



UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO

CENTRO UNIVERSITARIO UAEM ATLACOMULCO

**“MEJORA DE LA INFRAESTRUCTURA DE RED Y
COMUNICACIÓN DE BASE DE DATOS EN CONSTRUCTORA
NAVMER”**

MEMORIA DE EXPERIENCIA LABORAL

Que para obtener el Título de:

Ingeniero en Computación

Presenta:

Juan Abimael García Ordoñez

Asesor:

Dr. Everardo Efrén Granda Gutiérrez

Atlacomulco, México; agosto de 2026

RESUMEN

La presente memoria por experiencia laboral documenta el diseño, la implementación técnica y la puesta en marcha de una infraestructura de red convergente y de un sistema de gestión de datos para la Constructora NAVMER. El objetivo central de este proyecto es la consolidación de un entorno digital unificado que resuelva de manera definitiva las deficiencias críticas de comunicación y la fragmentación de la información entre las tres sedes principales de la organización, optimizando así su capacidad operativa y competitiva.

Mediante la integración de una arquitectura de red de área extensa definida por software (SD-WAN) y el despliegue de bases de datos centralizadas, se estableció un flujo de información seguro, persistente y en tiempo real. Esta intervención técnica permitió la institucionalización de procesos de control de inventarios y de recursos, mitigando errores de captura y garantizando la integridad de los activos digitales corporativos mediante políticas de seguridad perimetral. Como resultado, la empresa cuenta hoy con una plataforma tecnológica resiliente que sustenta la coordinación eficiente de sus obras y procesos administrativos.

La metodología de trabajo se fundamentó en un ciclo de mejora continua que abarcó desde el diagnóstico técnico-situacional hasta el aseguramiento de la calidad mediante pruebas de conectividad y de estrés. El impacto logrado trasciende el ámbito tecnológico, profesionalizando las competencias digitales del personal y entregando un producto final que constituye una ventaja estratégica para la Constructora NAVMER, asegurando la escalabilidad y la estabilidad de sus servicios de voz y datos en un mercado altamente exigente.

Palabras clave: red, bases de datos, conectividad, seguridad, red de área local definida por software.

ABSTRACT

This report documents the design, technical implementation, and commissioning of a converged network infrastructure and data management system for NAVMER Construction. The central objective of this project is to consolidate a unified digital environment that definitively resolves critical communication deficiencies and information fragmentation across the organization's three main locations, thereby optimizing its operational and competitive capacity.

By integrating a software-defined wide area network (SD-WAN) architecture and deploying centralized databases, a secure, persistent, and real-time information flow was established. This technical intervention institutionalized inventory and resource control processes, mitigating data entry errors and ensuring the integrity of corporate digital assets through perimeter security policies. As a result, the company now has a resilient technological platform that supports the efficient coordination of its construction projects and administrative processes.

The methodology was based on a continuous improvement cycle that encompassed everything from technical and situational diagnosis to quality assurance, connectivity, and stress testing. The impact achieved transcends the technological realm, professionalizing staff digital skills and delivering a final product that constitutes a strategic advantage for NAVMER Construction, ensuring the scalability and stability of its voice and data services in a highly demanding market.

Keywords: network, databases, connectivity, security, software-defined local area network.

ÍNDICE

RESUMEN	2
ABSTRACT	3
ÍNDICE.....	4
ÍNDICE DE FIGURAS	6
ÍNDICE DE TABLAS.....	8
1. ANTECEDENTES.....	1
2. IMPORTANCIA DE LA TEMÁTICA.....	2
3. DESCRIPCIÓN DEL PUESTO	3
4. PLANTEAMIENTO DEL PROBLEMA	4
4.1 Definición del problema	4
4.2 Objetivos.....	5
4.3 Justificación.....	6
4.4 Impactos	6
5. FUNDAMENTOS TEÓRICOS	8
5.1 Infraestructura de red.....	8
5.2 Tipos de redes de computadoras.....	9
5.3 Nuevas propuestas de arquitectura de red	10
5.4 Dispositivos de red principales para una red	12
5.5 Componentes del cableado estructurado y herramientas.....	13
5.6 Requerimientos de medios de transmisión de datos.....	13
5.7 Bases de datos.....	14
5.8 Seguridad.....	15
5.9 Áreas de oportunidad y elementos de apoyo	16
6. INFORME DE LAS ACTIVIDADES	21
7. DESARROLLO DE LA SOLUCIÓN	26
7.1 Estructura de la empresa previa a la implementación	26
7.2 Estructura de las áreas en las sucursales.....	27
7.3 Arquitectura física y lógica de la red.....	30
7.3.1 Estructura física	31
7.3.2 Requerimientos de interconexión de la red	32
7.3.3 Perspectiva económica	36

7.4	Estructura lógica	38
8.	DISEÑO E IMPLEMENTACIÓN	39
8.1	Simulación en Cisco Packet Tracer 8.2.2	39
8.2	Implementación de infraestructura	46
8.3	Acceso a interfaz de gestión	49
8.3.1	Configuración de la Red Local (LAN)	50
8.3.2	Interconexión entre Sedes (Enrutamiento Estático)	51
8.3.3	Túneles VPN	52
8.3.4	Conexión estable del túnel VPN.....	56
8.3.5	Conexión de las Sedes Remotas (Sedes 2 y 3)	56
8.4	Pruebas de conectividad y seguridad.....	59
8.4.1	Pruebas lógicas	59
8.4.2	Pruebas de aplicación (base de datos)	63
8.4.3	Conectividad para operación multisede.....	66
8.4.4	Creación de unidad de red	68
8.4.5	Seguridad de la red	72
8.4.6	Seguridad en los equipos de cómputo	73
8.4.7	Seguridad de la base de datos	73
8.4.8	Seguridad de la unidad compartida	74
8.4.9	Seguridad mediante respaldos de información	75
8.4.10	Monitoreo y disponibilidad de los recursos.....	75
9.	CAPACITACIÓN	76
9.1	Personal de nuevo ingreso	76
9.2	Encargados de almacén, materiales y ferretería	78
9.3	Arquitectos, ingenieros civiles, administradores y contadores.....	81
	CONCLUSIONES.....	84
	REFERENCIAS	86
	GLOSARIO	90

ÍNDICE DE FIGURAS

Figura 1. Diagrama de flujo de la metodología de este proyecto	22
Figura 2. Estructura física general de las tres sedes de la constructora NAVMER.	27
Figura 3 Área de recursos humanos y contabilidad.....	28
Figura 4 Área de trabajo de auxiliares de proyectos.	28
Figura 5. Área de trabajo principal, jefes de proyecto, arquitectos e ingenieros.....	29
Figura 6 Espacios de la sede 2.....	30
Figura 7 Espacios de la sede 3.....	30
Figura 8 Estructura de comunicación general.	31
Figura 9 Router a utilizar: TP-Link Archer BE3600.....	35
Figura 10. Switch TP.Link TL-SG116	35
Figura 11. Estructura lógica general de la red.	38
Figura 12. Diagrama implementado en el simulador Cisco Packet Tracer 8.2.2.	40
Figura 13. Configuración DHCP de routers.	41
Figura 14. Configuración de equipos para ip dinámicas.	42
Figura 15. Interfaz de puertos seriales.....	42
Figura 16. Comunicación entre sedes mediante una interfaz serial.	43
Figura 17. Configuración de servidor.....	44
Figura 18. Servicio HTTP/HTTPS	44
Figura 19. Edición de archivo index.html	45
Figura 20 Evitar error de asignación.	45
Figura 21 Prueba de conexión entre sedes.....	46
Figura 22 Instalación de nuevos equipos.....	47
Figura 23 Instalación Router y switch sede 1.....	48
Figura 24 Instalación Router y switch sede 2.....	48
Figura 25 Instalación Router y switch sede 3.....	49
Figura 26 Interfaz modem del proveedor	50
Figura 27 Interfaz router Archer BE3600.....	50
Figura 28 Configuración LAN Router	51
Figura 29 Interconexión de sedes en Router de sede 1.....	51
Figura 30 NO-IP creación de dominio.	52
Figura 31 Alta de dominio en Router Archer BE3600	53

Figura 32 Configuración de servidor VPN en Router Archer BE3600	54
Figura 33 Generando archivo (.ovpn) para comunicar sedes.	54
Figura 34 Archivo (.ovpn)	54
Figura 35 Apertura de Puertos (Port Forwarding) en el Módem.....	55
Figura 36 Vinculación router a una IP estática en modem.	56
Figura 37 Configuración módem Sede 2.....	57
Figura 38 Configuración módem Sede 3.....	57
Figura 39 Configuración Router Sede 2.....	57
Figura 40 Configuración de Router Sede 3	58
Figura 41 Vinculación VPN en Sede 2 y 3.....	58
Figura 42 VPN Conectada.....	59
Figura 43 prueba ping misma LAN.....	60
Figura 44 Prueba de conexión a Sede 2.....	61
Figura 45 Prueba de conexión a Sede 3.....	62
Figura 46 Prueba ipconfig all.	62
Figura 47 Prueba tracert de conexión a Sede 2.	63
Figura 48 Prueba tracert de conexión a Sede 3.	63
Figura 49 Interfaz del sistema de inventarios NAVMER.	64
Figura 50 Entidad Relación Sistema de Inventarios NAVMER.	65
Figura 51 Database Splitter, dividir Base de Datos.....	67
Figura 52 Archivos Back-End y Front-End.....	67
Figura 53 Creación de carpeta compartida para la unidad de red.	68
Figura 54 Creación de carpetas por sede en unidad de red.	69
Figura 55 Conectar a la unidad de red.....	69
Figura 56 Unidad de red vinculada.	70
Figura 57 Archivos de Sistema de Inventarios NAVMER.	70
Figura 58 Ubicación de archivo Front-End.....	71
Figura 59 Permisos para la unidad de red.....	74
Figura 60 Capacitación nuevo ingreso.	77
Figura 61 Capacitación área de almacén, materiales y ferretería.	79
Figura 62 Capacitación de arquitectos, contadores y administradores.....	81

ÍNDICE DE TABLAS

Tabla 1 Principales referencias en relación con las tecnologías de comunicación e implementación de infraestructura de red.	17
Tabla 2. Descripción de las actividades expuestas en el cronograma.	23
Tabla 3. Diagrama de Gantt del desarrollo del proyecto.	24
Tabla 4. Recursos a utilizar para la implementación de la red en las tres sedes.	36
Tabla 5 Requerimientos y costos.	37
Tabla 6 Equipos existentes e instalados.	47

1. ANTECEDENTES

Constructora NAVMER, fundada en mayo de 1996 con sede principal en Loma del Sitio, Jiquipilco, ha evolucionado de procesos manuales a una dependencia crítica de los activos digitales. Tras la apertura de nuevas sedes y almacenes, se identificaron brechas en la integridad de los datos y cuellos de botella en la comunicación que afectaban la competitividad organizacional. Como respuesta a este escenario, el presente proyecto contempla la optimización de la infraestructura de red y el despliegue de sistemas avanzados de comunicación de datos. Se ha modernizado la base tecnológica de la constructora, integrando procesos que hoy garantizan la seguridad de la información y la alta disponibilidad de los recursos. Este resultado constituye el activo digital que permite el crecimiento escalable de la empresa y la coordinación eficiente entre sedes, asegurando la continuidad operativa y la satisfacción del cliente final. Para Constructora NAVMER, esto ha significado la integración operativa de clientes, proveedores y colaboradores en un entorno digital seguro y unificado, satisfaciendo los requerimientos de conectividad y seguridad identificados en el diagnóstico inicial.

A partir del diagnóstico de la infraestructura existente, se determinó e implementó una arquitectura de red de área extensa (WAN) mediante tecnologías modernas, como el SD-WAN. Esta solución ha permitido la convergencia de distintos enlaces (fibra óptica, cable y LTE/5G), logrando una infraestructura funcional y resiliente que garantiza la comunicación ininterrumpida entre las sedes y los puntos de suministro.

En cuanto a la gestión de activos, se ha establecido un entorno basado en Sistemas de Gestión de Bases de Datos (SGBD). La implementación de esta arquitectura ha institucionalizado la administración centralizada de proyectos, inventarios y recursos informáticos. Este manejo técnico mitiga la duplicidad de tareas, garantiza la disponibilidad de los datos y asegura la integridad de la información mediante políticas de seguridad perimetral y control de acceso.

La sinergia entre la red de nueva generación y la base de datos administrada ha dotado a NAVMER de una capacidad de coordinación superior. Esta infraestructura permite reducir los riesgos de pérdida de información y responder con agilidad técnica a las demandas de cada nuevo proyecto de obra, consolidando la transformación digital de la empresa.

2. IMPORTANCIA DE LA TEMÁTICA

El intercambio de información implica el uso de distintos medios que permiten la transmisión de datos entre equipos de cómputo. Este proceso se realiza mediante redes de computadoras que comparten información entre sí. No obstante, cuando los dispositivos se encuentran a grandes distancias, pueden presentarse dificultades como el aumento en el tiempo de transmisión o la posible pérdida de datos. Por esta razón, la tecnología continúa evolucionando con el objetivo de desarrollar métodos más eficientes para transferir información, aumentando la velocidad de transmisión y reduciendo al mínimo las pérdidas de datos durante la comunicación.

En este contexto, los dispositivos de red desempeñan un papel fundamental en la infraestructura tecnológica, ya que permiten gestionar y controlar el tráfico de datos de manera más segura y organizada. Para garantizar una comunicación eficiente, se emplean diversos tipos de canales físicos que amplían la cobertura de la red y facilitan la transmisión de información incluso cuando los equipos están a gran distancia entre sí.

Contar con una infraestructura de red adecuada contribuye a mejorar la comunicación digital en una organización. En la actualidad, es necesario implementar sistemas de cableado estructurado capaces de soportar la creciente demanda de transmisión de información que enfrentan muchas empresas. La incorporación de dispositivos y tecnologías actualizadas permite que las organizaciones mantengan una comunicación eficiente mediante el uso de aplicaciones en internet, sistemas de telefonía digital y equipos de cómputo, lo que favorece el intercambio de información entre los distintos procesos y áreas de la empresa. Además, implementar una infraestructura de red segura y actualizada es esencial para mejorar el rendimiento y la calidad del servicio. La comunicación en tiempo real, como en videoconferencias o servicios de voz en línea, depende en gran medida de esta calidad.

La falta de actualización tecnológica puede generar vulnerabilidades y posibles ataques cibernéticos; el uso de tecnologías obsoletas puede afectar el funcionamiento de las redes. Por ello, resulta fundamental que los sistemas tecnológicos incorporen mecanismos de seguridad que permitan proteger la información, responder de manera oportuna ante problemas en el tráfico de datos y adaptarse a la integración con nuevas tecnologías.

3. DESCRIPCIÓN DEL PUESTO

Dentro de Proyectos y Construcciones NAVMER se desempeñó el cargo de Encargado de Soporte de equipos de cómputo y equipos de apoyo tecnológico, teniendo como responsabilidad principal garantizar el correcto funcionamiento de los recursos informáticos utilizados en las actividades administrativas y operativas de la empresa, entre las funciones asignadas se encontraban la instalación, configuración y mantenimiento de equipos de cómputo, impresoras, dispositivos de comunicación y demás recursos empleados por el personal de las diferentes áreas de trabajo. Asimismo, se brinda soporte técnico preventivo y correctivo, atendiendo incidencias relacionadas con el hardware, el software, la conectividad y la operación de los sistemas utilizados por la organización.

Como parte de las actividades desarrolladas, se realizó el monitoreo de la infraestructura tecnológica existente, identificando áreas de oportunidad en la comunicación entre sedes, el acceso a la información institucional y la gestión de los recursos compartidos. A través de este proceso se detectaron limitaciones derivadas de la operación independiente de cada sucursal, lo que dificultaba el intercambio oportuno de información y el control centralizado de los procesos administrativos. Identificadas estas necesidades, se planteó implementar una infraestructura de red que permitiera mejorar la comunicación entre las sedes de la empresa, fortalecer la seguridad de la información y optimizar la gestión de los recursos tecnológicos. La propuesta contempló la interconexión de las sucursales mediante una red privada virtual (VPN), así como la centralización de la base de datos del sistema de inventarios para facilitar el acceso controlado a la información desde las diferentes ubicaciones de la organización.

La participación en este proceso no se limitó a actividades de soporte técnico, sino que también incluyó el análisis de requerimientos, la evaluación de alternativas para la actualización de equipos, la planeación de la infraestructura de comunicaciones y la validación de las soluciones implementadas. Estas actividades contribuyeron al fortalecimiento de la infraestructura tecnológica de NAVMER y constituyen la base del presente proyecto de mejora de la infraestructura de red y de comunicación de la base de datos.

