



REPÚBLICA DE PANAMÁ
UNIVERSIDAD INTERNACIONAL DE CIENCIA Y TECNOLOGÍA
FACULTAD DE CIENCIAS DE LA COMPUTACIÓN Y TECNOLOGÍA

**FORTALECIMIENTO DE LA CONTINUIDAD OPERATIVA Y
MODERNIZACIÓN DE LOS SERVICIOS DE CONECTIVIDAD
INSTITUCIONAL**

INFORME FINAL DE PASANTÍA PARA OPTAR AL GRADO DE LICENCIADO
Licenciatura en Ingeniería en Redes y Comunicación con Énfasis en Seguridad
Opción de Titulación: Pasantía de Extensión Ocupacional Profesional

Autor(a): Julio Cesar López Fernández

Cédula / Pasaporte: 8-829-2426

Cohorte: 042022

Tutor(a) Académico(a): Omar Christopher Demercado Lewis

Tutor(a) Industrial / Empresarial: Mayor Jusseff Flores

Organización Colaboradora: Servicio Nacional De Fronteras

Ciudad de Panamá, julio de 2026



REPÚBLICA DE PANAMÁ
UNIVERSIDAD INTERNACIONAL DE CIENCIA Y TECNOLOGÍA
FACULTAD DE CIENCIAS DE LA COMPUTACIÓN Y TECNOLOGÍA

**FORTALECIMIENTO DE LA CONTINUIDAD OPERATIVA Y
MODERNIZACIÓN DE LOS SERVICIOS DE CONECTIVIDAD
INSTITUCIONAL**

INFORME FINAL DE PASANTÍA PARA OPTAR AL GRADO DE LICENCIADO
Licenciatura en Ingeniería en Redes y Comunicación con Énfasis en Seguridad
Opción de Titulación: Pasantía de Extensión Ocupacional Profesional

Autor(a): Julio Cesar López Fernández

Ciudad de Panamá, julio de 2026



CARTA DE APROBACIÓN DEL TUTOR ACADÉMICO

Ciudad de Panamá, 29 de julio de 2026

Profesor

Héctor Mazurkiewicz, Ed.D.

Coordinador del Comité de Titulación de Estudios de Grado y Postgrado

Universidad Internacional de Ciencia y Tecnología Presente.

Por medio de la presente, en mi carácter de Tutor(a) Académico(a) de la Pasantía de Extensión Ocupacional Profesional titulada "Fortalecimiento de la Continuidad Operativa y Modernización de los Servicios de Conectividad Institucional", realizada por el(la) estudiante Julio Cesar López Fernández, con cédula o pasaporte número 8-829-2426, aspirante al grado de Licenciado en Ingeniería en Redes y Comunicación con Énfasis en Seguridad, en la organización Servicio Nacional de Fronteras (SENAFRONT), hago constar que el Informe Final reúne los requisitos académicos y méritos suficientes para ser sometido a presentación pública y evaluación por parte del jurado examinador que oportunamente designe el Comité de Titulación.

Atentamente,

Omar Christopher Demercado Lewis

Documento de identidad N°: 1-713-1945

Tutor(a) Académico(a)



INFORME DE ACTIVIDADES DE TUTORÍA **OPCIÓN DE TITULACIÓN: PASANTÍA DE EXTENSIÓN OCUPACIONAL** **PROFESIONAL**

Carrera: Licenciatura en Ingeniería en Redes y Comunicación con Énfasis en Seguridad

Estudiante: Julio Cesar López Fernández

Cohorte: 042022

Tutor(a) Académico(a): Omar Christopher Demercado Lewis

Tutor(a) Industrial / Empresarial: Mayor Jusseff Flores

Organización Colaboradora: Servicio Nacional de Fronteras

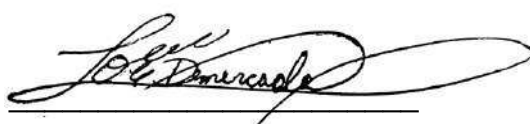
Título de la pasantía: "fortalecimiento de la continuidad operativa y modernización de los servicios de conectividad institucional"

N°	Fecha	Hora	Lugar / medio	Objetivo principal	Observaciones / acuerdos
1	15/04/2026	10:30-11:30	Virtual (Teams)	Postulación y Alcance: Formalización de la tutoría académica y confirmación de la carta de postulación	Solicitud aceptada. Autorización para iniciar borradores.
2	21/04/2026	11:15-12:15	Virtual (Teams)	Planificación y Logística: Revisión del cronograma de actividades de la pasantía y reestructuración de la red.	Visto bueno del tutor. Se solicita envío de formatos oficiales.
3	24/04/2026		Virtual (Teams)	Estrategia de Seguridad	Avance correcto.

		09:50-10:50		Lógica: Análisis de redacción y blindaje de términos técnicos para la confidencialidad	Solicitud de revisión de versión corregida
4	26/04/2026	16:55-18:00	Presencial	Modelado y Levantamiento: Diseño de resiliencia y documentación técnica del Data Center (diagramas).	Enfoque aprobado. Se resalta la relevancia de la auditoría inicial
N°	Fecha	Hora	Lugar / medio	Objetivo principal	Observaciones / acuerdos
5	18/05/2026	09:15-10:15	Virtual (Teams)	Integración de Servicios: Revisión de métricas de rendimiento y estado técnico de entornos virtuales.	Parámetros evaluados positivamente. Autorización de procesamiento.
6	29/05/2026	13:30-14:30	Virtual (Teams)	Optimización Gráfica: Instrucción para la integración de diagramas de red adicionales.	Se solicita robustecer el respaldo visual de la topología.
7	06/07/2026	15:00-16:30	Presencial	Validación y Cierre de Informe: Auditoría final del informe de pasantía y preparación para sustentación pública.	Proyecto concluido con éxito. Visto bueno para la defensa.

Comentarios finales acerca de la pasantía: el(la) suscrito(a) declara que las especificaciones anteriores representan fielmente el proceso de acompañamiento académico de la pasantía arriba mencionada.


Firma del estudiante


Firma del Tutor(a) Académico(a)

DEDICATORIA

A mi madre, por constituirse como el pilar fundamental de mi existencia, por el inagotable poder de sus oraciones y por haberme inculcado que, mediante el esfuerzo sostenido, ninguna cumbre es inalcanzable. A mis hijos, quienes representan mi impulso vital y el motivo genuino por el cual persigo la excelencia cotidiana; este triunfo académico les pertenece, como prueba fehaciente de que la preparación y la tenacidad derriban cualquier barrera. Los amo profundamente.

AGRADECIMIENTOS

A Dios, por brindarme la salud, la fortaleza y la perseverancia necesarias para alcanzar esta meta profesional.

A mi institución, el Servicio Nacional de Fronteras (SENAFRONT), y de manera especial a mi equipo en la Dirección de Telemática. Gracias por el inmenso respaldo operativo durante las exigentes ventanas de mantenimiento de madrugada; sin ese esfuerzo conjunto, la modernización de nuestra infraestructura no habría sido posible.

A mi Tutor Industrial, el Mayor Jusseff Flores, por su liderazgo y la confianza depositada en mi criterio técnico para la ejecución de este proyecto. A mi Tutor Académico, el Profesor Omar Christopher Demercado Lewis, por su paciencia y excelente guía metodológica. Extiendo este agradecimiento a los docentes de UNICyT por forjar mis bases como ingeniero.

Finalmente, a mi pilar más importante: mi familia. A mi madre, por el poder de sus oraciones y su apoyo incondicional. A mis dos hijos, por comprender mis ausencias durante las noches y los fines de semana de estudio y trabajo; ustedes son el motor de mi excelencia. Este triunfo es nuestro.

ÍNDICE GENERAL

CARTA DE APROBACIÓN DEL TUTOR ACADÉMICO	iii
INFORME DE ACTIVIDADES DE TUTORÍA	iv
DEDICATORIA	vi
AGRADECIMIENTOS	vii
ÍNDICE GENERAL	viii
ÍNDICE DE TABLAS	ix
ÍNDICE DE FIGURAS	ix
RESUMEN	xi
ABSTRACT	xii
INTRODUCCIÓN	1
Capítulo I. Marco de referencia de la institución	3
1.1. Definición de la carrera que estudia	3
1.2. Antecedentes de la empresa o institución	3
1.3. Misión de la empresa o institución	3
1.4. Visión de la empresa o institución	4
1.5. Estructura organizativa de la empresa o institución	4
1.6. Descripción de la actividad de la institución	5
1.7. Departamento donde realizó la pasantía	5
Capítulo II. Análisis de la experiencia	8
2.1. Funciones realizadas	8
2.2. Análisis de desempeño	8
2.3. Limitaciones o dificultades presentadas	8
2.4. Aportes y conocimientos de la experiencia a la formación profesional	9
2.5. Relación de la pasantía profesional con la carrera estudiada	10
2.6. Cronograma de actividades	10
Capítulo III. Diagnóstico observacional	13
3.1. Descripción de la problemática observada	13
3.2. Alternativas de solución a la problemática planteada	14
3.3. Propuesta recomendada	15
Conclusiones	21
Recomendaciones	23

<i>Recomendaciones para futuros pasantes</i>	24
<i>Referencias bibliográficas</i>	26
<i>Anexos</i>	28
<i>Anexo A. Carta de aceptación o convenio con la organización colaboradora</i>	28
<i>Anexo B. Plan de Actividades aprobado en Fase I</i>	29
<i>Anexo C. Evaluación del Tutor Industrial</i>	32
<i>Anexo D. Constancia de horas cumplidas</i>	35
<i>Anexo E. Bitácora de actividades semanales</i>	37
<i>Anexo F. Fotografías de las actividades realizadas</i>	41
<i>Anexo G. Otros documentos de soporte</i>	58

ÍNDICE DE TABLAS

Tabla 1 Cronograma de actividades ejecutadas durante la pasantía.....	10
Tabla 2 Matriz de Organización Lógica de Servicios.....	17
Tabla 3 Plan de implementación de la propuesta recomendada.....	19

ÍNDICE DE FIGURAS

Figura 1 Organigrama general del Servicio Nacional de Fronteras	4
Figura 2 Arquitectura de Comunicaciones y Conectividad Inalámbrica (Estado Inicial)	14
Figura 3 Arquitectura de Comunicaciones y Conectividad Inalámbrica (Estado Propuesto - Post-Solución)	16
Figura 4 Matriz de Gestión Granular de Políticas de Seguridad Perimetral	18
Figura 5 Arquitectura de Red y Alta Disponibilidad Institucional	42
Figura 6 Pataforma de Gestión de Servicios Virtualizados (Consola de arranque).....	43
Figura 7 Plataforma de Gestión de Servicios Virtualizados (Monitoreo de recursos)...	44
Figura 8 Supervisión de Recursos y Estado del Nodo de Cómputo	45
Figura 9 Secuencia de Inicialización de la Gestión de Movilidad (Menú de opciones)..	46
Figura 10 Secuencia de Inicialización de la Gestión de Movilidad (Carga de servicios)	47
Figura 11 Intervención y Optimización de la Infraestructura Física (Pantalla de inicio de sesión)	48

Figura 12 Intervención y Optimización de la Infraestructura Física (Dashboard general)	49
Figura 13 Intervención y Optimización de la Infraestructura Física (Resumen de red) .	50
Figura 14 Validación de Resiliencia y Continuidad del Servicio en el Clúster de Movilidad	51
Figura 15 Validación de Resiliencia y Continuidad del Servicio en el Clúster de Movilidad Primario.....	52
Figura 16 Validación de Resiliencia y Continuidad del Servicio en el Clúster de Movilidad Secundario.....	53
Figura 17 Intervención y Optimización de la Infraestructura Física de Red.....	54
Figura 18 Optimización de Vías de Distribución en el Centro de Datos	55
Figura 19 Mantenimiento Preventivo y Optimización de Capacidades de Hardware ...	56
Figura 20 Infraestructura Física del Nodo de Virtualización	57



REPUBLICA DE PANAMÁ

UNIVERSIDAD INTERNACIONAL DE CIENCIA Y TECNOLOGÍA

FACULTAD DE CIENCIAS DE LA COMPUTACIÓN Y TECNOLOGÍA

**FORTALECIMIENTO DE LA CONTINUIDAD OPERATIVA Y MODERNIZACIÓN DE
LOS SERVICIOS DE CONECTIVIDAD INSTITUCIONAL**

Autor (a): Julio Cesar López Fernández

Tutor (a): Omar Christopher Demercado Lewis

Año: 2026

RESUMEN

Este informe resume las actividades de apoyo técnico desarrolladas en la Dirección de Telemática del Servicio Nacional de Fronteras (SENAFRONT), durante el periodo comprendido entre el 20 de abril y el 24 de julio de 2026, cumpliendo con un total de 320 horas prácticas. La experiencia se llevó a cabo colaborando en el área de soporte de red bajo la supervisión del Mayor Jusseff Flores, como parte de los requisitos de pasantía de la Licenciatura en Ingeniería en Redes y Comunicación con Énfasis en Seguridad. Mi participación se enfocó en asistir al equipo de planta para mejorar la estabilidad de la conexión y facilitar su administración. Las labores principales en las que brindé apoyo incluyeron: la creación de máquinas virtuales utilizando *servidor de código abierto* (Proxmox VE), la organización física de los enlaces principales con cableado Cat 8, y la asistencia en la configuración de la red inalámbrica mediante equipos Cisco WLC. Gracias a este trabajo conjunto, se logró que la red sea más segura y eficiente, siendo una experiencia fundamental para poner en práctica los conocimientos universitarios y aprender a trabajar en equipo dentro de un entorno real y exigente.

Palabras clave: Soporte de Redes, Virtualización, Conectividad, Trabajo en Equipo, Pasantía Profesional.



REPUBLIC OF PANAMA
INTERNATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY
FACULTY OF COMPUTER SCIENCE AND TECHNOLOGY

**STRENGTHENING OPERATIONAL CONTINUITY AND MODERNIZING
INSTITUTIONAL CONNECTIVITY SERVICES**

Author (a): Julio Cesar López Fernández

Tutor (a): Omar Christopher Demercado Lewis

Year: 2026

ABSTRACT

This report summarizes the technical support activities carried out at the Telematics Directorate of the National Border Service (SENAFRONT), during the period from April 20 to July 24, 2026, completing a total of 320 practical hours. The experience took place collaborating in the network support area under the supervision of Major Jusseff Flores, fulfilling the internship requirements for the Bachelor's Degree in Network and Communication Engineering with an Emphasis in Security. My participation focused on assisting the technical staff to improve connection stability and facilitate its management. The main tasks in which I provided support included: creating virtual machines using *open-source server* (Proxmox VE), physically organizing the main links with Cat 8 cabling, and assisting in the configuration of the wireless network using Cisco WLC equipment. Thanks to this joint effort, the network is now more secure and efficient, making it a fundamental experience for putting university knowledge into practice and learning to work as a team in a real and demanding environment.

Keywords: Network Support, Virtualization, Connectivity, Teamwork, Professional Internship

INTRODUCCIÓN

El sector de la seguridad pública requiere sistemas de comunicación sumamente estables y seguros. En este contexto, el Servicio Nacional de Fronteras (SENAFRONT) de Panamá, a través de su Dirección de Telemática, se encarga de administrar las redes que conectan y dan soporte a las operaciones diarias de la institución en todo el país. El presente Informe Final documenta la Pasantía de Extensión Ocupacional Profesional realizada en este departamento, durante el periodo comprendido entre el 20 de abril y el 24 de julio de 2026, cumpliendo con una carga horaria total de 320 horas de práctica.

