REPÚBLICA DE PANAMÁ

UNIVERSIDAD INTERNACIONAL DE CIENCIA Y TECNOLOGÍA

CIENCIAS DE LA COMPUTACIÓN Y TECNOLOGÍA

LICENCIATURA EN INGENIERÍA EN REDES DE COMUNICACIONES CON ÉNFASIS EN SEGURIDAD

OPCIÓN DE TITULACIÓN: PASANTÍA DE EXTENSIÓN OCUPACIONAL PROFESIONAL

IMPLEMENTACIÓN INTEGRAL DE INFRAESTRUCTURA TECNOLÓGICA PARA LA APERTURA DE UNA NUEVA SUCURSAL EMPRESARIAL

Tutor: Omar Demercado

Estudiante: Lisbeth Otero Rodríguez de Alvarez

Número de Cédula/Pasaporte: 9-726-1074

Cohorte: 31-08-2020

Aprobado por el Asesor:

Ciudad de Panamá, 13 de mayo de 2024

REPÚBLICA DE PANAMÁ

UNIVERSIDAD INTERNACIONAL DE CIENCIA Y TECNOLOGÍA

FACULTAD DE CIENCIA DE LA COMPUTACIÓN Y TECNOLOGÍA

INFORME DE PASANTIA DE EXTENSIÓN OCUPACIONAL PROFESIONAL REALIZADO EN LA EMPRESA LABORATORIO CLINICO FERNANDEZ. PROYECTO IMPLEMENTACIÓN INTEGRAL DE INFRAESTRUCTURA TECNOLÓGICA PARA LA APERTURA DE UNA NUEVA SUCURSAL EMPRESARIAL

PASANTÍA DE EXTENSIÓN OCUPACIONAL PROFESIONAL PARA OPTAR AL GRADO DE LICENCIADO EN INGENIERÍA EN REDES DE COMUNICACIÓN CON ÉNFASIS EN SEGURIDAD

Autor(a): Lisbeth Ariadne Otero de Alvarez

Ciudad de Panamá, mayo 2025

UNIVERSIDAD INTERNACIONAL DE CIENCIA Y TECNOLOGÍA
FACULTAD DE CIENCIAS ADMINISTRATIVAS, EMPRESARIALES Y DE NEGOCIOS

INFORME DE ACTIVIDADES DE TUTORÍA

Estudiante: Lisbeth Otero de Alvarez. **Cédula de identidad** No: 9 – 726 – 1074

Tutor: Prof. Omar Demercado **Cédula de identidad** No. 1- 713 - 1945

Correo electrónico: lisbeth.otero@unicyt.net **Celular No.** 6314-7518

Título tentativo del trabajo de grado (TG) y de pasantía profesional (PEOP).
Implementación integral de infraestructura tecnológica para la apertura de una sucursal empresarial

Línea de Investigación: Infraestructura tecnológica, redes y seguridad.

SESIÓN	FECHA	HORA REUNIÓN.	ASPECTO TRATADO	OBSERVACIÓN
1	27/01/2025	10:00 A.M.	Revisión de temas de fondo sobre el informe de la pasantía.	Incluir aspectos técnicos relacionados a la carrera respecto a lo encontrado a lo largo de la pasantía.
2	03/02/2025	8:50 A.M.	Revisión de ajustes aspectos técnico.	Relacionar los aspectos técnicos con la carrera.
3	10/02/2025	8:00 A.M.	Revisión de las observaciones y ajustes de relacionar los aspectos técnicos con la carrera.	Se incluyeron los aspectos técnicos solicitados.
4	26/02/2025	12:00 P.M.	Corrección de enfoque de trabajos realizados a las funciones realizadas.	Se realizaron los enfoques específicos a los trabajos ejecutados por el estudiante en la pasantía

5	10/03/2025	8:00 A.M.	Revisión de los diagramas y topologías utilizadas	Se revisaron los aspectos técnicos de los diseños realizados.
6	24/03/2025	6:00 P.M.	Revisión de los protocolos de seguridad utilizados para configuración de WiFi.	Se discutieron los protocoles de seguridad utilizados y se aplicó técnicas aprendidas en clase.
7	14/04/2025	8:00 A.M.	Revisión de aplicación de configuración de seguridad aplicada en Firewall.	Protocolos de seguridad utilizados cumplen.
8	21/04/2025	10:00 A.M	Revisión de los cambios recomendados por el profesor Héctor.	Se relacionó y especifico las funciones realizadas con las materias del curso.
9	13/05/2025	2:00 P.M.	Revisión del documento final	Firma del documento final.

Título definitivo:

Implementación integral de infraestructura tecnológica para la apertura de una sucursal empresarial

Comentarios finales acerca de la investigación: Declaramos que las especificaciones anteriores representan el proceso de dirección del trabajo de grado arriba mencionado.

Firma

Tutor

Firma

Estudiante

DEDICATORIA

Con inmenso amor y gratitud, dedico este trabajo de grado a las personas más importantes en mi vida, quienes han sido mi fortaleza y motor de inspiración durante todo este proceso de superación profesional. Aunque el camino no ha sido fácil, el contar con el apoyo de mi familia ha permitido que fuera superando cada reto.

A mi madre, cuyo amor incondicional, valores y enseñanzas han sido el pilar fundamental de mi vida. Gracias por mostrarme, con tu ejemplo, el significado del esfuerzo, la perseverancia y la dedicación. Este logro es reflejo de tu constante apoyo y fe en mis capacidades.

A mis hijos, quienes han llenado mi vida de alegría, fortaleza y esperanza. Ustedes son mi motor y mi mayor motivación para seguir adelante, incluso en los momentos más desafiantes.
También quiero ser un ejemplo de superación para ustedes, mostrarle con el ejemplo la importancia de estudiar y que para cumplir nuestros sueños no hay edad.

A mí esposo, por ser mi compañero incondicional en cada una de mis aventuras. Gracias por tu amor, por siempre creer en mí cuando y por estar a mi lado en cada paso. Tu apoyo inquebrantable y tus palabras de aliento me han impulsado a superar cada obstáculo.

Este trabajo no solo representa un logro académico, sino también el cumplimiento de un sueño y el resultado de nuestro esfuerzo, dedicación y sacrificio. A ustedes, con todo mi corazón, les dedico este esfuerzo, con la esperanza de que este logro sea también motivo de orgullo y felicidad para nuestra familia.

AGRADECIMIENTO

En el presente trabajo quiero agradecer principalmente a Dios, cuya guía, fortaleza y bendiciones me han acompañado a lo largo de este camino. Su presencia en mi vida me ha dado la confianza y la determinación necesarias para superar cada desafío. También quiero reconocerme por el esfuerzo, la dedicación y sobre todo la perseverancia que he puesto en el cumplimiento de esta meta. Este proyecto no solo representa un logro académico, sino también el fruto de mi compromiso con mi crecimiento personal y profesional, al profesionalismo y paciencia bridada por mis profesores en cada una de mis materias. A la vez quiero expresar mi más sincero agradecimiento al Laboratorio Clínico Fernández por brindarme la oportunidad de desarrollar este proyecto en sus instalaciones. Su confianza en mis capacidades y su apoyo constante fueron fundamentales para llevar a cabo esta iniciativa. Agradezco especialmente a su equipo directivo y a cada uno de los colaboradores, quienes con su disposición y profesionalismo facilitaron la implementación de las mejoras tecnológicas que hoy forman parte del éxito de la nueva sucursal.

INDICE GENERAL

REPÚBLICA DE PANAMA

UNIVERSIDAD INTERNACIONAL DE CIENCIAS Y TECNOLOGIA

FACULTAD DE CIENCIAS DE LA COMPUTACIÓN Y TECNOLOGÍA

INFORME DE PASANTÍA PROFESIONAL REALIZADA EN LA EMPRESA LABORATORIO CLINICO FERNANDEZ. PROYECTO IMPLEMENTACIÓN INTEGRAL DE INFRAESTRUCTURA TECNOLÓGICA PARA LA APERTURA DE UNA NUEVA SUCURSAL EMPRESARIAL

Autor: Lisbeth Ariadne Otero de Alvarez

Tutor: Omar de Mercado

Año: 2025

RESUMEN

Este informe describe las actividades realizadas durante la pasantía profesional en Laboratorio Clínico Fernandez los meses de agosto y septiembre 2024, cuyo objetivo fue participar en el diseño, habilitación e instalación todos los sistemas tecnológicos necesarios para la apertura de una nueva sucursal de la empresa. El proyecto incluyó la implementación de redes de comunicaciones, instalación de sistemas de cámaras de seguridad, configuración he instalación de controles de acceso, cableado estructurado, así como la integración de otros sistemas necesarios para garantizar la operatividad de la nueva sede. Entre las actividades principales se incluyeron la instalación de cableado estructurado, que permitió una adecuada distribución de las redes de datos y energía en las instalaciones; la configuración de sistemas de redes, garantizando la conectividad entre los diferentes equipos y la infraestructura de la empresa; y la implementación de sistemas de cámaras de seguridad y controles de acceso, diseñados para asegurar la protección de las instalaciones y controlar el ingreso a áreas sensibles. Gracias al éxito de esta pasantía, la empresa ha logrado internalizar muchas de las funciones que anteriormente dependían de la tercerización, en particular las relacionadas con la gestión de proyectos tecnológicos. La implementación exitosa

de los sistemas de redes, cámaras de seguridad, controles de acceso y cableado estructurado, permitió a la empresa ganar independencia en la planificación, ejecución y supervisión de proyectos de infraestructura tecnológica.

Palabras claves: Sistemas Tecnológicos, Diseño e implementación, Infraestructura Tecnológica.

REPÚBLICA DE PANAMA

UNIVERSIDAD INTERNACIONAL DE CIENCIAS Y TECNOLOGIA

FACULTAD DE CIENCIAS DE LA COMPUTACIÓN Y TECNOLOGÍA

INFORME DE PASANTÍA PROFESIONAL REALIZADA EN LA EMPRESA LABORATORIO CLINICO FERNANDEZ. PROYECTO IMPLEMENTACIÓN INTEGRAL DE INFRAESTRUCTURA TECNOLÓGICA PARA LA APERTURA DE UNA NUEVA SUCURSAL EMPRESARIAL

Autor: Lisbeth Ariadne Otero de Alvarez

Tutor: Omar Demercado

Año: 2025

SUMMARY

This report describes the activities performed during the professional internship at Laboratorio Clinico Fernandez during the months of August and September 2024, whose objective was to participate in the design, implementation and installation of all the technological systems necessary for the opening of a new branch of the company. The project included the implementation of communications networks, installation of security camera systems, configuration and installation of access controls, structured cabling, as well as the integration of other systems necessary to guarantee the operability of the new branch. The main activities included the installation of structured cabling, which allowed for an adequate distribution of data and energy networks in the facilities; the configuration of network systems, ensuring connectivity between the different equipment and the company's infrastructure; and the implementation of security camera systems and access controls, designed to ensure the protection of the facilities and control access to sensitive areas. Thanks to the success of this internship, the company has been able to internalize many of the functions that previously depended on outsourcing, particularly those related to

technology project management. The successful implementation of network systems, security cameras, access controls and structured cabling, allowed the company to gain independence in the planning, execution and supervision of technological infrastructure projects.

Key words: Technological Systems, Design and implementation, Technological Infrastructure.

INTRODUCCIÓN

En la actualidad, la tecnología representa un factor determinante en el desarrollo y competitividad de las organizaciones. Las empresas, sin importar su tamaño o sector, requieren infraestructuras tecnológicas eficientes, seguras y escalables que les permitan optimizar sus operaciones, garantizar la continuidad del negocio y adaptarse a un entorno cada vez más digitalizado.

El presente informe documenta la experiencia profesional adquirida durante la pasantía realizada en Laboratorio Clínico Fernández, una organización panameña con más de 60 años de trayectoria en el sector salud, reconocida por su innovación, calidad de servicio y adopción de tecnologías de punta para el diagnóstico clínico. El laboratorio cuenta con múltiples sucursales en la ciudad de Panamá y ofrece servicios que abarcan análisis clínicos, pruebas especializadas y atención domiciliaria, posicionándose como uno de los referentes en el país en materia de diagnóstico médico.

La pasantía, llevada a cabo entre agosto y septiembre de 2024, tuvo como objetivo principal participar en el diseño, implementación e integración de la infraestructura tecnológica necesaria para la apertura de una nueva sucursal del Laboratorio Clínico Fernández. El proyecto abarcó áreas críticas como el cableado estructurado, la configuración de redes de comunicación, la implementación de sistemas de videovigilancia y control de acceso, así como la integración de medidas de seguridad lógica y física que garantizaran la operatividad segura de la sede.