4. PLANTEAMIENTO DEL PROBLEMA

La evolución del sector de la construcción ha transformado la gestión de proyectos, convirtiendo la infraestructura tecnológica en un pilar que garantiza la competitividad, la trazabilidad de los procesos y la eficiencia operativa. En el caso específico de Constructora NAVMER, la expansión de sus actividades operativas y administrativas a múltiples sedes evidenció brechas en la conectividad y en la gestión centralizada de la información, que comenzaron a constituir un obstáculo tangible para la coordinación logística de la organización.

El presente capítulo expone de manera detallada el diagnóstico situacional que motivó esta intervención ingenieril, describiendo las limitaciones técnicas, operativas y de seguridad que caracterizaban el entorno tecnológico de la empresa, y que dieron origen a la definición precisa del problema que fue abordado y resuelto en esta memoria.

4.1 Definición del problema

En la actualidad, las empresas del sector de la construcción requieren de recursos materiales y humanos para garantizar su competitividad, pero también de una infraestructura tecnológica sólida. La Constructora NAVMER, consciente de esta necesidad, busca optimizar su infraestructura de red y los sistemas de comunicación de bases de datos con el fin de asegurar una conexión eficiente, segura y en tiempo real. En este sentido, la optimización tecnológica se convierte en un elemento estratégico para impulsar la eficiencia, la sostenibilidad y la competitividad de la empresa.

La Constructora NAVMER desarrolla sus actividades en tres sedes principales: la oficina central, la distribuidora de material y una sucursal adicional. Cada una de ellas requiere acceso constante y confiable a la información corporativa para coordinar actividades administrativas, operativas y logísticas. Sin embargo, la infraestructura de red y los mecanismos de comunicación de las bases de datos presentan deficiencias que dificultan la interconexión eficiente entre las sedes.

Entre los problemas más relevantes se encuentra la ausencia de un sistema de comunicación unificado. Esto provoca retrasos en la sincronización de información, duplicidad de registros,

inconsistencias en los datos y dificultades para acceder en tiempo real a información importante, como reportes de obra, inventarios y órdenes de compra. Aunado a esto, y no menos importante, cabe resaltar la falta de conocimientos y de manejo de equipo y software por parte del personal de las áreas responsables. Estas limitaciones impactan directamente en la productividad, la calidad de la información y la capacidad de respuesta ante las demandas del mercado.

La situación actual genera consecuencias como tiempos muertos, errores en la planeación y dificultades en la coordinación entre las distintas áreas y sedes de la empresa. Todo esto incrementa los costos operativos y limita la competitividad de NAVMER frente a otras constructoras que ya cuentan con sistemas de red modernos y eficientes.

4.2 Objetivos

Objetivo general

Optimizar la infraestructura de red y los sistemas de comunicación de bases de datos de la Constructora NAVMER, con el propósito de garantizar una conexión eficiente, segura y en tiempo real entre sus tres sedes: la oficina principal, la distribuidora de material y la sucursal, para mejorar la velocidad y estabilidad de la transmisión de datos, así como fortalecer la integridad y disponibilidad de la información corporativa, en un periodo de 6 meses.

Objetivos específicos

1. Diseñar una infraestructura de red tipo SD-WAN que interconecte las tres sedes de Constructora NAVMER, integrando enlaces híbridos (cable, fibra óptica y LTE), topología redundante y políticas de enrutamiento sensibles a aplicaciones, que garanticen la disponibilidad de la red.
2. Implementar un sistema integral de seguridad informática que incluya un firewall perimetral, control de acceso, cifrado de datos en tránsito mediante TLS y respaldos automáticos, asegurando la confidencialidad e integridad de la información crítica.
3. Centralizar la gestión de bases de datos mediante una solución en la nube, con replicación síncrona entre sedes y monitoreo continuo del rendimiento, para garantizar el acceso en tiempo real a los datos y reducir la duplicidad de registros.
4. Capacitar al personal administrativo y operativo de las tres sedes mediante talleres

prácticos y guías visuales, logrando que al menos el 80 % de los participantes demuestren competencia en el manejo seguro de herramientas digitales, el acceso a bases de datos y el reporte de incidencias al término del proyecto.

4.3 Justificación

El desarrollo de este proyecto es necesario porque la Constructora NAVMER enfrenta actualmente limitaciones en la eficiencia de su red de comunicaciones y en la gestión de sus bases de datos. Al contar con tres sedes, la empresa depende de un flujo constante de información para coordinar sus operaciones. Sin embargo, la infraestructura de red provoca retrasos en la transmisión de datos y dificultades en la integración de procesos, lo que impacta directamente en la productividad y la toma de decisiones en los proyectos de obra.

Hoy en día, la competitividad de una constructora no solo se mide por su capacidad de producción física, sino también por la agilidad y precisión con que gestiona su información. Por lo tanto, resulta indispensable implementar una red que garantice la conexión en tiempo real para reducir los errores administrativos y acortar los tiempos de respuesta.

Otro elemento importante a considerar en este proyecto es que la inversión en tecnología, por sí sola, no garantiza resultados si no va acompañada de la capacitación del personal en el manejo de bases de datos, plataformas de comunicación y herramientas informáticas, lo cual asegura que los recursos tecnológicos implementados se utilicen adecuadamente.

Este proyecto responde a tres necesidades críticas de la Constructora NAVMER: mejorar la eficiencia operativa mediante la integración tecnológica, sincronizar el manejo de la información a través de la infraestructura de red y fortalecer la competencia empresarial. Mediante esta optimización integral, la empresa podrá garantizar su sostenibilidad y mantenerse competitiva en un sector en el que la gestión de la información es tan importante como los recursos físicos de construcción.

4.4 Impactos

Tecnológico

La implementación de la red optimizada habilitó una comunicación segura y en tiempo real entre la oficina principal, la distribuidora y la sucursal, lo que disminuyó significativamente

la latencia, la pérdida de paquetes y las caídas del servicio. Se logró una mejora sustancial en la estabilidad y disponibilidad de los sistemas corporativos y de las bases de datos. Asimismo, la seguridad digital se fortaleció mediante la implementación de políticas de acceso, respaldos automatizados y protocolos de integridad, lo que mitigó los riesgos de fuga de información crítica (como inventarios, órdenes de compra y reportes de obra). La disponibilidad inmediata de los datos permitió una toma de decisiones más oportuna e integró eficazmente las áreas administrativas, logísticas y operativas.

Económico

La integración tecnológica y la optimización del flujo de información redujeron los tiempos de respuesta entre sedes, eliminaron tiempos muertos y minimizaron errores administrativos. La centralización de datos y la eliminación de duplicidades redujeron la necesidad de compras urgentes o correctivas debido al desabasto. De igual manera, la alta disponibilidad de la base de datos evitó paros operativos y la duplicidad de esfuerzos, optimizando el uso de los recursos económicos de la organización.

Social

La disponibilidad de herramientas tecnológicas confiables, sumada a la capacitación impartida, elevó la productividad del personal y fomentó el desarrollo de competencias digitales, lo que contribuyó a la profesionalización de los puestos de trabajo. La agilidad en la gestión de la información mejoró la atención al cliente y fortaleció la reputación de la empresa mediante respuestas más rápidas y datos confiables. Adicionalmente, se consolidó una cultura de seguridad de la información, protegiendo activamente los datos de los empleados, clientes y proveedores.

Profesional

Este proyecto constituyó una evidencia práctica de cómo la optimización de las infraestructuras de red y de la comunicación de las bases de datos mejora la coordinación multi sede en el sector de la construcción, un entorno tradicionalmente poco documentado en la aplicación de tecnologías de la información. La ejecución del proyecto permitió consolidar lineamientos y criterios de diagnóstico, de disponibilidad y de gestión de riesgos, demostrando la aplicación directa de las competencias de análisis, diseño e implementación propias del perfil de egreso del Ingeniero en Computación en un entorno real.

5. FUNDAMENTOS TEÓRICOS

El presente capítulo establece el marco conceptual y técnico que sustentó el análisis, el diseño y la implementación de la infraestructura tecnológica en Constructora NAVMER. Con el fin de garantizar que las soluciones aplicadas respondieran a los más altos estándares de la ingeniería en computación, se exponen los principios fundamentales de las redes de computadoras, las arquitecturas de interconexión y los modelos de gestión de bases de datos. Asimismo, se detallan las especificaciones técnicas de los dispositivos de red, los componentes del cableado estructurado y los protocolos de ciberseguridad que sirvieron de base para la toma de decisiones durante el despliegue del proyecto, asegurando así la viabilidad, escalabilidad y robustez del sistema finalmente implementado.

5.1 Infraestructura de red

Primeramente, se deben conocer los conceptos fundamentales de la infraestructura de red y sus características. Lo principal que hay que analizar es la red de computadoras: un conjunto de dispositivos enlazados por un medio físico o inalámbrico cuyo objetivo es compartir recursos e información. Según (Dordoigne, 2015), una red es un medio de comunicación que permite a las personas o grupos compartir información y servicios; “es un conjunto de computadoras conectadas entre sí que comparten información, recursos como CD-ROM, impresoras, grabadoras de DVD y servicios como e-mail, chat, conexiones a Internet, juegos, etc.

Las tecnologías de comunicación desarrolladas en el artículo de (Poveda, 2014) implementan un sistema de distribución eléctrica capaz de ser autónomo y condicionarse en el medio, el objetivo es obtener un control automatizado en la zona y en ahorrar energía. Las tecnologías de comunicación pueden clasificarse en dos tipos: inalámbricas y cableadas, cada clasificación cuenta con sus propias derivaciones.

La propuesta de diseño de una red de comunicaciones requiere un procedimiento de ingeniería. La secuencia de operaciones para llevar a cabo una implementación de red de manera satisfactoria y que el proyecto sea alcanzable es la siguiente: recopilación de requisitos, definición del alcance, estructura de descomposición del trabajo y control del alcance. Una mala gestión del alcance y definición de requerimientos acaba repercutiendo de una manera negativa en el tiempo y el presupuesto estimado (García J. M., 2025).

Al igual que (Zone, 2026), define el diseño previo de una red como un proceso fundamental en una empresa, ya que permite establecer una base sólida para su funcionamiento. A través de esta planificación, se pueden prevenir fallos y asegurar que la red opere de manera eficiente y confiable, lo cual es esencial para el desarrollo adecuado de las actividades organizacionales.

En (PlanNet, 2024) se dice que todas las redes de computadoras son únicas, pero cada organización tiene distintas necesidades; aun así, existen algunos pasos comunes en un proceso típico de planificación de redes empresariales:

1. Identificar las necesidades de conectividad, ancho de banda, seguridad y escalabilidad de la organización.
2. Definir la arquitectura, la topología y el hardware necesarios, como enrutadores, switches y firewalls.
3. Elegir los proveedores adecuados para adquirir el hardware y software necesarios.
4. Implementación: Instalar, configurar y desplegar los elementos de la red.
5. Validar y realizar pruebas: Asegurarse de que la red funcione correctamente y realizar pruebas para evaluar su rendimiento.
6. Implementar rutinas de monitoreo para garantizar la continuidad y seguridad de la red.

Con base en estos pasos, se puede generar la arquitectura de la red, valorando cada espacio para determinar las necesidades de cada uno y llevarlas a cabo.

5.2 Tipos de redes de computadoras

Para comprender de manera amplia este proyecto, se deben definir los tipos de red que existen, de acuerdo con sus características, según (Gil Vázquez Pablo, 2010).

Primero, las LAN (*Local Area Network*, o red de área local) comprenden varias computadoras de escritorio ubicadas cerca unas de otras y conectadas a una red que permite a los usuarios compartir archivos y dispositivos periféricos como impresoras, faxes o dispositivos de almacenamiento. Las redes de área local se utilizan para conectar computadoras en una o varias oficinas, abarcando distancias que van desde unos pocos cientos de metros hasta varios kilómetros. Las computadoras conectadas a una LAN también se conocen como estaciones de trabajo, clientes o nodos. Estas se conectan a un servidor, un *host* de red que proporciona servicios a los clientes. El servidor suele tener mayor capacidad de almacenamiento y puede procesar datos a mayor velocidad que las computadoras cliente.

Un segundo tipo de red utilizado en muchas empresas es la red de área metropolitana (MAN, *por sus siglas en inglés, Metropolitan Area Network*). Este tipo de red transmite datos e información a toda la ciudad (hasta 48 kilómetros) y a una velocidad mayor que la de una red de área local. A diferencia de las redes de área local, las redes de área metropolitana están optimizadas para la transmisión de voz y datos y, por lo tanto, pueden transportar más tipos de datos que estas.

El tercer tipo de red es la de área extensa (*Wide Area Network, WAN*). Estas redes se componen de múltiples computadoras ampliamente dispersas e interconectadas. Las WAN suelen utilizar redes de comunicaciones de alta velocidad y larga distancia, o satélites, para conectar las computadoras dentro de la red. Una WAN tiene múltiples usos. Por ejemplo, una cadena minorista puede usar una WAN para conectar sus tiendas en todo el país o en todo el mundo, lo que le permite compartir datos de inventario y de ventas, así como enviar correos electrónicos.

El proceso de instalación de la red incluye el diseño, la planificación y la implementación de hardware y software que dan como resultado una red informática cohesiva y bien configurada, esto nos permite definir cómo es que se relacionan los componentes del sistema que ayuden a satisfacer las necesidades de la empresa, establecer una conexión de red estable y confiable y ser fácil de mantener, así mismo facilitar la interfaz de usuario gráfica, táctil, y basada en formularios principalmente (Iglesias Mouteira, 2004). Fase crucial para el óptimo funcionamiento de la red a implementar en NAVMER.

Una vez determinadas las necesidades de la red a implementar, ya sea para crear una nueva o optimizar una existente, también deben considerarse los requisitos de diseño. El primer paso es identificar el tipo de red que se requiere de acuerdo con la cobertura deseada, pudiendo ser, principalmente, una red MAN, WAN o de larga distancia. Posteriormente, se puede definir la topología de la red, donde, en el caso del diseño de redes DWDM (*Dense Wavelength Division Multiplexing*, o multiplexación por división de longitud de onda densa), se aplica preponderantemente a redes MAN, WAN o de larga distancia y a topologías de anillo (Varela, 2023).

5.3 Nuevas propuestas de arquitectura de red

Las telecomunicaciones son un campo de cambios rápidos; no ha terminado de surgir una tecnología cuando ya aparece una alternativa en el horizonte. Estos cambios no son espontáneos, sino el resultado de las presiones para la prestación de nuevos y mejores servicios. Las redes de

área local se han convertido en un elemento estándar en las empresas, lo que incluso presiona la interconexión de redes locales y remotas; de otro lado, han surgido aplicaciones y grandes bases de datos que, junto con aplicaciones en tiempo real como video y multimedia, constituyen grandes consumidores de recursos de comunicaciones (Pérez, 2021).

Parte importante de esto es conocer una red en particular que podría ser óptima para atender la problemática identificada en este proyecto: la SD-WAN (*Software Defined Wide Area Network*) es un tipo de tecnología de red que utiliza los principios de las redes definidas por software para gestionar y optimizar el rendimiento de las WAN. Permite a las organizaciones conectar de forma segura usuarios, aplicaciones y datos en múltiples ubicaciones, al tiempo que proporciona un mayor rendimiento, confiabilidad y escalabilidad. SD-WAN también simplifica la gestión de las WAN al proporcionar control y visibilidad centralizados sobre toda la red (QuickTechie, A career growth machine, 2025).

La topología de estrella es la conexión de dispositivos a un equipo central que controla el flujo de datos entre las estaciones de comunicación. Según (Herrera Pérez, 2010),” En la topología de estrella, la comunicación de los ordenadores periféricos con el central es rápida, pero la comunicación entre estaciones es lenta. Por otra parte, la capacidad de la red es elevada si el flujo de información es entre estaciones y central; la velocidad de la red depende muy poco del flujo de información que circula por la misma”. La telefonía IP brinda un esquema de seguridad, por otro lado, con un sistema de telefonía tradicional no

De acuerdo con (Hernández, 2025), cuando la continuidad es crítica, muchas empresas incorporan 5G/LTE como respaldo o enlace primario temporal. Se muestran diseños con “*overlays*” celulares integrados a SD-WAN; así, si el enlace fijo falla, el tráfico de BD y aplicaciones esenciales sigue fluyendo por el enlace móvil sin intervención manual. Las arquitecturas SD-WAN modernas se usan para unir sedes con enlaces heterogéneos (fibra, cable, LTE/5G), aplicando enrutamiento sensible a aplicaciones y políticas centralizadas para priorizar tráfico crítico (ERP/BD) y estabilizar la experiencia ante pérdidas o *jitter* (variabilidad de llegada de datos).