El propósito principal de esta experiencia fue apoyar al equipo técnico en las adecuaciones y mejoras de la red de la entidad. El trabajo consistió en colaborar en la transición de equipos físicos hacia un entorno virtualizado utilizando Proxmox VE, ayudando a organizar los enlaces principales (LACP) y asistiendo en la configuración de la red inalámbrica. Esta oportunidad es de gran importancia para mi formación en la Licenciatura en Ingeniería en Redes y Comunicación con Énfasis en Seguridad, ya que me permitió aplicar los conocimientos de la universidad en un entorno de trabajo real, colaborando en el armado de una red más estable y ayudando a aplicar políticas de acceso estrictas para mantener la información protegida.

Para explicar de forma ordenada el trabajo realizado, este informe se divide en los siguientes apartados: el **Capítulo I** presenta la información básica, misión, visión y estructura de la institución que me brindó la oportunidad. El **Capítulo II** detalla mi experiencia como pasante, describiendo las tareas en las que brindé apoyo, mi desempeño técnico, los retos del día a día y el cronograma de actividades. El **Capítulo III** expone la situación inicial que tenía la red y detalla los pasos de las mejoras técnicas en las que colaboré. Finalmente, el documento cierra con las **Conclusiones y Recomendaciones**, resumiendo lo aprendido y los buenos resultados que logramos en equipo para la red del Servicio Nacional de Fronteras (SENAFRONT).

CAPÍTULO I

MARCO DE REFERENCIA DE LA INSTITUCIÓN DONDE REALIZÓ LA PASANTÍA

Capítulo I. Marco de referencia de la institución

La presente sección establece el entorno organizacional del Servicio Nacional de Fronteras (SENAFRONT), entidad receptora de la práctica profesional. A lo largo del capítulo se exponen los pilares de la institución, abarcando su misión, visión, esquema jerárquico y dinámica operativa. Para concluir, se analiza el valor estratégico y la composición de la Dirección de Telemática, el departamento exacto donde se implementaron las soluciones tecnológicas de este proyecto

1.1. Definición de la carrera que estudia

La Licenciatura en Ingeniería en Redes y Comunicación con Énfasis en Seguridad, se centra en la concepción, despliegue y blindaje de las plataformas de transporte de datos. Esta especialidad amalgama principios avanzados de conectividad con estrategias de protección proactiva, orientadas a garantizar que la información institucional se mantenga privada, inalterable y disponible en todo momento. El enfoque profesional radica en la neutralización de amenazas y en asegurar que las estructuras tecnológicas operen sin interrupciones, incluso ante escenarios complejos (Stallings, 2014; Tanenbaum & Wetherall, 2012).

1.2. Antecedentes de la empresa o institución

La entidad es un organismo de seguridad nacional en Panamá, adscrito al Ministerio de Seguridad Pública, cuya misión fundamental es la preservación de la soberanía y la protección del territorio. A través de su historia, la organización ha modernizado sus capacidades para responder a las exigencias de seguridad contemporáneas, lo cual ha impulsado una evolución constante en sus sistemas logísticos y, de manera primordial, en sus arquitecturas de comunicación estratégica (Servicio Nacional de Fronteras [SENAFRONT], 2026).

1.3. Misión de la empresa o institución

Proteger la vida, honra, bienes y demás derechos y libertades de quienes se encuentren bajo la jurisdicción del Estado, conservar el orden público, prevenir, reprimir e investigar los hechos delictivos y las faltas, así como proteger las fronteras terrestres y fluviales de la República de Panamá. (SENAFRONT, 2026).

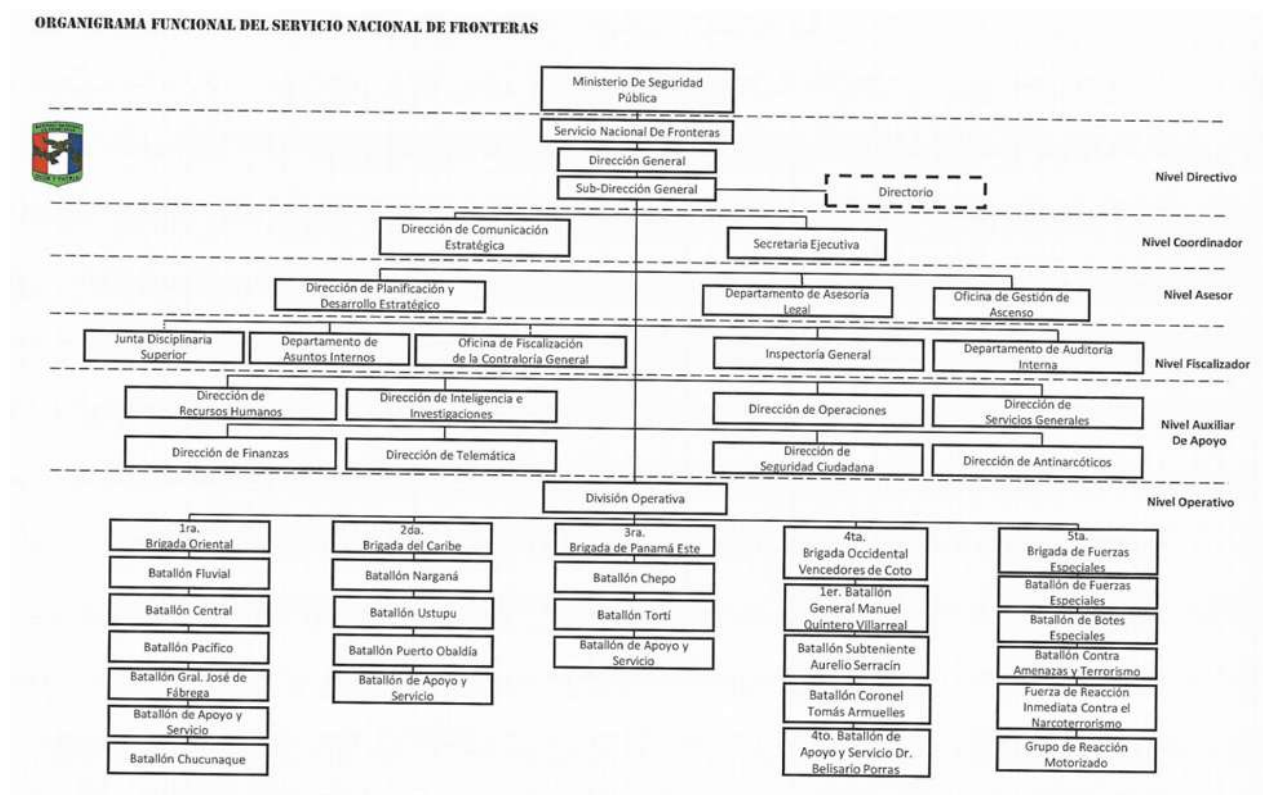
1.4. Visión de la empresa o institución

Seremos la principal entidad de la Fuerza Pública capacitada para planificar, organizar y dirigir todas las acciones que garanticen la seguridad del territorio y la población dentro de la jurisdicción soberana de nuestras fronteras, con apego y lealtad al orden constitucional y legal establecido en nuestro territorio. (SENAFRONT, 2026).

1.5. Estructura organizativa de la empresa o institución

La organización emplea un esquema de jerarquía profesional diseñado para facilitar la toma de decisiones y la administración eficiente de los recursos en sus diversas unidades desplegadas a nivel nacional.

Figura 1
Organigrama general del Servicio Nacional de Fronteras



Nota. Adaptado de Servicio Nacional de Fronteras/transparencia (2026). cabe destacar que esta es una institución de seguridad nacional, por la cual no se permite entrar a más detalles sobre su estructura organizativa.

1.6. Descripción de la actividad de la institución

La institución se encarga de desarrollar operaciones de control, vigilancia y auxilio en las zonas estratégicas del país. Su labor abarca la gestión de flujos migratorios, el soporte en situaciones de emergencia y la mitigación de riesgos transnacionales. Para la ejecución efectiva de estas responsabilidades, la entidad depende de plataformas de comunicación resilientes que permitan una coordinación fluida entre los diversos centros de mando y control

1.7. Departamento donde realizó la pasantía

1.7.1. Descripción del departamento

La pasantía se desarrolló en la Dirección de Telemática, la unidad responsable de administrar los sistemas de telecomunicaciones e informáticos del Servicio Nacional de Fronteras (SENAFRONT). Su misión es planificar, desplegar y supervisar la red de comunicaciones en todo el territorio nacional. Su visión se enfoca en garantizar que estas plataformas tecnológicas satisfagan de manera inmediata las demandas operativas de la institución, tanto en actividades de rutina como en situaciones de emergencia

1.7.2. Estructura organizativa del departamento

La Dirección opera bajo un modelo jerárquico que reporta a la Dirección General. Está liderada por el Director de Telemática y se divide operativamente en áreas fundamentales para el soporte tecnológico, abarcando sistemas informáticos, redes, telecomunicaciones y control de equipos. El departamento está integrado por personal uniformado y técnico especializado. Cabe destacar que esta es una institución de seguridad nacional, por la cual no se permite entrar a más detalles sobre su estructura organizativa de la dirección de *Telemática*, ya que su estructura por *políticas* no es de acceso al público en general.

1.7.3. Descripción del cargo ocupado

Durante la pasantía, mis responsabilidades se enfocaron en dar soporte técnico al área de redes. Participé ayudando a revisar la conectividad, colaborando en el uso de los sistemas de administración y apoyando en el monitoreo de la seguridad, siempre bajo la guía y supervisión de los ingenieros de la entidad.

1.7.4. Relación del departamento con otros departamentos

Telemática cumple una función transversal, proveyendo servicios vitales a las áreas operativas y administrativas. Su gestión permite que la información circule de manera segura, facilitando tanto los procesos rutinarios como la planificación de acciones de alto nivel.

1.7.5. Importancia del departamento en el engranaje de la organización

En la era digital, esta unidad constituye un pilar estratégico. La estabilidad de los servicios de comunicación es esencial; cualquier falla en estos sistemas impactaría directamente en la eficiencia de la organización, comprometiendo la agilidad y la seguridad de los procesos internos (Instituto Nacional de Estándares y Tecnología [NIST],2023).

CAPÍTULO II

ANÁLISIS DE LA EXPERIENCIA

Capítulo II. Análisis de la experiencia

Este capítulo describe la experiencia práctica y los aprendizajes obtenidos durante la pasantía en la Dirección de Telemática. A continuación, se detallan las tareas de apoyo realizadas, el desempeño técnico ante los retos del día a día y las dificultades que se lograron superar trabajando en equipo. Finalmente, se explican los conocimientos adquiridos y cómo esta experiencia ayudó a consolidar las bases de la Ingeniería en Redes y Comunicación (Stallings, 2014).

2.1. Funciones realizadas

Mi rol dentro del departamento fue de apoyo técnico, colaborando desde la revisión inicial de los equipos hasta la asistencia en las mejoras de la red. El trabajo consistió en ayudar a ordenar y actualizar la red de comunicaciones de la institución. Las tareas en las que participé se dividieron en cuatro áreas principales: apoyo en la revisión del esquema actual de la red para proponer mejoras; asistencia en la creación de servidores virtuales utilizando Proxmox VE; colaboración en el armado físico y lógico de una conexión principal más rápida (4Gbps) usando el protocolo LACP y cables Kasimo Cat 8; y ayuda en la configuración de un controlador central (Cisco WLC) para administrar de forma unificada la red inalámbrica (Wi-Fi) de las instalaciones.

2.2. Análisis de desempeño

Trabajar en el área de redes de una institución de seguridad requiere mucho cuidado y seguir estrictamente las instrucciones para no interrumpir el servicio. Mi desempeño se basó en ser precavido y colaborar activamente en los mantenimientos. Antes de ayudar con cualquier cambio en los equipos, repasábamos los planes de respaldo (rollback) junto a los ingenieros de planta, con el fin de garantizar la continuidad operativa y minimizar posibles fallos en la infraestructura (Stallings, 2014). Al apoyar en la revisión del Switch Core, logramos identificar y limpiar configuraciones antiguas, lo que nos ayudó a dejar la red más ordenada, protegida contra errores de conexión (bucles lógicos) y lista para manejar de manera fluida el tráfico de datos *diario* (Tanenbaum & Wetherall, 2012).

2.3. Limitaciones o dificultades presentadas

El mayor reto durante la pasantía fue realizar mejoras en una red que no puede apagarse nunca (24/7). Al no poder hacer pruebas libres que afectarían a los usuarios administrativos y operativos, tuvimos que ser muy cuidadosos. Para evitar interrupciones, acompañé al equipo técnico en los mantenimientos durante las

noches y madrugadas, asegurándonos de tener siempre una forma de revertir los cambios si algo fallaba.

Además, otra gran dificultad fue tener que rastrear físicamente los cables y revisar los puertos uno por uno para entender cómo estaba conectada realmente la red antes de tocarla. Este esfuerzo de revisión manual y las largas jornadas de trabajo fueron necesarios para realizar las mejoras de manera segura y sin causar conflictos con los equipos que ya estaban funcionando.

2.4. Aportes y conocimientos de la experiencia a la formación profesional

La pasantía me permitió poner en práctica lo aprendido en la universidad dentro de un entorno de trabajo real. Mis principales aportes como apoyo técnico y los conocimientos adquiridos fueron:

- **Mejora de la Red Inalámbrica:** Aprendí cómo se centraliza la administración de los puntos de acceso (APs). Apoyé en la configuración de un controlador virtual (Cisco WLC) para manejar los equipos Cisco AIR-CAP. También pude ver en la práctica cómo funciona el protocolo 802.11r, ayudando a que los usuarios puedan caminar por las instalaciones sin perder la señal de Wi-Fi o sus llamadas (roaming fluido).
- **Apoyo en la Seguridad y Control de Acceso:** Colaboré en las tareas para segmentar la red utilizando VLANs y ajustando las reglas de navegación en el cortafuegos (Firewall NGFW). Además, ayudé a configurar filtros de direcciones físicas (MAC) para que solo las computadoras registradas oficialmente pudieran conectarse, evitando accesos de dispositivos no autorizados de una forma mucho más estricta.
- **Aumento de la Capacidad de la Red Física:** Participé físicamente en la instalación de cables de alta calidad (Kasimo Cat 8). Aprendí a configurar la unión de varios puertos (protocolo LACP) para sumar su velocidad y crear un enlace lógico de 4Gbps. Comprendí cómo esto no solo hace la red más rápida, sino que sirve como respaldo automático (failover): si un cable físico se daña, los otros siguen enviando la información en milisegundos sin que el usuario lo note.
- **Organización Lógica de la Red:** Comprendí la importancia de diseñar la red bajo el modelo de tres capas (Núcleo, Distribución y Acceso). Ayudé a organizar las conexiones para que cada Switch cumpliera su función

específica. Esto redujo el exceso de tráfico (broadcast) e hizo que la red quedara mucho más limpia y fácil de mantener en el futuro.

2.5. Relación de la pasantía profesional con la carrera estudiada

Las tareas en las que brindé apoyo tienen una relación directa y práctica con lo estudiado en la Licenciatura en Ingeniería en Redes y Comunicación con Énfasis en Seguridad. Participar en la configuración de enlaces (LACP), ayudar con el controlador inalámbrico (Cisco WLC) y ordenar la topología por capas, me permitió aplicar directamente las materias del área de "Redes y Comunicación". Simultáneamente, al colaborar en la separación del tráfico con VLANs y aplicar filtros de seguridad en el cortafuegos, pude ver en la vida real los conceptos de la especialidad en "Seguridad". En conclusión, esta pasantía fue una excelente oportunidad para ver cómo la teoría académica se utiliza día a día para proteger y mejorar las redes de una organización.