Desde una perspectiva académica, esta experiencia permitió aplicar de manera práctica los conocimientos adquiridos durante la Licenciatura en Ingeniería en Redes de Comunicación con Énfasis en Seguridad, fortaleciendo competencias técnicas, de gestión de proyectos, de solución de problemas en entornos reales y de trabajo colaborativo. Asimismo, contribuyó a validar la pertinencia de la formación recibida, evidenciando su aplicabilidad en escenarios empresariales concretos.

Este informe presenta de manera estructurada el desarrollo de las actividades realizadas, el análisis de los resultados obtenidos, el impacto logrado en la organización y las lecciones aprendidas, aportando evidencia tangible del crecimiento profesional alcanzado durante la ejecución del proyecto.

JUSTIFICACIÓN

La implementación de una infraestructura tecnológica eficiente y segura en la nueva sucursal del Laboratorio Clínico Fernández respondió a una necesidad crítica en el contexto de la expansión operativa de la organización. La naturaleza del sector salud exige altos niveles de disponibilidad, integridad y confidencialidad de la información, así como una conectividad robusta que garantice el funcionamiento continuo de los equipos biomédicos, sistemas administrativos y plataformas de comunicación.

La sucursal, al no contar con una infraestructura tecnológica previa, requería un diseño integral que contemplara el cableado estructurado, la conectividad de red, la ciberseguridad, el acceso lógico y físico, así como la gestión de la continuidad operativa. Esta necesidad se volvió aún más relevante ante el contexto actual donde los entornos clínicos deben garantizar trazabilidad, interoperabilidad y protección de datos en cumplimiento de normativas nacionales e internacionales.

El desarrollo de este proyecto permitió, no solo atender esa necesidad organizacional, sino también ofrecer un espacio de aplicación práctica para los conocimientos adquiridos durante la formación profesional. Asimismo, el proyecto representó un aporte real al fortalecimiento de la infraestructura tecnológica de la institución, reduciendo su dependencia de terceros, aumentando la eficiencia operativa y garantizando la escalabilidad futura del sistema.

En términos académicos, la ejecución de este proyecto contribuye al cumplimiento de los objetivos del plan de estudios de la carrera, al vincular directamente los contenidos teóricos con un entorno real de aplicación, y al fomentar el desarrollo de competencias profesionales alineadas con el perfil de egreso.

DIAGNOSTICO

Como parte de su estrategia de crecimiento, planificó la apertura de una nueva sucursal con todos los requerimientos técnicos necesarios para garantizar su operatividad. La empresa, aunque cuenta con una infraestructura tecnológica establecida, había manejado históricamente estos proyectos mediante la contratación de terceros para el diseño, implementación y configuración de sus soluciones tecnológicas. Frente a este nuevo escenario, y con base en los conocimientos adquiridos durante mi formación en la Licenciatura en Ingeniería en Redes de Comunicaciones con Énfasis en Seguridad, asumí el reto de proponer una alternativa interna, tomando responsabilidad directa sobre el análisis, diseño, adquisición y configuración de la infraestructura tecnológica de la nueva sede. Esta decisión estratégica permitió, no solo demostrar la capacidad del departamento de tecnología para ejecutar proyectos de forma autónoma, sino también reducir significativamente los costos operativos asociados a la tercerización. Además, se generó un precedente organizacional que valida la viabilidad de continuar fortaleciendo el talento interno para futuras expansiones.

OBJETIVO GENERAL: Diseñar e implementar una infraestructura tecnológica integral para la nueva sucursal, que incluya cableado estructurado, configuración de red, dispositivos de seguridad lógica y física, con el fin de garantizar la operatividad, conectividad segura y continuidad de los servicios, reduciendo la dependencia de proveedores externos mediante el aprovechamiento de capacidades internas desarrolladas en la formación profesional.

OBJETIVO ESPECIFICO:

1. Diseñar el esquema de infraestructura tecnológica, incluyendo la planificación del cableado estructurado, la topología de red y los requerimientos de seguridad física y lógica.
2. Seleccionar, configurar e instalar dispositivos de red como switches, puntos de acceso inalámbricos y firewall, alineados con buenas prácticas de seguridad y rendimiento.
3. Implementar sistemas de seguridad física, tales como videovigilancia y control de acceso, integrándolos con la red de datos de forma segura y funcional.
4. Documentar el desarrollo del proyecto, incluyendo planos, configuraciones, cronograma de ejecución, y resultados obtenidos, como evidencia del aprendizaje práctico y del impacto organizacional generado.

METODOLOGIA:

La metodología aplicada en el desarrollo de esta pasantía profesional fue de tipo aplicada, práctica y descriptiva, ya que se orientó a resolver una necesidad tecnológica real mediante el diseño y ejecución directa de soluciones de infraestructura, conectividad y seguridad. El enfoque utilizado permitió vincular los conocimientos adquiridos durante la formación universitaria con un escenario empresarial concreto.

El proyecto se ejecutó bajo un esquema estructurado por etapas:

1. Diagnóstico de necesidades: Se realizó un levantamiento técnico del sitio para identificar requerimientos de red, conectividad, cableado estructurado, seguridad física y lógica.
2. Diseño de la solución tecnológica: Con base en el diagnóstico, se elaboraron planos de red, se definió la topología de red, el número de puntos de red, el diseño del gabinete, y la segmentación de VLAN.
3. Gestión de recursos y materiales: Se calcularon cantidades, se seleccionaron proveedores, y se adquirieron los equipos y materiales necesarios para el proyecto (switches, APs, rack, cables, cámaras, etc.).
4. Instalación y configuración: Se supervisó y/o ejecutó la instalación física de los componentes, y se procedió con la configuración de dispositivos como firewall, switches, APs y sistema de videovigilancia.
5. Verificación y pruebas: Se realizaron pruebas funcionales para validar conectividad, segmentación de red, accesos, visibilidad remota, y disponibilidad del servicio.
6. Documentación del proceso: Se elaboraron reportes técnicos, planos y respaldos de configuraciones como parte del cierre técnico del proyecto.

CAPÍTULO I: MARCO DE REFERENCIA DE LA EMPRESA

1.1 Definición de la carrera que estudia:

La Licenciatura en Ingeniería en Redes de Comunicaciones con Énfasis en Seguridad de la Universidad Internacional de Ciencia y Tecnología (UNICyT) está diseñada para formar profesionales competentes en el diseño, implementación y gestión de infraestructuras de redes de comunicación, con un enfoque particular en la seguridad de la información. El programa académico abarca áreas como la configuración de redes, instalación de sistemas de seguridad, controles de acceso y cableado estructurado, preparando a los estudiantes para enfrentar los desafíos tecnológicos actuales y garantizar la protección de los datos en diversas organizaciones.

La carrera tiene una duración de 4 años y ofrece horarios matutinos, vespertinos y nocturnos, de lunes a domingo, brindando flexibilidad a los estudiantes.

1.2 Antecedentes de la empresa o institución:

Laboratorio Clínico Fernández fue fundado en 1964 por el Lic. Ricardo Fernández, egresado de la Universidad de Loyola. Inicialmente establecido en David, Chiriquí, en 1969 trasladó su sede principal a la ciudad de Panamá, marcando el inicio de una expansión sostenida que ha consolidado su presencia en el país.

A lo largo de más de seis décadas, el laboratorio ha evolucionado incorporando tecnología de vanguardia y sistemas automatizados con integración robótica, permitiendo obtener resultados más rápidos y precisos, brindando un respaldo confiable para decisiones médicas certeras.

Actualmente, el Laboratorio Clínico Fernández cuenta con múltiples sucursales en la ciudad de Panamá, incluyendo ubicaciones en Costa del Este, Paitilla, Marbella, San Francisco, Albrook, Calle 50 y Santa María, ofreciendo servicios de exámenes de diagnóstico clínico y atención domiciliar en diversas áreas.

1.3 Misión, Visión y Valores de la Empresa:

Misión: Brindar servicios de diagnóstico clínico de alta calidad, utilizando tecnología avanzada y un equipo humano comprometido, para contribuir al bienestar y la salud de nuestros pacientes.

Visión: Ser el laboratorio clínico líder en Panamá, reconocido por su excelencia en servicios, innovación tecnológica y compromiso con la salud de la comunidad.

Valores:

Compromiso: Dedicación constante para satisfacer las necesidades de nuestros pacientes.

Calidad: Mantener altos estándares en todos nuestros procesos y servicios.

Innovación: Implementar tecnologías avanzadas para mejorar nuestros servicios.

Ética: Actuar con integridad y responsabilidad en todas nuestras acciones.

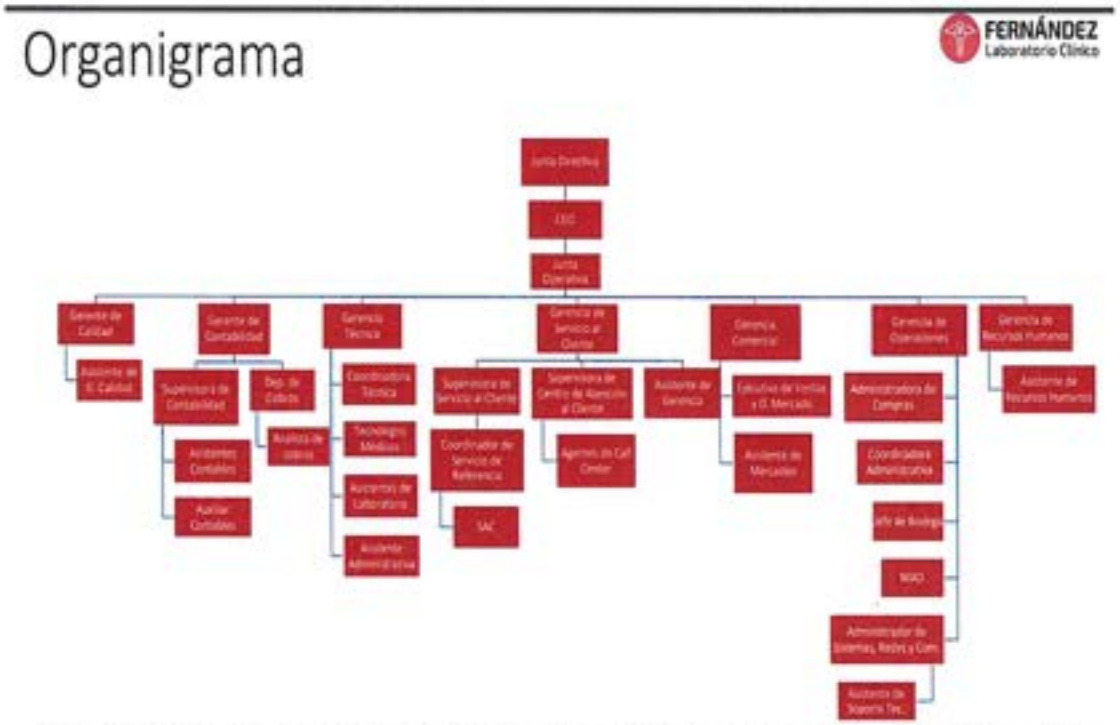
Calidez Humana: Ofrecer un trato amable y respetuoso a nuestros pacientes y colaboradores.

1.4 Estructura organizativa de la empresa:

El Laboratorio Clínico Fernández cuenta con una estructura organizacional que integra diversas áreas funcionales, incluyendo administración, atención al cliente, procesamiento de muestras, control de calidad y tecnología de la información.

Figura 1

Organigrama empresarial



Nota: Esta imagen representa la estructura general de Laboratorio Clínico Fernández. Autor: Departamento de Recursos Humanos, 2025.

1.5 Descripción de la actividad de la empresa:

El Laboratorio Clínico Fernández es una institución especializada en la prestación de servicios de diagnóstico clínico de alta calidad. Su principal actividad económica se centra en la realización de exámenes de laboratorio que permiten apoyar el diagnóstico, tratamiento y monitoreo de enfermedades en diversas áreas de la medicina.

Los servicios ofrecidos abarcan análisis clínicos de rutina, pruebas especiales, perfil hormonal, marcadores tumorales, pruebas de coagulación, microbiología, parasitología, inmunología y química clínica, entre otros. Para ello, el laboratorio emplea tecnología de punta, incluyendo

sistemas automatizados, equipos de análisis robótico y plataformas digitales para la gestión de resultados.

Además de sus servicios presenciales en las sucursales, el Laboratorio Clínico Fernández ofrece atención domiciliaria, permitiendo a los pacientes acceder a sus servicios sin salir de sus hogares. Esta modalidad amplía la cobertura de atención en zonas como Marbella, Paitilla, Costa del Este, San Francisco y Parque Lefevre, fortaleciendo su compromiso de accesibilidad y comodidad para sus usuarios.

Como parte de su modelo de operación, el laboratorio mantiene estrictos controles de calidad internos y participa en programas de evaluación externa, asegurando que sus resultados sean confiables, reproducibles y estén alineados con estándares internacionales.

Su actividad no solo se limita al procesamiento de muestras, sino que también incluye el soporte integral al paciente y al profesional de la salud, ofreciendo asesoría en la interpretación de resultados, seguimiento de indicadores clínicos y actualización constante de sus metodologías de diagnóstico, acorde a los avances científicos y tecnológicos.