Cisco describe cómo SD-WAN reduce la latencia percibida y mantiene el SLA por aplicación con plantillas y “*App-Aware Routing*”, un patrón útil para oficinas, almacenes y sucursales como las de la constructora NAVMER si se diera el caso (Cisco Systems, Inc., 2024).

Para el acceso inalámbrico interno puede ser recomendable Wi-Fi 6E que abre la banda de 6 GHz,

disminuyendo la interferencia y permitiendo canales anchos (80/160 MHz) que mejoran la capacidad y las latencias en oficinas y bodegas. 6 GHz con WPA3-only y planificación de RF específica por densidad y aplicaciones de tiempo real (Cisco Systems, Inc., 2024). Esto es clave si NAVMER digitaliza más procesos en almacén u obra.

La seguridad en redes consiste en crear y mantener una política incluyendo una política de firewall, algunos de los beneficios del firewall en una red son: Previenen la exposición de los hosts y las aplicaciones sensibles a usuarios no confiables, examina el flujo de datos de los protocolos, bloquea el acceso de datos maliciosos a servidores y clientes y mejora la administración de la seguridad de la red, clave importante para la constructora NAVMER ya que se podrá reducir el control de acceso a la misma; pero también tiene limitaciones como: si está mal configurada puede tener consecuencias de vulnerabilidad, las aplicaciones no podrán pasar atreves de el de manera segura, el rendimiento de la red puede disminuir y los datos importantes no podrán ser protegidos y pueden ser extraídos (Ariganello, 2025).

5.4 Dispositivos de red principales para una red

Un *router*, también denominado “enrutador”, es un dispositivo que conecta redes y enruta datos entre ellas. Se pueden clasificar en dos grandes grupos: *router* de acceso y de distribución. El primer grupo, de acceso, son *router* utilizados para unir dos redes, por ejemplo: un proveedor de internet y el cliente. Los *router* de distribución son aquellos que funcionan para conectar a más de dos redes, enrutar datos entre varias redes conectados y procesar gran cantidad de información

Un *switch* o conmutador es un dispositivo que interconecta los equipos en una red por medios cableados, permitiendo compartir archivos, impresoras y la conexión a internet. Las principales características de los *switch* son los siguientes: los puertos, siendo los principales elementos quienes permiten la conexión de otros dispositivos al mismo y la velocidad a la que pueden trabajar. La conmutación consiste en transferir datos y es la función principal que realiza un *switch*; el elemento clave para llevar a cabo el proceso de transferencia de estos datos son los buffers. Los buffers son zonas de memoria donde las tramas (unidades de envío de datos) se almacenan para después ser reenviadas al puerto correspondiente (Stokes, 2025).

Un ordenador o computadora es un dispositivo electrónico diseñado para procesar grandes volúmenes de información, compuesto por dos elementos fundamentales: el hardware y el software. Primero, el software consiste en un conjunto de instrucciones que indican al sistema qué

operaciones debe ejecutar, mientras que el hardware corresponde a los componentes físicos que permiten llevar a cabo dichas instrucciones; entre estos componentes se encuentran los dispositivos de entrada y salida, como el teclado, el monitor, la impresora y la cámara, entre otros. Mediante la interacción entre software y hardware, el sistema puede procesar datos y generar resultados en un formato comprensible para el usuario final. (Calume, 2015).

5.5 Componentes del cableado estructurado y herramientas

Al adentrarse en la instalación de cableado estructurado, se consideran los elementos principales de la red. Se involucran elementos como paneles, conectores, cables, por ejemplo:

Plug: Es la pieza física (macho) que se conecta a un Jack o enchufe hembra para transmitir electricidad o datos, como en los cables de red RJ-45.

Jack conector (hembra), está diseñado para ajustarse a las placas de pared, paneles de conexión y cajas de conexión, ofreciendo un despliegue rápido.

Faceplate o tapas para RJ-45.

Patch Cord o cable de conexión, es un cable UTP constituido por cuatro pares flexibles terminado en un plug; se puede encontrar en distintos colores.

Así mismo las herramientas básicas para armar un cableado estructurado son las siguientes:

Herramienta de impacto posee un resorte que se puede graduar para distintas precisiones.

Cortador y pelador de cables: realiza el pelado de las vainas de los cables UTP y empareja los pares internos.

Probador rápido de cableado, es una herramienta que comprueba si existen anomalías en los cables, permite detectar cables cortados o en cortocircuito.

5.6 Requerimientos de medios de transmisión de datos

Los medios de transmisión son el medio físico que permite el envío de información entre dos dispositivos dentro de un sistema de comunicación, utilizando ondas electromagnéticas. Se clasifican en dos tipos: medios guiados y no guiados. Entre los medios guiados se encuentran el par trenzado, el cable coaxial y la fibra óptica, entre otros. Por su parte, los medios no guiados no requieren un soporte físico directo, ya que utilizan el aire o el vacío para transmitir señales.

Ejemplos de estos medios son la radio, las microondas y la luz (infrarroja/láser).

El cable de par trenzado es un tipo de cable de cobre utilizado en comunicaciones de voz y en redes Ethernet. Está formado por pares de hilos que constituyen un circuito para la transmisión de datos. Estos hilos se trenzan para reducir las interferencias o el ruido generado por otros pares dentro del mismo cable.

Existen dos tipos principales de cable de par trenzado: UTP (par trenzado no blindado) y STP (par trenzado blindado). El cable UTP está compuesto por dos o cuatro pares de hilos, es el más común en redes y tiene un alcance aproximado de 100 metros. En cambio, el cable STP cuenta con un recubrimiento metálico en cada par de hilos, lo que proporciona una mejor protección contra el ruido. Además, los cuatro pares están envueltos en una capa adicional de blindaje. Aunque el cable STP ofrece mayor aislamiento, su costo es más alto y su instalación resulta más compleja debido a su mayor grosor.

5.7 Bases de datos

Conceptualmente, se entiende por base de datos una colección de datos organizados por diferentes temas, la cual permite la gestión de estos, facilitando su mantenimiento, como ventaja respecto a la utilización de ficheros, estos, además de almacenar dichos datos, presentan su descripción y especifican una serie de relaciones lógicas entre los datos almacenados (García C. J., 2021).

Los modelos de implantación de bases de datos en la nube son principalmente de dos tipos (Postigo, 2022):

1. Base de datos en la nube: la gestión es análoga a la que se haría si la base de datos estuviera alojada físicamente en la intranet de la organización, pero el sistema está alojado en máquinas virtuales y en soportes de almacenamiento que se alquilan a un proveedor de servicios en la nube.
2. Base de datos como servicio (DBaaS): la base de datos se ejecuta en la nube y el proveedor se encarga de las tareas operativas de mantenimiento, de gestión, de administración, y todo en tiempo real, con la mayor seguridad y alta disponibilidad y con procesos de automatización de software.

El modelo de datos es uno de los principales criterios de clasificación de un SGBD (Sistema de Gestión de Base de Datos) puesto que se fundamenta en el modelo lógico de datos. Entre los más

empleados se encuentran los modelos relacionales, orientados a objetos, jerárquicos y en red. Uno que proporciona una serie de plantillas predefinidas que agilizan la creación de objetos de la base de datos, como tablas, formularios e informes, en la paquetería de Microsoft 365, a través de sus aplicaciones como Excel y Access, y que tiene como característica principal el alojamiento y uso en la nube (Cabello, 2025).

Tomar en cuenta la seguridad necesaria mencionada en (Miranda, 2020) es una de las consideraciones fundamentales que se deben tener en cuenta en el momento de seleccionar el mecanismo de control de acceso a través del cifrado de datos, la autenticación y la autorización. Este grado de seguridad puede variar mucho de una organización a otra, según el nivel de riesgo que representan los datos.

5.8 Seguridad

Tomar en cuenta la seguridad necesaria, mencionado en (Miranda, 2020), es una de las consideraciones fundamentales que se deben de tener en cuenta en el momento de seleccionar el mecanismo de control de acceso a través del cifrado de datos, la autenticación y la autorización, este grado de seguridad puede variar mucho entre una organización y otra, dependiendo del nivel de riesgo que representa los datos, el nivel o grado de seguridad que debe implementarse en un sistema de información depende del valor de los activos a proteger, la sensibilidad de los datos y el impacto que tendría un incidente de seguridad sobre la organización.

En términos generales, la seguridad informática puede clasificarse en tres niveles: *básico*, *medio* y *alto*.

El *nivel básico* está orientado a sistemas que manejan información de uso general y cuyo compromiso representa un impacto limitado para la organización. En este nivel suelen implementarse controles elementales como contraseñas de acceso, antivirus, respaldos periódicos y políticas básicas de uso de los recursos tecnológicos.

El *nivel medio* se aplica a organizaciones que administran información operativa, administrativa o financiera cuyo acceso no autorizado, modificación o pérdida puede afectar el funcionamiento normal de los procesos institucionales. Este nivel incorpora mecanismos adicionales de protección, como la segmentación de redes, el control de acceso basado en usuarios, el cifrado

de comunicaciones, las auditorías de acceso y los procedimientos formales de respaldo y recuperación de información.

Por su parte, el *nivel alto* está destinado a entornos donde se gestionan datos altamente sensibles, confidenciales o regulados, como información bancaria, gubernamental, médica o estratégica. En estos casos se implementan controles avanzados de seguridad que incluyen autenticación multifactor, sistemas de detección de intrusos, cifrado integral de la información, monitoreo permanente y políticas estrictas de gestión de riesgos.

Considerando las características del presente proyecto, la infraestructura tecnológica propuesta para Constructora NAVMER se ubica dentro de un nivel de seguridad medio, debido a que administra información relacionada con inventarios, recursos materiales, registros operativos y documentación interna utilizada por diversas áreas de la organización. Por esta razón, la propuesta contempla la utilización de redes privadas virtuales (VPN), control de acceso a recursos compartidos, administración de usuarios, respaldos periódicos de la base de datos y restricciones de acceso a los archivos críticos del sistema, con el propósito de preservar la confidencialidad, integridad y disponibilidad de la información.

5.9 Áreas de oportunidad y elementos de apoyo

Como parte del proceso de investigación, se realizó una revisión de la literatura especializada para identificar experiencias, metodologías y soluciones tecnológicas relacionadas con la implementación de infraestructuras de red, sistemas de comunicación multisede, seguridad informática y administración de la información empresarial. La consulta de artículos científicos, tesis y tesinas permitió analizar distintas propuestas desarrolladas en organizaciones con necesidades similares a las identificadas en Constructora NAVMER.

Los antecedentes recopilados constituyen un referente para la construcción de la propuesta planteada en esta memoria, ya que permiten reconocer tecnologías aplicadas, estrategias de implementación, mecanismos de seguridad y modelos de administración de información que contribuyen a la optimización de los recursos tecnológicos. En la siguiente tabla se presentan los principales trabajos analizados, así como los aspectos metodológicos y las áreas de oportunidad que resultaron de interés para el desarrollo del presente proyecto.

Tabla 1 Principales referencias en relación con las tecnologías de comunicación e implementación de infraestructura de red.

Referencia	Síntesis	Métodos	Áreas de oportunidad
(Andrés F. Betancur-Pérez1, 2015) <i>Redes elásticas del futuro: beneficios para la red interna de telecomunicaciones de Colombia.</i>	Examina las tecnologías de comunicación emergentes y destaca el auge de las redes ópticas pasivas (PON) como una arquitectura punto-a-multipunto eficiente y de bajo costo. Se proyecta la implementación de sistemas WDM/PON para gestionar el incremento exponencial del tráfico mediante la multiplexación por división de longitud de onda.	Sinergia entre dominios ópticos y radioeléctricos. Implementación de sistemas Wifi de próxima generación. Diseño de red elástica basado en la topología de malla.	Simplificación de la infraestructura de red actual. Optimización de la transmisión de datos mediante fibra óptica de nueva generación. Interoperabilidad de hardware con múltiples proveedores (ISP).
(Corella-Parra, 2023) <i>Desarrollo de un sistema de control de inventario para una empresa comercial</i>	Presenta el desarrollo de un sistema de control de inventarios orientado a mejorar la gestión y organización de productos dentro de una empresa. La investigación analiza las problemáticas derivadas del control manual de existencias y propone una solución basada en herramientas tecnológicas que automatizan los procesos de registro, clasificación y seguimiento de inventarios. Los resultados muestran mejoras significativas en la disponibilidad de información, la reducción de errores operativos y la optimización de la toma de decisiones relacionadas con el abastecimiento y el control de materiales.	Diagnóstico de procesos de inventario. Diseño de un sistema de control automatizado. Implementación de una base de datos para registros. Validación de resultados mediante pruebas operativas.	Automatización de procesos administrativos. Mejora de la disponibilidad de la información. Reducción de errores de captura. Optimización del control de existencias.
(Molina, 2022) <i>Seguridad en bases de datos</i>	Explora los mecanismos de protección para garantizar la seguridad de la información almacenada en las bases de datos organizacionales. Se analizan herramientas, políticas y buenas prácticas relacionadas con la administración de	Revisión bibliográfica especializada. Análisis de mecanismos de seguridad.	Fortalecimiento de la seguridad de bases de datos. Implementación de respaldos de información.

	usuarios, el control de acceso, los respaldos y la protección de datos. Los autores destacan que la seguridad de las bases de datos es un elemento fundamental para garantizar la continuidad operativa y la protección de la información institucional.	Estudio de controles de acceso. Evaluación de políticas de protección de datos.	Protección de recursos compartidos. Control de acceso a sistemas empresariales.
(Acosta, 2022) <i>Gestión y control de inventario en pequeñas y medianas empresas (PYMES) como herramienta de información para la toma de decisiones en tiempos de crisis</i>	Analiza la importancia de la gestión y control de inventarios como un elemento estratégico para la toma de decisiones dentro de las pequeñas y medianas empresas. Los autores estudian el impacto de la administración adecuada de existencias sobre la rentabilidad, la continuidad operativa y la capacidad de respuesta ante situaciones de incertidumbre. Los resultados muestran que la implementación de sistemas de control de inventarios permite mejorar la disponibilidad de información, optimizar recursos y fortalecer los procesos administrativos.	Revisión documental. Análisis de modelos de control de inventario. Evaluación de prácticas empresariales. Análisis de información para la toma de decisiones.	Automatización del control de inventarios. Optimización de recursos empresariales. Mejora de procesos administrativos. Mayor disponibilidad de información operativa.
(Evila, 2026) <i>Implementación de grupos de trabajo por medio de VLAN</i>	Aborda las arquitecturas de redes LAN y WAN, analizando sus características estructurales y los mecanismos de transporte de datos bajo el paradigma del modelo de referencia OSI. Se profundiza en la infraestructura física (routers y bridges) y en el concepto de redes de área local virtuales (VLAN) como una solución para la agrupación lógica de estaciones y dispositivos, independientemente de su ubicación física. La investigación detalla los procesos de subneteo para optimizar el	Investigación: estudio de tipos de encapsulamiento y segmentación de red. Despliegue: creación de grupos de trabajo lógicos y configuración de estaciones. Validación: pruebas de comunicación de paquetes y reporte final con conclusiones.	Seguridad: mejora del control administrativo mediante el aislamiento de tráfico. Optimización: uso eficiente de recursos en dispositivos situados a largas distancias. Propuesta de mejora: anexa diagramas de diseño, simulaciones de software y un glosario técnico para aclarar la

	direccionamiento IP, permitiendo la división de redes físicas en subredes lógicas que operan bajo un mismo dominio administrativo.		terminología de red empleada.
(Almazán Galeno, 2007) <i>“Proyecto de una red privada virtual (VPN) a la empresa Proyección y Administración Empresarial de México S.A. de C.V.”</i>	Su objetivo es diseñar e implementar una red privada virtual para mejorar la comunicación entre diferentes áreas de una organización empresarial. El estudio analiza los requerimientos de conectividad, seguridad y administración de recursos compartidos, proponiendo una solución basada en VPN que permite el intercambio seguro de información mediante Internet. Los resultados muestran una reducción en costos de comunicación y una mejora significativa en la disponibilidad de los servicios de red para los usuarios de la organización.	Diseño de infraestructura VPN. Análisis de requerimientos de conectividad. Configuración de dispositivos de red. Validación de acceso remoto seguro.	Fortalecimiento de la seguridad en la comunicación entre sedes. Reducción de costos de infraestructura dedicada. Centralización de recursos empresariales.
(Osorno Saavedra, 2003) <i>“Implementación de una red privada virtual (VPN) basada en protocolo MPLS sobre una red IP”</i>	Desarrolla una propuesta de interconexión de redes mediante tecnología MPLS y VPN para garantizar una comunicación eficiente entre sitios geográficamente dispersos. La investigación se enfoca en el diseño de una infraestructura que proporcione mayor disponibilidad, seguridad y rendimiento en la transmisión de datos. Los resultados obtenidos evidencian mejoras en la administración del tráfico de red y en la estabilidad de los servicios utilizados por los usuarios.	Diseño de red WAN. Implementación de VPN MPLS. Pruebas de conectividad y rendimiento. Evaluación de disponibilidad.	Optimización de enlaces de comunicación. Mejora en la disponibilidad de servicios Escalabilidad para futuras expansiones.