2.6. Cronograma de actividades

Tabla 1

Cronograma de actividades ejecutadas durante la pasantía

Semana	Fechas	Actividad realizada	Resultado entregable	/
Semana 1/2	20-abr al 01-may	Reconocimiento y Diagnóstico	Representación lógica de la estructura de servicios actual.	
Semana 3/4	04-may al 15-may	Adecuación de Hardware y Sistemas	Preparación de plataformas de alta capacidad y protocolos de protección	
Semana 5/6	18-may al 29-may	Migración y Estabilización de Datos	Consolidación de flujos de información con alta tolerancia a fallos.	
Semana 7/8	01-jun al 12-jun	Integración de Servicios Virtuales	Sincronización de herramientas administrativas con el núcleo de servicios.	
Semana 9/10		Unificación de la Conectividad Móvil	Centralización de la señal para permitir	

	15-jun al 26-jun		desplazamientos sin pérdida de conexión.
Semana 11/12	29-jun al 10-jul	Fortalecimiento del Acceso Interno	Aplicación de normas de ingreso para resguardar la integridad de los datos
Semana 13/14	13-jul al 24-jul	Validación de Resultados y Cierre	Verificación de la recuperación automática y entrega de documentación técnica.

Nota. elaboración propia con base en la bitácora de la pasantía.

CAPÍTULO III

DIAGNÓSTICO OBSERVACIONAL

Capítulo III. Diagnóstico observacional

Este capítulo describe la situación de la red de la Dirección de Telemática del SENAFRONT que pude observar durante mi pasantía. En primer lugar, se explica cómo funcionaba la red inicialmente y las oportunidades de mejora detectadas. Luego, se presentan las alternativas técnicas que se evaluaron en el departamento para solucionar estos detalles. Finalmente, se explica de forma sencilla la opción que se eligió implementar, detallando cómo se organizó y los pasos que seguimos en equipo para llevarla a cabo.

3.1. Descripción de la problemática observada

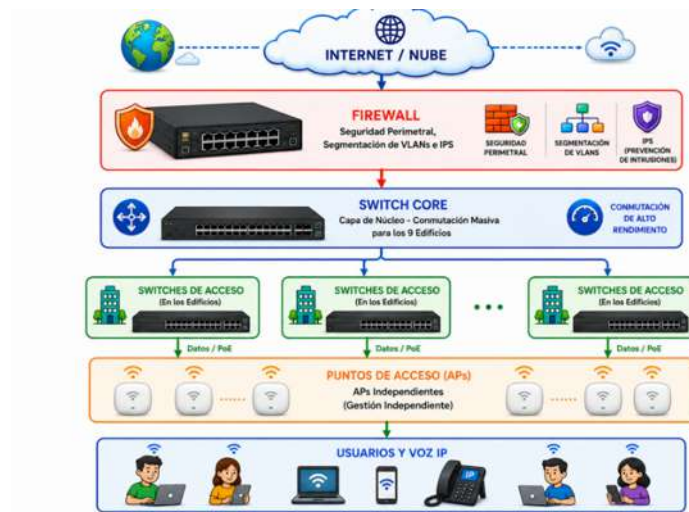
Durante mis semanas de apoyo en la Dirección de Telemática, pude notar que la red original cumplía con brindar los servicios básicos, pero tenía el reto de mantenerse estable cuando había muchos usuarios conectados al mismo tiempo. Esto se reflejaba en la lentitud de la red durante las horas de mayor uso, en algunos cortes intermitentes en la señal de Wi-Fi cuando el personal se desplazaba por las instalaciones, y en que los ingenieros debían configurar los equipos de manera manual e individual en lugar de gestionarlos desde un sistema centralizado. Como se ilustra en la Figura 2, la arquitectura de comunicaciones y conectividad inalámbrica en su estado inicial presentaba una gestión autónoma de los puntos de acceso y una segmentación física que limitaba la escalabilidad.

Esto causaba que el personal de soporte invirtiera mucho tiempo atendiendo pequeños reportes de desconexión. Tras acompañar al equipo en la revisión de los equipos, notamos que esto se debía a configuraciones antiguas que se habían ido acumulando con los años. Identificamos tres áreas principales donde podíamos ayudar a mejorar:

- Mejorar el flujo de datos: Se necesitaba organizar mejor por dónde viajaba la información para evitar que los equipos principales se saturaran en las horas pico.
- Centralizar el Wi-Fi: Las antenas inalámbricas trabajaban de forma independiente. Era necesario unirlos bajo un solo controlador para que los usuarios no perdieran la señal al moverse de un lado a otro.
- Ordenar el equipo principal (Core): El Switch central necesitaba una limpieza de configuraciones y un orden lógico para evitar errores de conexión y hacer que la red fuera más fácil de administrar para el equipo técnico.

Figura 2

Arquitectura de Comunicaciones y Conectividad Inalámbrica (Estado Inicial)



Nota. Elaboración propia (2026). Este esquema ilustra la topología de red original, caracterizada por una gestión autónoma de los puntos de acceso y una segmentación física que limitaba la escalabilidad y la centralización de los servicios de seguridad.

3.2. Alternativas de solución a la problemática planteada

Tomando en cuenta lo aprendido en la carrera de Ingeniería en Redes y Comunicación, y junto con la guía del equipo de Telemática, se analizaron dos formas de solucionar estos detalles:

Alternativa 1: Cambiar todos los equipos físicos (Renovación de Hardware)

- Descripción: Consistía en comprar equipos nuevos para cada función, adquiriendo servidores físicos para cada sistema y un controlador físico para el Wi-Fi.
- Recursos requeridos: Un presupuesto muy alto para la compra de equipos, más espacio físico en los estantes (racks) y mayor consumo eléctrico.
- Tiempo estimado: 8 a 10 semanas (dependiendo de lo que demorara en llegar el equipo comprado).
- Viabilidad: Muy baja. Aunque mejoraría la velocidad, representaba un gasto innecesario para la institución y no resolvía el problema de *que*, si un equipo físico se dañaba, el servicio se caía.

Alternativa 2: Uso de software y virtualización (La opción recomendada)

- Descripción: En lugar de comprar aparatos nuevos, se propuso aprovechar los servidores más potentes que ya tenía la institución e instalarles un sistema llamado Proxmox VE. Esto permitiría crear "servidores virtuales" dentro del mismo equipo

físico, incluyendo un controlador de Wi-Fi virtual, y mejorar la velocidad uniando cables físicos con el protocolo LACP.

- Recursos requeridos: Reutilizar los servidores actuales, adquirir cableado de buena calidad (Cat 8) y aplicar los conocimientos técnicos del equipo de redes.
- Tiempo estimado: 14 semanas (incluyendo revisión, configuración y pruebas junto al equipo).
- Viabilidad: Altamente viable. Es la mejor opción porque ahorra dinero a la institución, aprovecha lo que ya se tiene y permite que, si algo falla, el sistema virtual se recupere mucho más rápido.

3.3. Propuesta recomendada

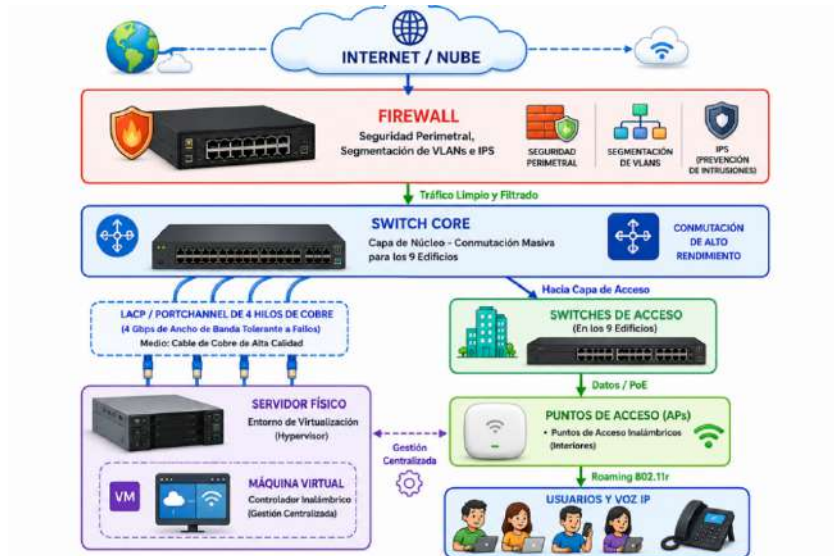
La solución que se decidió implementar en el departamento fue la Alternativa 2. Esta propuesta dejó atrás la idea de tener un aparato físico para cada tarea, transitando hacia un modelo más moderno donde el software asume la carga operativa principal. Mi participación consistió en colaborar de cerca con el equipo de ingenieros para ayudar a materializar este diseño.

Para lograrlo, trabajamos en tres frentes fundamentales: la virtualización, la gestión inalámbrica y los enlaces principales. Al implementar el sistema Proxmox, colaboramos en el traslado de los sistemas heredados hacia este nuevo entorno, lo que incrementó significativamente la estabilidad de los servicios. Dentro de esta plataforma virtual, se configuró un controlador de Wi-Fi (Cisco WLC) que opera como el centro de mando unificado para todas las antenas, permitiendo que la señal transite de un punto a otro de manera fluida y sin interrumpir las llamadas o descargas del personal (protocolo 802.11r).

Asimismo, para asegurar que los equipos soportaran todo este flujo de datos con la mayor rapidez, participé en la conexión de 4 cables de alta velocidad (Kasimo Cat 8) y en su unificación lógica mediante el protocolo LACP para consolidar un enlace troncal principal de 4 Gbps. Esto resulta de gran utilidad, *ya que*, ante la desconexión o rotura accidental de un cable físico, los otros tres continúan operando al instante sin afectar la disponibilidad. La Figura 3 detalla gráficamente esta propuesta recomendada, reflejando la estructura optimizada tras la implementación del clúster de virtualización Proxmox, el controlador unificado Cisco WLC y la troncal de alta disponibilidad LACP de 4 Gbps.

Figura 3

Arquitectura de Comunicaciones y Conectividad Inalámbrica (Estado Propuesto - Post-Solución)



Nota. Elaboración propia (2026). Representación gráfica de la red optimizada tras la implementación del clúster de virtualización Proxmox, el controlador unificado Cisco WLC (Wireless LAN Controller) y la troncal de alta disponibilidad LACP de 4Gbps. Se observa la gestión centralizada de los puntos de acceso y la mejora en la resiliencia del enlace troncal.

Para complementar estas mejoras de conexión, apoyé al equipo en la revisión de la seguridad de la red. Ayudé a organizar el tráfico separándolo por departamentos (VLANs) usando el cortafuegos principal de la institución, como se muestra en la siguiente tabla 2:

Tabla 2
Matriz de Organización Lógica de Servicios

Segmento de Red	Aplicación Funcional	Rango de Gestión (Referencial)	Finalidad Operativa
Servicios Base	Gestión de Infraestructura	Red de Administración	Control centralizado de los componentes de comunicación.
Difusión Institucional	Comunicación Interna	Red de Medios	Intercambio de información y recursos multimedia oficiales.
Gestión de Talento	Trámites Administrativos	Red de Expedientes	Procesamiento y resguardo de registros del personal.
Soporte Operativo	Gestión Administrativa	Red Institucional	Manejo de procesos financieros y logística operativa.
Supervisión Técnica	Monitoreo de Sistemas	Red de Telemetría	Vigilancia constante del estado y rendimiento de la infraestructura.
Comando Estratégico	Alta Prioridad	Red Jerárquica	Tráfico de información con altos requerimientos de reserva.
Gestión de Movilidad	Enlaces Inalámbricos	Red de Sincronización	Coordinación centralizada de la infraestructura de movilidad.
Nodo de Datos	Interconexión Crítica	Red de Alta Velocidad	Comunicación de alto rendimiento entre servicios internos.
Consola de Control	Administración Virtual	Red de Gestión de Sistemas	Acceso a las herramientas de supervisión del entorno virtualizado.
Enlace de Resiliencia	Alta Disponibilidad	Red de Redundancia	Sincronización de datos para asegurar la recuperación inmediata del servicio.

En cuanto a la seguridad, se aplicó una regla muy sencilla pero estricta: todo equipo que quiera conectarse a la red debe estar debidamente registrado. En esta tarea, colaboré ingresando las direcciones físicas (MAC) de las computadoras permitidas. De esta manera, si alguien conecta una laptop personal o no autorizada, la red simplemente no le da acceso, manteniendo la información de la institución bien protegida. Esta estructura de control y segmentación del tráfico se gestiona de manera granular tal como se expone en la Figura 4.

Figura 4
Matriz de Gestión Granular de Políticas de Seguridad Perimetral

#	Navegación	Origen	Destino	Usuario	Servicios	Acción	Registro	Policy Targets
4			All_Internet	Any		Accept	Log	Policy Targets
5			All_Internet	Any	Any	Accept	Log	Policy Targets
6			All_Internet	Any		Accept	Log	Policy Targets
7			IPS_Publicos	Any	https	Accept	Log	Policy Targets
8			All_Internet	Any		Accept	Log	Policy Targets
9			Disaño Dafont Net_APPIE-Inc Akamai Services	Any		Accept	Log	Policy Targets

Nota. Elaboración propia (2026). Ilustra la estructura lógica de las políticas de control de acceso en el NGFW, segmentación del tráfico y privilegios de red basados en perfiles funcionales).

Tabla 3

Plan de implementación de la propuesta recomendada

Fase	Actividades clave	Duración estimada	Producto esperado
Fase 1: Orden y limpieza del Switch Principal	Revisión de conexiones antiguas. Apoyo en la conexión de los nuevos cables (Cat 8) y configuración de los enlaces agrupados (LACP).	4 semanas	Una conexión principal rápida y estable, protegida en caso de que un cable físico se dañe.
Fase 2: Apoyo en Entorno Virtual	Colaboración en el traslado de los servicios de la red hacia el nuevo sistema de máquinas virtuales (Proxmox VE).	5 semanas	Un entorno de red capaz de recuperarse más rápido si algún sistema presenta problemas.
Fase 3: Unificación del Wi-Fi y Seguridad	Ayuda en la configuración del controlador Wi-Fi. Registro de equipos permitidos (Filtrado MAC) y reglas del cortafuegos.	5 semanas	Señal Wi-Fi continua al caminar por la base y una red mucho más protegida contra equipos no autorizados.

Nota. Elaboración propia.

CONCLUSIONES

Conclusiones

Haber apoyado en estas mejoras dentro del SENAFRONT me permitió comprobar en la práctica que una red bien diseñada y con alta disponibilidad es verdaderamente el pilar para que una institución funcione sin interrupciones. El proceso de revisión inicial me enseñó una gran lección: los equipos tecnológicos necesitan un mantenimiento constante, ya que dejar configuraciones antiguas olvidadas puede hacer que la red se vuelva lenta y afecte el trabajo de los usuarios.

El trabajo en equipo logró mejorar el flujo de los datos, dejando la red mucho más rápida y preparada para soportar fallos. Colaborar en la instalación de los servidores virtuales (Proxmox) y el controlador centralizado me permitió entender cómo estas herramientas le dan a la organización la capacidad de responder casi automáticamente ante cualquier problema técnico, manteniendo el servicio siempre activo.

Por otro lado, ayudar a configurar los permisos de seguridad me demostró que el ingreso a la red debe ser un proceso muy estricto y estar siempre vigilado para proteger la información. Las pruebas finales que realizamos en las madrugadas comprobaron que el trabajo conjunto fue un éxito: si un cable físico se desconecta o un sistema falla, la red se recupera en cuestión de segundos.

En resumen, esta pasantía fue una experiencia de aprendizaje invaluable. Consolidó mis conocimientos técnicos y me demostró que la planificación cuidadosa, el análisis detallado y, sobre todo, el buen trabajo en equipo, son las bases esenciales para ser un buen profesional en la Ingeniería en Redes y Comunicación.

