma segura.

4.1.4 Optimización mediante Intersight

Finalmente, sobre la gestión de la plataforma, el uso de Cisco Intersight (Intersight Managed Mode) mejoró bastante la administración en comparación con las herramientas locales antiguas. Al tener la gestión en la nube, se facilitó la configuración usando perfiles y políticas unificadas (Profiles y Policies), lo que permite al personal de TI tener un monitoreo centralizado de la salud de todo el hardware para resolver problemas más rápido.

4.2 Evaluación Económica

La viabilidad de la propuesta se fundamenta en eliminar las pérdidas operativas por inactividad debido a la inminente falla de los equipos de red y servidores físicos antiguos que carecían de soporte por obsolescencia. De acuerdo con los datos de la Encuesta Económica Anual (INEI, 2026), la clínica se clasifica como una Gran Empresa, contando con una planilla de 1,650 trabajadores. Partiendo de esta dimensión corporativa, para la evaluación económica del proyecto se estableció una tasa de oportunidad del 12% y un horizonte de cinco años. Se proyectó una facturación anual para la institución de S/ 314.90 millones sin IGV, equivalente a un ingreso institucional promedio de S/ 35,948.30 por hora.

Para calcular el impacto real de la clínica, se aplicó un factor de reducción del 70.93% sobre el ingreso por hora de la clínica, basado en el volumen de

Consultas Externas reportado por la Superintendencia Nacional de Salud (SUSALUD, 2025). El criterio considera que este servicio se paraliza por completo al requerir validación de seguros en tiempo real, excluyendo las emergencias que sí tienen la posibilidad de funcionar fuera de línea. De este modo, el ingreso que se deja de percibir se fijó en S/ 25,498.13 por hora de caída, sin incluir IGV. Bajo la infraestructura legada, el riesgo operativo se fijó en 16 horas de indisponibilidad total al año. Este escenario genera una pérdida de S/ 407,970.08 anuales, aproximadamente 108,792 USD al tipo de cambio referencial de 3.75 en la época de la implementación. Esto coincide con la estadística de pérdidas monetarias por interrupciones de red severas en el 54% de empresas estudiadas, al estar dentro del umbral de los 100,000 USD de pérdidas mínimas (Uptime Institute, 2024).

La inversión inicial (CAPEX) totaliza S/ 569,234.74 sin IGV, compuestos de la siguiente manera: S/ 317,105.25 por el costo del Chasis, Nodos UCS y componentes internos; S/ 71,856.68 por los Fabric Interconnect; S/ 59,376.83 en los Switches LAN; S/ 43,383.23 por los Switches SAN; S/ 45,102.11 por los transceptores y cables adquiridos de Cisco; y S/ 32,410.65 en servicios profesionales de implementación, instalación y migración. Por su parte, los gastos operativos anuales (OPEX) ascienden a S/ 234,672.41 al año, compuestos por: S/ 22,461.64 de licenciamiento de gestión Intersight por cinco años; S/ 190,808.66 en soporte de fabricante (Cisco) por cinco años; S/ 4,981.88 en soporte del NOC de Noovus por cinco años; S/ 31,320.00 al año por planilla del personal de TI calificado (Michael Page, 2026); S/ 53,275.75 al año por consumo eléctrico de equipamiento TI y S/ 106,426.22 al año por costos energéticos en aire acondicionado de precisión. Estos dos últimos costos por energía se calcularon basándose en las tarifas de Media Tensión MT3 (Pluz Energía, 2026). Para modelar el costo eléctrico, se tomó la capacidad máxima de entrada de potencia de los equipos Cisco de 14.16 kW, sobre la cual se aplicó un PUE de 3.0, el límite conservador de eficiencia energética obtenida por estadísticas (The Green Grid, 2012). Bajo este parámetro, por cada kilovatio de demanda TI, la clínica asume el costo de dos kilovatios adicionales en refrigeración para mantener la temperatura idónea en los equipos Cisco nuevos.