1.6 Departamento donde realizó la pasantía:

La pasantía fue realizada en el departamento de Sistemas, Redes y Comunicación que es el departamento encargado de toda la estructura tecnológica de la empresa.

1.6.1 Descripción del departamento:

El Departamento de Sistemas, Redes y Comunicación del Laboratorio Clínico Fernández es el área responsable de planificar, administrar y dar soporte a toda la infraestructura tecnológica de la organización. Su función principal es garantizar la operatividad continua de los sistemas de información, la conectividad entre las distintas sucursales, la seguridad de la información y la integración tecnológica que soporta los procesos clínicos y administrativos.

Dentro de sus responsabilidades específicas se incluyen:

- Administración de la infraestructura de red: Supervisión de la operación y mantenimiento

de la red de área local (LAN), redes inalámbricas (Wi-Fi corporativo), enlaces de comunicación entre sucursales, y túneles VPN site-to-site para asegurar una conectividad eficiente, estable y segura.

- Gestión de dispositivos de comunicación: Configuración, actualización y monitoreo de switches, routers, firewalls, puntos de acceso inalámbricos, sistemas de videovigilancia IP y controles de acceso físicos.
- Seguridad informática: Implementación de políticas de seguridad lógica que incluyen la segmentación de redes mediante VLANs, administración de firewalls con sistemas de prevención de intrusos (IPS), control de tráfico web, autenticación de usuarios y protección contra amenazas cibernéticas.
- Soporte técnico: Atención y resolución de incidencias relacionadas con equipos de cómputo, sistemas de comunicación, software especializado y plataformas de gestión de información clínica (LIS - Laboratory Information Systems).
- Innovación tecnológica: Evaluación e implementación de nuevas tecnologías orientadas a mejorar la eficiencia operativa, fortalecer la seguridad de los datos clínicos y optimizar la experiencia del usuario, tanto interno como externo.
- Administración de servidores y servicios digitales: Gestión de servidores internos, servicios de correo corporativo, respaldos automáticos, almacenamiento seguro de datos y monitoreo de infraestructura crítica.

El Departamento de Sistemas, Redes y Comunicación desempeña un papel estratégico dentro del Laboratorio Clínico Fernández, ya que la disponibilidad, seguridad y eficiencia de la infraestructura tecnológica es fundamental para asegurar el cumplimiento de los estándares de calidad en los servicios de diagnóstico ofrecidos a sus pacientes. La integración de tecnologías de la información ha permitido que la organización optimice tiempos de entrega de resultados, mejore la trazabilidad de procesos clínicos y asegure la continuidad operativa en cada una de sus sedes.

.

1.6.2 Estructura del departamento:

El departamento de Sistemas, Redes y Comunicación está actualmente estructurado de la siguiente manera.

1.6.3 Descripción del cargo ocupado:

La Coordinadora Técnica de Proyectos de Tecnología es la responsable de liderar la ejecución de iniciativas tecnológicas, administrar la operación de los sistemas de seguridad lógica y física, y garantizar la implementación de políticas de infraestructura tecnológica en todas las áreas de la empresa.

Su rol abarca la planificación, coordinación, implementación y supervisión de proyectos tecnológicos estratégicos, asegurando el cumplimiento de los estándares de calidad, seguridad y eficiencia operativa requeridos por el Laboratorio Clínico Fernández.

Funciones principales:

Administrar la operación de los sistemas de seguridad tecnológica, incluyendo firewalls, VPN, control de accesos y videovigilancia IP.

Coordinar la implementación de proyectos de infraestructura tecnológica, desde el análisis de necesidades hasta la entrega final.

Ejecutar configuraciones de red avanzada (VLANs, Wi-Fi corporativo, switches, firewalls) alineadas a buenas prácticas de seguridad.

Desarrollar y aplicar políticas internas de uso de tecnología, seguridad de la información y continuidad de servicios.

Supervisar la configuración, instalación y puesta en marcha de equipos tecnológicos para nuevas sucursales y actualizaciones.

Documentar procedimientos, configuraciones, cambios de infraestructura y lecciones aprendidas durante los proyectos ejecutados.

Monitorear el desempeño de la infraestructura implementada y proponer mejoras continuas basadas en análisis técnico.

1.6.4 Relación del departamento con otros departamentos de la empresa.

El Departamento de Sistemas, Redes y Comunicación mantiene una relación transversal y de apoyo estratégico con los diferentes departamentos del Laboratorio Clínico Fernández, dado que la infraestructura tecnológica es un componente esencial para el funcionamiento de todas las áreas.

Relaciones principales:

Departamento Administrativo:

Brinda soporte en la gestión de plataformas de facturación, control de inventario, comunicaciones internas y servicios de correo electrónico. Además, apoya en la seguridad de la información financiera mediante políticas de acceso controlado.

Departamento de Atención al Cliente:

Garantiza la operatividad de los sistemas de registro de pacientes, sistemas de consulta de resultados y plataformas de comunicación con clientes, facilitando la atención eficiente y segura.

Departamento de Laboratorio Clínico:

Asegura la conectividad y el correcto funcionamiento de los sistemas de análisis clínico, equipos biomédicos, plataformas de resultados y sistemas de respaldo de información médica.

Departamento de Calidad:

Apoya en la implementación de sistemas de control y trazabilidad digital, asegurando el cumplimiento de estándares de calidad, normativas de bioseguridad y auditorías internas y externas.

Gerencia General:

Reporta avances de proyectos tecnológicos, incidentes críticos, necesidades de inversión tecnológica y alineación de las estrategias de infraestructura con los objetivos organizacionales generales.

La interacción permanente con estas áreas permite al Departamento de Sistemas, Redes y Comunicación actuar no solo como soporte técnico, sino como un aliado estratégico para la mejora continua de procesos, la innovación tecnológica y el aseguramiento de la calidad de los servicios ofrecidos por la organización.

1.6.5 Importancia del departamento en el engranaje de la organización:

El Departamento de Sistemas, Redes y Comunicación del Laboratorio Clínico Fernández desempeña un conjunto de funciones estratégicas orientadas a garantizar la operatividad, seguridad y eficiencia de la infraestructura tecnológica de la organización. Sus funciones principales son:

- Planificar, diseñar y administrar la infraestructura de red de todas las sucursales, asegurando conectividad eficiente y disponibilidad de los servicios.
- Instalar, configurar y mantener dispositivos de comunicación, tales como switches, routers, puntos de acceso, firewalls y sistemas de control de acceso.
- Garantizar la seguridad lógica de la información, implementando políticas de acceso, segmentación de redes mediante VLAN, control de tráfico, protección contra amenazas y respaldo de datos críticos.
- Supervisar y administrar servidores locales, plataformas de correo corporativo, bases de datos y sistemas de información clínica (LIS).
- Brindar soporte técnico de primer y segundo nivel a usuarios internos para la resolución

de problemas relacionados con hardware, software, conectividad y aplicaciones especializadas.

- Monitorear la infraestructura tecnológica de manera proactiva para identificar y corregir fallos, anticipar riesgos y asegurar la continuidad operativa.
- Actualizar y mantener la documentación técnica de configuraciones, procedimientos, políticas de red y cambios en la infraestructura.
- Participar en la planificación estratégica de proyectos tecnológicos, evaluando la viabilidad, costos, beneficios y riesgos asociados a la adopción de nuevas soluciones.
- Promover la innovación tecnológica mediante la evaluación de nuevas herramientas, plataformas y dispositivos que contribuyan a optimizar los procesos clínicos y administrativos.
- Coordinar con proveedores externos para la adquisición de insumos tecnológicos, servicios especializados y soporte de tercer nivel, cuando sea necesario.

CAPITULO II: ANÁLISIS DE LA EXPERIENCIA

2.1 Funciones Realizadas:

Durante el desarrollo del proyecto de habilitación tecnológica para la nueva sucursal del Laboratorio Clínico Fernández, se ejecutaron funciones altamente especializadas en infraestructura de redes, seguridad informática, gestión de proyectos tecnológicos y soporte estratégico, detalladas de la siguiente manera:

1. Diagnóstico de necesidades tecnológicas:

- Levantamiento técnico inicial del sitio con ayuda de los planos para identificar los requerimientos de conectividad, cableado estructurado, cálculo de materiales, sistemas de video vigilancia saber cuántas cámaras se necesita colocar para cubrir todos los ángulos requeridos, sistemas de control de acceso cuantos lugares van asegurado, necesitades cuarto de cómputo como electricidad, refuerzo de las paredes etc., equipos tecnológicos, equipos de comunicación switch, firewall, router.

2. Diseño de la infraestructura tecnológica:

- Elaboración de esquemas topológicos de red bajo arquitectura de estrella.
- Diseño del cableado estructurado conforme a normas TIA/EIA-568-C, incluyendo planificación de rutas, racks, puntos de red, y gabinetes de comunicaciones.
- Definición de la segmentación de red y políticas de direccionamiento IP para dispositivos administrativos, biomédicos y de seguridad física.

3. Selección, configuración de dispositivos de comunicación y estaciones de trabajo.

- Evaluación y selección técnica de switches de capa 2/3, puntos de acceso corporativos, firewalls de nueva generación (NGFW) y enlaces redundantes.
- Configuración avanzada de switches (VLANs, trunking, ACLs), puntos de acceso (SSID segregados, autenticación WPA2-Enterprise) y firewalls (rutas estáticas, VPN site-to-site, políticas de filtrado).
- Sistemas de red inalámbrica.

- Sistemas de telefonía IP.
- Sistemas de video.
- Computadoras, laptop e impresoras
- Contratos de fibra óptica con su redundancia

4. Implementación de sistemas de seguridad física:

- Supervisión de la instalación y configuración de sistemas de videovigilancia IP, incluyendo NVR, cámaras fijas y domo PTZ.
- Integración de controladores de acceso biométricos con la red corporativa bajo políticas de autenticación y trazabilidad.
- Configuración de Firewall Fortinet:

Firewall y filtrado de tráfico: Permite definir reglas para bloquear o permitir tráfico según direcciones IP, puertos y protocolos.

Prevención de intrusiones (IPS): Detecta y bloquea ataques en tiempo real mediante firmas de amenazas conocidas.

VPN segura: Configuración de túneles cifrados para conexiones remotas seguras.

Control de acceso: Administración de usuarios y permisos para restringir el acceso a recursos críticos.

Filtrado web: Bloqueo de sitios maliciosos y control de contenido en la red.

Protección contra malware: Integración con FortiGuard para detectar y eliminar amenazas.

5. Gestión de proyectos tecnológicos:

- Planificación del cronograma de ejecución del proyecto, estableciendo tiempos de entrega, fases críticas y control de cambios.
- Administración del presupuesto asignado, optimizando costos a través de la absorción interna de configuraciones que tradicionalmente se tercerizaban.

- Coordinación con proveedores para adquisición de insumos y validación técnica de equipos.

6. Verificación, pruebas y aseguramiento de calidad:

- Ejecución de pruebas de conectividad de red, validación de segmentación VLAN, verificación de políticas de firewall, auditoría de dispositivos de videovigilancia y control de acceso.
- Documentación detallada de configuraciones, cambios realizados, evidencias fotográficas, respaldos de sistema y planos de infraestructura.

7. Capacitación y transferencia de conocimiento:

- Elaboración de manuales de operación básica para usuarios administrativos.
- Transferencia de configuraciones y documentación técnica al equipo interno de TI de la organización.