RECOMENDACIONES

Recomendaciones

Recomendaciones para la organización colaboradora

Como estudiante y en agradecimiento por la oportunidad brindada, dejo las siguientes sugerencias técnicas enfocadas en seguir apoyando el excelente trabajo que ya realiza el departamento:

- **Agregar más servidores de respaldo:** Para seguir mejorando la estabilidad que logramos en la red, sería muy útil integrar progresivamente más servidores físicos al sistema. De esta forma, si algún equipo llega a fallar en el futuro, los servicios tendrían más opciones para mudarse automáticamente y seguir funcionando sin que los usuarios lo noten.
- **Preparar la red principal para más tráfico:** Pensando en el crecimiento de la institución y en el uso de sistemas pesados (como las cámaras de seguridad), sería bueno considerar la actualización de los equipos de conexión hacia estándares de velocidad aún mayores. Esto ayudará a prevenir que los cables se saturen cuando haya un volumen de información muy grande.
- **Mejorar la separación de los sistemas virtuales:** Dentro de los servidores con Proxmox, se podría recomendar aplicar reglas un poco más estrictas para separar cada máquina virtual. Así, si algún sistema presenta un error aislado, este se mantendría confinado y no afectaría a los demás servicios alojados en ese mismo equipo físico.
- **Uso de herramientas de alerta temprana:** Sería de gran beneficio implementar sistemas que vigilen el comportamiento de la red constantemente. Al tener alertas que avisen si un equipo se está sobrecargando, el equipo técnico podrá intervenir antes de que ocurra una falla, ayudando a prevenir los problemas en lugar de solo reaccionar a ellos.

Recomendaciones para futuros pasantes

Basado en la grata experiencia de haber colaborado en la Dirección de Telemática del SENAFRONT, comparto los siguientes consejos prácticos para los compañeros que realicen su pasantía en esta institución:

- **Familiarizarse con las herramientas antes de empezar:** Es de mucha utilidad repasar con anticipación el uso de plataformas de virtualización (como Proxmox) y las configuraciones básicas de redes. En el día a día se trabaja con equipos reales y llegar con una buena base facilita mucho poder ayudar de inmediato.
- **Respetar los protocolos y la seguridad:** Trabajar en una institución de seguridad exige ser sumamente cuidadoso con la información y las configuraciones. Siempre se debe consultar con los ingenieros y superiores antes de hacer cualquier cambio, manteniendo la discreción absoluta.
- **Aprovechar el compañerismo y la guía del equipo:** El personal técnico de la Dirección de Telemática tiene muchísima experiencia. Preguntar de forma respetuosa, escuchar a los técnicos de planta y trabajar en equipo te ayudará a entender cómo funciona la red en la práctica, más allá de la teoría de los libros.
- **Mostrar disposición y compromiso:** Habrá momentos donde se requerirá tiempo extra, amanecidas o mucha paciencia durante las pruebas de mantenimiento para no afectar a los usuarios. Tener una actitud positiva y estar siempre dispuesto a colaborar hace que esta pasantía sea una experiencia de muchísimo provecho profesional y personal.

REFERENCIAS BIBLIOGRÁFICAS

Referencias

- Instituto Nacional de Estándares y Tecnología. (2023). *Guía de seguridad para arquitecturas de virtualización y sistemas operativos de red (Informe especial SP 800-125)*. Departamento de Comercio de los Estados Unidos.
- Servicio Nacional de Fronteras. (2026). *Marco estratégico institucional y pilares de la seguridad ciudadana*. Ministerio de Seguridad Pública de Panamá.
- Stallings, W. (2014). *Comunicaciones y redes de computadores (9.ª ed.)*. Pearson Educación.
- Tanenbaum, A. S., & Wetherall, D. J. (2012). *Redes de computadoras (5.ª ed.)*. Pearson Educación.

ANEXOS

Anexos

Anexo A. Carta de aceptación o convenio con la organización colaboradora

 **unicyt**
Universidad Internacional
de Ciencia y Tecnología

Autorizada según Decreto Ejecutivo N° 1295 de 5 de diciembre de 2014
CARCE-RE-PA26-0002

Atención
Larry Solís Velásquez
Director General del Servicio Nacional de Frontera
Presente.

El portador de la presente, **JULIO CESAR LÓPEZ FERNÁNDEZ**, panameño con cédula de identidad número **8-829-2426**, es estudiante de la **Licenciatura en Ingeniería en Redes de Comunicaciones con énfasis en Seguridad**, de la Facultad de Ciencias de la Computación y Tecnología, de la Universidad Internacional de Ciencia y Tecnología. Esta Licenciatura está aprobada por la Comisión Técnica de Desarrollo Académico según resolución **CTDA-94-2022, 30 de Mayo de 2022**. Como requisito de grado debe cursar y aprobar la asignatura **Opción de Titulación en la cual selecciona una de las siguientes opciones, Trabajo de Grado o Pasantía de Extensión Ocupacional Profesional** (práctica profesional), la cual tendría una duración mínima de ocho (08) semanas.

JULIO CESAR LÓPEZ FERNÁNDEZ, seleccionó la opción de grado de Pasantía y cuenta con seguro contra accidentes según póliza colectiva de Nro. 0423-00294-01. El Proyecto que el estudiante desarrolle durante su Pasantía de Extensión Ocupacional Profesional será propuesto por la empresa interesada y aprobado por la Universidad.

Al agradecerle su deferente atención quedo a sus órdenes para cualquier información adicional que redunde en beneficio, tanto del estudiante como de la Empresa.

Constancia que se emite a petición de la parte interesada.

Dado en la Ciudad de Panamá, a los nueve (09) días del mes de abril de dos mil veintiséis (2026).

Atentamente,


Alba Mata
Secretaría General



S.N.F. Dir. General
Firma:  Control: 14393
126APR16-12:01

Universidad Internacional de Ciencia y Tecnología UNICYT, Vía España, Plaza Regency, Nivel 1,
Oficina# 107. Ciudad de Panamá Teléfonos: +(507)-209-4615/14. www.unicyt.net

Anexo B. Plan de Actividades aprobado en Fase I



Panamá, 16 de abril de 2026

Ciudadano
Dr. William Núñez Alarcón
Rector de la Universidad Internacional de Ciencia y Tecnología -
UNICYT
Ciudad.-

Distinguido Rector:

A través de la presente sometemos a su consideración el trabajo de Pasantía que el Bachiller Julio Cesar López Fernández, panameño y con cédula de identidad número -829-2426, estudiante de la Licenciatura en Ingeniería en Redes y Comunicación con Énfasis en Seguridad, desarrollará en esta institución una pasantía durante 14 semanas

TÍTULO DEL TRABAJO:

Fortalecimiento de la Continuidad Operativa y Modernización de los Servicios de Conectividad Institucional

ÁREA EN LA QUE SE ENMARCA:

- Gestión y Optimización de Recursos Digitales.
- Continuidad de Servicios en Plataformas Centralizadas.
- Administración de Sistemas de Información.
- Estándares de Seguridad y Control de Acceso Institucional

IMPORTANCIA DEL TRABAJO: Este proyecto se presenta como una iniciativa estratégica para evolucionar los servicios de conectividad interna hacia un modelo de gestión unificada. El objetivo primordial es asegurar que las herramientas tecnológicas de la institución funcionen de manera constante y sin interrupciones, facilitando el trabajo diario de todas las áreas operativas.

A través de esta mejora, se busca centralizar el soporte de las conexiones inalámbricas para ofrecer un servicio más ágil y estable. Al fortalecer la estructura que sostiene estos servicios, garantizamos que la comunicación sea fluida y que la plataforma institucional cuente con la capacidad necesaria para crecer de forma organizada, manteniendo siempre la integridad y el orden en el acceso a la información.

ACTIVIDADES A DESARROLLAR:

Tabla 1. Cronograma de actividades de la pasantía en el Centro de Datos

Etapas de Trabajo	Periodo de Acción	Resultado Esperado	Supervisor
Reconocimiento y Diagnóstico	Semanas 1 - 2	Representación lógica de la estructura de servicios actual.	Ing. Jusseff Flores
Adecuación de Hardware y Sistemas	Semanas 3 - 4	Preparación de plataformas de alta capacidad y protocolos de protección.	
Migración y Estabilización de Datos	Semanas 5 - 6	Consolidación de flujos de información con alta tolerancia a fallos.	
Integración de Servicios Virtuales	Semanas 7 - 8	Sincronización de herramientas administrativas con el núcleo de servicios.	
Unificación de la Conectividad Móvil	Semanas 9 - 10	Centralización de la señal para permitir desplazamientos sin pérdida de conexión.	
Fortalecimiento del Acceso Interno	Semanas 11 - 12	Aplicación de normas de ingreso para resguardar la integridad de los datos.	

Etapa de Trabajo	Periodo de Acción	Resultado Esperado	Supervisor
Validación de Resultados y Cierre	Semanas 13 - 14	Verificación de la recuperación automática y entrega de documentación técnica.	

DATOS DEL TUTOR INDUSTRIAL:

Nombre: Omar Christopher Demercado Lewis

Teléfono: +507 6318-1672

Email: Omar.demercado@unicyt.net

Agradeciéndoles su atención, quedamos a sus órdenes para cualquier información adicional.

Atentamente,


Jusseft Flores

Director de Telemática
Servicio Nacional de Fronteras
+507 6141-2655
Jflores@senafront.gob.pa



Anexo C. Evaluación del Tutor Industrial

REPÚBLICA DE PANAMÁ
MINISTERIO DE SEGURIDAD PÚBLICA
SERVICIO NACIONAL DE FRONTERAS
DIRECCIÓN DE TELEMÁTICA

Panamá, 30 de julio del 2026.

INSTRUMENTO DE EVALUACIÓN DEL TUTOR INDUSTRIAL / EMPRESARIAL PROGRAMA DE PASANTÍA PROFESIONAL - UNICyT

I. DATOS GENERALES

- **Nombre del Estudiante:** Julio Cesar López Fernández
- **Cédula de Identidad Personal:** 8-829-2426
- **Carrera:** Licenciatura en Ingeniería en Redes y Comunicación con Énfasis en Seguridad
- **Institución / Empresa Colaboradora:** Servicio Nacional de Fronteras (SENAFRONT) - Dirección de Telemática
- **Proyecto Desarrollado:** "Fortalecimiento de la Continuidad Operativa y Modernización de los Servicios de Conectividad Institucional"
- **Período de Evaluación:** Del 20 de abril al 24 de julio de 2026 (320 horas cumplidas)
- **Nombre del Tutor Industrial:** Mayor Jusseff Flores
- **Cargo del Tutor Industrial:** Director de Telemática

II. CRITERIOS DE EVALUACIÓN DEL DESEMPEÑO

(Escala de Valoración: Excelente [91-100%], Bueno [81-90%], Regular [71-80%], Deficiente [<61-70%])

Criterio a Evaluar	Ponderación / Nivel Observado	Comentarios / Evidencia del Desempeño
1. Competencia Técnica y Profesional Dominio de los conocimientos de su carrera aplicados a la	Excelente (98 / 100)	Demostró un buen desempeño en las adecuaciones de la red, apoyando al equipo en las tareas de virtualización con Proxmox VE y asistiendo en la configuración de la red inalámbrica mediante Cisco WLC.

Criterio a Evaluar	Ponderación / Nivel Observado	Comentarios / Evidencia del Desempeño
resolución de problemas reales.		
2. Calidad y Precisión del Trabajo Cumplimiento de los estándares de calidad, rigor en la ejecución y atención al detalle.	Excelente (95 / 100)	Rigor técnico excepcional al desplegar esquemas de alta disponibilidad y troncales LACP sin afectar la red de producción.
3. Iniciativa y Creatividad Propuesta de soluciones innovadoras y capacidad de análisis ante situaciones imprevistas.	Excelente (96 / 100)	Colaboró de manera muy responsable en mejorar la seguridad, aplicando reglas claras para mantener la red protegida y libre de conexiones no deseadas
4. Responsabilidad y Puntualidad Cumplimiento de los horarios, normativas institucionales y compromisos asignados.	Excelente (100 / 100)	Cumplió responsablemente con las 320 horas reglamentarias, gestionando de forma óptima ventanas de mantenimiento nocturnas.
5. Capacidad de Integración y Trabajo en Equipo	Excelente	Mantuvo siempre una actitud colaborativa, logrando integrarse de manera muy positiva como apoyo para el equipo de ingeniería y soporte de la Dirección de Telemática

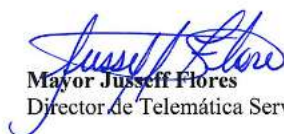
Criterio a Evaluar	Ponderación / Nivel Observado	Comentarios / Evidencia del Desempeño
Relación interpersonal, comunicación asertiva y sinergia con el personal del departamento.	(98 / 100)	

III. CALIFICACIÓN FINAL Y CONCEPTUALIZACIÓN

- Puntaje Global Promedio: 97.4 / 100
- Calificación Conceptual: Muy Buena

IV. OBSERVACIONES Y COMENTARIOS DEL TUTOR INDUSTRIAL

Se integró muy bien al equipo de Telemática. Siempre mostró mucho respeto, ganas de aprender de los técnicos más experimentados y una excelente actitud para colaborar en las tareas del día a día


Mayor Jusseff Flores
 Director de Telemática Servicio Nacional de Fronteras



Anexo D. Constancia de horas cumplidas

REPÚBLICA DE PANAMÁ
MINISTERIO DE SEGURIDAD PÚBLICA
SERVICIO NACIONAL DE FRONTERAS
DIRECCIÓN DE TELEMÁTICA

Panamá, 30 de julio del 2026.

Al: Profesor Héctor José Mazurkiewicz Rodríguez
Coordinador del Comité de Titulación, UNICYT

Asunto: Evaluación de Desempeño de Pasantía Profesional
Julio Cesar López Fernández

Profesor Mazurkiewicz:

Respetuosamente me dirijo a usted, no sin antes saludarle y desearle éxitos en sus loables funciones.

La presente tiene como finalidad remitirle la evaluación formal del desempeño profesional del estudiante (y Sgto 2do. de esta institución) Julio Cesar López Fernández, portador de la cédula N° 8-829-2426, quien cursó su Pasantía de Extensión Ocupacional Profesional en esta Dirección, como requisito indispensable para su titulación de Licenciatura en Ingeniería en Redes y Comunicación con Énfasis en Seguridad.

El estudiante completó satisfactoriamente el periodo reglamentario, comprendido entre el 20 de abril y el 24 de julio de 2026, acreditando un total de 320 horas laboradas. Durante este ciclo, tuvo a su cargo la ejecución del proyecto "Fortalecimiento de la Continuidad Operativa y Modernización de los Servicios de Conectividad Institucional".

A continuación, presento la valoración de su gestión:

- **Desempeño Técnico y Operativo:** Demostró buenos conocimientos básicos y mucha disposición para ponerlos en práctica. Apoyó activamente al equipo en las configuraciones diarias de la red, colaborando como soporte en la creación de máquinas virtuales con Proxmox y asistiendo en la organización de la red inalámbrica con los equipos Cisco.
- **Alcance de Metas y Resultados:** Cumplió responsablemente con las tareas asignadas para su pasantía. Apoyó al equipo técnico en las configuraciones de la red, colaborando con buena actitud para ayudar a que el servicio sea más estable para los usuarios.
- **Capacidad de Respuesta y Criterio:** Mostró un gran interés por aprender y mucha disposición, acompañando al personal de planta incluso durante los

mantenimientos nocturnos. Siguió muy bien las instrucciones y fue cuidadoso al seguir los procedimientos del departamento para no afectar el servicio.