(Reyes Felipe, 2007) <i>“Informe del proyecto de un sistema de inventarios basado en administración de bases de datos”</i>	Desarrolla un sistema de inventarios sustentado en una base de datos relacional orientada al control de existencias y movimientos de materiales. La propuesta contempla la automatización de procesos administrativos mediante formularios, consultas y reportes que facilitan la gestión de información. Como resultado, se logra mejorar la organización de los registros, disminuir errores de captura y optimizar la disponibilidad de información para la toma de decisiones.	Diseño de base de datos relacional. Implementación de formularios y consultas. Generación de reportes administrativos. Validación funcional del sistema.	Centralización de información. Mejor control de inventarios. Automatización de procesos administrativos.
(Escobar Hernández, 2019) <i>“Sistema de información que controla y administra el inventario y ventas de una empresa comercial”</i>	Desarrollo de un sistema de información para el control de inventarios y ventas en una organización comercial. El trabajo analiza los procesos administrativos existentes y plantea una solución tecnológica que permite registrar operaciones, generar reportes y mantener actualizada la información de existencias. Los resultados muestran mejoras en la eficiencia operativa y en el acceso oportuno a la información empresarial.	Análisis de procesos de negocio. Diseño de base de datos. Desarrollo de módulos administrativos. Pruebas funcionales del sistema.	Integración de procesos empresariales. Reducción de errores de captura. Disponibilidad de información en tiempo real.
(González Morales, 2006) <i>“Redes Privadas Virtuales (VPN)”</i>	Analiza el funcionamiento de las redes privadas virtuales como alternativa para la interconexión segura de redes remotas a través de Internet. Examina los protocolos para la creación de túneles seguros, así como las ventajas de implementar este tipo de soluciones en entornos empresariales. Los resultados destacan la reducción de costos y el fortalecimiento de la seguridad en el intercambio de información.	Análisis de protocolos VPN. Diseño de túneles de comunicación. Configuración de autenticación y acceso. Evaluación de desempeño.	Comunicación segura entre sucursales. Protección de información empresarial. Reducción de costos de interconexión.

6. INFORME DE LAS ACTIVIDADES

El objetivo de este proyecto es resolver los problemas relacionados con la expansión de la infraestructura y el rendimiento de los servicios digitales de la empresa en cuestión. Para ello, se lleva a cabo un análisis de los requerimientos y de las dificultades existentes, con la finalidad de proponer una solución adecuada, cuya elaboración se basa en la siguiente metodología:

1. **Levantamiento y Diagnóstico:** Identificación de requerimientos y especificaciones críticas.
2. **Análisis de Costos:** Valoración económica para optimizar la inversión.
3. **Desarrollo:** Diseño detallado e implementación de la nueva arquitectura.
4. **Validación:** Protocolos de pruebas de rendimiento.
5. **Capacitación:** Transferencia de conocimientos operativos al personal para asegurar la continuidad de los servicios.

En la Figura 1 se presenta el diagrama de flujo que detalla las etapas del desarrollo implementado para la expansión de la infraestructura de red de la constructora “NAVMER”.

Un diagrama de flujo es una herramienta gráfica que permite mostrar de manera ordenada los pasos necesarios para resolver un problema, lo que facilita su comprensión y comunicación, especialmente en situaciones complejas. Gracias a este recurso, es posible representar con claridad el proceso a seguir para alcanzar una solución.

Entre sus principales ventajas se encuentran que mejora la interpretación de los procesos, reduce la necesidad de explicaciones extensas y permite identificar con claridad cada una de las etapas necesarias para completar un proyecto. Además, contribuye a visualizar las actividades involucradas y la forma en que se distribuye el trabajo en cada fase del proceso.

A fin de visualizar el desarrollo del proyecto, se presentan en la Tabla 2, la descripción de las principales actividades desarrolladas y en la Tabla 3, el diagrama de Gantt para destacar la cronología del proyecto.

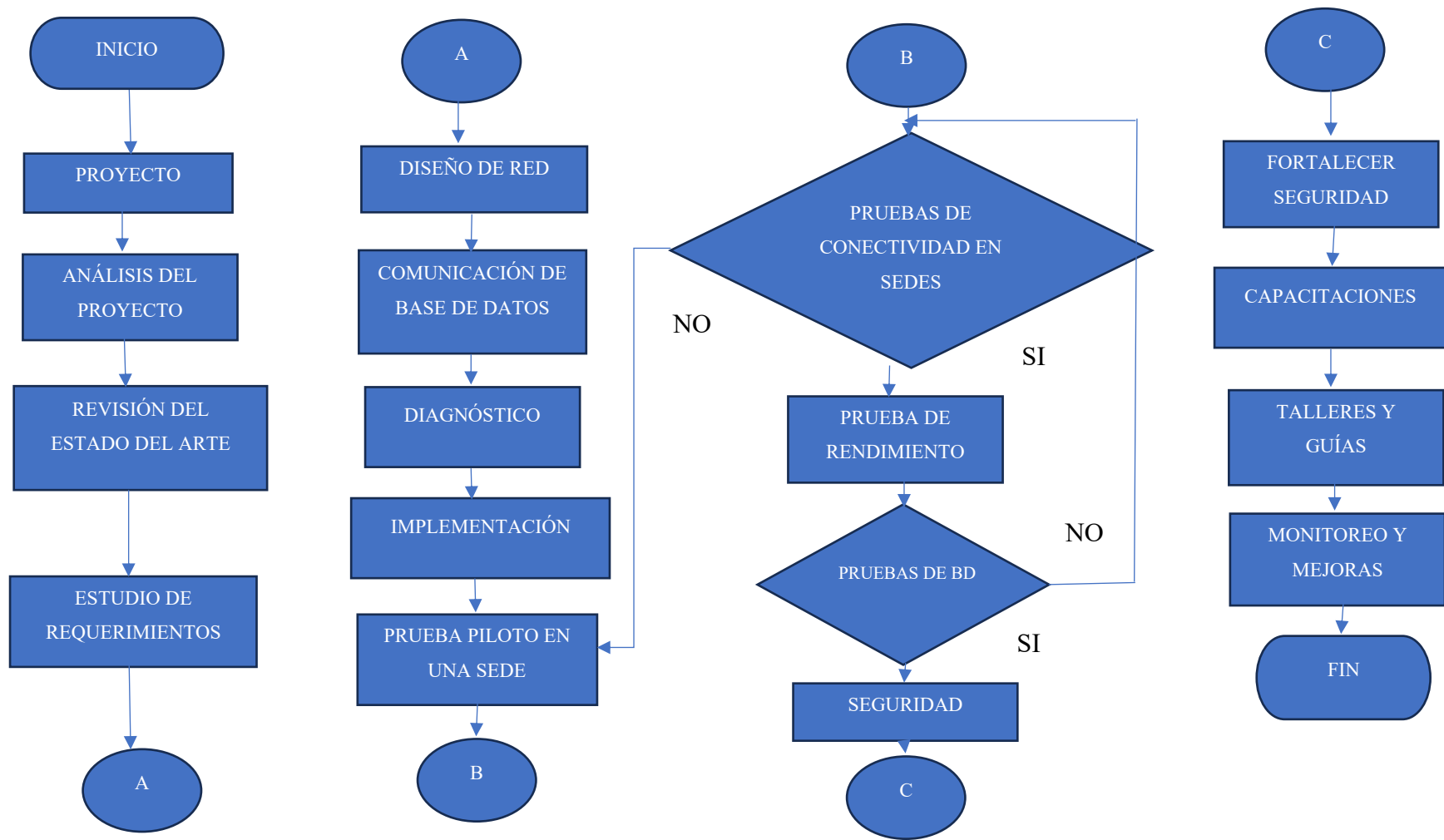
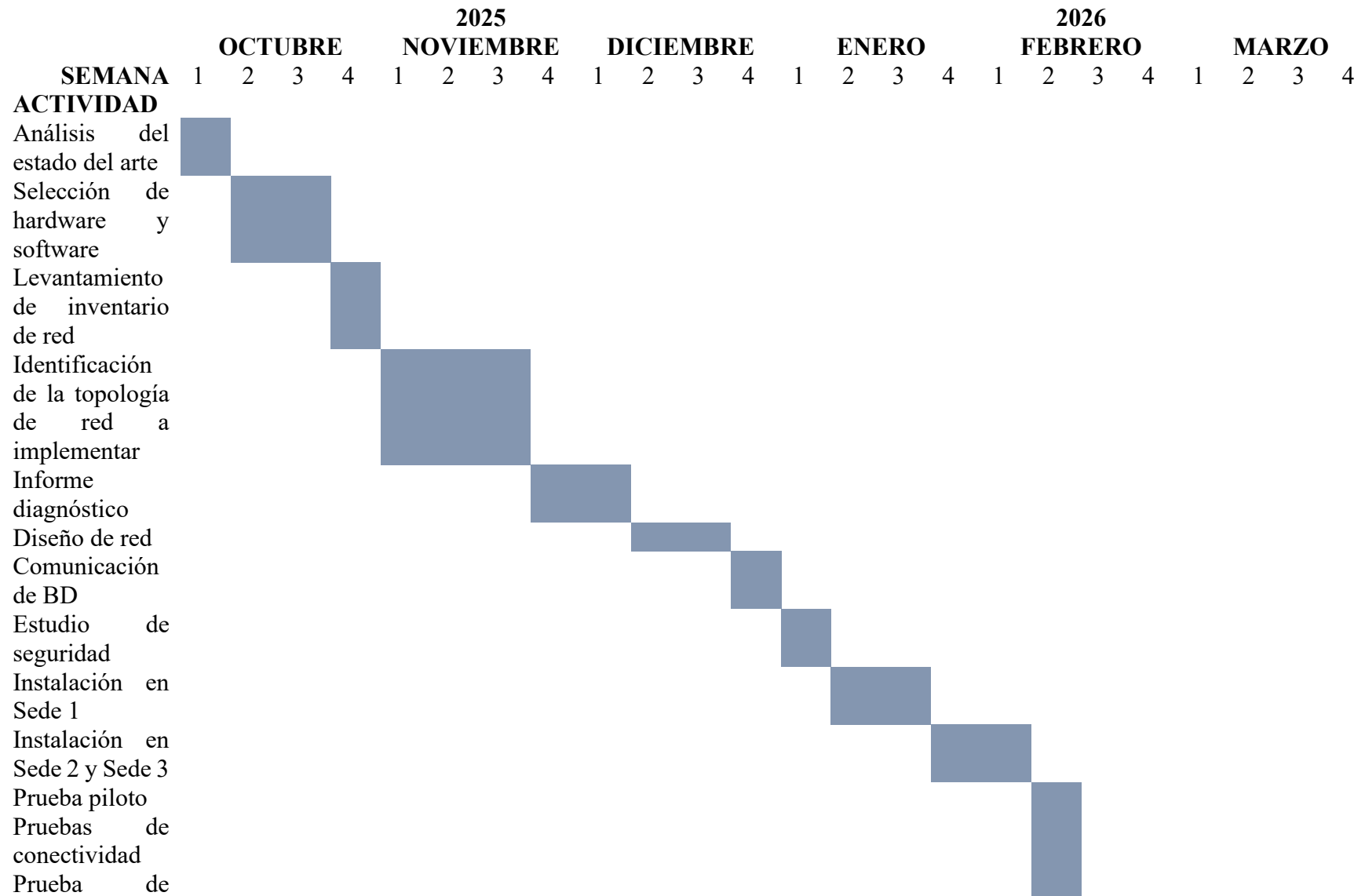


Figura 1. Diagrama de flujo de la metodología de este proyecto

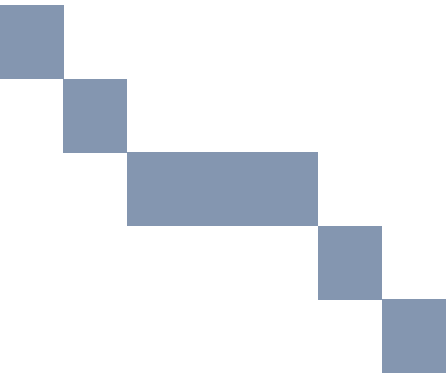
Tabla 2. Descripción de las actividades expuestas en el cronograma.

ACTIVIDAD	DESCRIPCIÓN GENERAL
Análisis del estado del arte	Conocer los principios fundamentales de la infraestructura de red y sus características.
Selección de hardware y software	De acuerdo con las áreas de la constructora se determinan los equipos nuevos, así como los programas requeridos para un mejor desempeño.
Levantamiento de inventario de red	Evaluación inicial de las condiciones físicas, tecnológicas y lógicas de los equipos de red preexistentes para identificar vulnerabilidades y necesidades operativas.
Identificación de la topología de red a implementar	Para estructurar correctamente la red y conocer en detalle cómo se organiza y se expande en las sedes.
Mapa de riesgos	identificar las vulnerabilidades, amenazas y posibles puntos de falla dentro de la infraestructura tecnológica
Informe diagnóstico	Entrega de un informe en el que se describen los problemas y necesidades de la empresa.
Diseño de red	Elaboración de la topología lógica con la ayuda de software de simulación, para estructurar el direccionamiento IP y planeación del enrutamiento óptimo para interconectar de forma segura las sucursales.
Comunicación de BD	Estudio del sistema de inventarios que utiliza la constructora para determinar la mejor forma de enlace de comunicación entre las sedes.
Estudio de seguridad	Identificar las vulnerabilidades de la red y equipos (usuarios, contraseñas, Firewalls y Routers)
Instalación en Sede 1, Sede 2 y Sede 3	Implementación de red y equipos.
Prueba piloto	Configuración de módem y routers para comunicación entre sedes 1 y 2
Pruebas de conectividad	Prueba ping entre equipos
Prueba de conexión de BD	Creando acceso a base de datos a través de una ip estática.
Chequeo de estabilidad	Monitoreo de conectividad
Capacitación: Talleres y guías	Capacitación de personal para el uso correcto de los equipos y el uso de las TICs
Monitoreo y mejoras	Optimizar procesos para garantizar la calidad y adaptarse a los cambios.
Entrega de proyecto	Aprobación de los entregables técnicos y de la documentación del proyecto

Tabla 3. Diagrama de Gantt del desarrollo del proyecto.



conexión de
BD
Chequeo de
estabilidad
Capacitación:
Talleres y guías
Monitoreo y
mejoras
Entrega de
proyecto



7. DESARROLLO DE LA SOLUCIÓN

El presente capítulo documenta la materialización técnica del proyecto, detallando el proceso de transición desde la infraestructura inicial fragmentada hasta el ecosistema de red unificado que actualmente opera en Constructora NAVMER.

A partir del diagnóstico situacional previamente establecido, se describe la ejecución de la solución, que abarca tanto la reestructuración física de las instalaciones como el diseño lógico de la nueva topología de red. A continuación, se exponen las fases operativas del despliegue, que incluyeron la selección e instalación del hardware, el tendido del cableado estructurado y la configuración avanzada de los servicios de conectividad y de bases de datos, acciones que permitieron resolver las deficiencias operativas y garantizar la interoperabilidad segura entre las tres sedes de la organización.

7.1 Estructura de la empresa previa a la implementación

En esta sección se describe la distribución de los espacios de trabajo de la empresa antes de implementar el proyecto. La red estaba dividida en tres subredes; dos de ellas tenían servicios de datos y voz que pertenecían al área de oficina central, al almacén y a la ferretería, y a la sucursal 2, en Ixtlahuaca.

El servicio de datos, en su mayoría, se brinda mediante conexiones inalámbricas a través de los módems convencionales proporcionados por las compañías de servicios de internet y telefonía. Ante la distancia y las interrupciones causadas por obstáculos y dispositivos como principales limitantes, se requería una red estable y de menor latencia para mejorar los tiempos de respuesta en los trabajos de la constructora NAVMER.

La implementación se realizó en las tres zonas donde opera la constructora, a fin de dar una idea de los alcances y beneficios de la red. La empresa se distribuye en tres sucursales, cuya distribución física se presenta en la Figura 2.