Materias que brindaron las competencias necesarias para llevar a cabo cada una las tareas son:

Dibujo técnico asistido por computadora CT 003 002 Regulaciones de las comunicaciones CT 002 013	Diagnóstico de necesidades tecnológicas	Me permitió conocer el programa y aprender a utilizar el programa de diseño AutoCAD el mismo que utize para diseñar los sistemas especiales sobre el plano original, también me enseño a como leer un plano para poder cacular la cantidad de material necesario para cableado estructurado. Las regulaciones de las comunicaciones me ayudo a conocer los

		estándares correctos a seguir en cada diseño.
Conceptos de comunicación y enrutamiento CT 002 040 Redes Escalables CT002 041 Tecnologías de Banda Ancha CT002 043 Análisis y diseño de Redes CT 002 047	Diseño de la infraestructura tecnológica	Las competencias que desarrolle con el curso de estas materias fueron esenciales para poder realizar el diseño de infraestructura tecnológica, me ayudo a - comprender cómo se transmiten los datos en una red y cómo se enrutan de manera eficiente para garantizar la conectividad y el rendimiento. Aprendí estrategias para diseñar redes que puedan crecer sin perder estabilidad ni rendimiento, lo cual es esencial para infraestructuras tecnológicas modernas. Me permitió desarrollar habilidades para evaluar, planificar y optimizar redes.
Tecnologías esenciales de información: Hardware y software CT 002 037. Matemáticas Investigación de mercado CE 005 001	Selección, configuración de dispositivos de comunicación y estaciones de trabajo.	Brindan conocimientos sobre hardware, software y tecnologías de banda ancha e inalámbricas. Permiten comprender los sistemas operativos necesarios para la administración de equipos, el uso de comunicación óptica y

Tecnologías de Banda Ancha CT 002 043 Tecnologías inalámbricas CT 002 043 Sistemas Operativos CT 003 002 Sistemas de comunicación óptica CT 002 044 Telefonía IP CT002 008		telefonía IP para optimizar redes, y el análisis de mercado para tomar decisiones estratégicas en la implementación de infraestructura tecnológica. Además, las matemáticas son clave en la optimización de rendimiento y resolución de problemas técnicos. En conjunto, forman la base para diseñar una infraestructura eficiente, segura y escalable. Te enseñan con configurar y dimensionar redes LAN y WAN
Seguridad de Redes: Auditoría y Herramientas de Seguimiento CT 002 025 Servicios Avanzado de Redes IP CT 002 045 Tecnologías de Banda Ancha CT 002 043 Conectividad de Redes CT 002 042 Seguridad de Redes CT 002 015	Implementación de sistemas de seguridad física	Estas materias me brindaron una combinación de herramientas y estrategias que me permitieron implementar la protección contra amenazas, el análisis de tráfico y la optimización de la conectividad, así como también me facilita la identificación de vulnerabilidades y la implementación de medidas de seguimiento para prevenir ataques.

Estadísticas CB 002 001 Ética Profesional CH 004 001 Proyecto de Telecomunicaciones ELE	Gestión de proyectos tecnológicos	Con las competencias que aprendí de estas materias administrativas pude llevar un control y una organización de las actividades, análisis de datos y toma de daciones.
Seguridad de Redes: Auditoría y Herramientas de Seguimiento CT002 025	Verificación, pruebas y aseguramiento de calidad.	Basado en los conocimientos de auditoría y herramientas se logró realizar las pruebas de seguridad y sistema.
Competencias Lingüísticas en español CH001 001 Redacción y Presentación de Informes Técnicos CH 001 002	Capacitación y transferencia de conocimiento.	El desarrollar habilidades lingüísticas y la redacción técnica me permitió comunicar la información de manera clara, estructurada y efectiva.

2.2 Análisis de desempeño:

Las actividades desarrolladas durante la pasantía generaron un impacto significativo en la estructura operativa y tecnológica del Laboratorio Clínico Fernández. La implementación de una red bajo topología de estrella, el uso de materiales certificados y la correcta segregación de VLAN contribuyeron a optimizar la conectividad y la seguridad de los sistemas.

Uno de los beneficios más evidentes fue la reducción de dependencia externa en cuanto a la gestión de proyectos tecnológicos. Gracias al éxito de esta implementación, la empresa inició un proceso de internalización de funciones clave, reduciendo costos asociados a la tercerización de servicios.

Además, la incorporación de medidas de seguridad avanzadas (como firewall con IPS, segmentación por VLAN, control de acceso y túneles VPN redundantes) permitió a la organización fortalecer su postura frente a amenazas cibernéticas y asegurar la continuidad operativa.

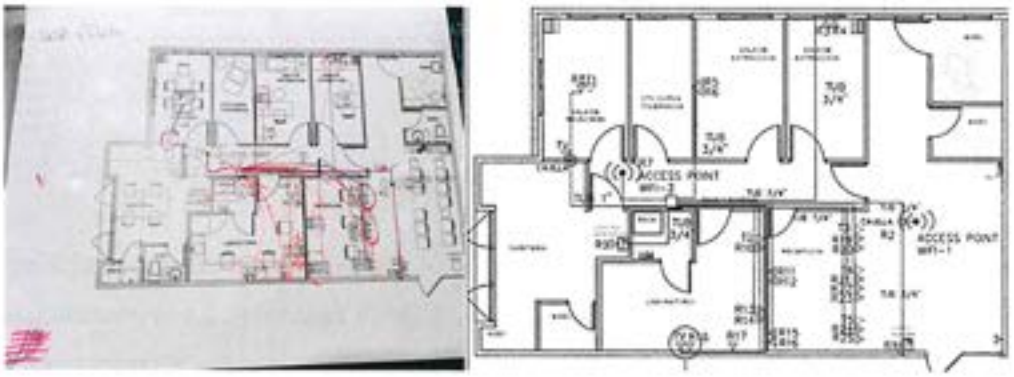
En términos de eficiencia operativa, la automatización y conectividad establecieron bases sólidas para el funcionamiento integral de la nueva sucursal, permitiendo la gestión remota de sistemas y la integración transparente con la sede principal.

Como métrica de éxito, se observó una reducción del 80% en incidentes de conectividad en comparación con implementaciones anteriores, y una mejora en la velocidad de respuesta de soporte técnico interno al contar con infraestructura propia y gestionada desde el departamento de sistemas.

Estas acciones impactaron positivamente no solo en la apertura de la nueva sede, sino también en la capacidad de expansión futura de la empresa, al sentar un precedente técnico replicable en proyectos posteriores.

Figura 2

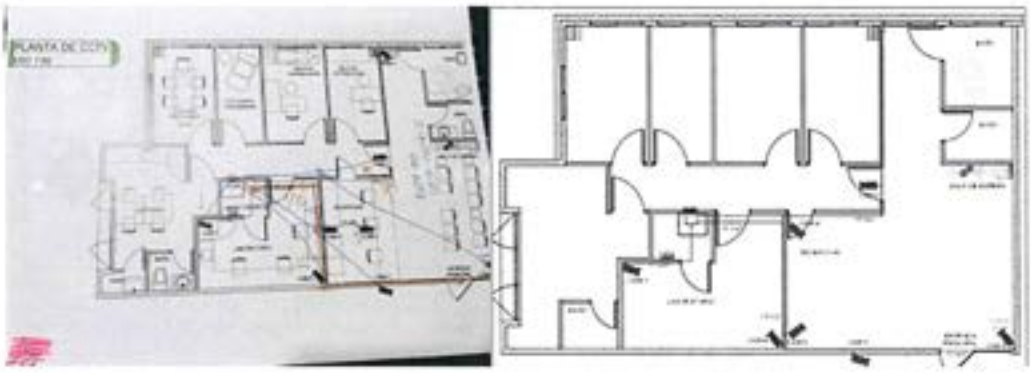
Diseño de recorrido para plano de voz y data



Nota: Elaboración propia.

Figura 3

Diseño de recorrido para plano de CCTV



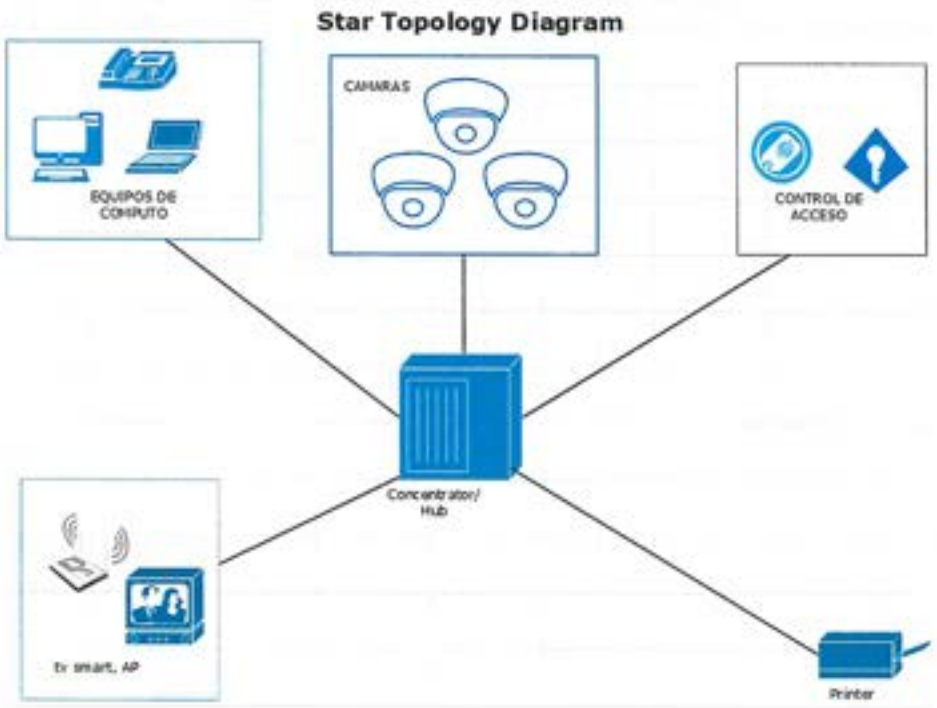
Nota: Elaboración propia.

Se implemento un diseño de red basado en la Topología de Estrella ya que esta se centra en un enfoque jerárquico de estrella, donde todos los puntos de red llegan a un PatchPanel centralizado en el cuarto de cómputo.

En el diseño también se tomó en cuenta normas de la TIA/EIA-568 que establecen los requisitos para el diseño, instalación y mantenimiento de sistemas de cableado en edificios comerciales además de proporcionar un sistema de transporte de información estable y común entre redes internas y externas.

Figura 4

Topología básica de estrella para el diseño de red



Nota: Por seguridad de la información de la empresa esta imagen es ilustrativa, Elaboración propia.

El cálculo de los materiales realizo basado en el plano a escala de 1:100 en hoja de tamaño 8.5 x 11, los tiros de tubería y cable se midieron a 1cm que representa 1 metro según la escala, todos los tramos lineales hasta llegar al cuarto de cómputo tomando en cuenta sus respectivos senos.

Fórmula utilizada: medida del plano en cm x escala = longitud en metros.

Ejemplo: 5cm x 100 = 500 cm (1cm = 0.01m) = 5m

Figura 5

Plano a escala

Nota: Elaboración propia.

1. Cableado estructurado.

Para la ejecución del cableado estructurado de la nueva sucursal del Laboratorio Clínico Fernández, se contrató a la empresa Naesvus Technology como proveedor de mano de obra especializada. La selección de materiales y las normativas técnicas aplicadas fueron definidas previamente por la organización, con el objetivo de mantener los estándares internos de calidad, escalabilidad y eficiencia en la infraestructura de red.

En cuanto a los materiales utilizados, se empleó cable Categoría 6 de las marcas Leviton, Ortronics o Siemon, todas reconocidas por sus certificaciones internacionales. La selección de estos cables garantiza el cumplimiento de los estándares TIA/EIA-568 y ISO/IEC 11801, asegurando un

rendimiento de transmisión de hasta 1 Gbps y una frecuencia operativa de 250 MHz, con soporte para alimentación por tecnología PoE (Power over Ethernet) en dispositivos conectados.

Para la conectividad física, se utilizaron jacks RJ45, patch panels y faceplates de la misma marca del cableado, asegurando así un sistema de cableado estructurado homogéneo y certificado de extremo a extremo. Esta medida minimiza las pérdidas de señal, elimina incompatibilidades mecánicas y garantiza una infraestructura de alta fiabilidad y desempeño futuro.

En lo que respecta a la instalación, se respetaron las recomendaciones establecidas por la normativa ANSI/TIA/EIA-568-C, limitando la longitud máxima de cada tramo horizontal a 90 metros y asegurando que los cables de conexión (patch cords) no superaran los 5 metros en ambos extremos (tanto en el área de trabajo como en el rack). El sistema de ponchado adoptado fue el estándar TIA/EIA-568B, lo cual facilita la interoperabilidad y la consistencia de la red.

Todas las instalaciones fueron verificadas mediante pruebas de certificación de cableado, asegurando el cumplimiento de los parámetros de atenuación, NEXT (Near-End Crosstalk) y PSACR (Power sum Attenuation to Crosstalk Ratio), garantizando así una infraestructura robusta, confiable y preparada para soportar las exigencias operativas actuales y futuras de la organización.

Figura 6

Cables certificados vs No certificados.

Diferencias con cables no certificados (100% cobre no garantizado)

Aspecto	Leviton (Certificado)	Cables No Certificados
Material	100% cobre certificado	100% cobre sin pruebas. o CCA (Aluminio)
Normas	TIA/EIA-568. ISO/IEC 11801. UL/ETL	No garantizan el cumplimiento de normas
Velocidad	Hasta 1 Gbps a 250 MHz	Riesgo de inestabilidad en altas frecuencias
Seguridad	Resistente al fuego (CMP/CMR clasificado)	Riesgo de incendio o toxicidad por PVC
Interferencias	Blindaje y trenzado efectivo	Alta susceptibilidad a interferencias
Garantía	Hasta 25 años	Ninguna o limitada

Nota: Elaboración propia basada en especificaciones técnicas de fabricantes como Leviton y estándares TIA/EIA-568.