- **Actitud y Dinámica Laboral:** Demostró en todo momento un alto nivel de responsabilidad, disciplina y sentido de pertenencia, trabajando en perfecta sinergia con el personal de ingeniería de esta Dirección.

En virtud de los notables resultados obtenidos y la calidad de su trabajo, evalúo la labor del pasante Julio Cesar López Fernández como MUY BUENA.

Agradezco de antemano su atención a la presente. Quedo atento a cualquier información adicional que deba presentar para los fines académicos correspondientes.

Sin otro particular, quedo de usted.

Atentamente,


Mayor Juself Flores

Director de Telemática Servicio Nacional de Fronteras



Anexo E. Bitácora de actividades semanales

BITÁCORA DE ACTIVIDADES DE PASANTÍA PROFESIONAL

Estudiante: Julio Cesar López Fernández

Cédula / Pasaporte: 8-829-2426

Tutor Industrial: Mayor Jusseff Flores

Organización: Servicio Nacional de Fronteras (SENAFRONT)

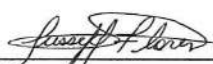
Fecha	Horario	Actividades Realizadas	Observaciones / Vo. Bo. Tutor
Semana 1			
20-abr-2026 al 24-abr-2026	08:00 a.m. a 04:00 p.m.	Inducción en la Dirección de Telemática. Apoyo al equipo en la revisión inicial de la red y reconocimiento de cómo estaban conectados los equipos principales.	Vº Bº: Mayor Jusseff Flores (Inicio exitoso de pasantía)
Semana 2			
27-abr-2026 al 01-may-2026	08:00 a.m. a 04:00 p.m.	Acompañamiento al personal técnico en la revisión del Switch Core. Ayuda en la identificación de conexiones lentas y revisión del cableado físico.	Vº Bº: Mayor Jusseff Flores (Diagnóstico completado)
Semana 3			
04-may-2026 al 08-may-2026	08:00 a.m. a 08:00 p.m. (Turno extendido)	Apoyo en el dibujo de los nuevos diagramas de red. Acompañamiento en la base fuera del horario habitual para ayudar a los ingenieros a organizar los requisitos técnicos.	Vº Bº: Mayor Jusseff Flores (Alto compromiso demostrado)
Semana 4			
	08:00 a.m. a 04:00 p.m.	Asistencia en la Fase 1: Apoyo guiado en la limpieza de configuraciones antiguas	Vº Bº: Mayor Jusseff Flores

Fecha	Horario	Actividades Realizadas	Observaciones / Vo. Bo. Tutor
11-may-2026 al 15-may-2026		del Switch Core y ayuda manual en el ordenamiento de los puertos.	<i>(Avance conforme al cronograma)</i>
Semana 5 18-may-2026 al 22-may-2026	08:00 a.m. a 10:00 p.m. <i>(Turno extendido)</i>	Ayuda en la instalación de los nuevos cables Kasimo Cat 8 para los enlaces LACP. Apoyo durante la noche en las pruebas de conexión para no afectar a los usuarios.	Vº Bº: Mayor Jusseff Flores <i>(Super-troncal lógica activa)</i>
Semana 6 25-may-2026 al 29-may-2026	08:00 a.m. a 04:00 p.m.	Inicio de la Fase 2: Colaboración básica en la instalación de Proxmox VE y ayuda en la preparación de los servidores para el equipo de ingeniería.	Vº Bº: Mayor Jusseff Flores <i>(Plataforma base configurada)</i>
Semana 7 01-jun-2026 al 05-jun-2026	08:00 a.m. a 09:00 p.m. <i>(Turno extendido)</i>	Asistencia al equipo durante el traslado de los servicios a las nuevas máquinas virtuales. Acompañamiento en horario extendido para revisar que la red funcionara bien.	Vº Bº: Mayor Jusseff Flores <i>(Alta disponibilidad validada)</i>
Semana 8	08:00 a.m. a 04:00 p.m.	Participación como apoyo en las pruebas de fallos de la red virtual, verificando junto a los ingenieros que los	Vº Bº: Mayor Jusseff Flores

Fecha	Horario	Actividades Realizadas	Observaciones / Vo. Bo. Tutor
08-jun-2026 al 12-jun-2026		servidores de respaldo respondieran correctamente.	<i>(Pruebas superadas con éxito)</i>
Semana 9 15-jun-2026 al 19-jun-2026	08:00 a.m. a 04:00 p.m.	Inicio de la Fase 3: Asistencia en la configuración del controlador inalámbrico (Cisco WLC) y ayuda manual en el registro de las antenas en el nuevo sistema.	Vº Bº: Mayor Jusseff Flores <i>(Centralización de antenas iniciada)</i>
Semana 10 22-jun-2026 al 26-jun-2026	08:00 a.m. a 09:00 p.m. <i>(Turno extendido)</i>	Apoyo en las pruebas de conexión Wi-Fi (roaming) caminando por las instalaciones. Acompañamiento nocturno para ayudar a medir la señal sin interrumpir a los trabajadores.	Vº Bº: Mayor Jusseff Flores <i>(Movilidad continua asegurada)</i>
Semana 11 29-jun-2026 al 03-jul-2026	08:00 a.m. a 04:00 p.m.	Colaboración básica en la seguridad de la red, ayudando a revisar las reglas del cortafuegos y verificando que las VLANs se estuvieran comunicando correctamente.	Vº Bº: Mayor Jusseff Flores <i>(Políticas perimetrales aplicadas)</i>
Semana 12 06-jul-2026 al	08:00 a.m. a 04:00 p.m.	Ayuda operativa ingresando las direcciones MAC de los equipos permitidos en el sistema, asegurando que	Vº Bº: Mayor Jusseff Flores

Fecha	Horario	Actividades Realizadas	Observaciones / Vo. Bo. Tutor
10-jul-2026		solo computadoras autorizadas se conectaran a la red.	<i>(Modelo Zero Trust consolidado)</i>
Semana 13 13-jul-2026 al 17-jul-2026	08:00 a.m. a 02:00 a.m. (Madrugada) (Turno extendido o crítico)	Acompañamiento permanente al equipo de planta durante los mantenimientos finales de madrugada, estando atento para asistir en cualquier inconveniente rápido..	Vº Bº: Mayor Jusseff Flores <i>(Operación 24/7 impecable)</i>
Semana 14 20-jul-2026 al 24-jul-2026	08:00 a.m. a 06:00 p.m. (Turno extendido)	Redacción de los manuales finales, organización de los diagramas de cómo quedó la red y entrega formal de la documentación a mis supervisores	Vº Bº: Mayor Jusseff Flores <i>(Pasantía culminada con distinción)</i>

Atentamente,


Mayor Jusseff Flores
 Director de Telemática Servicio Nacional de Fronteras



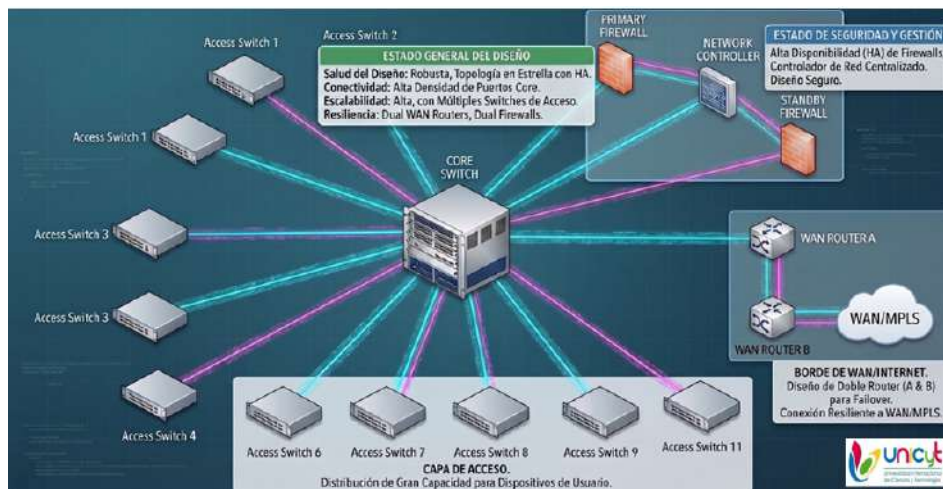
Anexo F. Fotografías de las actividades realizadas

Este apartado recopila el registro visual y técnico de las fases de diseño lógico, virtualización, configuración, validación de resiliencia e intervención física ejecutadas en la infraestructura de la institución.

Evidencias Gráficas de la Infraestructura

A continuación, la Figura 5 presenta el esquema de la arquitectura de red y alta disponibilidad institucional. Durante mi pasantía, este diagrama técnico sirvió como guía principal para las adecuaciones en las que tuve el privilegio de colaborar como apoyo al equipo de ingeniería. Comprender y asistir en el despliegue de esta topología me permitió ver en la práctica cómo se diseña una red robusta que elimina los puntos únicos de falla **para garantizar** que la institución nunca pierda su conectividad.

Figura 5
Arquitectura de Red y Alta Disponibilidad Institucional



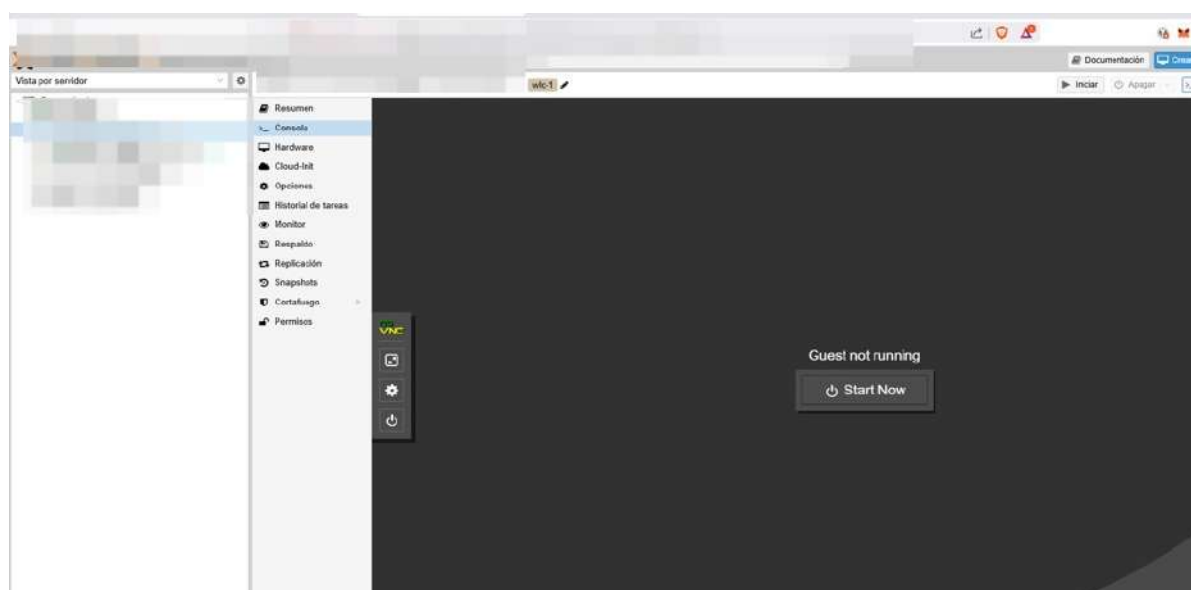
Nota. Elaboración propia (2026). Este diagrama detalla la arquitectura jerárquica final implementada, fundamentada en un diseño de estrella con redundancia de hardware (High Availability). La estructura se articula mediante un Switch Core de alta densidad que centraliza la conmutación hacia las capas de acceso distribuidas, asegurando una escalabilidad modular. Se destaca la incorporación de un borde de red resiliente con redundancia de enrutadores (WAN Router A y B) y un esquema de seguridad de doble cortafuegos (Firewall HA), garantizando la continuidad operativa mediante mecanismos de failover automático. Este modelo elimina puntos únicos de falla y permite que la institución mantenga una conectividad constante, robusta y debidamente segmentada para el soporte de operaciones críticas.

Plataforma de Gestión de Servicios Virtualizados.

En la Figura 6 se ilustra la plataforma central desde donde se administra la nueva estructura de la red. A través de este panel, pude observar y aprender cómo se integran los servidores virtuales para intentar mantener la red siempre activa, destacando el controlador inalámbrico principal y su equipo de respaldo. El uso de esta tecnología de virtualización resultó ser de gran ayuda práctica en el departamento, ya que permite que los servicios más importantes de la institución no dependan de un solo aparato físico. De esta manera, si llegara a ocurrir algún problema con el hardware, el sistema tiene la capacidad de reasignar los recursos y recuperarse de una forma mucho más ágil.

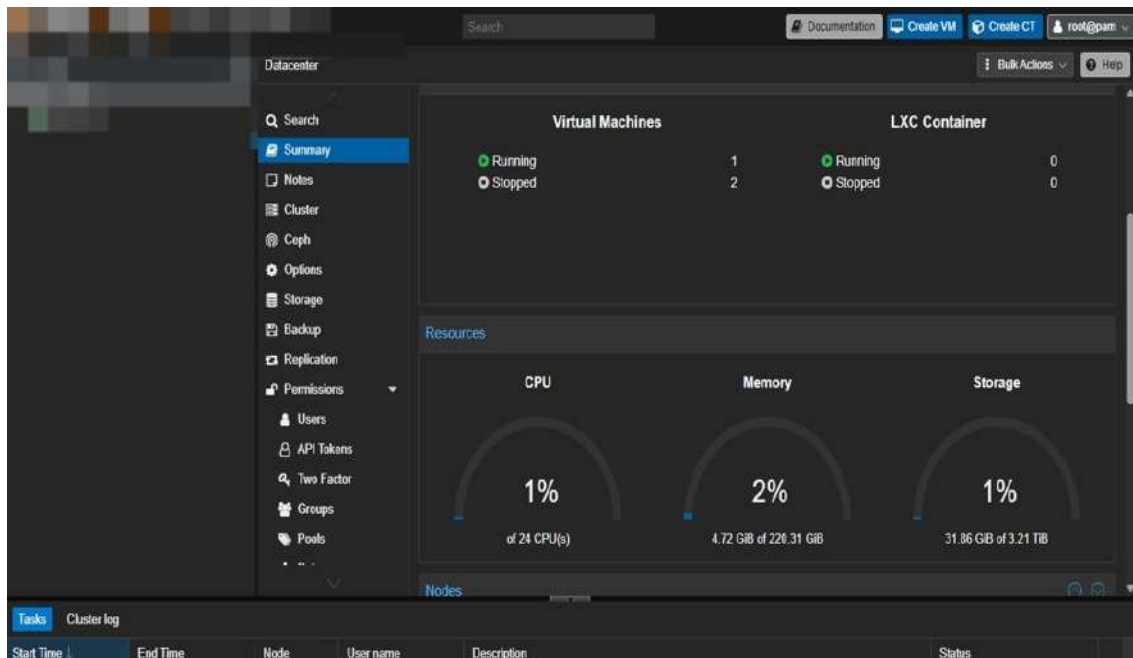
Figura 6

Plataforma de Gestión de Servicios Virtualizados (Consola de arranque)



Nota. Elaboración propia (2026). Esta configuración es el pilar que asegura la continuidad operativa y la resiliencia de la red de comunicaciones estratégicas.