En la sede 1 se tiene solo el uso de tres equipos, distribuidos de la siguiente manera, uno en área de la ferretería y los otros dos dentro del área de oficinas para uso de personal de proyectos, siendo el área de distribuidor de material y almacén quienes no cuentan con equipos para control.

En la sede 2 se tiene el uso más amplio de equipos; esta es la instancia de arquitectos e ingenieros, con un total de 5 equipos, y el área de zona de despacho de material es la que no cuenta con ninguno. Pero cabe señalar que esta sucursal será la de mayor equipamiento, ya que se pretende brindar a cada analista de proyectos su propio espacio.

En la sede 3 solo se cuenta con un equipo para el área de ferretería, mientras que las áreas de oficinas y almacén no cuentan con ningún equipo para la comunicación rápida ni para el despacho.



Figura 2. Estructura física general de las tres sedes de la constructora NAVMER.

7.2 Estructura de las áreas en las sucursales

En la Figura 3 se presenta el área del nivel 1 de la sede 1, que cuenta con dos espacios de trabajo, cada uno con su equipo de cómputo; ambos compartirán 1 impresora. En esta misma sede, el nivel 2 que se muestra en la Figura 4 cuenta con un espacio de reuniones y 5 espacios de trabajo para los jefes de proyecto. Finalmente, la Figura 5 corresponde al nivel 3, siendo el más importante de la empresa, ya que este es el espacio del arquitecto líder de la empresa, asimismo, de los analistas de proyectos y del área de control principal.

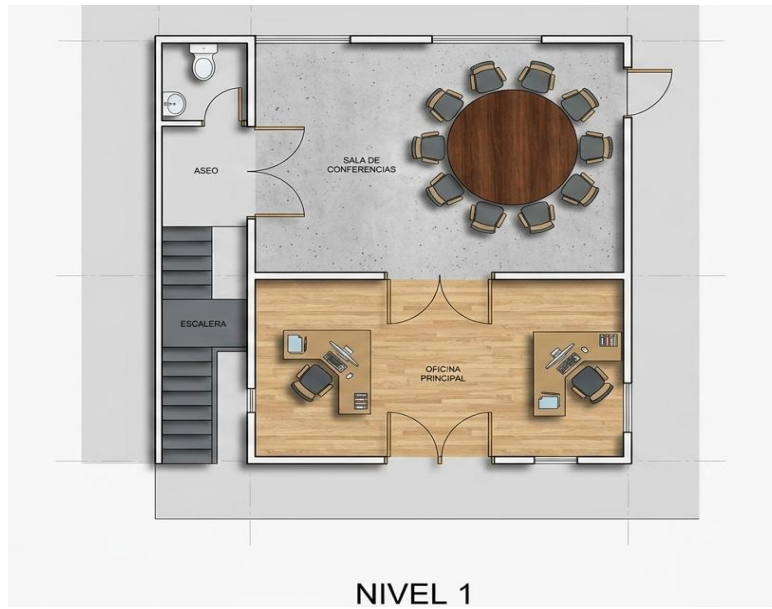


Figura 3 Área de recursos humanos y contabilidad.

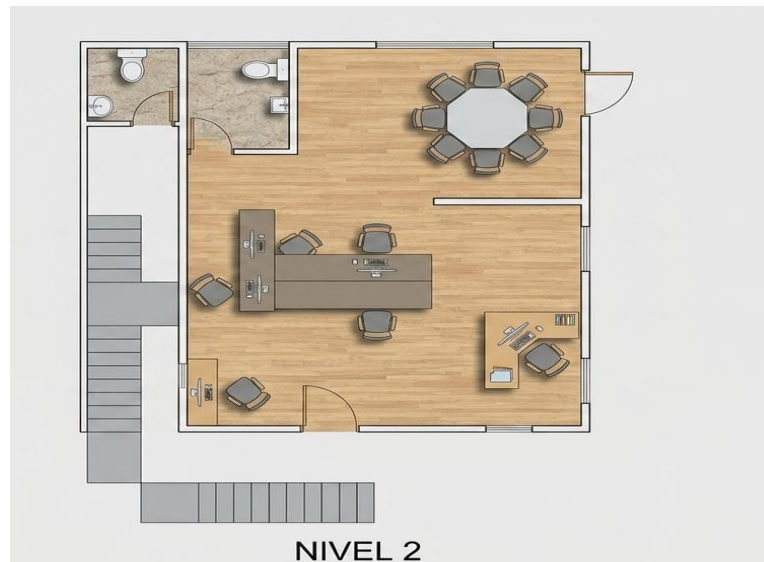


Figura 4 Área de trabajo de auxiliares de proyectos.

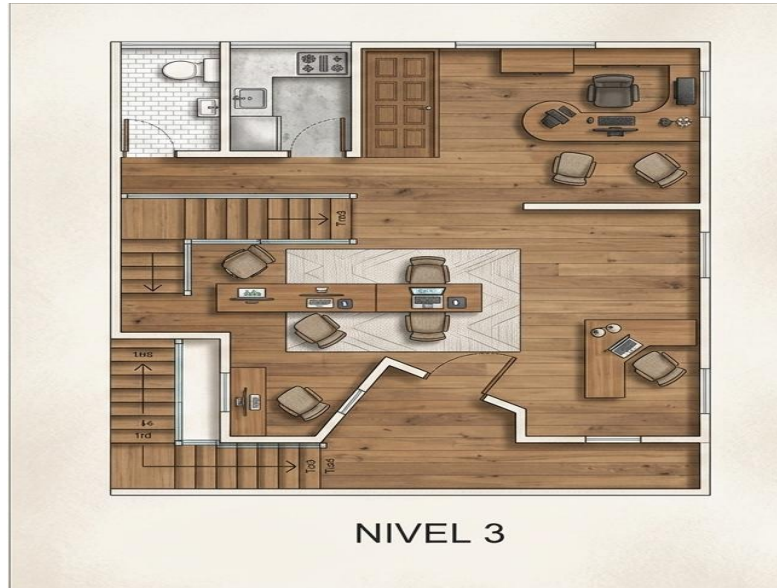


Figura 5. Área de trabajo principal, jefes de proyecto, arquitectos e ingenieros.

Por otra parte, para la sede 2 se presenta la Figura 6, en la que se observa la distribución de las oficinas y la ferretería, que maneja el sistema de inventarios, así como el espacio de aceros y materiales, los cuales están sujetos a valoración para la integración de equipo.

Finalmente, en lo que respecta a la sede 3, mostrada en la Figura 7, se contemplan 3 espacios de oficina por implementar, así como un espacio para la venta de materiales, vinculado al sistema de inventarios de la sede 1.



Figura 6 Espacios de la sede 2

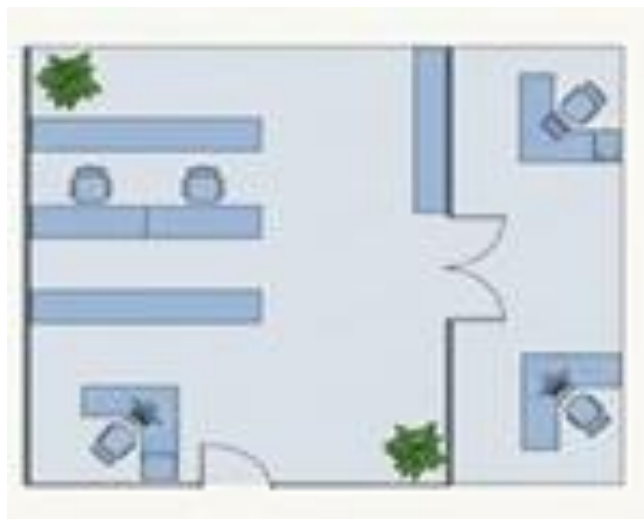


Figura 7 Espacios de la sede 3.

7.3 Arquitectura física y lógica de la red

Se logra implementar una estructura de red en las zonas retiradas y, sobre todo, la apertura de áreas donde no se cuenta con ella; también se contempla la instalación de nuevos dispositivos de red escalables para la comunicación digital.

7.3.1 Estructura física

El diagrama de la Figura 8 presenta la arquitectura general de comunicación implementada en Constructora NAVMER, en la que se muestra la integración de los tres sitios principales (NAVMER 1, NAVMER 2 y NAVMER 3) mediante una topología de red interconectada. En el centro de la infraestructura se encuentra la Sede 1 (Branch Office), que funciona como nodo principal de control y administración y alberga el sistema de control en el server rack.

Las sedes restantes se distribuyen estratégicamente: la Sede 2 concentra las operaciones de ferretería y almacén, mientras que la Sede 3 corresponde al área de taller/fábrica (Blockera). La comunicación entre estos puntos se establece mediante enlaces Ethernet protegidos con mecanismos de seguridad (Security Lock), lo que garantiza la integridad de los datos transmitidos. Todos los sitios mantienen conectividad a través de la nube de red (Cloud/WAN), lo que permite la sincronización en tiempo real de la información corporativa.

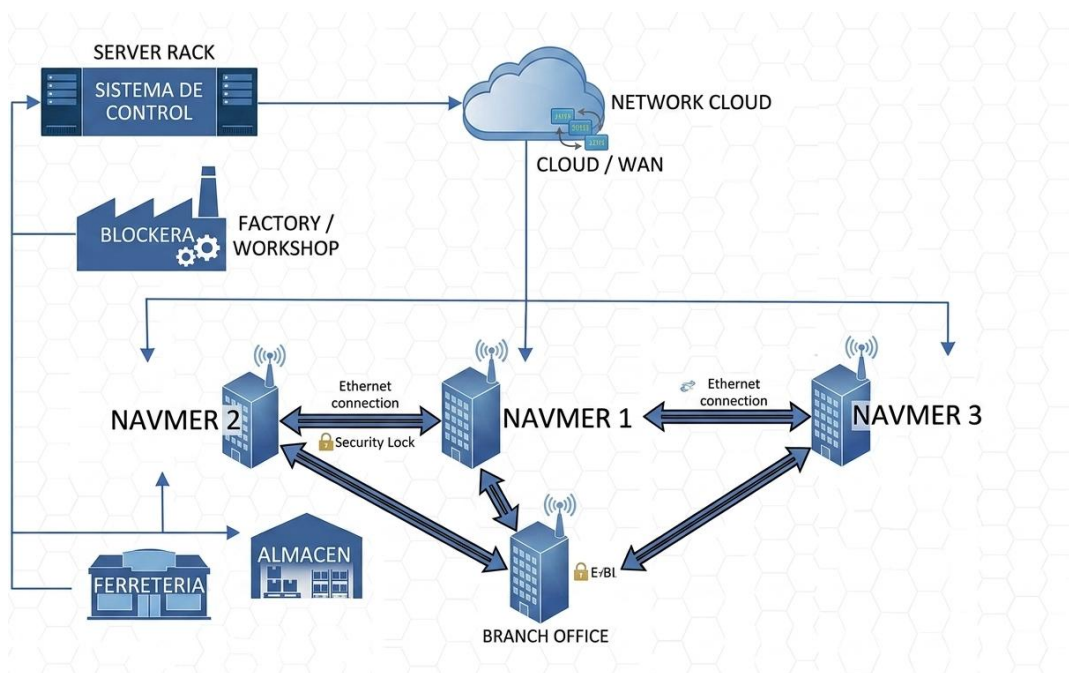


Figura 8 Estructura de comunicación general.

La filosofía de implementación se fundamentó en tres principios rectores: centralización del control, redundancia operativa y escalabilidad. El enfoque de centralización permitió concentrar los recursos críticos de administración y almacenamiento en la sede principal,

facilitando el mantenimiento, la seguridad y la gestión de respaldos. La redundancia se logró mediante la interconexión directa entre todas las sedes, evitando puntos únicos de falla y garantizando la continuidad operativa incluso si se interrumpe un enlace. Finalmente, la escalabilidad se incorporó desde el diseño físico mediante el uso de dispositivos con puertos disponibles y de cableado estructurado, lo que permite la incorporación futura de nuevos equipos o áreas sin requerir modificaciones estructurales mayores. Esta estrategia asegura que la infraestructura crezca al ritmo de las necesidades operativas de la constructora, protegiendo la inversión tecnológica a largo plazo.

7.3.2 Requerimientos de interconexión de la red

En el diseño de una infraestructura de red para una empresa con múltiples sedes como la Constructora NAVMER, la selección del switch es determinante para la estabilidad del flujo de datos. Según (link, 2023), los estándares de la industria, existen tres categorías principales de dispositivos:

Switches No Administrables (Unmanaged): Son dispositivos diseñados para una conectividad básica "Plug-and-Play". Su función principal es permitir que los equipos se comuniquen entre sí sin necesidad de configuración previa.

Ventajas:

1. Costo de adquisición significativamente bajo.
2. No requieren personal especializado para su instalación.
3. Ideales para redes domésticas o pequeñas oficinas con baja carga de datos.

Desventajas:

1. Invisibilidad: No poseen una dirección IP, por lo que no pueden ser monitoreados de forma remota.
2. Falta de Control: No permiten segmentar el tráfico ni priorizar servicios críticos como la base de datos de inventarios.
3. Riesgo de Bucles: No cuentan con protocolos para evitar bucles de red que pueden colapsar la infraestructura completa.

Switches Inteligentes (Smart / Web Smart): Representan un punto medio entre la simplicidad y el control profesional. Permiten una configuración básica a través de una

interfaz gráfica basada en navegador web.

Ventajas:

1. Permiten la creación de VLANs para separar el tráfico (ej. separar cámaras de seguridad de los datos de inventario).
2. Ofrecen funciones de QoS (Calidad de Servicio) para dar prioridad a aplicaciones críticas.
3. Costo moderado con funciones de gestión esenciales.

Desventajas:

1. No ofrecen acceso a través de consola (CLI) para configuraciones masivas.
2. Sus funciones de seguridad y diagnóstico son limitadas en comparación con los modelos de alta gama.

Switches Administrables (Fully Managed): Son el estándar para redes corporativas y sedes interconectadas. Ofrecen un control total sobre cada puerto y el flujo de datos que transita por ellos.

Ventajas:

1. Seguridad Avanzada: Permiten restringir el acceso a la red por puerto o por dirección MAC.
2. Protocolos de Redundancia: Implementan STP (Spanning Tree Protocol) para evitar caídas de red por bucles físicos.
3. Diagnóstico Remoto: Permiten el monitoreo constante a través de protocolos como SNMP, facilitando la detección de fallos antes de que afecten al usuario final.

Desventajas:

1. Inversión inicial más alta.
2. Requieren conocimientos técnicos avanzados para su configuración y administración.

Otra de las piezas fundamentales de una red es el router, un dispositivo de red encargado de dirigir y gestionar el tráfico de datos entre diferentes redes informáticas. Su función principal consiste en recibir paquetes de información provenientes de una red y determinar la ruta más adecuada para enviarlos a su destino en otra red, utilizando los protocolos de comunicación

establecidos en Internet.

En entornos domésticos y empresariales, permite interconectar múltiples dispositivos, como computadoras, teléfonos móviles o impresoras, mediante una red local y, al mismo tiempo, facilitar el acceso a Internet. Además, muchos incorporan funciones adicionales, como la asignación automática de direcciones IP, la creación de redes inalámbricas (Wi-Fi) y mecanismos básicos de seguridad para proteger las comunicaciones entre los dispositivos conectados.

Según (Citys, 2024), existen diferentes tipos de routers según su forma de funcionamiento. El de cable utiliza conexiones físicas para transmitir los datos entre el módem y los equipos conectados. En cambio, el inalámbrico envía la información mediante señales de radio, lo que permite que varios dispositivos se conecten a la red sin necesidad de utilizar cables. Además, en las redes de mayor tamaño se emplean otros tipos. Por otro lado, el router de borde se encarga de conectar una red con otras redes externas, mientras que el de núcleo opera dentro de una misma red y permite el transporte de grandes volúmenes de información a alta velocidad. Finalmente, el router VPN integra un sistema que permite establecer conexiones seguras para proteger la información de los dispositivos conectados.

A partir de esto, se determina, de consenso con la empresa, el uso de un router que solo cumpla con el funcionamiento de la red, con un alto nivel de seguridad por ahora, ya que se deja como antecedente la información presentada sobre qué es el requerimiento óptimo en máxima seguridad, pero cumpliendo con las funciones para el óptimo funcionamiento.