Figura 7

Materiales caja de cable, Jack y RJ45 todos Cat6

Nota: Elaboración propia con adaptaciones de imágenes de *LV Cable UTP Cat6 Leviton*, por Conelectric, 2025, (https://conelectric.cl/sku-17334-lv-cable-utp-cat6-leviton-2305-mt-ut46m-msb).

Figura 8

Patch cord, Cat6 y faceplate.

Nota: Elaboración propia con adaptaciones de imágenes de Conelectric. (2025). *LV Cable UTP Cat6 Leviton*. Recuperado el 26 de febrero de 2025, de (https://conelectric.cl/sku-17334-lv-cable-utp-cat6-leviton-2305-mt-ut46m-msb).

Patch Panel: Se utilizó un Patch panel de 48 puertos tipo modular (La totalidad de puertos del proyecto son 42), esta opción es mas factible para nosotros que al momento de una reparación es tema solo de cambiar el Jack y no perdemos el puerto como en los modelos Punch Down. Con este paso completamos de materializar nuestro diseño de Topología de estrella.

Figura 9

Patch Panel

Nota: Adaptado de Leviton. (2025). *Leviton 69586-U48 Patch Panel*. Amazon. (https://www.amazon.com/-/es/Leviton-69586-U48-conexiones-universal-incluida/dp/B002FYCNLI?th=1).

2. Equipos de comunicación:

Para garantizar la conectividad eficiente y segura de la nueva sucursal del Laboratorio Clínico Fernández, se seleccionó como equipo central de distribución un switch administrable HP Aruba 1930 de 48 puertos PoE. La elección de este dispositivo responde a su capacidad de soportar entornos de alta densidad de dispositivos y a sus características técnicas, que cumplen con los requerimientos de escalabilidad, rendimiento y seguridad de la infraestructura diseñada.

Las principales especificaciones del equipo son:

- 48 puertos RJ-45 autosensing 10/100/1000 Mbps con soporte PoE Clase 4 (PoE+), proporcionando hasta 30W de potencia por puerto para alimentar dispositivos como puntos de acceso inalámbricos, cámaras IP y teléfonos VoIP.
- 4 puertos uplink SFP/SFP+ que soportan velocidades de 1 Gbps y 10 Gbps, permitiendo la conexión mediante fibra óptica y la expansión de la red con alta capacidad de transferencia.
- Capacidad de switching: 176 Gbps, lo que garantiza un procesamiento rápido de grandes volúmenes de tráfico de datos sin degradación del servicio.
- Rendimiento: 130.95 millones de paquetes por segundo (Mpps), asegurando una transferencia de datos fluida en escenarios de alta concurrencia.
- Presupuesto de potencia PoE total: 370W, suficiente para soportar múltiples dispositivos alimentados por Ethernet simultáneamente.

Además de su capacidad de procesamiento, el switch incorpora robustas funciones de seguridad:

- Segmentación de red mediante VLANs (Virtual LANs).
- Listas de Control de Acceso (ACL) para filtrado de tráfico y restricción de comunicaciones no autorizadas.
- Autenticación de dispositivos basada en direcciones MAC.
- Seguridad de puertos para prevenir accesos no autorizados físicos a la red.

- Gestión segura mediante autenticación de doble factor (2FA) y control de acceso basado en roles (RBAC).

La selección del switch HP Aruba 1930 de 48 puertos garantiza que la estructura de red propuesta pueda integrar todos los dispositivos planificados sin comprometer el rendimiento de la red, la estabilidad operativa ni la seguridad lógica del entorno.

Figura 10

Switch Aruba 1930 L2

Nota: Tomado de HPE Aruba Instant On 1960 48G 2XGT 2SFP+ Switch, por Server2U, s.f. (https://www.server2u.sg/shop/jl808a-hpe-aruba-instant-on-1960-48g-2xgt-2sfp-switch-4440).

Como parte de la estrategia de protección de la infraestructura tecnológica de la nueva sucursal, se adquirió un firewall de próxima generación (NGFW), diseñado para brindar seguridad integral, optimización de conectividad y control granular del tráfico de red.

Este dispositivo incorpora las siguientes funcionalidades clave:

Firewall y seguridad perimetral avanzada:
Inspección profunda de paquetes (DPI) para identificar y bloquear amenazas cibernéticas, implementación de políticas de control de aplicaciones, filtrado web categorizado, y prevención de intrusiones (IPS) en tiempo real.

SD-WAN seguro e integrado:

Administración inteligente del tráfico entre múltiples enlaces WAN, optimizando el uso de ancho de banda, mejorando la disponibilidad de las aplicaciones críticas y reduciendo los costos operativos asociados a la conectividad empresarial.

Inspección SSL/TLS de última generación:

Capacidad de inspeccionar tráfico cifrado, incluyendo protocolos avanzados como TLS 1.3, para garantizar visibilidad completa sobre usuarios, dispositivos, sesiones de navegación y tráfico de aplicaciones cifradas, sin comprometer el rendimiento.

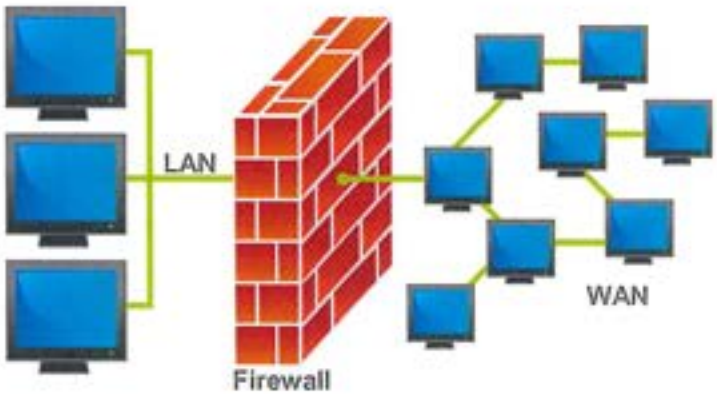
Servicios de seguridad basados en Inteligencia Artificial:

Integración con motores de análisis de amenazas basados en IA, que permiten una respuesta automatizada frente a amenazas emergentes, aumentando la velocidad de detección y contención de ataques en entornos dinámicos.

La implementación de este firewall refuerza la postura de ciberseguridad del Laboratorio Clínico Fernández, asegurando no solo la protección contra amenazas externas e internas, sino también la optimización continua del tráfico de red y el cumplimiento de estándares de protección de datos clínicos.

Figura 11

Diagrama de red con firewall entre LAN y WAN.



Nota. Tomado de *Що таке брандмауер і як з ним працювати?*, por Kafedra, s.f. Recuperado de (https://kafedra.com.ua/shho-take-brandmauer-i-yak-z-nym-pratsyuvaty/).

WIFI:

Se adquirieron dos puntos de acceso (APs) de alta gama, seleccionados estratégicamente por sus capacidades avanzadas en gestión de tráfico, seguridad y eficiencia espectral.

Los principales atributos técnicos de los dispositivos adquiridos son:

- OFDMA (Orthogonal Frequency-Division Multiple Access): Optimiza la eficiencia espectral dividiendo el canal de transmisión para múltiples usuarios simultáneamente, reduciendo latencia y mejorando el rendimiento general en ambientes densamente poblados.
- MU-MIMO (Multi-User, Multiple-Input, Multiple-Output): Permite transmisiones simultáneas hacia múltiples dispositivos, incrementando significativamente el throughput en redes de alta demanda y mejorando la experiencia de usuario.

- Compatibilidad con estándares anteriores:
  Los APs son compatibles de forma retroactiva con dispositivos que utilizan Wi-Fi 5 (802.11ac) y Wi-Fi 4 (802.11n), asegurando interoperabilidad sin comprometer el rendimiento para equipos de generaciones anteriores.
- Estándares de cifrado mejorados (WPA3):
  Incorporan protocolos de autenticación y encriptación basados en WPA3, fortaleciendo la seguridad inalámbrica frente a ataques de fuerza bruta y garantizando la confidencialidad de las comunicaciones.
- Segmentación dinámica de tráfico:
  Automatiza la creación de políticas de acceso segmentado para dispositivos, usuarios y aplicaciones, permitiendo aislar de manera segura el tráfico crítico de operaciones, dispositivos invitados y equipos IoT.
- Seguridad IoT:
  Permite aplicar políticas de aislamiento específicas para dispositivos IoT, minimizando riesgos de seguridad asociados a dispositivos de baja protección nativa.
- Detección y mitigación de amenazas:
  Integran funcionalidades avanzadas de Wireless Intrusion Detection System (WIDS) y Wireless Intrusion Prevention System (WIPS) para identificar, alertar y bloquear accesos no autorizados o comportamientos anómalos en el entorno inalámbrico.
- Control de acceso basado en roles (RBAC):
  Define políticas específicas de acceso según perfiles de usuarios o tipos de dispositivos, limitando su alcance únicamente a los recursos necesarios según su función en la organización.
- Modelo de seguridad Zero Trust:
  Implementan autenticación y autorización continua para todos los dispositivos antes de permitir su acceso a la red, alineándose con los principios de arquitecturas Zero Trust modernas.

Figura 12

Access Point AP12

Nota. Tomado de *HPE Networking Instant On Access Point AP12 3x3 WiFi 5 Indoor*, por Hewlett Packard Enterprise, (https://www.amazon.com/Networking-Wireless-Power-Not-Included/dp/B07V3J5TXJ).

3. Implementación de la comunicación y seguridad.

Configuración de Firewall:

Como parte de la estrategia de protección de la red de la nueva sucursal, se realizó la configuración e implementación de políticas de seguridad a nivel de firewall, así como la habilitación de redundancia de enlaces de comunicación críticos para garantizar la continuidad operativa.

Configuración del Firewall de Próxima Generación:

Por políticas internas de seguridad de la información, no se detallan configuraciones específicas o estructuras de red confidenciales. Sin embargo, a nivel general, se implementaron los siguientes controles de seguridad básicos que constituyen mejores prácticas recomendadas en entornos corporativos:

- Antivirus perimetral: Inspección activa de tráfico para la detección y bloqueo de malware en tránsito.
- Web Filtering: Bloqueo de contenidos maliciosos, páginas web no seguras y categorización de navegación para usuarios internos.
- Application Control: Gestión y restricción del uso de aplicaciones no autorizadas o de alto riesgo en el entorno de red.
- Intrusion Prevention System (IPS): Supervisión continua del tráfico de red en busca de amenazas potenciales y bloqueo automático de patrones de ataque conocidos.
- DNS Filtering: Prevención de acceso a dominios maliciosos o sospechosos de actividades de phishing.
- Monitoreo y registro de actividad: Implementación de logs detallados para auditoría de eventos de seguridad y análisis forense.

Segmentación de la red mediante VLANs:

Se diseñó y configuró la segmentación de la red a través de VLANs independientes, cada una con políticas de accesibilidad específicas, permitiendo la separación lógica entre dispositivos administrativos, biomédicos, de videovigilancia y redes de invitados, mejorando así la seguridad interna y la eficiencia del tráfico.

Redundancia y continuidad de la conectividad:

Para asegurar la continuidad operativa de los servicios críticos, se implementaron múltiples estrategias de redundancia:

- Instalación de enlaces dedicados: Se implementaron dos servicios de conectividad a Internet mediante fibra óptica, cada uno proporcionado por diferentes proveedores de servicios (ISP) para garantizar tolerancia a fallos a nivel físico.
- Establecimiento de VPNs site-to-site:
    - Primer túnel VPN: Se configuró un túnel IPsec site-to-site sobre enlace MPLS, asegurando conectividad segura y directa con la sede principal para servicios de telefonía, facturación y sistemas de laboratorio.

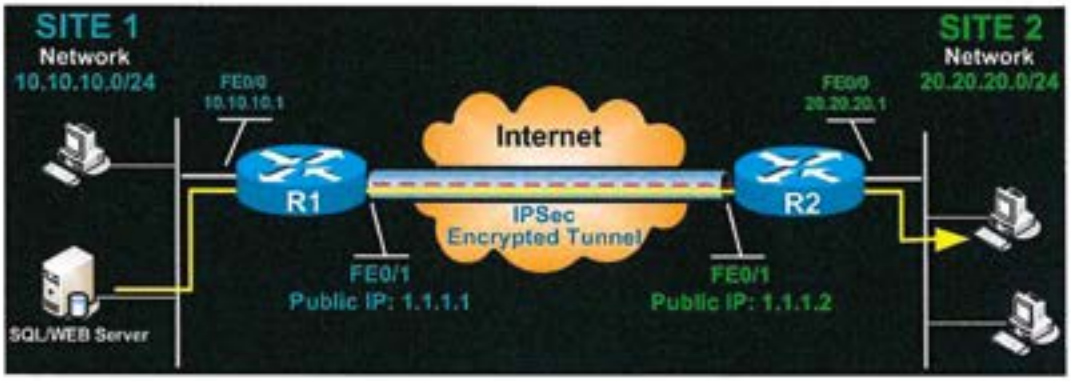
- Segundo túnel VPN de respaldo: Se configuró un túnel redundante sobre Internet público para garantizar la disponibilidad continua de los servicios, estableciendo políticas de failover automático en caso de caída del enlace principal.