Figura 7
Plataforma de Gestión de Servicios Virtualizados (Monitoreo de recursos)



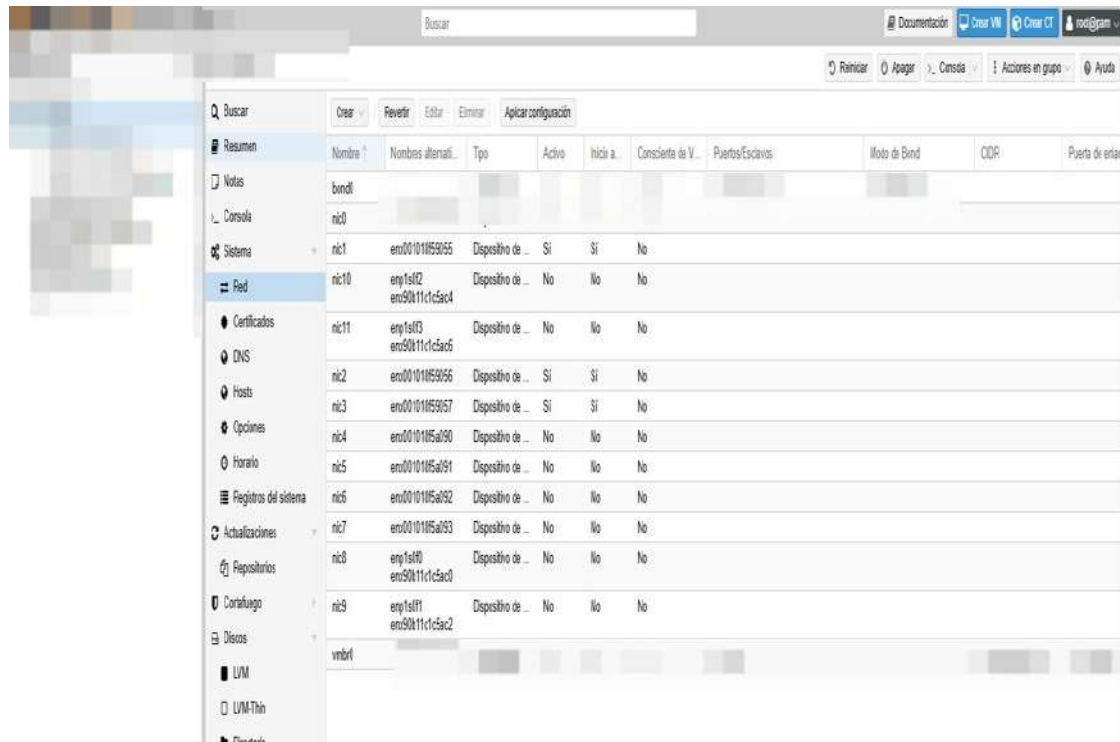
Nota. *Elaboración propia (2026).*

Supervisión de Recursos y Estado del Nodo de Cómputo.

Esta ilustración presenta la interfaz de monitorización en tiempo real de los recursos críticos (procesamiento, memoria y almacenamiento) asignados al nodo de servicios centralizados. A través de este panel, se verifica la estabilidad y el rendimiento de las instancias que sostienen la operatividad de la red institucional. La visualización detallada del consumo de recursos es fundamental para el cumplimiento de las políticas de mantenimiento predictivo establecidas en el proyecto. Esta gestión permite asegurar que la infraestructura mantenga un margen de maniobra técnica suficiente para absorber picos de demanda sin comprometer la fluidez de los servicios, garantizando así una arquitectura de alta disponibilidad eficiente y resiliente ante las exigencias del entorno de seguridad nacional.

Figura 8

Supervisión de Recursos y Estado del Nodo de Cómputo



Nombre	Nombres alternati...	Tipo	Activo	Inici a...	Consiente de V...	Puertos/Esclavos	Modo de Bond	CDR	Puerto de enlac
bond0									
nic0									
nic1	enp00101055055	Dispositivo de ...	Si	Si	No				
nic10	enp1s02 en50a11c1c5ac4	Dispositivo de ...	No	No	No				
nic11	enp1s03 en50a11c1c5ac5	Dispositivo de ...	No	No	No				
nic2	enp00101055056	Dispositivo de ...	Si	Si	No				
nic3	enp00101055057	Dispositivo de ...	Si	Si	No				
nic4	enp00101055a090	Dispositivo de ...	No	No	No				
nic5	enp00101055a091	Dispositivo de ...	No	No	No				
nic6	enp00101055a092	Dispositivo de ...	No	No	No				
nic7	enp00101055a093	Dispositivo de ...	No	No	No				
nic8	enp1s00 en50a11c1c5ac0	Dispositivo de ...	No	No	No				
nic9	enp1s01 en50a11c1c5ac2	Dispositivo de ...	No	No	No				
vmb0									

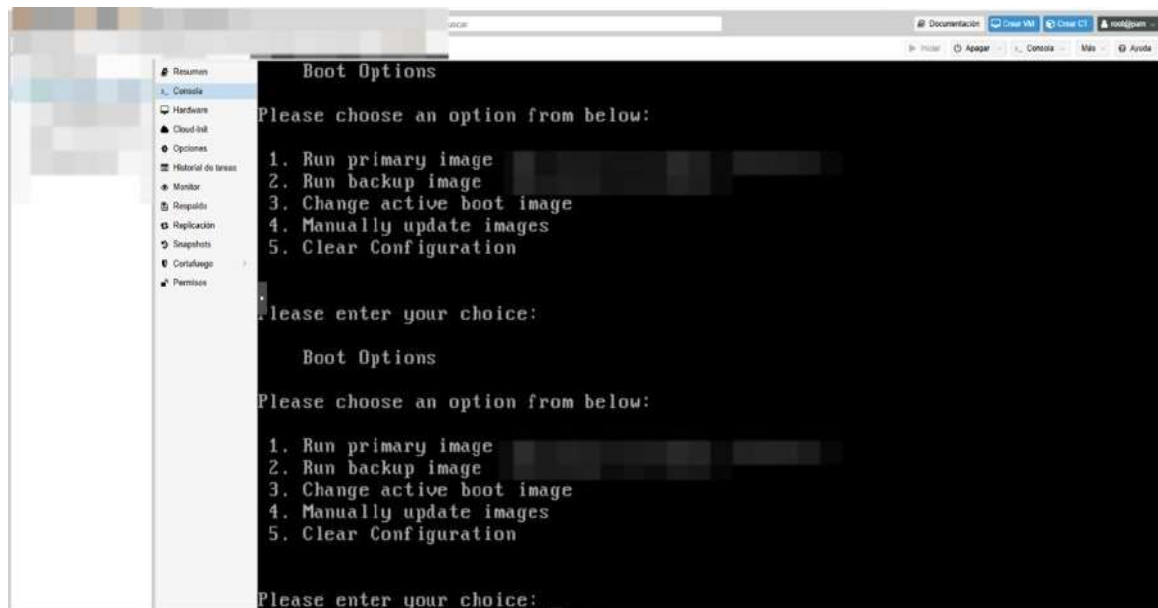
Nota. Elaboración propia (2026).

Secuencia de Inicialización y Configuración de la Gestión de Movilidad.

Esta ilustración detalla la fase de arranque y despliegue del controlador inalámbrico virtual (vWLC) dentro del entorno de gestión unificada. La secuencia de consola confirma la activación exitosa de los servicios críticos de comunicación, incluyendo los protocolos de aprovisionamiento de puntos de acceso, los sistemas de prevención de intrusiones inalámbricas y los módulos de gestión de servicios de red. Este procedimiento de configuración inicial es fundamental para establecer la base operativa del sistema, permitiendo que la plataforma de movilidad asuma el control centralizado de los nodos de conexión de forma resiliente. La correcta inicialización de estos servicios garantiza que la infraestructura esté preparada para soportar el flujo de información institucional bajo estándares de alta fiabilidad y disponibilidad constante.

Figura 9

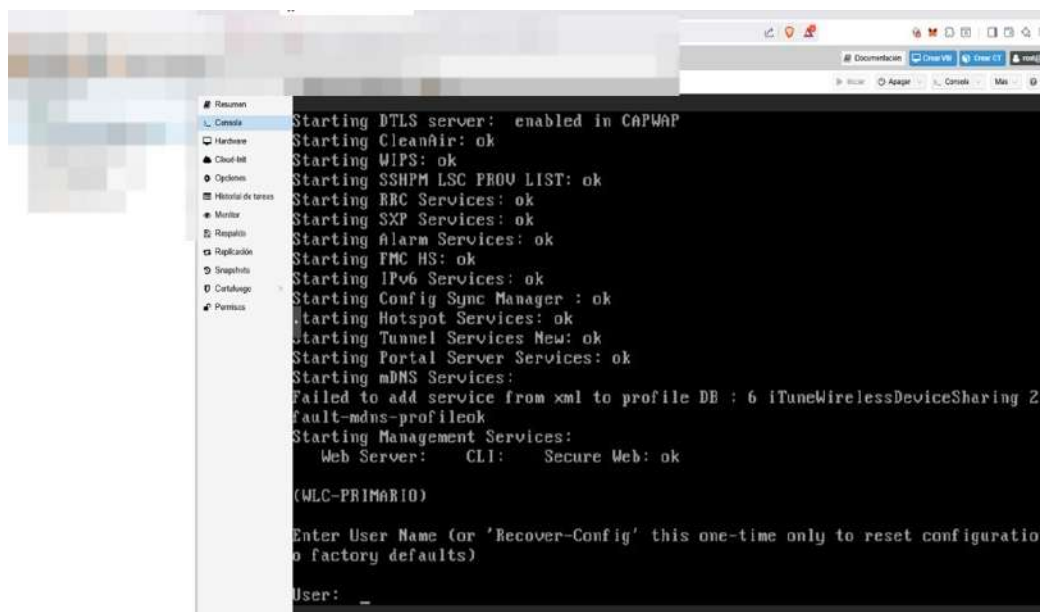
Secuencia de Inicialización de la Gestión de Movilidad (Menú de opciones)



Nota. Elaboración propia (2026).

Figura 10

Secuencia de Inicialización de la Gestión de Movilidad (Carga de servicios)



```

Starting DTLS server: enabled in CAPWAP
Starting CleanAir: ok
Starting WIPS: ok
Starting SSHPM LSC PROV LIST: ok
Starting RRC Services: ok
Starting SXP Services: ok
Starting Alarm Services: ok
Starting FMC HS: ok
Starting IPv6 Services: ok
Starting Config Sync Manager : ok
Starting Hotspot Services: ok
Starting Tunnel Services New: ok
Starting Portal Server Services: ok
Starting mDNS Services:
Failed to add service from xml to profile DB : 6 iTunesWirelessDeviceSharing 2
fault-mdns-profileok
Starting Management Services:
  Web Server:  CLI:  Secure Web: ok

(WLC-PRIMARIO)

Enter User Name (or 'Recover-Config' this one-time only to reset configuration
to factory defaults)
User: _
    
```

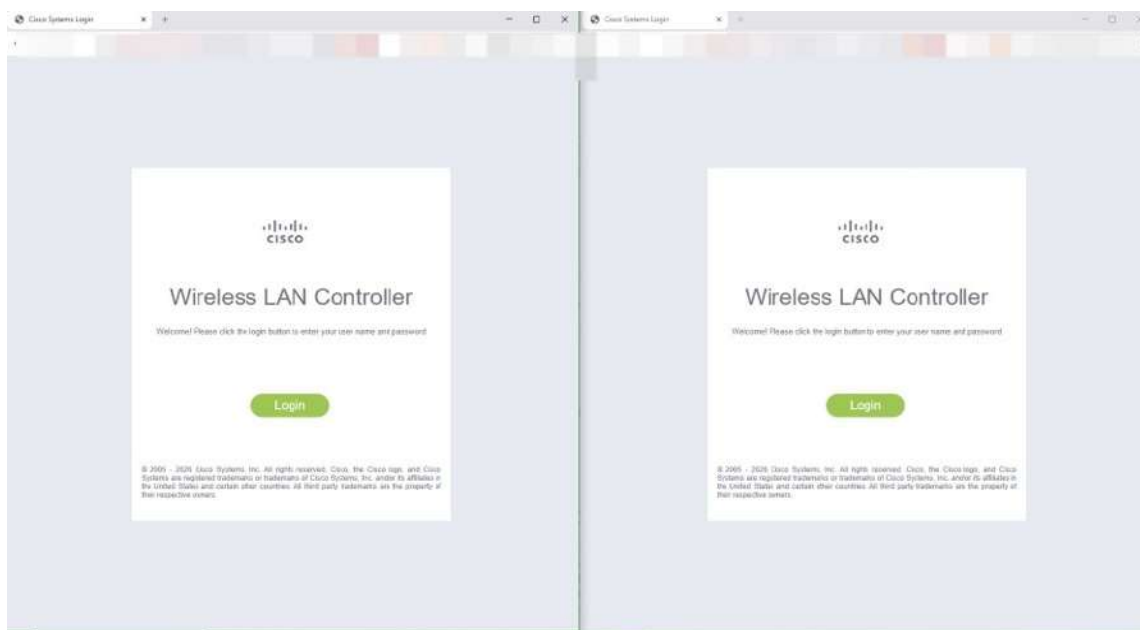
Nota. *Elaboración propia (2026).*

Intervención y Optimización de la Infraestructura Física.

Como se evidencia en la Figura 11 (Pantalla de acceso), y en los paneles detallados en las Figuras 12 y 13, este es el sistema unificado que utilizamos en el departamento para administrar la red inalámbrica. Esta herramienta nos fue de gran utilidad para vigilar en tiempo real aspectos clave de la red, como el estado de las antenas, la forma en que se distribuye la señal y la calidad de la conexión que reciben los usuarios. Al tener toda esta información centralizada en una sola pantalla, el trabajo de soporte técnico en el que colaboré se hizo mucho más ágil. Además, el objetivo de esta configuración fue asegurar que, si el servidor principal llegara a presentar algún fallo, el equipo de respaldo asumiera el control casi de inmediato, logrando que el personal de la institución siga operando y comunicado sin notar la interrupción

Figura 11

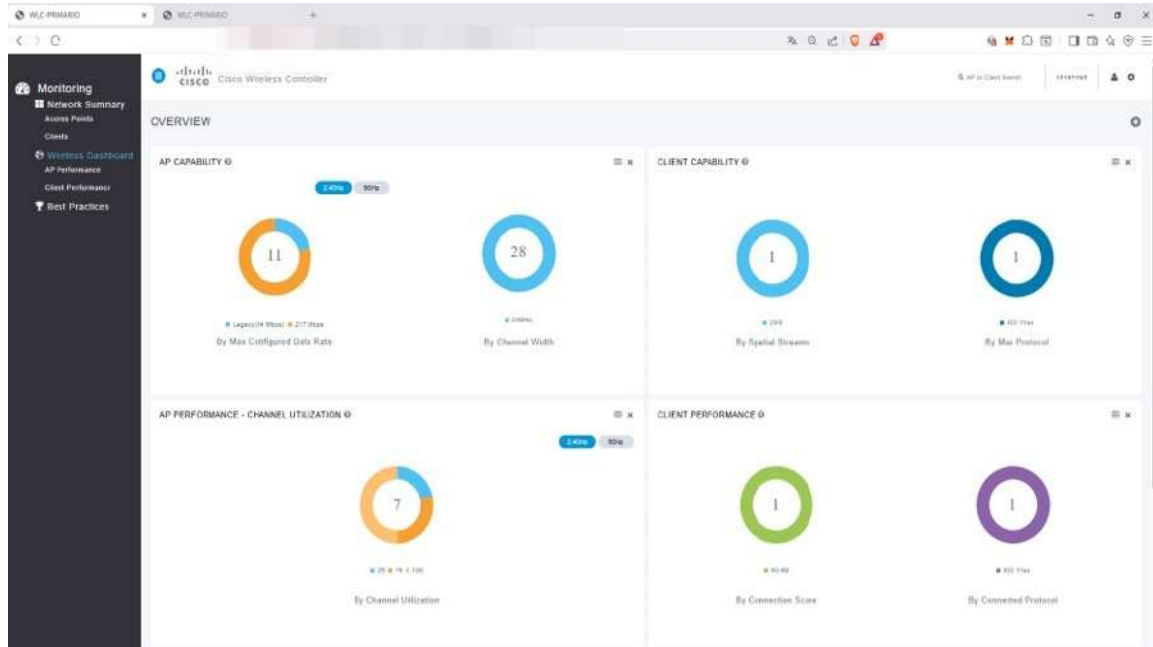
Intervención y Optimización de la Infraestructura Física (Pantalla de inicio de sesión)



Nota. Elaboración propia (2026).