Con ello se opta por el router TP-Link Archer BE3600 (Figura 9), se trata de un router dual-band 2x2, con un ancho de banda de 2882 Mbps en 5 GHz y 688 Mbps en 2.4 GHz, que ahora superan 1 Gbps, tener la capacidad de conectar un módem de fibra a 2.5GbE y enlazar la red cableada local a esa velocidad es un gran diferenciador, y sobre todo que implementa wifi 7 y 6 con el cual la transferencia de archivos de Excel/Access dentro de cada sede será extremadamente rápida, alta capacidad de funcionamiento pero sobre todo con funciones de configuración que en la práctica real se sustituyó el enlace serial por enlaces de banda ancha comercial protegidos por la VPN del router TP-Link y utiliza cifrado moderno, lo cual protege la base de datos de inventario compartida (referencia).



Figura 9 Router a utilizar: TP-Link Archer BE3600.

Haciendo referencia a los estándares de industria definidos por fabricantes líderes como TP-Link se opta por el uso de switch no administrable ya que por petición de la empresa no lo ve por ahora necesario, no por qué no lo sea, sino que consideran esta una opción como reducción de los gastos para esta infraestructura y que al final no influye en la funcionalidad de lo que se busca. Es por ello que se consideró el uso de Switch TP-Link TL-SG116 (Figura 10) Gigabit Ethernet 16 y 8 puertos RJ45 de negociación automática de 10/100 / 1000Mbps que admite Auto-MDI / MDIX, carcasa de acero, soporta 802.1p / DSCP QoS e IGMP Snooping, Plug and Play, sin necesidad de configuración.



Figura 10. Switch TP.Link TL-SG116

Adicionalmente, para la implementación de la red, a elaborar y, sobre todo, para tener un estimado de los recursos a utilizar. Para ello, se coordinó una jornada de trabajo con una empresa externa para realizar el reconocimiento de campo en las áreas destinadas a la infraestructura de red. Durante esta inspección, se determinaron los puntos estratégicos de instalación y se realizó el inventario técnico de los insumos necesarios, que abarcó tanto el cableado estructurado como los componentes específicos del sistema. El resumen de los equipos solicitados y el cálculo del cableado, se detallan en la Tabla 4.

Tabla 4. Recursos a utilizar para la implementación de la red en las tres sedes.

SEDE	EQUIPOS	CABLE	OTROS
1	EQUIPO 1	3 METROS	SWITCH TP LINK 16 PUERTOS
	EQUIPO 2	3 METROS	5 REGULADORES
	EQUIPO 3	4 METROS	5 NO BREAK
	EQUIPO 4	4 METROS	MULTIFUNCIONAL LÁSER A
	EQUIPO 5	7 METROS	COLOR BROTHER
	EQUIPO 6	8 METROS	
	EQUIPO 7	6 METROS	
	EQUIPO 8	9 METROS	
	EQUIPO 9	10 METROS	
	EQUIPO 10	10 METROS	
	EQUIPO 11	12 METROS	
	EQUIPO 12	14 METROS	
	EQUIPO 13	14 METROS	
2	EQUIPO 1	2 METROS	3 REGULADORES
	EQUIPO 2	4 METROS	SWITCH 8 PUERTOS
	EQUIPO 3	6 METROS	
	EQUIPO 4	10 METROS	
	EQUIPO 5	22 METROS	
3	EQUIPO 1	4 METROS	
	EQUIPO 2	4 METROS	
	EQUIPO 3	5 METROS	
	EQUIPO 4	20 METROS	
	TOTAL	175 METROS	

7.3.3 Perspectiva económica

Luego del recorrido por las sedes, se presenta un cálculo del monto de los requerimientos, basado en costos estandarizados en la web y en proveedores locales. El resumen de los precios estimados se presenta en la Tabla 5. Posteriormente, se generó la requisición correspondiente para la adquisición del material, la cual se remite a la aprobación del jefe de arquitectos de la constructora; el tiempo de espera para contar con el material es de al menos 2 días hábiles.

Tabla 5 Requerimientos y costos.

Equipo	Cantidad	Precio	Total
Switch POE TP-Link Gigabit, 8 puertos, no administrable.	2	\$580.00	\$1,160.00
Switch TP-Link Gigabit Ethernet TL-SG116 puertos. No administrable.	1	\$1,100.00	\$1,100.00
TP-Link Archer BE3600 Router Compatibilidad con Wi-Fi 7. Velocidades superiores a 3.6 Gbps. Procesador multinúcleo.	3	\$1,200.00	\$3,600.00
Cable U/ftp Cat6a 305mts Xcase Blindada P/exterior 10gbps	1	\$2,400.00	\$2,400.00
Pinzas Para Ponchar Conectores Rj45, Mxcna-001	1	\$540.00	\$540.00
Conector Intellinet Rj45 Cat 6 Bote Con 100 Piezas	1	\$445.00	\$445.00
Impresora multifunción a color Canon Pixma G4170, sistema de tinta continua. Conectividad Wi-Fi. Escáner integrado.	4	\$4,799.00	\$19,196.00
Multifuncional Láser A Color Brother Tecnología láser. Impresión rápida. Alta calidad de impresión. Conectividad de red.	1	\$16,400.00	\$16,400.00
HP impresora DesignJet T630 de 36 pulgadas	1	\$34,000.00	\$34,000.00
Computadora Lenovo 23.8" All-In-One PC Procesador Intel Core i5. 16 GB de memoria RAM. Unidad SSD de 512 GB. Pantalla de 23.8 pulgadas. Conectividad Gigabit Ethernet.	5	\$5,100.00	\$25,500.00
PC con enfriamiento líquido Corei7 RTX 4060Ti Procesador Intel Core i7. Tarjeta gráfica RTX 4060 Ti. Sistema de enfriamiento líquido. Unidad SSD de alta velocidad. Capacidad de expansión.	2	\$27,000.00	\$54,000.00
Canaletas PCV 10 m.	10	\$380.00	\$3,800.00
Licencia Microsoft 365	3	\$1,800.00	\$5,400.00
		TOTAL	\$167,541.00

7.4 Estructura lógica

En la Figura 11 se ilustra la estructura general de la red con el propósito de visualizar la segmentación en la que está dividida, lo que permite una mejor administración y un mejor rendimiento.

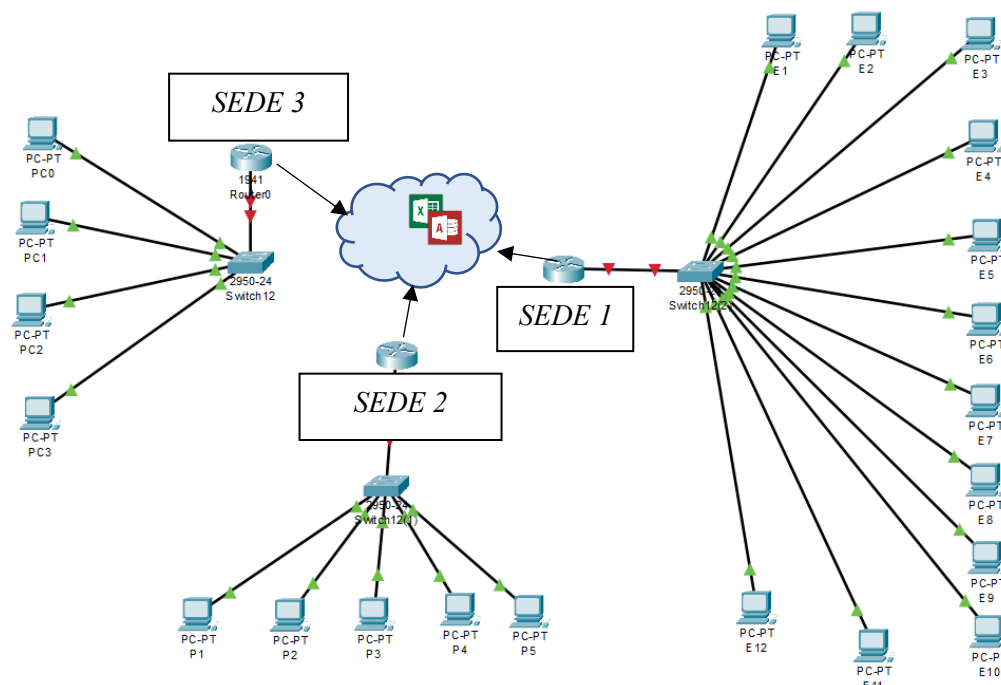


Figura 11. Estructura lógica general de la red.

8. DISEÑO E IMPLEMENTACIÓN

Antes de proceder al despliegue de la infraestructura, es necesario diseñar un esquema de red que defina la interrelación entre los dispositivos. Dado que la manipulación directa de equipos físicos aumenta la probabilidad de incidentes técnicos y averías, se recomienda emplear entornos de simulación virtual. Estos programas facilitan la realización de pruebas iterativas en un entorno seguro, permitiendo depurar la configuración y la conectividad sin comprometer los recursos materiales ni el presupuesto del proyecto.

8.1 Simulación en Cisco Packet Tracer 8.2.2

La importancia de la simulación, es demostrar que la estructura lógica planteada es funcional para después ser implementada, así vez demostrar en presentación con la NAVMER las ventajas en simplificación de tiempos para ventas requerimientos y sobre todo consultas.

Cisco Packet Tracer es un programa de simulación de redes desarrollado por la empresa Cisco que permite diseñar, configurar y probar redes informáticas de manera virtual, lo que facilita el aprendizaje práctico, ya que permite experimentar con configuraciones de red en un entorno seguro. También ayuda a comprender el funcionamiento de protocolos y dispositivos de red, permitiendo visualizar cómo se comunican entre sí. Otra ventaja importante es que reduce costos, ya que no es necesario adquirir equipos reales para realizar prácticas.

En la Figura 12 se muestra el diagrama completo de la red propuesta para la conexión de las tres sedes donde es importante resaltar la configuración principal de los routers los cuales son quienes darán la conexión, las IP de los equipos se dejarán de modo automático.

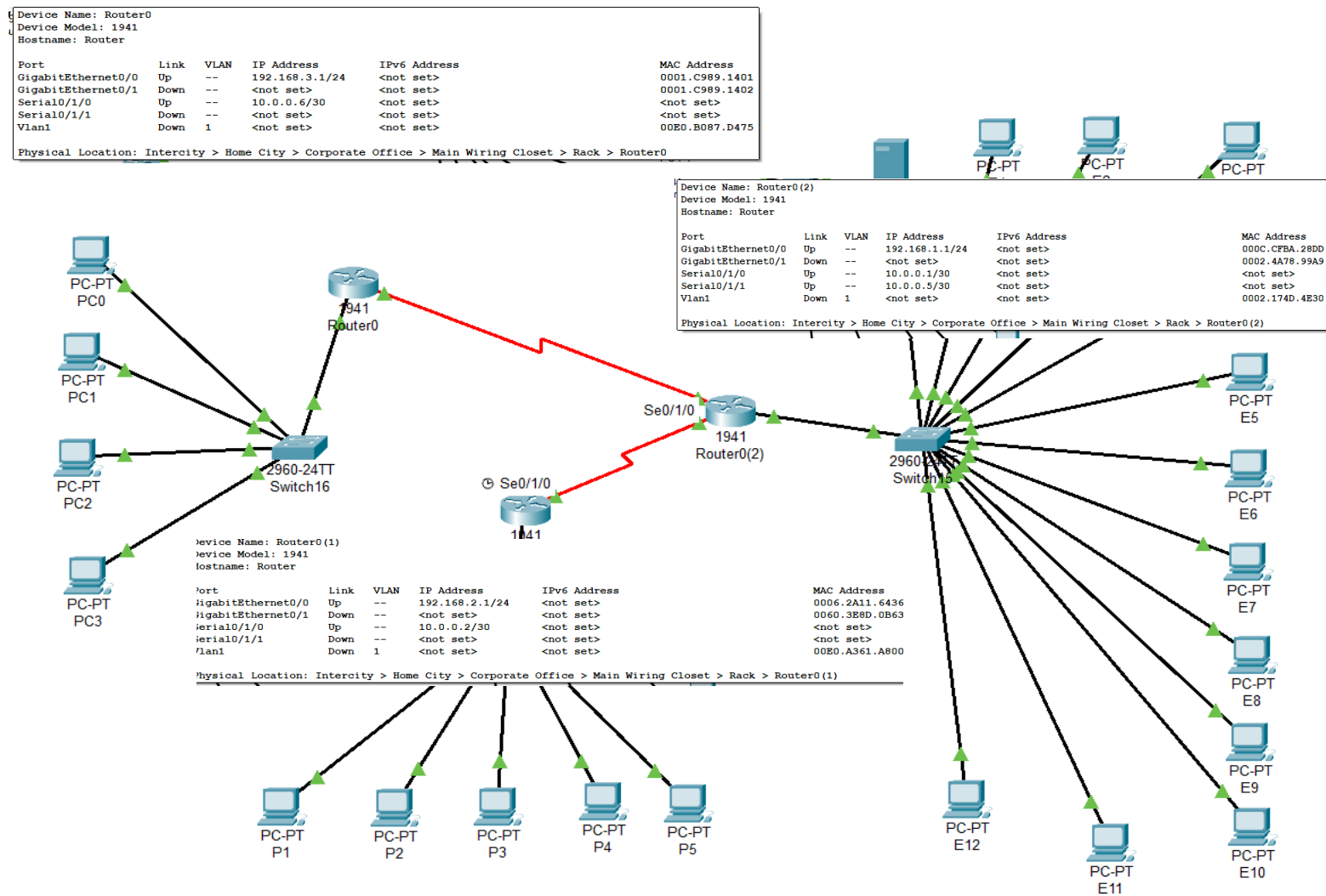


Figura 12. Diagrama implementado en el simulador Cisco Packet Tracer 8.2.2.

Uno de los elementos más importantes de esta infraestructura son los routers, ya que son los que ayudan a generar una conexión entre las tres sedes de NAVMER, dentro del simulador; para que puedan trabajar en el archivo de inventario, primero se configuran las interfaces GigabitEthernet0/0 de cada router para que actúen como el Gateway de sus respectivas redes:

Sede 1 -- Gig0/0 -- 192.168.1.1 -- 255.255.255.0

Sede 2 -- Gig0/0 -- 192.168.2.1 -- 255.255.255.0

Sede 3 -- Gig0/0 -- 192.168.3.1 -- 255.255.255.0

Se configura el router (Figura 13) de cada una de las sedes para que trabaje con el switch y se generen de forma automática las direcciones IP de los equipos, y dejando estática la IP que se le dio antes al router.

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip dhcp pool SEDE1 POOL
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
```

Figura 13. Configuración DHCP de routers.

Para obtener la IP automática en los equipos (Figura 14), en el menú del equipo nos dirigimos a la pestaña de configuración, hacemos clic en ip Configuration y seleccionamos DHCP (Dynamic Host Configuration Protocol); automáticamente se asignará la IP.

Después, para el enlace, habilitaremos los módulos HWC-2T (Figura 15). Esto ayudará a simular la conexión y el envío de datos entre las sedes. Lo lograremos a través de un cable Serial DCE que uniremos en los puertos (Serial0/1/0 y Serial0/1/1) habilitados de cada router, siendo la sede 1 quien ocupará los dos como la principal. Primero, le debemos dar identidad a la red externa; nuevamente, lo haremos en la figura de CLI.

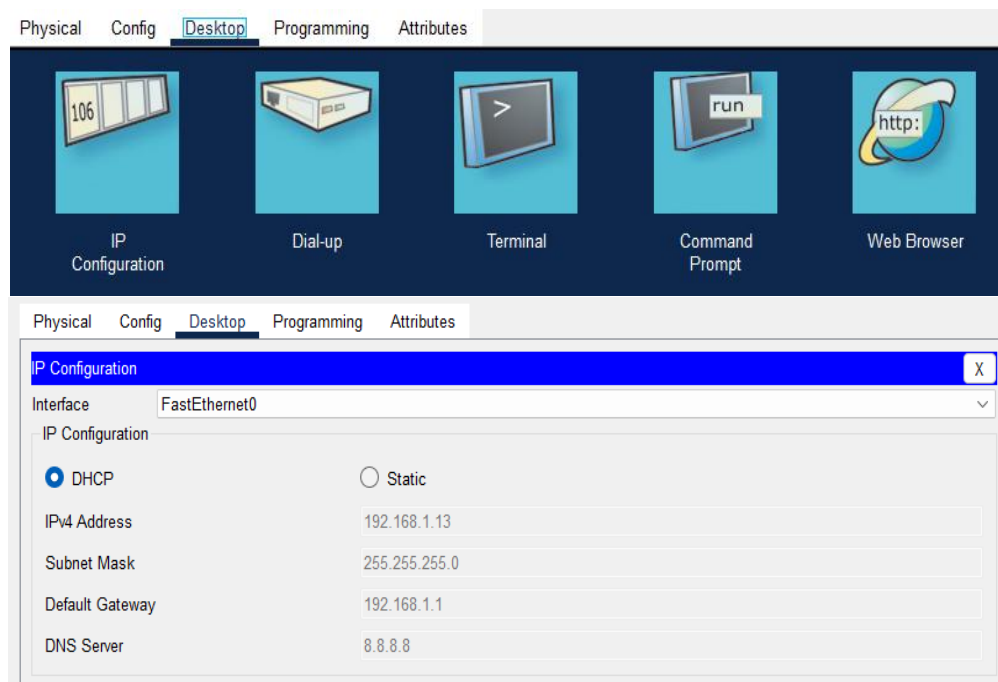


Figura 14. Configuración de equipos para ip dinámicas.