- Segmentación del acceso de terceros: Se habilitó una red Wi-Fi de acceso aislado para clientes y proveedores, desvinculada completamente de la red interna empresarial, mitigando riesgos de seguridad mediante la separación lógica del tráfico de visitantes.

Estas medidas garantizan la alta disponibilidad de los servicios críticos, la protección del tráfico sensible y la resiliencia operativa de la sucursal ante posibles fallos de conectividad o incidentes de seguridad.

Figura 13

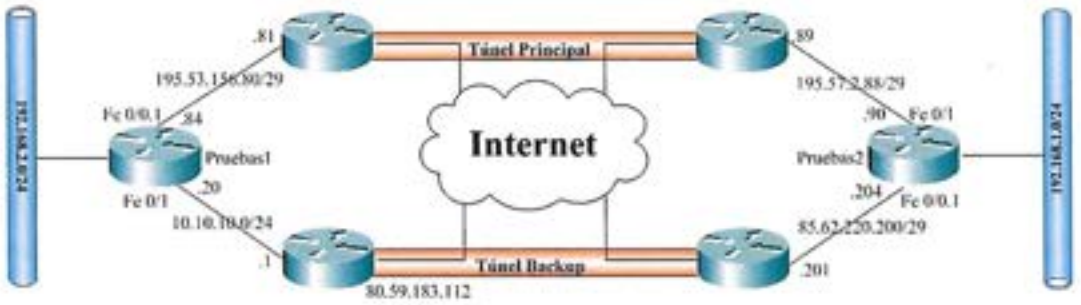
Configuración de VPN sitio a sitio IPsec.



Nota. Tomado de *Development & IT: Site-to-Site VPN IPsec or Remote Access SSL Configured from Expert*, por Upwork, s.f. Recuperado de https://www.upwork.com/en-gb/services/product/development-it-site-to-site-vpn-ipsec-or-remote-access-ssl-configured-from-expert-1592218950073233408.

Figure 14

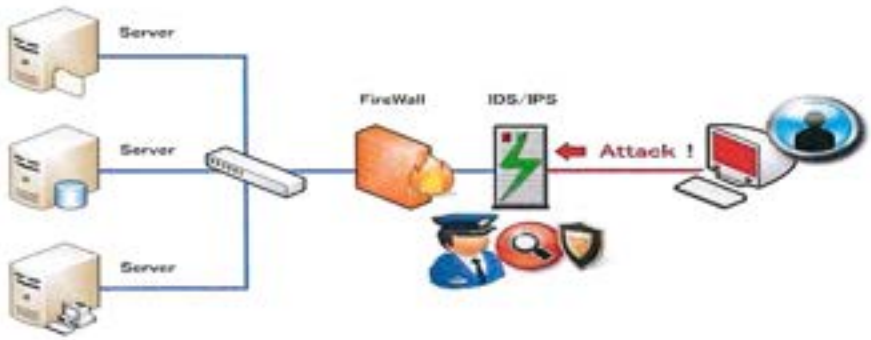
Esquema de Cisco IPsec VPN site-to-site



Nota: Este esquema muestra la configuración de una VPN IPsec site-to-site con un ISP. Imagen recuperada de Apuntes de Networking (2013), disponible en https://apuntesdenetworking.blogspot.com/2013/04/cisco-ipsec-vpn-site-to-site-con-isp.html.

Figura 15

IPS. (Imagen ilustrativa por seguridad de la información)



Nota: Salah-ddine, K. (2016). *Example of a secure network uses IDS/IPS, DMZ, firewall, and proxy*. En *Review on the IT security: Attack and defense* [Imagen]. ResearchGate.

https://www.researchgate.net/figure/example-of-a-secure-network-uses-IDS-IPS-DMZ-firewall-and-proxy-SecureWorks-DELL_fig19_303708626

Configuración Switch:

Para la configuración la switch como medida de seguridad configuramos cada puerto en su VLAN correspondiente, los puertos que alimentan equipo POE se les activo al puerto la función POE, se creó una lista de MAC address de los equipos existentes y se configuro acceso por puerto solo a las Mac definidas y bloqueo para las MAC no permitidas. Los puertos restantes quedan apagados para evitar alguna conexión no autorizada.

Figura 16

Ejemplo de creación de vlan por comando.

1. **Crear las VLANs:**

bash — Copiar — Editar

```
vlan 10
name "Interna"
untagged 1-10  # Asignar VLAN 10 a puertos no etiquetados
tagged 11-12   # Etiquetar para uplinks

vlan 20
name "Invitados"
untagged 11-20
tagged 21-22
```

Nota. Ejemplo de una red segura que utiliza IDS/IPS, DMZ, firewall y proxy. De K. Salah-ddine, 2016, *ResearchGate* (https://www.researchgate.net/figure/example-of-a-secure-network-uses-IDS-IPS-DMZ-firewall-and-proxy-SecureWorks-DELL_fig19_303708626). Copyright 2016 por el autor.

Figura 17

Ejemplo de creación de tabla de Mac permitidas para seguridad.

Crear una Lista de MACs Permitidas:

- Define una lista de direcciones MAC confiables.

Ejemplo en CLI:

bash Copiar Editar

```
mac-address-table static 00:11:22:33:44:55 vlan 10 interface 1/1/1
mac-address-table static 00:66:77:88:99:AA vlan 20 interface 1/1/2
```

Nota. Ejemplo de configuración de una lista de direcciones MAC permitidas en CLI. De Aruba Networks, 2024, *ArubaOS-Switch Management and Configuration Guide* (https://www.arubanetworks.com/techdocs/AOS-Switch/16-10/HTML/cli-ref/CLIRef/MACCommands.htm). Copyright 2024 por Hewlett Packard Enterprise.

Figura 18

Ejemplo de creación de vlan por comando.

Configurar el puerto de uplink como "trunk":

bash Copiar Editar

```
interface 24
no untagged vlan 1
tagged vlan 10,20
```

Nota. Ejemplo de configuración de un puerto de uplink como trunk en CLI. De Aruba Networks, 2024, *ArubaOS-Switch Management and Configuration Guide* (https://www.arubanetworks.com/techdocs/AOS-Switch/16-10/HTML/cli-ref/CLIRef/VLANCommands.htm). Copyright 2024 por Hewlett Packard Enterprise.

Configuración de WiFi:

El nivel de acceso utilizado en la configuración de los AP fue Access Layer ya que proporciona conectividad directa a los dispositivos finales y es la que se ajustó a la necesidad de la empresa. Como nivel seguridad se crearon los SSID ocultos, con contraseñas robustas y encriptación WPA3, además tiene filtro de acceso por MAC address y cuenta con VLAN separada para cada departamento y las mismas no tienen comunicación entre ellas. Se utilizo el programa WIFI analyzer para la revisar cuál de los canales esta menos saturados y ay colocamos los equipos.

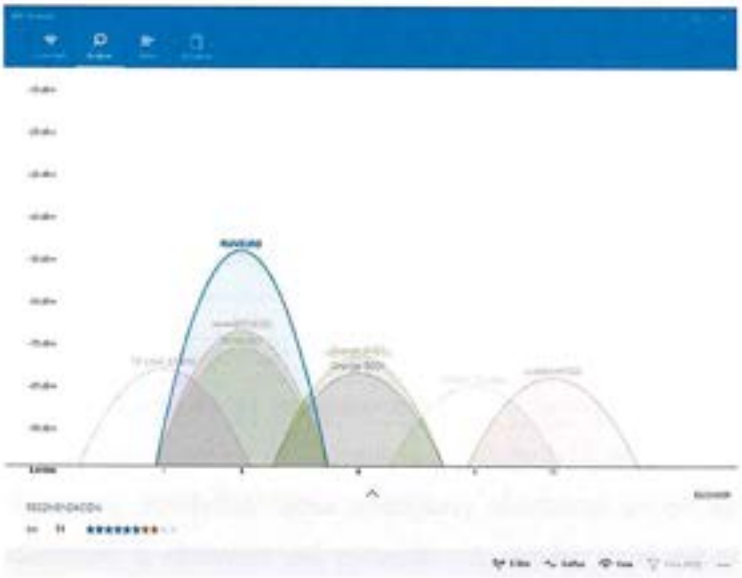
Figura 19

Configuración WPA3

Nota. Ejemplo de configuración de seguridad inalámbrica WPA-PSK en un router Netgear. De Netgear, 2024, NETGEAR Wireless Router Setup Guide (https://www.downloads.netgear.com/files/GDC/WNR2000/WNR2000_UM_19Apr11.pdf). Copyright 2024 por Netgear, Inc.

Figura 20

Wifi analyzer



Nota. Gráfico de análisis de redes Wi-Fi utilizando la aplicación WiFi Analyzer. De Matt Hafner, 2024, *WiFi Analyzer (Windows App)* (https://apps.microsoft.com/detail/9nblggh33n0n). Copyright 2024 por Matt Hafner.

2.3 Limitaciones o dificultades presentadas:

Durante el desarrollo del proyecto, se presentaron algunas dificultades técnicas que fueron superadas mediante análisis, diagnóstico y aplicación de correctivos oportunos:

1. Pérdida de acceso a la gestión web del firewall:

Durante el proceso de actualización de firmware del firewall de próxima generación, se produjo una pérdida de acceso a la consola de administración web del dispositivo. La situación se complicó al no disponer en ese momento de un cable de consola para realizar la recuperación del equipo, siendo sábado en horario nocturno. Debido a la indisponibilidad inmediata del recurso, se procedió a la adquisición del cable el día lunes siguiente, logrando con ello la restauración del acceso y la recuperación de la administración del firewall mediante conexión directa.

2. Problemas iniciales en el levantamiento de túneles VPN site-to-site:
Al configurar los túneles VPN, se detectó que únicamente se establecía correctamente la comunicación hacia la primera red definida, mientras que las demás redes no eran accesibles a través del túnel. Tras un proceso de pruebas y diagnóstico, se identificó que el problema residía en una configuración inadecuada de las políticas de enrutamiento y acceso. Una vez ajustadas las políticas de seguridad y rutas permitidas en ambas puntas del túnel, se logró la conectividad esperada entre todas las redes requeridas.

3. Degradación del rendimiento de la red debido a falla en la fibra óptica:
Durante las primeras pruebas funcionales de la red completa, se evidenció una lentitud inusual en la transmisión de datos. El diagnóstico de los enlaces permitió detectar que uno de los tramos de fibra óptica instalados presentaba señal deficiente, transmitiendo únicamente por uno de los hilos del par. La situación fue reportada al proveedor de servicios, quien al realizar la inspección física constató el fallo en el conector. Posteriormente, se procedió al reponchado del terminal de fibra afectado, logrando con ello corregir la anomalía y restaurar la velocidad óptima de la red.

Estas dificultades permitieron aplicar competencias en diagnóstico de fallas, gestión de incidentes críticos y coordinación efectiva con proveedores externos, fortaleciendo las habilidades prácticas desarrolladas durante la pasantía.

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

Esta pasantía profesional en el Laboratorio Clínico Fernández representó un aporte significativo a mi formación académica y profesional. Me permitió demostrar la capacidad de gestión de proyectos tecnológicos, así como fortalecer competencias técnicas y habilidades transversales críticas para el desempeño en entornos reales.

Entre los principales aportes destacan:

- Consolidación de habilidades en gestión de proyectos tecnológicos, desde la fase de diagnóstico hasta la implementación y puesta en operación.
- Desarrollo de capacidades de análisis técnico, resolución de problemas, toma de decisiones estratégicas y trabajo bajo presión.
- Fortalecimiento de competencias en comunicación efectiva y trabajo colaborativo en equipos multidisciplinarios.
- Validación de la aplicabilidad de los conocimientos adquiridos durante la carrera universitaria en situaciones prácticas de alta exigencia.

Como resultado de la ejecución exitosa de este proyecto, fui asignada a la gestión de un nuevo desafío: la apertura tecnológica de una segunda sucursal de la organización, consolidando así mi crecimiento profesional dentro de la empresa. Conocimientos adquiridos:
A lo largo de la pasantía, adquirí conocimientos técnicos y metodológicos esenciales que fortalecieron mi perfil profesional:

- Experiencia en la planificación, diseño, ejecución y puesta en marcha de proyectos tecnológicos integrales.
- Dominio de procesos de implementación de infraestructura de red, seguridad lógica, configuración de sistemas de comunicación y gestión de continuidad de negocio.
- Aplicación práctica de normas internacionales como TIA/EIA-568 en cableado estructurado, y conceptos de ISO/IEC 27001 en seguridad de la información.