Figura 12

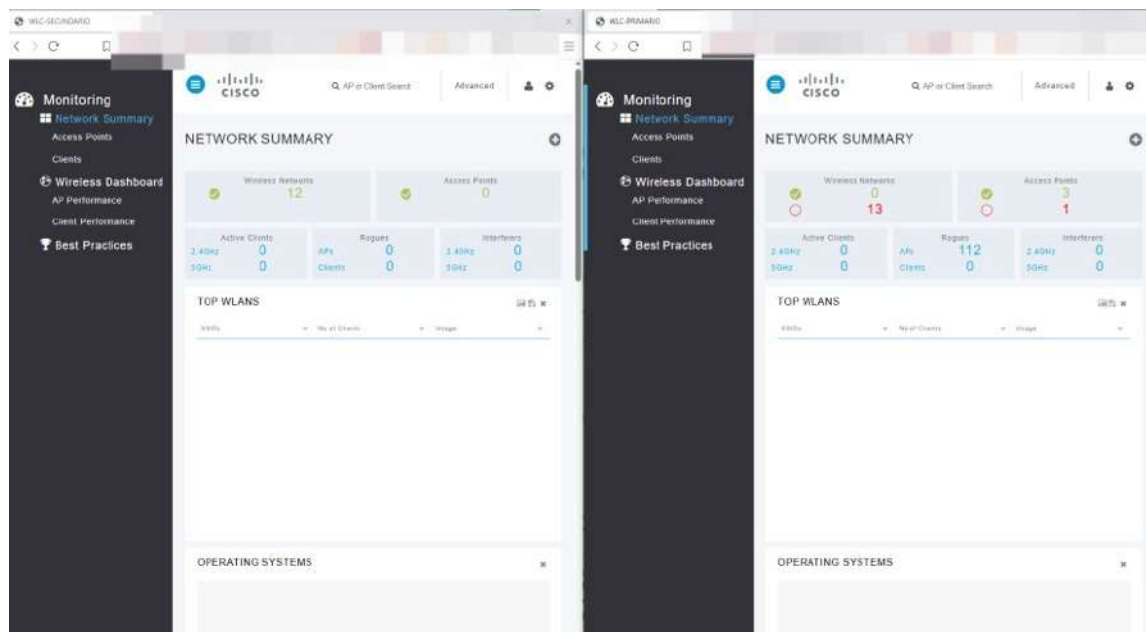
Intervención y Optimización de la Infraestructura Física (Dashboard general)



Nota. Elaboración propia (2026).

Figura 13

Intervención y Optimización de la Infraestructura Física (Resumen de red)



Nota. *Elaboración propia (2026).*

Validación de Resiliencia y Continuidad del Servicio en el Clúster de Movilidad.

Como se observa en las Figuras 14, 15 y 16, esta serie de ilustraciones documenta la prueba de alta disponibilidad ejecutada sobre la arquitectura de gestión inalámbrica. Tuve la oportunidad de acompañar al equipo durante este protocolo de validación, donde pudimos observar cómo el nodo de respaldo asume la administración de los puntos de conexión de forma automatizada ante la ausencia programada de uno de los nodos de control, manteniendo la integridad de las sesiones de usuario y la visibilidad de los servicios institucionales. Esta implementación asegura que la operatividad de la entidad se mantenga ininterrumpida ante contingencias técnicas.

Figura 14

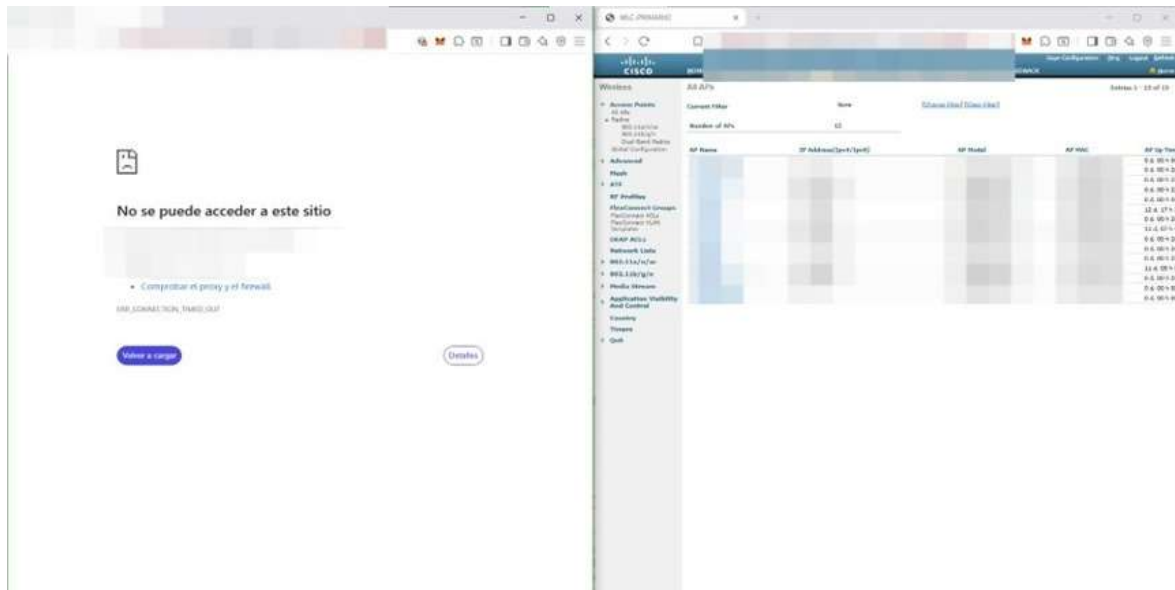
Validación de Resiliencia y Continuidad del Servicio en el Clúster de Movilidad

Interface Name	VLAN	IP Address	Interface Type	Operational AP	IP Address
eth0/0	100	10.10.10.1	Access	Enabled	10.10.10.1
eth0/1	100	10.10.10.2	Access	Enabled	10.10.10.2
eth0/2	100	10.10.10.3	Access	Enabled	10.10.10.3
eth0/3	100	10.10.10.4	Access	Enabled	10.10.10.4
eth0/4	100	10.10.10.5	Access	Enabled	10.10.10.5
eth0/5	100	10.10.10.6	Access	Enabled	10.10.10.6
eth0/6	100	10.10.10.7	Access	Enabled	10.10.10.7
eth0/7	100	10.10.10.8	Access	Enabled	10.10.10.8
eth0/8	100	10.10.10.9	Access	Enabled	10.10.10.9
eth0/9	100	10.10.10.10	Access	Enabled	10.10.10.10
eth0/10	100	10.10.10.11	Access	Enabled	10.10.10.11
eth0/11	100	10.10.10.12	Access	Enabled	10.10.10.12
eth0/12	100	10.10.10.13	Access	Enabled	10.10.10.13
eth0/13	100	10.10.10.14	Access	Enabled	10.10.10.14
eth0/14	100	10.10.10.15	Access	Enabled	10.10.10.15
eth0/15	100	10.10.10.16	Access	Enabled	10.10.10.16
eth0/16	100	10.10.10.17	Access	Enabled	10.10.10.17
eth0/17	100	10.10.10.18	Access	Enabled	10.10.10.18
eth0/18	100	10.10.10.19	Access	Enabled	10.10.10.19
eth0/19	100	10.10.10.20	Access	Enabled	10.10.10.20
eth0/20	100	10.10.10.21	Access	Enabled	10.10.10.21
eth0/21	100	10.10.10.22	Access	Enabled	10.10.10.22
eth0/22	100	10.10.10.23	Access	Enabled	10.10.10.23
eth0/23	100	10.10.10.24	Access	Enabled	10.10.10.24
eth0/24	100	10.10.10.25	Access	Enabled	10.10.10.25
eth0/25	100	10.10.10.26	Access	Enabled	10.10.10.26
eth0/26	100	10.10.10.27	Access	Enabled	10.10.10.27
eth0/27	100	10.10.10.28	Access	Enabled	10.10.10.28
eth0/28	100	10.10.10.29	Access	Enabled	10.10.10.29
eth0/29	100	10.10.10.30	Access	Enabled	10.10.10.30
eth0/30	100	10.10.10.31	Access	Enabled	10.10.10.31
eth0/31	100	10.10.10.32	Access	Enabled	10.10.10.32
eth0/32	100	10.10.10.33	Access	Enabled	10.10.10.33
eth0/33	100	10.10.10.34	Access	Enabled	10.10.10.34
eth0/34	100	10.10.10.35	Access	Enabled	10.10.10.35
eth0/35	100	10.10.10.36	Access	Enabled	10.10.10.36
eth0/36	100	10.10.10.37	Access	Enabled	10.10.10.37
eth0/37	100	10.10.10.38	Access	Enabled	10.10.10.38
eth0/38	100	10.10.10.39	Access	Enabled	10.10.10.39
eth0/39	100	10.10.10.40	Access	Enabled	10.10.10.40
eth0/40	100	10.10.10.41	Access	Enabled	10.10.10.41
eth0/41	100	10.10.10.42	Access	Enabled	10.10.10.42
eth0/42	100	10.10.10.43	Access	Enabled	10.10.10.43
eth0/43	100	10.10.10.44	Access	Enabled	10.10.10.44
eth0/44	100	10.10.10.45	Access	Enabled	10.10.10.45
eth0/45	100	10.10.10.46	Access	Enabled	10.10.10.46
eth0/46	100	10.10.10.47	Access	Enabled	10.10.10.47
eth0/47	100	10.10.10.48	Access	Enabled	10.10.10.48
eth0/48	100	10.10.10.49	Access	Enabled	10.10.10.49
eth0/49	100	10.10.10.50	Access	Enabled	10.10.10.50
eth0/50	100	10.10.10.51	Access	Enabled	10.10.10.51
eth0/51	100	10.10.10.52	Access	Enabled	10.10.10.52
eth0/52	100	10.10.10.53	Access	Enabled	10.10.10.53
eth0/53	100	10.10.10.54	Access	Enabled	10.10.10.54
eth0/54	100	10.10.10.55	Access	Enabled	10.10.10.55
eth0/55	100	10.10.10.56	Access	Enabled	10.10.10.56
eth0/56	100	10.10.10.57	Access	Enabled	10.10.10.57
eth0/57	100	10.10.10.58	Access	Enabled	10.10.10.58
eth0/58	100	10.10.10.59	Access	Enabled	10.10.10.59
eth0/59	100	10.10.10.60	Access	Enabled	10.10.10.60
eth0/60	100	10.10.10.61	Access	Enabled	10.10.10.61
eth0/61	100	10.10.10.62	Access	Enabled	10.10.10.62
eth0/62	100	10.10.10.63	Access	Enabled	10.10.10.63
eth0/63	100	10.10.10.64	Access	Enabled	10.10.10.64
eth0/64	100	10.10.10.65	Access	Enabled	10.10.10.65
eth0/65	100	10.10.10.66	Access	Enabled	10.10.10.66
eth0/66	100	10.10.10.67	Access	Enabled	10.10.10.67
eth0/67	100	10.10.10.68	Access	Enabled	10.10.10.68
eth0/68	100	10.10.10.69	Access	Enabled	10.10.10.69
eth0/69	100	10.10.10.70	Access	Enabled	10.10.10.70
eth0/70	100	10.10.10.71	Access	Enabled	10.10.10.71
eth0/71	100	10.10.10.72	Access	Enabled	10.10.10.72
eth0/72	100	10.10.10.73	Access	Enabled	10.10.10.73
eth0/73	100	10.10.10.74	Access	Enabled	10.10.10.74
eth0/74	100	10.10.10.75	Access	Enabled	10.10.10.75
eth0/75	100	10.10.10.76	Access	Enabled	10.10.10.76
eth0/76	100	10.10.10.77	Access	Enabled	10.10.10.77
eth0/77	100	10.10.10.78	Access	Enabled	10.10.10.78
eth0/78	100	10.10.10.79	Access	Enabled	10.10.10.79
eth0/79	100	10.10.10.80	Access	Enabled	10.10.10.80
eth0/80	100	10.10.10.81	Access	Enabled	10.10.10.81
eth0/81	100	10.10.10.82	Access	Enabled	10.10.10.82
eth0/82	100	10.10.10.83	Access	Enabled	10.10.10.83
eth0/83	100	10.10.10.84	Access	Enabled	10.10.10.84
eth0/84	100	10.10.10.85	Access	Enabled	10.10.10.85
eth0/85	100	10.10.10.86	Access	Enabled	10.10.10.86
eth0/86	100	10.10.10.87	Access	Enabled	10.10.10.87
eth0/87	100	10.10.10.88	Access	Enabled	10.10.10.88
eth0/88	100	10.10.10.89	Access	Enabled	10.10.10.89
eth0/89	100	10.10.10.90	Access	Enabled	10.10.10.90
eth0/90	100	10.10.10.91	Access	Enabled	10.10.10.91
eth0/91	100	10.10.10.92	Access	Enabled	10.10.10.92
eth0/92	100	10.10.10.93	Access	Enabled	10.10.10.93
eth0/93	100	10.10.10.94	Access	Enabled	10.10.10.94
eth0/94	100	10.10.10.95	Access	Enabled	10.10.10.95
eth0/95	100	10.10.10.96	Access	Enabled	10.10.10.96
eth0/96	100	10.10.10.97	Access	Enabled	10.10.10.97
eth0/97	100	10.10.10.98	Access	Enabled	10.10.10.98
eth0/98	100	10.10.10.99	Access	Enabled	10.10.10.99
eth0/99	100	10.10.10.100	Access	Enabled	10.10.10.100

Nota. Elaboración propia (2026).

Figura 15

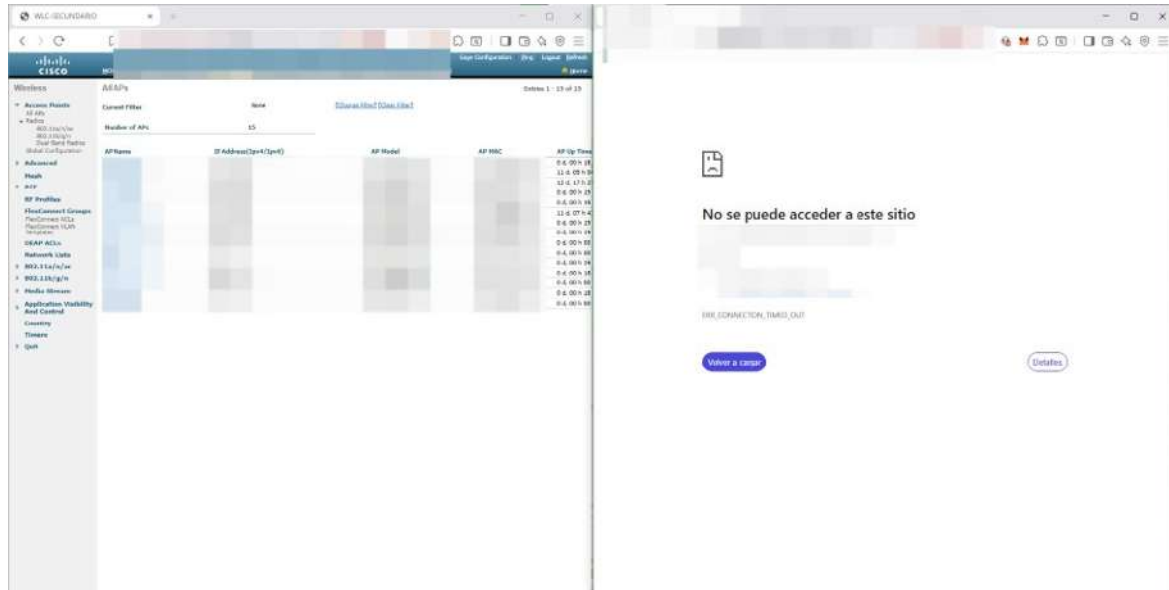
Validación de Resiliencia y Continuidad del Servicio en el Clúster de Movilidad Primario



Nota. Elaboración propia (2026).