```
Router>enable
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface Serial0/1/0
Router(config-if)#ip address 10.0.0.1 255.255.255.252
```

SEDE 1

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface Serial0/1/1
Router(config-if)#ip address 10.0.0.3 255.255.255.252
```

SEDE 1

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface Serial0/1/0
Router(config-if)#ip address 10.0.0.2 255.255.255.252
```

SEDE 2

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface Serial0/1/0
Router(config-if)#ip address 10.0.0.4 255.255.255.252
```

SEDE 3

Figura 15. Interfaz de puertos seriales.

Ya hecha la configuración de la interfaz serial de los routers, es indispensable indicar la ruta para la comunicación entre ellos, lo realizamos de la siguiente manera (Figura 16).

```
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 192.168.2.0 255.255.255.0 10.0.0.2
```

SEDE 1

```
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 192.168.3.0 255.255.255.0 10.0.0.3
```

SEDE 1

```
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 192.168.1.0 255.255.255.0 10.0.0.1
```

SEDE 2

```
Router>ENABLE
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 192.168.1.0 255.255.255.0 10.0.0.4
```

SEDE 3

Figura 16. Comunicación entre sedes mediante una interfaz serial.

Para simular la conexión con la base de datos de la constructora en el simulador ocuparemos poner un servidor que nos servirá como guía para la demostración de la comunicación entre las sedes, lo realizamos de la siguiente manera: En Packet Tracer, hacemos clic sobre el servidor, en la pestaña Desktop > IP Configuration (Figura 17) y asignamos los siguientes valores de forma manual (estática) para asegurar que la base de datos siempre sea localizable:

Dirección IP: 192.168.1.5

Máscara de subred: 255.255.255.0

Puerta de enlace predeterminada: 192.168.1.1 (la IP del router de la Sede 1)

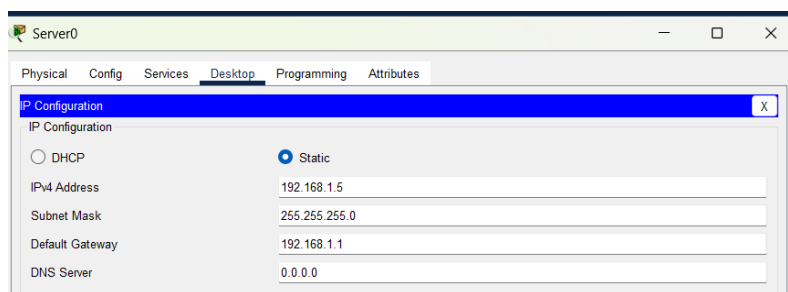


Figura 17. Configuración de servidor

Aunque Packet Tracer no ejecuta un motor SQL real, se utiliza el servicio HTTP/HTTPS para simular una interfaz de base de datos o el servicio DNS para resolver el nombre del servidor. Después, para simular el acceso web a la base de datos, nos dirigimos a la pestaña Services > HTTP y nos aseguramos de que esté en la posición “On” (Figura 18).

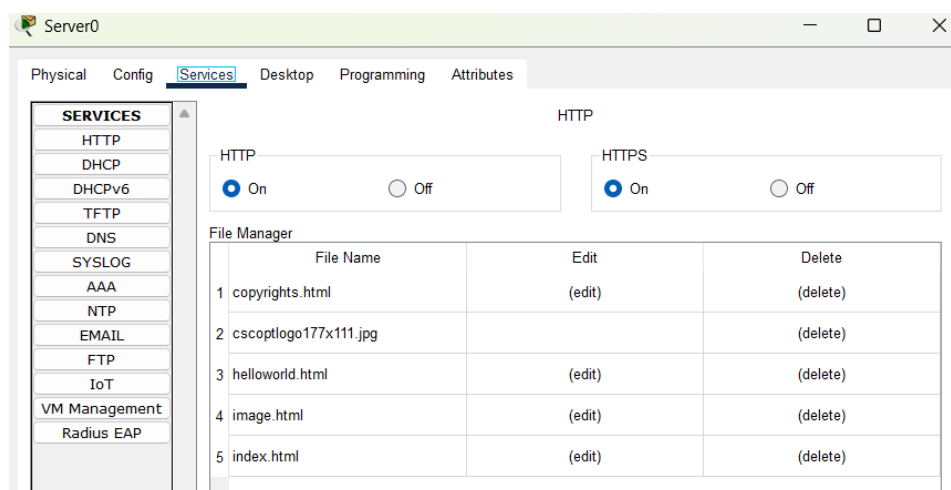


Figura 18. Servicio HTTP/HTTPS

Editamos el archivo index.html (Figura 19) para que diga algo representativo como: "BIENVENIDOS A CONSTRUCTORA NAVMER-SISTEMA DE INVENTARIOS CENTRALIZADOS".

Para evitar que el servicio DHCP le asigne la IP del servidor (192.168.1.5) a una computadora por error, agregamos este comando en el router de la Sede 1. *Figura 20* (Reserva las primeras 10 direcciones para servidores y equipos críticos).