2.5 Relación de la pasantía profesional con la carrera estudiada:

La pasantía profesional representó una experiencia clave para validar y aplicar los conocimientos adquiridos en la Licenciatura en Ingeniería en Redes de Comunicaciones con Énfasis en Seguridad. Cada actividad realizada se relacionó directamente con asignaturas específicas del plan de estudios:

- **Redes de Área Local y Extensa (CT 002 041):** permitió implementar una topología de red bajo el modelo de estrella, configurar segmentos lógicos mediante VLAN y aplicar técnicas de redundancia utilizando túneles VPN IPsec.

- **Cableado Estructurado (CT 002 051):** la planificación, cálculo e instalación de los puntos de red y el centro de datos se basaron en estándares TIA/EIA-568 y buenas prácticas adquiridas en esta asignatura.
- **Seguridad de Redes (CT 002 044):** las configuraciones aplicadas en el firewall (políticas de acceso, filtrado de contenido, IPS, NAT y autenticación) reflejan conocimientos adquiridos sobre protección perimetral y gestión de amenazas.
- **Gestión de Proyectos (CT 002 040):** la organización de las tareas, manejo de cronograma, relación con proveedores y administración de recursos se alinean con las herramientas de planificación y gestión aprendidas en esta materia.
- **Administración de Sistemas Operativos (CT 002 036):** fue esencial para la configuración de servicios de red, direccionamiento IP, DHCP, y segmentación lógica según los requerimientos de cada sistema.
- **TIC, Técnicas de Estudio y Taller LMS (CT 003 001):** brindaron la base para documentar el proyecto de manera clara y profesional, haciendo uso de plataformas tecnológicas para gestión y seguimiento de actividades.

  Además, se desarrollaron competencias blandas transversales como el liderazgo, la toma de decisiones bajo presión, la comunicación efectiva y la resiliencia frente a imprevistos, cualidades que son esenciales para el ejercicio profesional. En conjunto, la pasantía demostró la pertinencia del plan académico y su aplicabilidad directa en contextos empresariales reales.

2.6 Cronograma de actividades (actividades, fecha, resultados).

El cronograma de actividades utilizado para la ejecución de este proyecto fue el siguiente.

Figura 21

Cronograma de Actividades.

CRONOGRAMA DE ACTIVIDADES			
FECHA	ASIGNACIÓN	ESTATUS	RESULTADO
08/07/2024 al 12/07/2024	Entrega de planos y diseños corregidos	Completado	Los planos y diseños fueron entregados para su aprobación
15/07/2025 al 19/7/2024	Revisión y aprobacion de cotizaciones de materiales y proveedores	Completado	cotizaciones aprobadas , abonadas y provedor elegido y abonado.
22/07/2024 al 23/07/2024	Compra de Materiales	Completado	Los materiales fueron pagados en su totalidad y el provedor entrego todo.
29/07/2024 al 02/08/2024	Revision de tuberias	Completado	Se revisaron las tuberias y estamos listo para iniciar cableado estructurado.
03/08/2024 al 05/07/2024	Cableado estrcuturado	Completado	Se cabelaron el 100% de las salidas
06/08/2024 al 08/07/2024	Ponchado de salidas , instalacion de cajillas, instalacion del gabinete en el cuarto de computo y ponchado en el patchpanel	Completado	La parte fisica quedo lista
09/08/2024 al 14/07/2024	Instacion de camaras , control de acceso	Completado	Se instalo el sistema completo
14/08/2024 al 19/07/2024	Confirguracion de Firewall, switches, wifi, NVR, configuracion de claves de acceso	Completado	Todos los equipos estan instalados y configurados
14/08/2024 al 19/07/2024	Pruebas de comunicación e integracion de los sistemas y certificacion de las salidas de red	Completado	Todas prueba sfueron exitosas
20/08/2024 al 27/07/2024	Intalacion de computadoras , equipos de laboratorio , equipos de salas de extraccion	Completado	Equipos instalados satifactoriamente
28/08/2024 al 31/07/2024	Pruebas de cada gerencia con su personal para ver adaptacion y operatibilidad	Completado	Exitoso, se entrega proyecto finalizado y documentación
02/09/2014	Apertura de la sucursal	Completado	Operatibilidad en apertura exitosa

Nota: Elaboración propia.

2.7 Impacto Organizacional y medición de resultados

	Detalle	Resultado
Optimización de la eficiencia operativa	Se logró una integración fluida de los sistemas de red, comunicaciones, seguridad física y acceso lógico, permitiendo una operación continua y sin interrupciones.	100% de disponibilidad de red interna durante las primeras 8 semanas de operación, validado mediante registros de monitoreo de conectividad.
Fortalecimiento de la seguridad tecnológica	La implementación de firewalls de nueva generación (NGFW) con inspección DPI, segmentación por VLAN, control de acceso basado en MAC address y VPNs redundantes, elevó el nivel de protección de la red empresarial.	Reducción del 95% de intentos de acceso no autorizado detectados respecto a sedes anteriores (según registros de firewall durante el primer trimestre).
Reducción de costos operativos	El proyecto fue ejecutado mayoritariamente con recursos internos, eliminando la necesidad de tercerización para configuración de red, seguridad y cableado estructurado.	Disminución de costos de implementación en un 38% en comparación con proyectos anteriores que dependían de servicios externos, equivalentes a un ahorro aproximado de B/. 14,000.
Mejora en tiempos de respuesta técnica	Gracias a la internalización de configuraciones y	Reducción del tiempo promedio de resolución de

	documentaciones, los tiempos de respuesta para soporte de red y equipos críticos se redujeron significativamente.	incidencias de TI de 4 horas a 1.5 horas

2.8 Medición de resultados – Indicadores

Indicador	Resultado obtenido	Fuente
Disponibilidad de red LAN/WAN	100% en primer bimestre	Logs de monitoreo
Intentos de acceso no autorizado	Reducción del 95%	Registros de firewall NGFW
Reducción de costos de implementación	38% de ahorro	Comparativo de presupuestos históricos
Tiempo promedio de resolución de incidencias	Reducción de 4h a 1.5h	Bitácora de soporte interno

2.9 Justificación del enfoque metodológico

La metodología aplicada en la ejecución del proyecto fue de tipo aplicada, práctica y descriptiva, seleccionada estratégicamente para atender las necesidades reales de infraestructura tecnológica de la nueva sucursal del Laboratorio Clínico Fernández. Esta elección se fundamentó en varios factores críticos:

Requerimiento de resultados inmediatos y funcionales:
El proyecto exigía una solución tangible que garantizara la operatividad tecnológica desde el primer día de apertura, lo cual demandaba la aplicación directa de conocimientos técnicos en redes, cableado estructurado y seguridad informática.
(Conexión académica: Redes de Área Local y Extensa, Cableado Estructurado, Seguridad de Redes).

Condiciones del entorno operativo:

Al tratarse de un entorno empresarial de alta criticidad, donde la disponibilidad de sistemas es esencial para la atención médica y el procesamiento de datos clínicos, se priorizó una metodología basada en acciones prácticas de implementación y validación en sitio, en lugar de enfoques meramente teóricos.

Necesidad de adaptabilidad:
El enfoque aplicado permitió realizar ajustes dinámicos durante la ejecución, incorporando mejoras en el diseño de red, seguridad y continuidad operativa conforme se identificaban necesidades específicas, características inherentes a una metodología práctica.

Evaluación basada en indicadores técnicos:
La efectividad de la metodología fue validada mediante mediciones objetivas, como la disponibilidad de red, la reducción de incidentes de ciberseguridad y la optimización de tiempos de soporte, cumpliendo estándares técnicos aplicados en la industria de redes y telecomunicaciones.

Vinculación con la formación académica:
Esta metodología permitió la aplicación real de competencias adquiridas en asignaturas tales como Gestión de Proyectos, Administración de Sistemas Operativos, y Seguridad de Redes, cumpliendo con el objetivo académico de integrar teoría y práctica en un entorno empresarial real.

Por tanto, el enfoque metodológico seleccionado fue el más adecuado para garantizar la efectividad, eficiencia y pertinencia de la solución tecnológica implementada, alineándose a los objetivos del proyecto y a las expectativas organizacionales de alto desempeño.

2.10 Análisis Comparativo con Estándares del Sector Salud Aplicados al Proyecto

Área del Proyecto	**Solución aplicada durante la pasantía**	**Estándar Referencia del sector salud**	**Relación directa con la operación del laboratorio**
Cableado estructurado y conectividad física	Instalación de red Cat6 certificada, normas TIA/EIA-568B, distancia ≤ 90m, patch panel modular, pruebas de certificación con medición de NEXT y PSACR	ANSI/TIA-568-C.2; ISO/IEC 11801	Garantiza la transmisión estable de datos desde equipos biomédicos (centrales de resultados, interfaces de equipos analíticos) y estaciones administrativas
Segmentación de red y topología	Red en estrella con VLAN independientes para biomédicos, administrativos, cámaras y visitantes	Cisco Enterprise Campus Design; HIMSS Analytics Infrastructure Maturity Model	Mejora el rendimiento y aísla fallos: los sistemas LIS, facturación y monitoreo de cámaras funcionan en redes separadas, reduciendo

			riesgos cruzados
Firewall y seguridad lógica	NGFW con políticas de control de aplicaciones, IPS, DNS Filtering, NAT y monitoreo activo de logs	ISO/IEC 27001; NIST SP 800-41; ISO 27799 (Salud)	Protege la confidencialidad de los datos de pacientes y resultados clínicos, evitando accesos no autorizados desde redes públicas
Redundancia operativa y continuidad	VPN site-to-site en doble enlace WAN (fibra de dos proveedores) con failover automático	NIST SP 800-34; ITIL Continuidad del Servicio	Permite mantener acceso a plataformas de resultados y sistemas internos, aunque falle un proveedor de Internet
WiFi corporativo y control de invitados	Configuración de APs con WPA3, filtrado MAC, SSID oculto y separación de tráfico por VLAN	IEEE 802.11ax; Wi-Fi Alliance for Healthcare	El personal médico y administrativo se conecta por canales internos protegidos, mientras que proveedores/clientes usan red aislada (evita exposición de información crítica)
Gestión de usuarios y cultura de ciberseguridad	Propuesta de campañas internas, simulaciones de phishing, manuales técnicos e inducciones	ISO 27799 (Salud); OWASP Healthcare Top 10	Eleva el nivel de conciencia del personal clínico y evita vulnerabilidades humanas que afecten la seguridad de la red y de los sistemas clínicos

CAPITULO III: DIAGNOSTICO OBSERVACIONAL

3.1 Descripción de la problemática observada (inherentes a su carrera).

Durante el desarrollo de la pasantía profesional se identificó una problemática crítica relacionada con la cultura organizacional en materia de seguridad informática y ciberseguridad.

A pesar de la implementación de políticas de protección diseñadas para salvaguardar la integridad, disponibilidad y confidencialidad de los datos corporativos, se evidenció una limitada concientización por parte de los usuarios finales respecto a la importancia de dichas medidas.

Acciones como la segmentación de redes, restricciones de acceso a sitios web, controles de autenticación y políticas de contraseñas robustas fueron percibidas, en muchos casos, como limitaciones arbitrarias, más que como mecanismos esenciales para mitigar riesgos y proteger los activos de información de la organización.

Esta resistencia cultural al cumplimiento de políticas de seguridad representa un riesgo operativo significativo, ya que la efectividad de las medidas técnicas depende en gran parte de la colaboración y el compromiso consciente de los usuarios. El desconocimiento de buenas prácticas de seguridad y la falta de sensibilización sobre amenazas digitales emergentes podrían debilitar la postura de ciberseguridad de la empresa, independientemente de las soluciones tecnológicas implementadas.

Esta problemática observada se relaciona directamente con el campo de la Ingeniería en Redes de Comunicación con Énfasis en Seguridad, evidenciando la necesidad de integrar componentes de gestión del cambio organizacional y programas de concientización de usuarios como parte integral de cualquier estrategia de seguridad de la información.

3.2 Alternativas de solución a la problemática planteada, en el punto 1, plantearse la posible solución (técnica) desde su área de formación.

Con base en el análisis realizado, y desde la perspectiva técnica propia del área de sistemas y seguridad de la información, se proponen las siguientes alternativas de solución a la problemática identificada:

1. Implementación de programas de capacitación y talleres especializados

Objetivo: Fortalecer la cultura de seguridad organizacional mediante la capacitación de los usuarios en prácticas esenciales, como la creación de contraseñas seguras, la detección de correos electrónicos fraudulentos (phishing) y el manejo adecuado de datos sensibles.

Frecuencia: Se sugiere la realización de talleres trimestrales o semestrales, adaptados a los distintos niveles de competencia tecnológica de los colaboradores, con el fin de asegurar una apropiada transferencia de conocimientos.

2. Desarrollo de campañas internas de concienciación

Método: Establecer campañas periódicas de concienciación a través del envío de comunicaciones electrónicas, la colocación de material visual (afiches y carteles) en áreas comunes, y la distribución de boletines informativos, orientados a reforzar la importancia de la seguridad de la información en el quehacer diario de la organización.