Mitigar las 16 horas anuales de riesgo genera un ahorro por costos evitados de S/ 407,970.08 al año. Restando el OPEX anual de S/ 234,672.41, el proyecto rinde un flujo de caja neto de S/ 173,297.67 por año. Frente al CAPEX requerido, la evaluación arroja un Valor Actual Neto (VAN) de S/. 55,463.79 y una Tasa Interna de Retorno (TIR) de 15.87%, con una relación Beneficio/Costo de 1.04. Estos indicadores demuestran sólidamente que, incluso bajo el escenario de máxima demanda eléctrica y el ecosistema térmico más ineficiente de la industria, el proyecto absorbe los gastos operativos, supera el costo de capital exigido y consolida una rentabilidad segura para la institución, lo cual se plasma en las Tablas 43 y 44.

Tabla 43 Flujo de Caja proyectado en soles

Concepto	Año 0	Año 1	Año 2	Año 3	Año 4	Año 5
Ingresos						
Ahorro por Pérdidas Evitadas		407,970.08	407,970.08	407,970.08	407,970.08	407,970.08
Egresos						
CAPEX	-569,234.74					
OPEX		-234,672.41	-234,672.41	-234,672.41	-234,672.41	-234,672.41
Flujo de Caja Neto	-569,234.74	173,297.67	173,297.67	173,297.67	173,297.67	173,297.67

Fuente. Elaboración propia.

Tabla 44 Resultados de la evaluación económica

Indicador	Valor	Resultado
Tasa de Oportunidad	12%	Tasa de oportunidad exigida al proyecto.
Valor Actual Neto (VAN)	S/ 55,463.79	Viable. El proyecto genera valor positivo tras recuperar el CAPEX y cubrir la tasa de oportunidad.
Tasa Interna de Retorno (TIR)	15.87%	Viable. La rentabilidad del proyecto supera la tasa de oportunidad exigida (15.87% > 12.00%).
Relación Beneficio/Costo (B/C)	1.04	Viable. Por cada sol invertido (en valor actual), el proyecto retorna S/. 1.04.

Fuente. Elaboración propia.

CAPITULO V: CONCLUSIONES

1. Se concluye que el desarrollo del Diseño a Bajo Nivel (LLD), basado en las guías arquitectónicas del fabricante y los criterios técnicos de ingeniería, permitió una integración eficiente entre el nuevo hardware Cisco UCS Serie X y los sistemas de almacenamiento heredados, maximizando el rendimiento de la infraestructura y resolviendo los retos de compatibilidad en el entorno clínico.
2. La implementación de protocolos de redundancia como vPC y HSRP en la red LAN, junto con el enrutamiento FSPF y el mecanismo Multipath en la red SAN, garantizó la continuidad operativa de la plataforma. El diseño sin puntos únicos de falla asegura que las aplicaciones médicas mantengan sus servicios activos ante diversos escenarios de falla lógica o física.
3. Las estrategias de migración ejecutadas, combinando traslados de red "en frío" para la capa LAN y "en caliente" para la capa SAN, junto con el despliegue de una topología temporal de convivencia ISL, permitieron transferir las cargas de trabajo hacia el nuevo clúster VMware minimizando el impacto en las operaciones críticas del hospital.
4. La adopción de la plataforma Cisco Intersight (SaaS) optimizó significativamente la administración de la infraestructura local, centralizando el monitoreo, la gestión de alertas y el control del hardware en una única interfaz en la nube, lo que agiliza la capacidad de respuesta del equipo de soporte frente a incidentes.

CAPITULO VI: RECOMENDACIONES

1. Se recomienda a la gerencia de TI de la clínica mantener el documento LLD actualizado como un documento vivo (As-Built), registrando cualquier adición futura de servidores o arreglos de almacenamiento, para asegurar que las próximas expansiones mantengan la interoperabilidad y el orden técnico establecido en este proyecto.
2. Dado que la criticidad del entorno hospitalario no permitió realizar pruebas destructivas durante la implementación, se sugiere programar simulacros de failover (desconexión controlada de enlaces vPC o rutas SAN) durante futuras ventanas de mantenimiento de bajo impacto, con el fin de validar empíricamente los tiempos de convergencia de la red redundante.
3. Se aconseja planificar el retiro definitivo (Decommissioning) del chasis heredado UCS Serie B y los switches MDS antiguos una vez que se confirme que no albergan cargas de trabajo residuales. Esto permitirá eliminar la topología ISL de convivencia, simplificando la administración del fabric SAN y liberando espacio físico y recursos eléctricos en el centro de datos.
4. Se sugiere explorar las funcionalidades avanzadas de la plataforma Cisco Intersight, tales como la integración con el centro de asistencia técnica (Proactive TAC) para la apertura automatizada de casos ante fallas de hardware, con el objetivo de elevar aún más la eficiencia de la gestión operativa del equipo de soporte.