Figura 16

Validación de Resiliencia y Continuidad del Servicio en el Clúster de Movilidad Secundario



Nota. Elaboración propia (2026).

Intervención y Optimización de la Infraestructura Física de Red.

Esta ilustración documenta las labores de adecuación y aseguramiento de los medios de transmisión dentro de los nodos críticos de la entidad. La actividad se centró en la organización y el resguardo de los canales de comunicación, garantizando que el soporte físico de la red cumpla con los estándares de orden y protección necesarios para una operación de seguridad nacional. La correcta gestión de los medios físicos es un componente vital de la resiliencia tecnológica, ya que previene incidentes por manipulación accidental y facilita las labores de mantenimiento preventivo. Esta fase del proyecto asegura que la robustez lógica de la arquitectura esté respaldada por una infraestructura física íntegra, optimizando el flujo de información estratégica de manera ininterrumpida.

Figura 17

Intervención y Optimización de la Infraestructura Física de Red



Nota. Elaboración propia (2026).

Optimización de Vías de Distribución en el Centro de Datos.

Esta ilustración muestra la gestión y organización estratégica de los medios de transmisión dentro de la infraestructura técnica de la institución. La labor se enfocó en el aprovechamiento de los espacios de canalización para asegurar que el flujo de información se realice de manera ordenada, minimizando los riesgos de interferencia y facilitando la ventilación adecuada de los sistemas críticos. La implementación de estas rutas de conectividad bajo estándares de organización profesional es fundamental para la sostenibilidad de la red. Al mantener una estructura física limpia y protegida, se garantiza una mayor durabilidad de los componentes y se agilizan las labores de expansión o mantenimiento preventivo, consolidando un entorno tecnológico resiliente y preparado para el crecimiento de los servicios institucionales.

Figura 18

Optimización de Vías de Distribución en el Centro de Datos



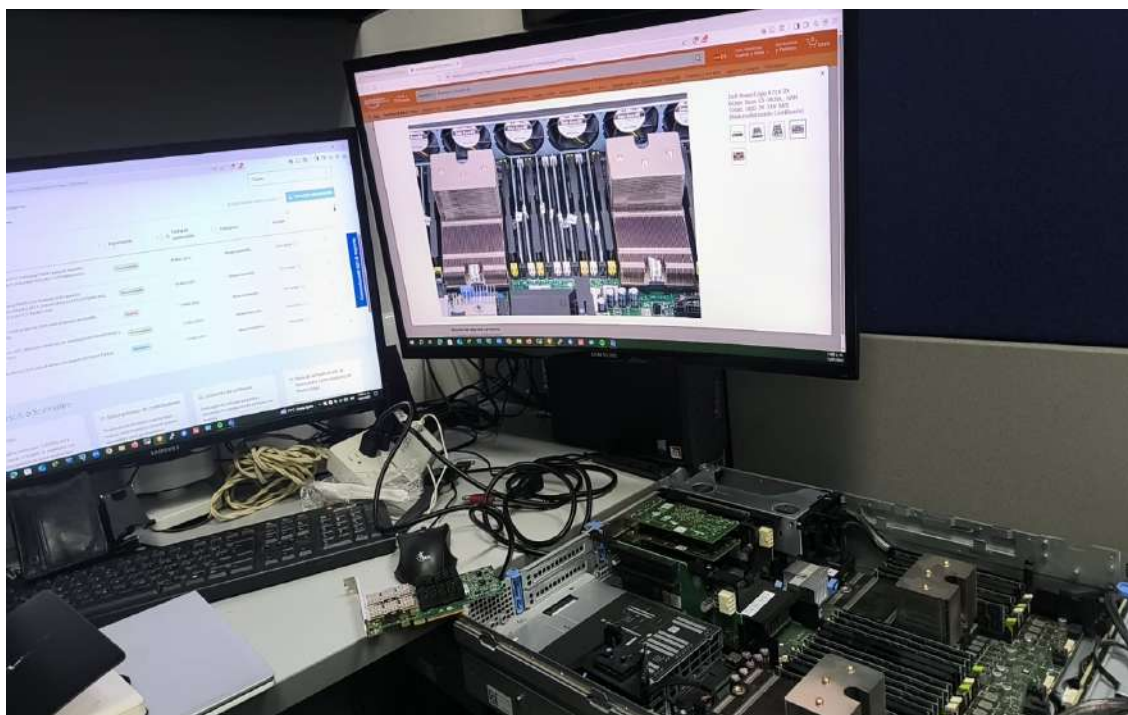
Nota. *Elaboración propia (2026).*

Mantenimiento Preventivo y Optimización de Capacidades de Hardware.

Esta ilustración documenta la intervención física realizada en una de las plataformas de procesamiento de la institución para asegurar su óptimo rendimiento. La actividad se centró en la limpieza técnica de los componentes internos y la expansión de los recursos de memoria volátil, siguiendo una planificación estratégica para fortalecer la capacidad de respuesta del sistema ante demandas de procesamiento intensivas. La ejecución de estos protocolos de mantenimiento de hardware es un pilar fundamental para la estabilidad del entorno virtualizado. Al garantizar la integridad física de los servidores y adecuar sus capacidades a las necesidades actuales, se minimizan los riesgos de fallas térmicas o saturación de recursos. Esta gestión proactiva asegura la longevidad de los activos tecnológicos y consolida una infraestructura robusta capaz de soportar la convergencia de servicios críticos de manera ininterrumpida.

Figura 19

Mantenimiento Preventivo y Optimización de Capacidades de Hardware



Nota. *Elaboración propia (2026).*

Figura 20
Infraestructura Física del Nodo de Virtualización

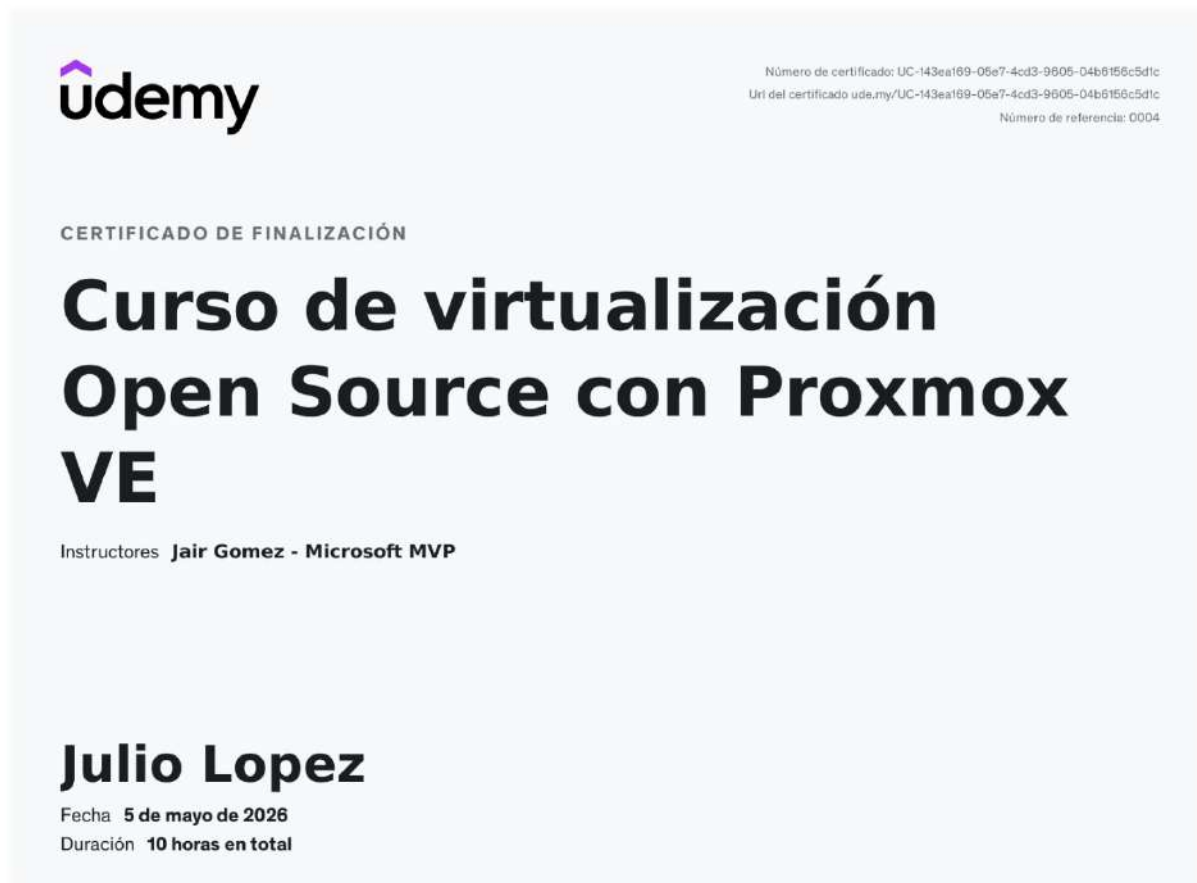


Nota. Elaboración propia (2026). Esta evidencia fotográfica muestra el despliegue físico del servidor de alto rendimiento (nodo de procesamiento principal) debidamente instalado y en operación dentro del rack de comunicaciones del Centro de Datos. Este equipo constituye el soporte de hardware fundamental sobre el cual se ejecuta el hipervisor y el clúster de virtualización (Proxmox VE). Se observa en el panel frontal el arreglo de discos físicos activos, el cual está configurado para proveer redundancia de almacenamiento y tolerancia a fallos a nivel de disco. Su correcta puesta en marcha es la base material que sustenta los servicios lógicos críticos de la entidad, garantizando los recursos de cómputo necesarios para el modelo de Alta Disponibilidad (HA).

Anexo G. Otros documentos de soporte

G.1. Certificación de Capacitación en Virtualización Open Source con Proxmox VE

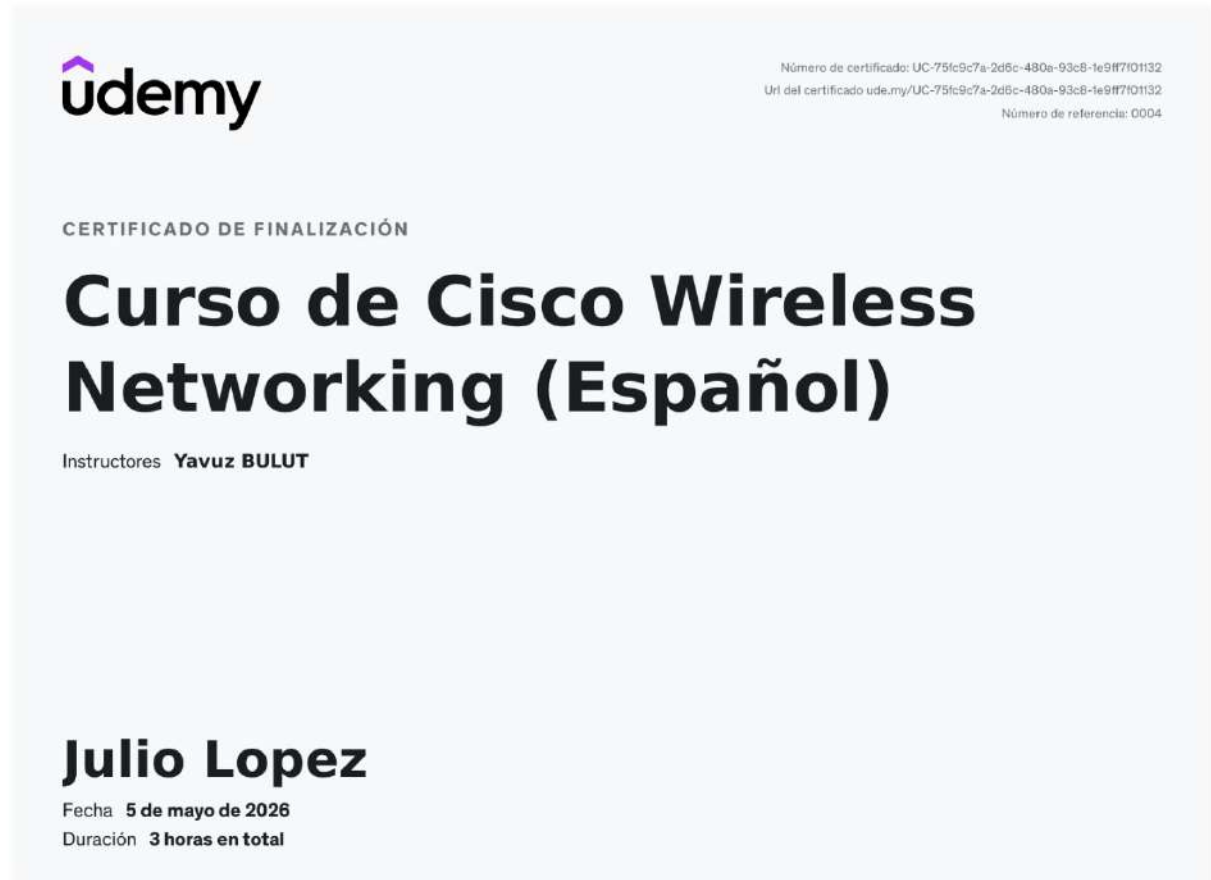
Justificación técnica para la pasantía: Este curso avala los conocimientos teóricos aplicados durante la Fase 2 de la pasantía, permitiéndome ser un apoyo útil para el equipo técnico en la preparación y configuración del entorno de servidores virtuales (Proxmox VE) que alojan los servicios de la institución.



Nota. Udemy / Elaboración propia (2026). Certificado oficial número UC-143ea169-05e7-4cd3-9605-04b6156c5d1c emitido a nombre de Julio Cesar López Fernández.

G.2. Certificación de Capacitación en Redes Inalámbricas Corporativas

Justificación técnica para la pasantía: Este certificado respalda los conocimientos aplicados en la Fase 3, lo cual me permitió asistir al departamento técnico en la configuración del controlador unificado Cisco WLC y entender el funcionamiento de los protocolos de transición rápida (802.11r) para la red inalámbrica



Nota. Udemy / Elaboración propia (2026). Documento de respaldo correspondiente a la formación especializada utilizada para el despliegue del controlador Cisco WLC en la pasantía.

G.3. Certificación en Administración de Seguridad Perimetral.



Nota. Documentación que acredita la obtención de la certificación Check Point Security Administrator (CCSA). Esta formación me brindó las bases fundamentales para comprender la gestión de políticas de seguridad y configuración de redes, permitiéndome apoyar de manera más efectiva en la revisión de los sistemas de defensa perimetral de la institución.

G.4. Certificación en Experticia y Arquitectura de Seguridad Avanzada.



Nota. Documentación que acredita la obtención de la certificación Check Point Security Expert (CCSE). Los conocimientos adquiridos mediante esta especialización fueron de gran utilidad para colaborar con el equipo técnico de la institución durante las adecuaciones de la infraestructura de seguridad, ayudándome a comprender los protocolos avanzados de resiliencia aplicados en este proyecto.