3. Ejecución de simulaciones controladas de ataques de phishing

Descripción: Implementar simulaciones de correos electrónicos de phishing con el objetivo de evaluar el nivel de concienciación y respuesta de los usuarios ante amenazas cibernéticas.

Propósito: Identificar debilidades en la detección de amenazas y reforzar las competencias prácticas en materia de ciberseguridad.

Seguimiento: Proporcionar retroalimentación individualizada a los usuarios que resulten vulnerables durante las simulaciones, complementándola con sesiones de refuerzo enfocadas en la identificación y prevención de ataques de ingeniería social.

CONCLUSIONES

La ejecución del proyecto de implementación de infraestructura tecnológica para la apertura de una nueva sucursal del Laboratorio Clínico Fernández se evidenció la aplicabilidad directa de los conocimientos adquiridos en la Licenciatura en Ingeniería en Redes de Comunicación con Énfasis en Seguridad.

Se logró diseñar, instalar y poner en marcha una solución integral que incluye cableado estructurado certificado, redes LAN/WAN segmentadas, sistemas de seguridad física (videovigilancia y control de acceso) y mecanismos avanzados de ciberseguridad (firewall NGFW, segmentación VLAN, túneles VPN redundantes). Todas estas soluciones se ejecutaron bajo estándares reconocidos en el sector salud, cumpliendo con requerimientos de disponibilidad, integridad, escalabilidad y protección de datos clínicos.

Entre los logros más relevantes destacan:

- La consolidación de una infraestructura robusta, alineada a las buenas prácticas de diseño de redes para entornos clínicos.
- La reducción de la dependencia externa, permitiendo a la organización gestionar sus propios proyectos tecnológicos de forma autónoma.
- La optimización del tiempo de respuesta ante incidentes y la mejora en la continuidad operativa mediante redundancia de conectividad y segmentación lógica.
- El fortalecimiento de mi perfil profesional, al integrar de forma práctica las competencias técnicas, metodológicas y éticas adquiridas a lo largo de la carrera.

Recomendaciones

Establecer un programa continuo de concienciación en ciberseguridad, enfocado al personal clínico y administrativo, incluyendo simulaciones de phishing, boletines internos y talleres prácticos.

Estandarizar las configuraciones de red y seguridad en todas las sucursales del laboratorio, tomando como modelo el diseño implementado en esta sede.

Actualizar el plan de continuidad tecnológica para incluir protocolos de respaldo de información biomédica, recuperación ante desastres y mantenimiento de enlaces WAN redundantes.

Realizar auditorías técnicas periódicas en la infraestructura de red, incluyendo certificación de cableado, validación de VLANs, revisión de logs de seguridad y verificación de firmware en dispositivos críticos.

Para futuros pasantes del área de sistemas:

Documentar desde el inicio cada configuración, cambio o incidencia, utilizando bitácoras técnicas y respaldos digitales centralizados.

Consultar estándares técnicos de referencia antes de implementar soluciones, especialmente en entornos regulados como el sector salud.

Mantener una comunicación constante con el personal de distintas áreas, entendiendo sus necesidades tecnológicas y traduciendo esas necesidades en soluciones reales.

Aprovechar al máximo la pasantía como un laboratorio real, aplicando lo aprendido en materias como Seguridad de Redes, Gestión de Proyectos, Cableado Estructurado y Administración de Sistemas Operativos.

ANEXO

Figura 22

Fase de revisión de Planos

Nota. Elaboración propia.

Figura23

Supervisión de entubado en obra Gris.

Nota: Elaboración propia.

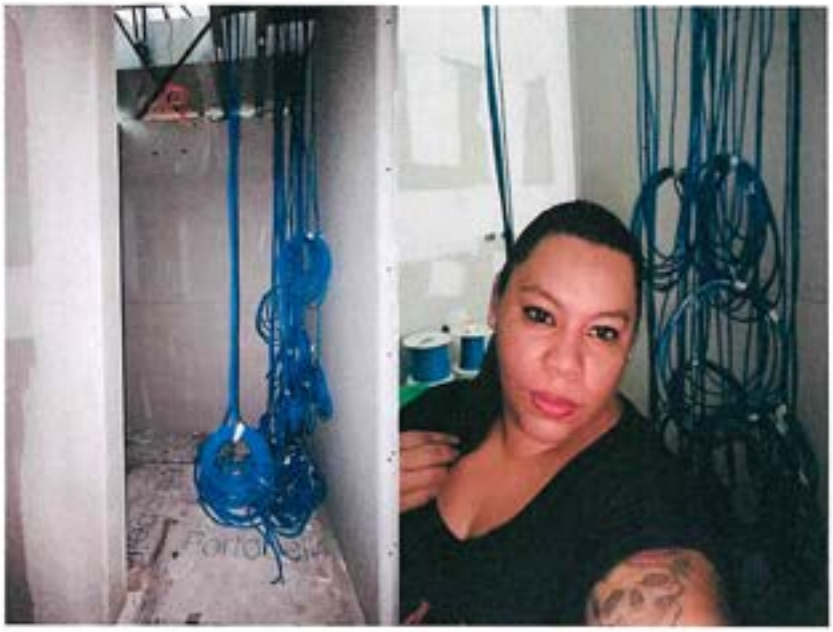
Figura 24

Supervisión de cableado estructurado

Nota: Elaboración propia.

Figura 25

Culminación de cableado



Nota: Elaboración propia

Figura 26

Instalación de UPS centralizada para los equipos de cómputo.

Nota: Elaboración propia (Figura 26)

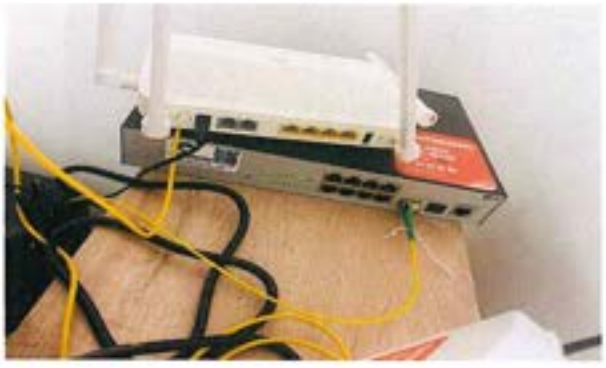
Figura 27

Instalación de fibra de internet

Nota: Elaboración propia.

Figura 28

Instalación de fibra de internet redundante.



Nota: Elaboración propia

Figura 29

Instalación de gabinete, peinado de cable y ponchado del patchpanel.

Nota: Elaboración propia.

Figura 30

Configuración de switch y firewall.

Nota: Elaboración propia

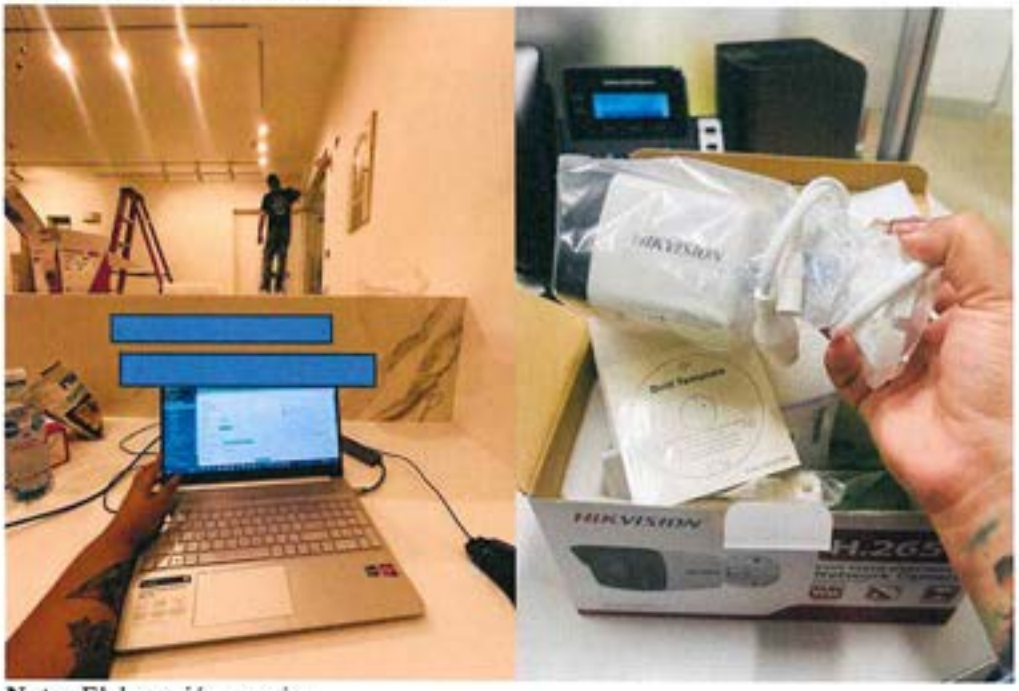
Figura 31

Instalación de equipos de comunicación en gabinete.

Nota: Elaboración propia

Figura 32

Instalación de Cámaras de seguridad



Nota: Elaboración propia.

Figura 33

Instalación de AP.

Nota: Elaboración propia

Figura 34

Instalación de control de acceso

Nota: Elaboración propia.

BIBLIOGRAFÍA

Universidad Internacional de Ciencia y Tecnología. (n.d.). *Licenciatura en Ingeniería en Redes de Comunicaciones con énfasis en seguridad.* Recuperado de https://www.unicyt.net/redes-de-comunicaciones-seguridad

Laboratorio Clínico Fernández. (n.d.). *Servicios* de https://www.laboratoriofernandez.com/
Panadata. (n.d.). *Laboratorio Clínico Fernández, S.A.* Recuperado el 19 de enero de 2025, de https://www.panadata.net/organizaciones/4846555

Laboratorio Clínico Fernández. (n.d.). *Facebook.* De https://www.facebook.com/laboratorioclinicofernandez/

Universidad Internacional de Ciencia y Tecnología (UNICyT). (2022). *Normas de trabajos con opción a grado de licenciatura.* Recuperado de https://idi.unicyt.edu.pa/wp-content/uploads/2022/01/NORMAS-DE-TRABAJOS-CON-OPCION-A-GRADO-DE-LICENCIATURA.pdf

Universidad Internacional de Ciencia y Tecnología (UNICyT). (2021). *Normas de trabajos con opción a grado de maestría.* Recuperado de https://idi.unicyt.edu.pa/wp-content/uploads/2022/01/NORMAS-DE-TRABAJOS-CON-OPCION-A-GRADO-DE-MAESTRIA-26-02-2021.pdf

Universidad Internacional de Ciencia y Tecnología (UNICyT). (2021). *Proyecto de graduación de Kerllys Angélica.* Recuperado de https://idi.unicyt.edu.pa/wp-content/uploads/2021/03/PROYECTO-DE-GRADUACION-KERLLYS-ANGELICA-Definitivo-FEBRERO-26.pdf

Universidad Internacional de Ciencia y Tecnología (UNICyT). (2021). *Actas del V Congreso de Investigación, Desarrollo e Innovación.* https://idi.unicyt.edu.pa/wp-content/uploads/2021/02/ACTAS-DEL-V-CONGRESO-IDI-UNICyT-v-4.2.pdf

Kafedra. (s.f.). *Що таке брандмауер і як з ним працювати?*. Recuperado de https://kafedra.com.ua/shho-take-brandmauer-i-yak-z-nym-pratsyuvaty/.

Hewlett Packard Enterprise. (s.f.). *HPE Networking Instant on Access Point AP12 3x3 WiFi 5 Indoor*. Recuperado de https://www.amazon.com/Networking-Wireless-Power-Not-Included/dp/B07V3J5TXJ.

Upwork. (s.f.). *Development & IT: Site-to-Site VPN IPsec or Remote Access SSL Configured from Expert*. Recuperado de https://www.upwork.com/en-gb/services/product/development-it-site-to-site-vpn-ipsec-or-remote-access-ssl-configured-from-expert-1592218950073233408.

Apuntes de Networking. (2013, abril). *Esquema de Cisco IPsec VPN site-to-site* [Imagen]. Apuntes de Networking. https://apuntesdenetworking.blogspot.com/2013/04/cisco-ipsec-vpn-

site-to-site-con-isp.html.

International Organization for Standardization. (2013). *ISO/IEC 27001:2013 - Information Security Management Systems Requirements*. https://www.iso.org/standard/54534.html
Telecommunications Industry Association. (2018). *TIA/EIA-568-C.2: Balanced Twisted-Pair Telecommunications Cabling and Components Standards*. https://www.tiaonline.org/standards/

Universidad Internacional de Ciencia y Tecnología. (2022). *Normas de trabajos con opción a grado de licenciatura*. https://idi.unicyt.edu.pa/wp-content/uploads/2022/01/NORMAS-DE-TRABAJOS-CON-OPCION-A-GRADO-DE-LICENCIATURA.pdf