CAPITULO VII: REFERENCIAS BIBLIOGRÁFICAS

Ayuso Fernández, J. (2019). *Sistema de virtualización basado en servidores físicos CISCO UCS y software de virtualización de VMware* [Trabajo fin de grado]. <https://oa.upm.es/54261/>

Bruno, A., y Jordan, S. (2024). *Designing Cisco Enterprise Networks (ENSLD) 300-420 Official Cert Guide (2a ed.)*. Cisco Press.

Broadcom. (2026). *VMware vSphere 8.0*. Recuperado de <https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere/8-0.html>

Cisco Systems. (2021). *Cisco UCS 6400 Series Fabric Interconnects Data Sheet*. Recuperado de <https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/datasheet-c78-741116.html>

Cisco Systems. (2023). *Cisco MDS 9132T 32-Gbps 32-Port Fibre Channel Switch Data Sheet*. Recuperado de <https://www.cisco.com/c/en/us/products/collateral/storage-networking/mds-9100-series-multilayer-fabric-switches/datasheet-c78-739613.html>

Cisco Systems. (2025a). *Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 10.6(x): Configuring vPCs*. Recuperado de https://www.cisco.com/c/en/us/td/docs/dcn/mds9000/sw/9x/configuration/interfaces/cisco-mds-9000-nx-os-interfaces-configuration-guide-9x/configuring_npv.html

Cisco Systems. (2025b). *Cisco Nexus 9300-FX3 Series Switches Data Sheet*. Recuperado de <https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-744052.html>

- Cisco Systems. (2025c). *Cisco UCS X210c M7 Compute Node Spec Sheet*. Recuperado de <https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-x-series-modular-system/x210cm7-specsheet.pdf>
- Cisco Systems. (2025d). *Meet the UN/BOX: Cisco UCS X-Series Modular System Solution Overview*. Recuperado de <https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-x-series-modular-system/solution-overview-c22-2432175.html>
- Cisco Systems. (2026a). *Cisco MDS 9000 Series Fabric Configuration Guide, Release 9.x*. Recuperado de <https://www.cisco.com/c/en/us/td/docs/dcn/mds9000/sw/9x/configuration/fabric/cisco-mds-9000-nx-os-fabric-configuration-guide-9x.pdf>
- Cisco Systems. (2026b). *Cisco MDS 9000 Series Interfaces Configuration Guide, Release 9.x: Configuring N Port Virtualization*. Recuperado de https://www.cisco.com/c/en/us/td/docs/dcn/mds9000/sw/9x/configuration/interfaces/cisco-mds-9000-nx-os-interfaces-configuration-guide-9x/configuring_npv.html
- Cisco Systems. (2026c). *Cisco UCS Manager Network Management Guide, Release 4.2: LAN Connectivity*. Recuperado de https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Network-Mgmt/4-2/b_UCSM_Network_Mgmt_Guide_4_2/b_UCSM_Network_Mgmt_Guide_chapter_011.html
- Castro, R., y López, M. (2023). *Evolución de las Tecnologías de Virtualización en Centros de Datos de Misión Crítica*. *Revista de Ingeniería y Telecomunicaciones*, 12(1), 45-58.
- Edgeworth, B., y Lacoste, R. (2023). *CCNP Enterprise Advanced Routing ENARSI 300-410 Official Cert Guide (2a ed.)*. Cisco Press.
- Guevara, J.; López, M. (2020). *Implementación de un sistema para la administración de las funciones básicas de los equipos del data center académico de la Universidad de las Américas mediante*

Cisco DevNet y Amazon Alexa [Tesis de pregrado].
 Universidad de las Américas, Quito.
<http://dspace.udla.edu.ec/handle/33000/12173>

Hwang, K., Fox, G. C., y Dongarra, J. J. (2021). *Distributed and Cloud Computing: From Parallel Processing to the Internet of Things*. Morgan Kaufmann.

INEI. (2026). *Perú: Características económicas y financieras de las empresas, 2023*. Gobierno del Perú.
<https://cdn.www.gob.pe/uploads/document/file/9901575/8081081-peru-caracteristicas-economicas-y-financieras-de-las-empresas-2023.pdf?v=1777904447>

Jiménez, P., y Torres, F. (2021). *Análisis Comparativo de Topologías de Red en Entornos Hospitalarios Modernos*. *International Journal of Network Engineering*, 8(4), 210-225.

Kurose, J. F., y Ross, K. W. (2022). *Computer Networking: A Top-Down Approach* (8th ed.). Pearson.

Maloo, S., Nikolov, I., y Ahmed, F. (2023). *CCNP and CCIE Data Center Core DCCOR 350-601 Official Cert Guide* (2a ed.). Cisco Press.

Michael Page. (2026). *Guía Salarial 2026: Tecnología*. Recuperado de <https://www.michaelpage.pe/estudios-y-tendencias/guia-salarial-2026-SG25>

Odom, W. (2024). *CCNA 200-301 Official Cert Guide, Volume 1* (2a ed.). Cisco Press.

Pluz Energía. (2026). *Pliego tarifario N° 6-2026: Tarifas para suministros en media tensión (Tarifa MT3)*. Recuperado de https://www.pluz.pe/content/dam/distribuidora-per%C3%BA-rebranding/documentos-pluz/tarifas/2026-05/260504_1%20Pliego%20PLUZ%20Consumo%20energ%C3%ADa%20y%20potencia_con%20IGV_ENV_v0.pdf

Pribadi, A., et al. (2022). *Analysis of Quality in Project Quality Management Based on PMBOK®*. *Journal of Software Engineering, Information and Communication Technology*

(SEICT), 3(2), 85-92.

<https://ejournal.upi.edu/index.php/SEICT/article/view/52460>

Project Management Institute. (2017). *A Guide to the Project Management Body of Knowledge (PMBOK Guide)* (6th ed.). Project Management Institute.

Purwanto, A., y Soewito, B. (2021). *Optimization Problem of Computer Network Using PPDIOO*. *ICIC Express Letters*, 15(7), 769-775.

SUSALUD. (2025). *Boletín estadístico: Tercer trimestre 2025*.

Swari, G. I., y Agussalim. (2023). *Analysis of Network Design and Management Using PPDIOO At SMA Labschool Unesa 1*. *West Science Information System and Technology*, 1(2), 99-108.

Tanenbaum, A. S., y Wetherall, D. J. (2021). *Computer Networks* (6th ed.). Pearson.

Tello Coello, G. (2014). *Implementación de la solución unified computing system (UCS) para la empresa cliente Puntonet a través de la empresa proveedora andean trade* [Proyecto de titulación previo a la obtención del Título de Ingeniería]. <http://repositorio.espe.edu.ec/handle/21000/9705>

Tello Illescas, T. (2024). *Diseño de la propuesta de actualización de la arquitectura de procesamiento y almacenamiento ubicado en el Data Center de la Carrera de Computación de la Universidad Politécnica Salesiana, sede Quito* [Trabajo de titulación previo a la obtención del Título de Ingeniero en Ciencias de la Computación]. <https://dspace.ups.edu.ec/bitstream/123456789/28171/1/TTS1873.pdf>

The Green Grid. (2012). PUE™: A comprehensive examination of the metric (White Paper #49). The Green Grid Association. https://datacenters.lbl.gov/sites/default/files/WP49-PUE%20A%20Comprehensive%20Examination%20of%20the%20Metric_v6.pdf

Uptime Institute. (2024). *Executive Summary: Annual outage analysis 2024*.

CAPITULO VIII: ANEXOS

Anexo A: Cronograma del proyecto

En la Figura A1 se lista la totalidad de actividades desde la emisión de la Orden de Compra por parte del cliente. Se han ocultado las fechas reales para salvaguardar la confidencialidad, pero se han mantenido las duraciones reales de las actividades.

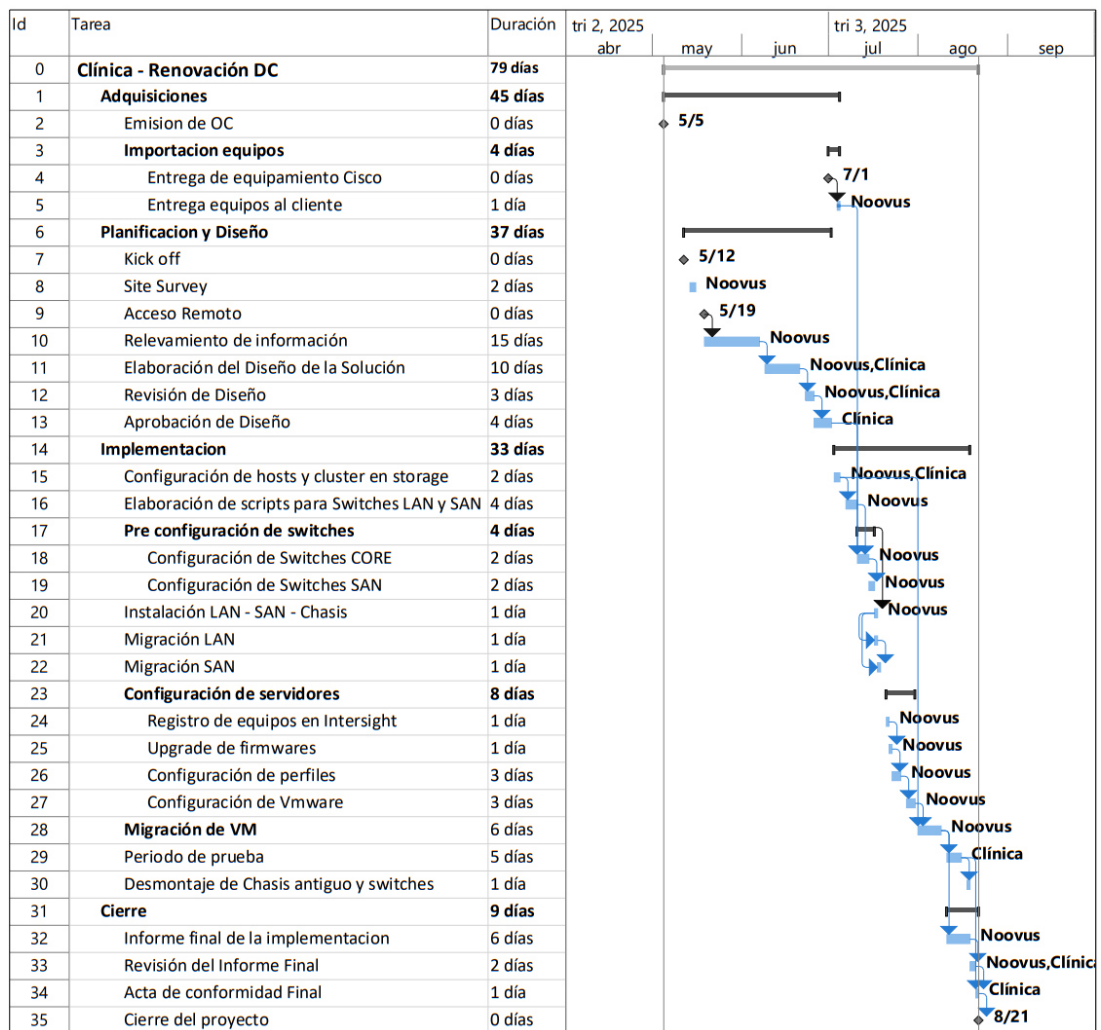


Figura A1 Cronograma del proyecto. Fuente. Elaboración propia.