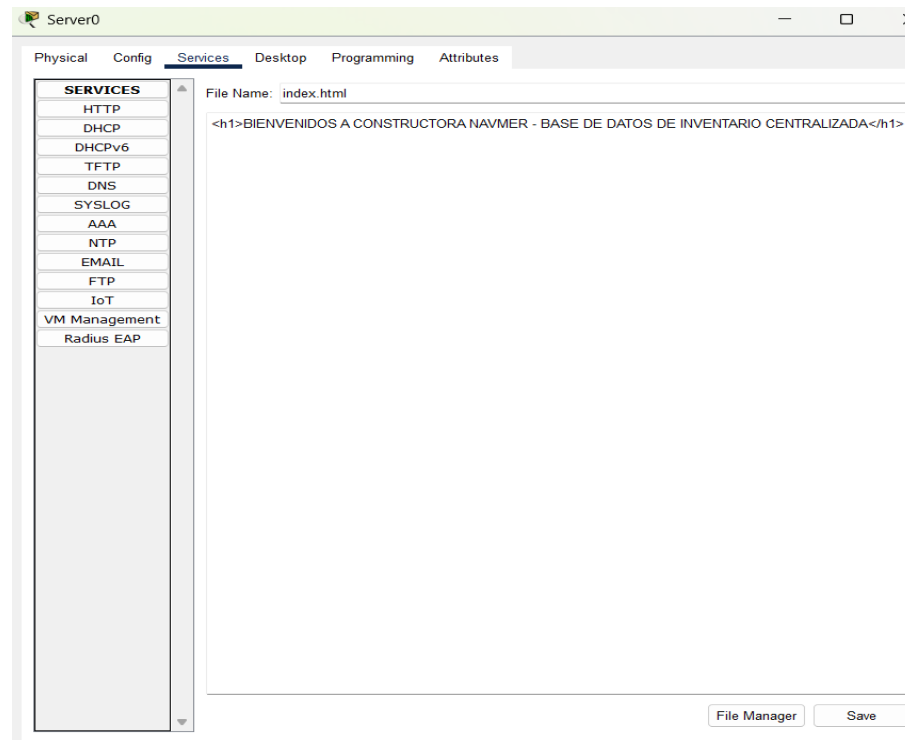


Figura 19. Edición de archivo index.html

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
```

Figura 20 Evitar error de asignación.

Ya terminada la configuración de los dispositivos, realizamos la prueba para saber si hay comunicación entre las sedes, elegimos cualquier equipo de las sedes 2 y 3 y nos dirigimos a Desktop y damos clic en Web Browser, en url escribimos la ip del servidor 192.168.1.5, *Figura 21*, si todo sale bien y hay comunicación entre las sedes nos aparecerá el texto que colocamos en el index.html.

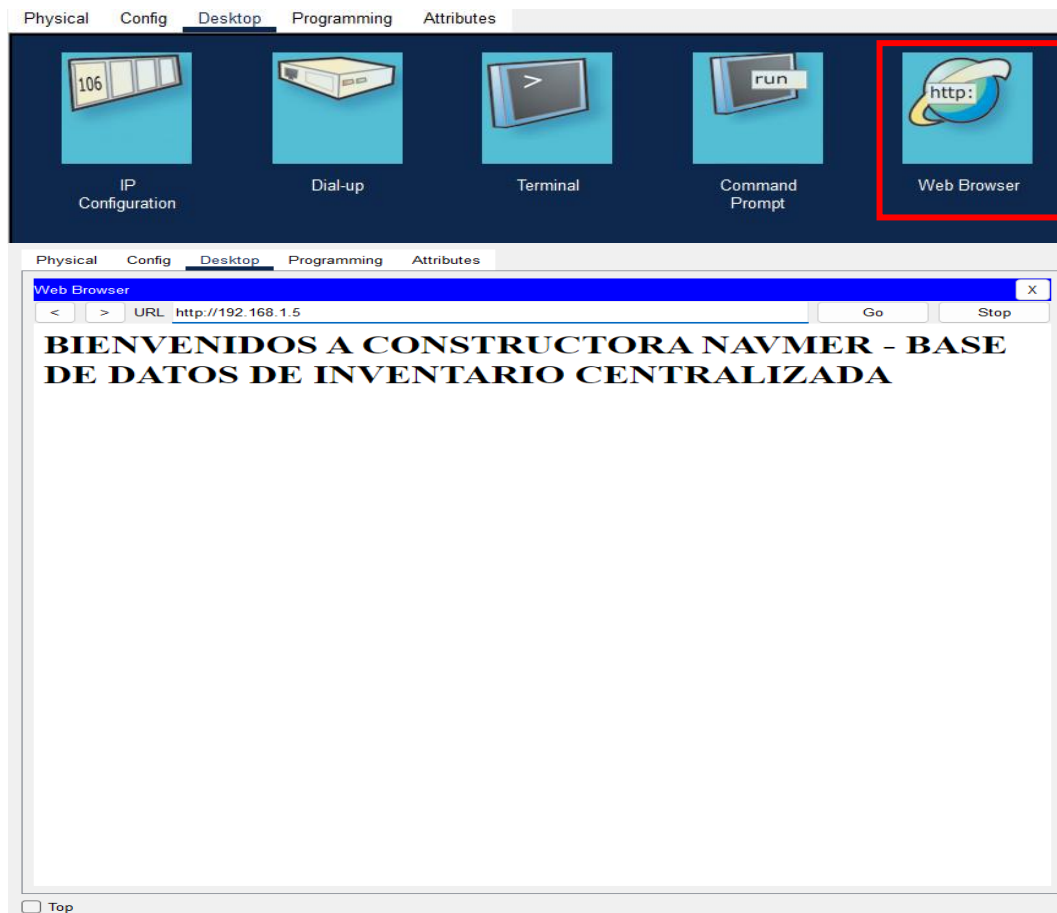


Figura 21 Prueba de conexión entre sedes.

8.2 Implementación de infraestructura

Para la implementación de la red en la constructora NAVMER, basándonos en los datos del recorrido previo, lo realizaremos en dos fases para poder el cumplimiento y sobre todo de la funcionalidad de la misma. Se comienza con el análisis de instalación de los nuevos equipos, así como la reubicación de los equipos ya colocados, de ser necesario.

Tabla 6 Equipos existentes e instalados.

SEDE	EQUIPOS NAVMER		
	EXISTENTES	INSTALADOS	TOTAL
1	9	4	13
2	3	2	5
3	2	2	4

Se instalaron los complementos de oficina como lo son: equipos de cómputo, reguladores e impresoras (*Figura 22*).



Figura 22 Instalación de nuevos equipos.

Se colocan el router y el switch en cada una de las sedes (*Figura 23*, *Figura 24* y *Figura 25*) para comenzar con la instalación de cableado en cada área que se necesita a través de tuberías y canaletas dependiendo del espacio y distancia.



Figura 23 Instalación Router y switch sede 1.



Figura 24 Instalación Router y switch sede 2.



Figura 25 Instalación Router y switch sede 3.

8.3 Acceso a interfaz de gestión

En la sede 1 se conecta un equipo de cómputo a uno de los puertos LAN del router mediante un cable Ethernet Categoría 6 y abrimos el navegador web, ingresamos la dirección [<http://192.168.1.254>] que corresponde a la IP del modem del proveedor de internet, en la *Figura 26* se muestra la interfaz para la configuración, con base a la propuesta de red, modificamos esta dirección a [192.168.254.254] para que no genere un conflicto de conectividad con el router. Se aplican los cambios y se cierra.

Ya que se configuró el módem, realizamos la del router Archer BE3600, abrimos el navegador y colocamos [<http://192.168.0.1>], que por configuración de fábrica es la IP de comunicación. En la *Figura 27* se muestra la interfaz.



Figura 26 Interfaz modem del proveedor

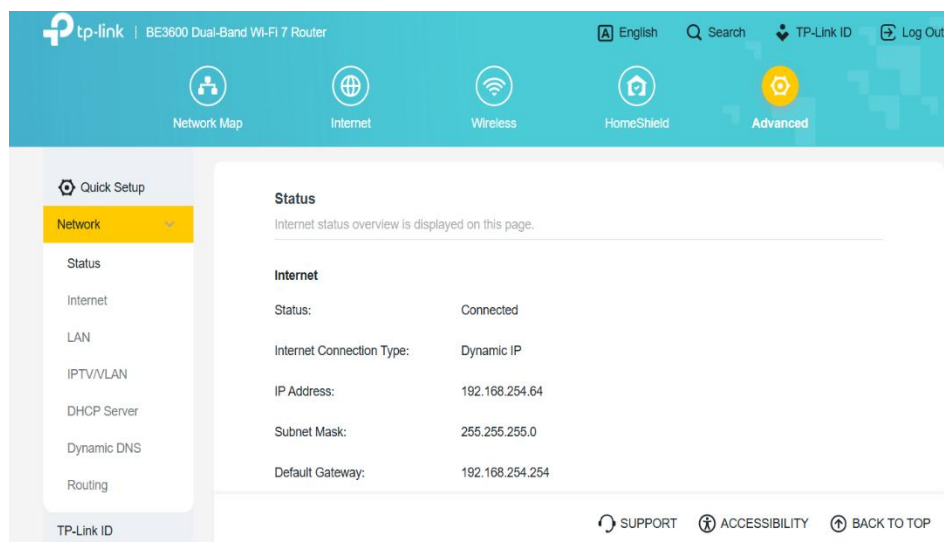


Figura 27 Interfaz router Archer BE3600

8.3.1 Configuración de la Red Local (LAN)

Nos dirigimos a la pestaña Advanced > Network > LAN y cambiamos la IP por la propuesta para el proyecto. *Figura 28*. Se da clic en Save, lo que hará que el router se reinicie, pero

para ingresar ahora se usará la nueva IP (192.168.1.1).

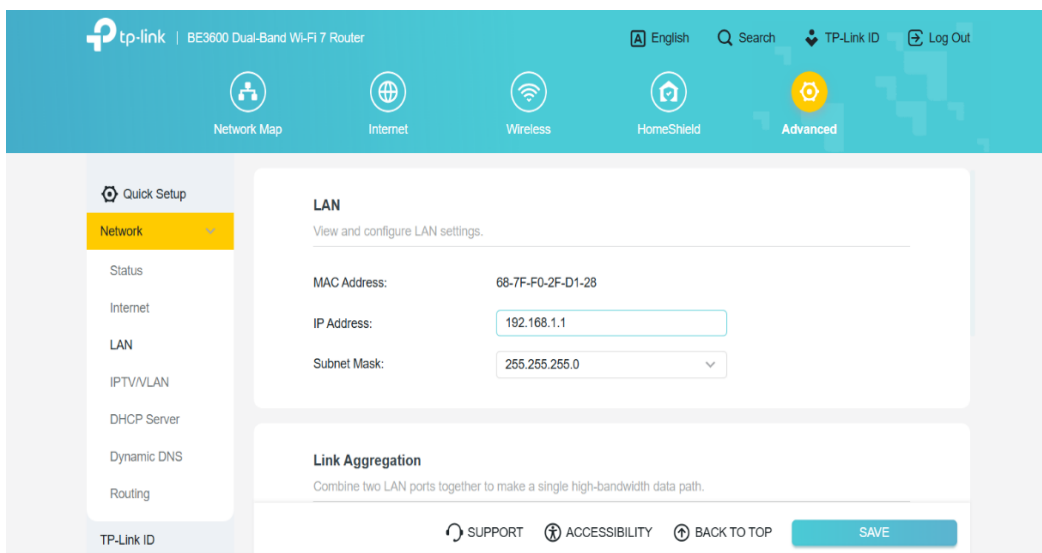


Figura 28 Configuración LAN Router

8.3.2 Interconexión entre Sedes (Enrutamiento Estático)

Para que el tráfico de la Sede 1 pueda alcanzar a la Sede 2 y Sede 3: entramos nuevamente a la interfaz y se navega a Advanced > Network > Routing, en Static Router, se añaden las entradas que corresponde a la sede 1 y sede 2. cómo se muestran en la *Figura 29*.

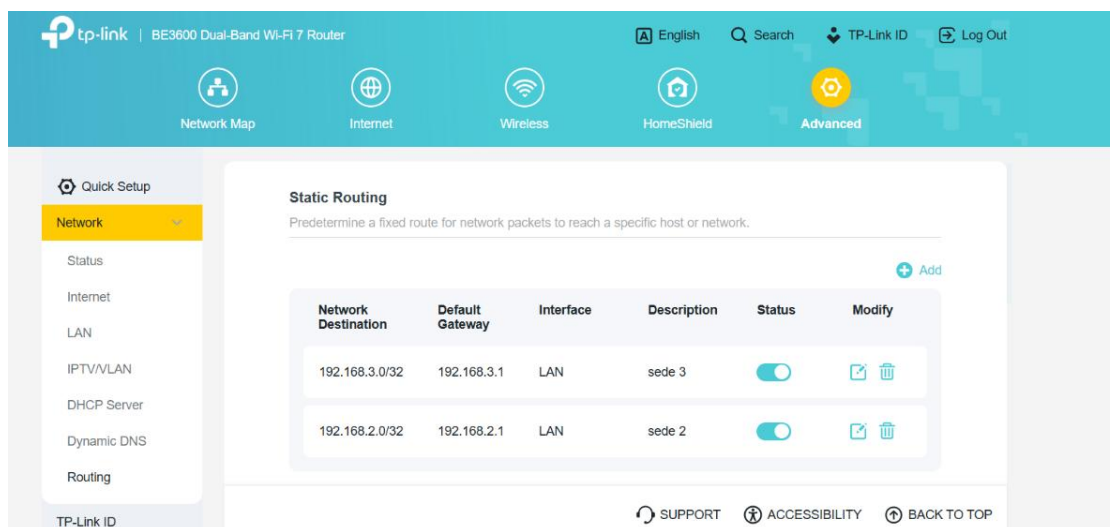


Figura 29 Interconexión de sedes en Router de sede 1

8.3.3 Túneles VPN

Como las sedes están lejos, no podemos tirar un cable físico entre ellas. En su lugar, crearemos un "túnel" virtual y cifrado a través de internet para garantizar la comunicación, se tiene aspectos a resaltar en esta implementación:

Privacidad: Aunque los datos viajen por el internet público de Infinitum u otro proveedor, van encriptados, por lo que la información de Constructora NAVMER viaja segura.

Transparencia: Una vez configurado el túnel, la Sede 2 y Sede 3 (con sus equipos) "creerá" que está conectada por cable directamente a la Sede 1, permitiendo el acceso al servidor de base de datos de forma fluida.

El router Archer BE3600 es una excelente herramienta para esto porque soporta protocolos de VPN profesionales (como OpenVPN o WireGuard) esto se logra en dos pasos:

Paso 1: Debido a que las conexiones residenciales o comerciales suelen tener IPs públicas que cambian, es necesario asignar un "nombre de dominio" a la Sede 1 para que las otras sedes siempre puedan localizarla, es por eso que comenzaremos por crear un host gratuito pero funcional para nuestra red, se opta por NO-IP ya que tiene la solución y ofrece un servicio de DNS dinámico totalmente gratuito que utilizan a diario (noip, 2026) en la *Figura 30* se muestra la creación de host para Constructora NAVMER.

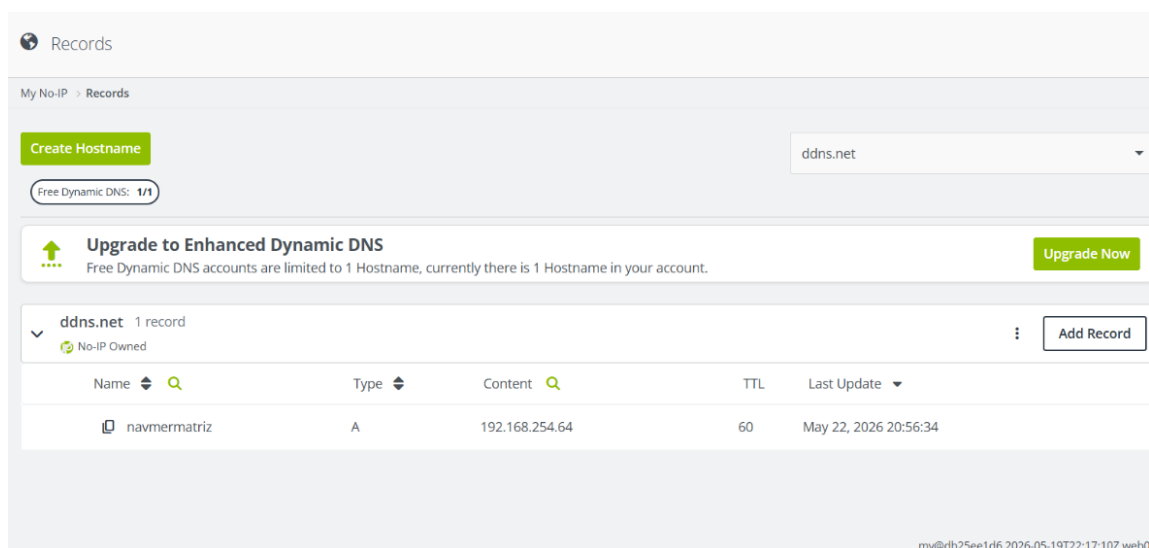


Figura 30 NO-IP creación de dominio.

Ya que se tiene el dominio se ingresa a la interfaz del Archer BE3600 a Advanced > Network > Dynamic DNS, normalmente se selecciona NO-IP, en username y password se usan los datos con los que nos registramos para dar de alta el dominio en la página de NO.IP (*Figura 31*). Una vez vinculado, este nombre apuntará siempre a la IP pública actual de la sede principal.

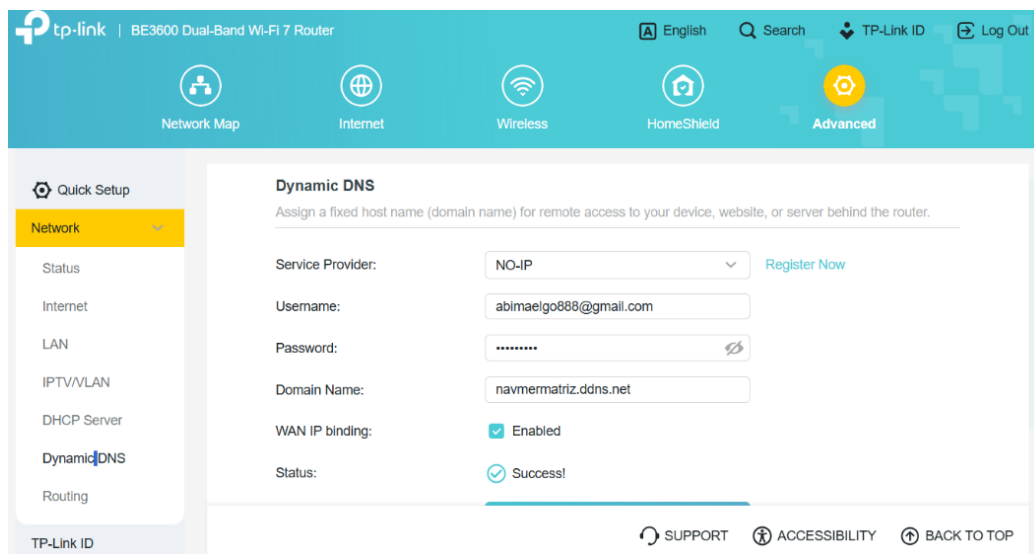


Figura 31 Alta de dominio en Router Archer BE3600

Paso 2: En este paso se crea el "túnel" que permitirá que los 13 equipos de la Sede 1 se hablen con los 5 equipos de la Sede 2 y los 4 de la Sede 3; en el Archer BE3600, nos dirigimos a Advanced > VPN Server, se selecciona OpenVPN (recomendado por su compatibilidad y seguridad), se habilita el servidor VPN, en Service Type > UDP, en Client Access > Internet and Home Network para que las sedes remotas puedan ver el servidor de base de datos.

Figura 32

Después se da clic en *Generate* para crear el certificado de seguridad (*Figura 33*) ya terminado damos clic en *Export* para descargar el archivo de configuración (.ovpn) *Figura 34*. Este archivo es el "pasaporte" que se usará en las otras sedes.

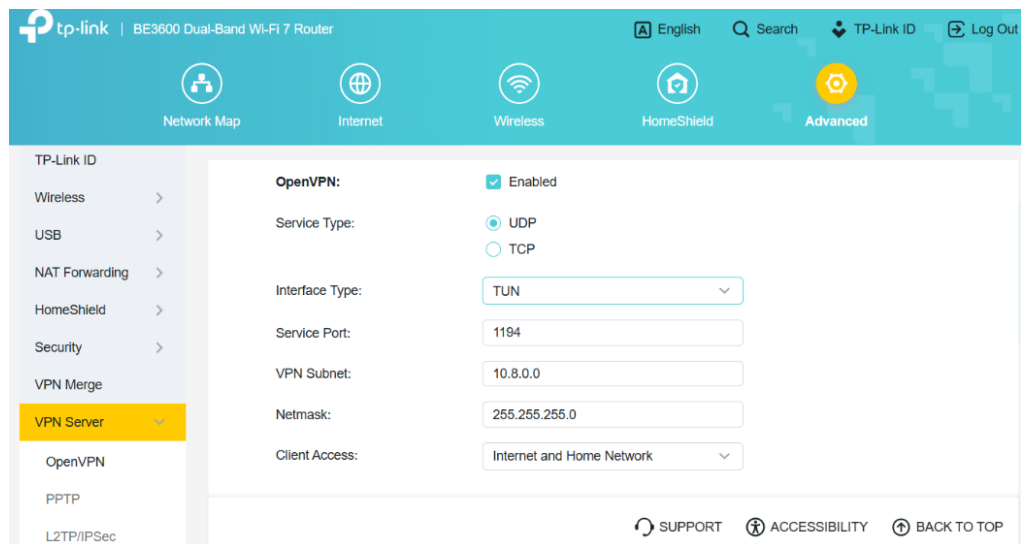


Figura 32 Configuración de servidor VPN en Router Archer BE3600

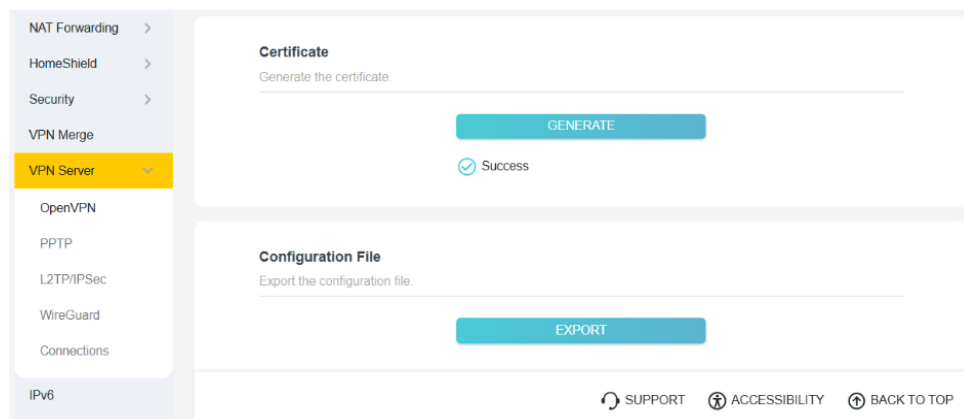


Figura 33 Generando archivo (.ovpn) para comunicar sedes.

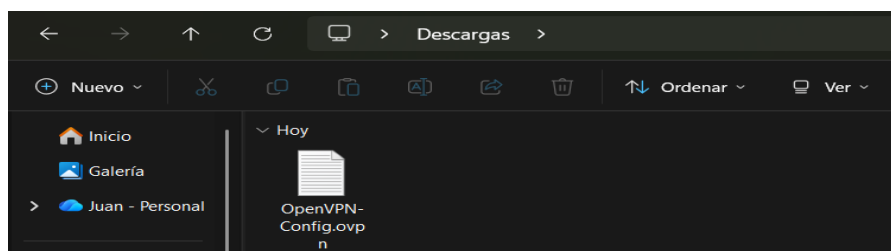


Figura 34 Archivo (.ovpn)

Paso 3: Para que el tráfico de la VPN pueda llegar desde el exterior hasta el router, el módem Huawei HG8145V5V3 debe permitir el paso de datos. Para lograrlo en la interfaz del módem, en la pestaña Reglas de desvío (Forwarding Rules), se selecciona Configuración de mapeo de puertos *Figura 35* (Port Mapping Configuration), creamos una nueva regla con los siguientes parámetros:

Nombre de la aplicación: VPN_NAVMER.

Host interno: 192.168.1.1 (IP del Archer BE3600).

Protocolo: UDP.

Puerto externo/interno: 1194 la cual es la que usa OpenVPN.

Suele pasar que los modem identifiquen el router y lo muestra, como en este caso que da la opción de seleccionar y te da la IP con la que lo identifica. Terminamos haciendo clic en Aplicar.

Reglas de desvío > Port Forwarding

Esta página permite configurar los parámetros para la función de Port Forwarding.
Nota: Los puertos conocidos para los servicios de voz no pueden estar en el rango de los puertos de asignación.

Nueva Eliminar

Nombre de mapeo	Nombre de WAN	Host interno	Host externo	Estado
☒ VPN_NAVMER	1_TR069_VOIP_INTERNET_R_VID_881	192.168.254.64	--	Habilitado

Tipo: ☒ Personalizar ☐ Aplicación

Aplicación:

Habilitar regla de mapeo: ☒

Nombre de mapeo:

Nombre de WAN:

Host interno:

Dirección IP de origen externa:

Protocolo:

Número de puerto interno:

Número de puerto externo:

Número de puerto de origen externo:

Eliminar

Agregar puerto

Aplicar Cancelar

Figura 35 Apertura de Puertos (Port Forwarding) en el Módem.

8.3.4 Conexión estable del túnel VPN

Para garantizar que la conexión se establezca entre los diferentes municipios donde se encuentran las sedes de la Constructora NAVMER y el túnel VPN no se rompa, es fundamental que el módem siempre reconozca al router con la misma identidad. Para realizar la reserva de IP en el módem, accedemos a la pestaña LAN > DHCP Static IP Reservation > Nuevo y vinculamos el router. *Figura 36*

The screenshot shows the 'LAN' configuration page of a modem. The left sidebar contains a menu with the following items: 'Configuración del puerto LAN', 'Configuración del Gateway', 'Configuración del servidor DHCP', and 'Configuración IP estática DHCP'. The main content area is titled 'LAN > Configuración IP estática DHCP'. A yellow informational box states: 'Esta página permite configurar la dirección IP reservada que está asignada via DHCP para la dirección MAC específica.' Below this, there are 'Nueva' and 'Eliminar' buttons. A table lists reserved IP addresses with columns for 'Dirección MAC' and 'Dirección IP'. The first entry is selected, showing MAC '68:7f:f0:2f:d1:29' and IP '192.168.254.64'. Below the table, there are input fields for 'Dirección MAC:' and 'Dirección IP:', followed by 'Aplicar' and 'Cancelar' buttons.

	Dirección MAC	Dirección IP
☒	68:7f:f0:2f:d1:29	192.168.254.64

Dirección MAC: (AA:BB:CC:DD:EE:FF)

Dirección IP:

Figura 36 Vinculación router a una IP estática en modem.

Al moverse entre municipios, las otras sedes buscarán a la Sede 1 a través de esta "puerta". Si la IP del router cambiara (por ejemplo, a la .65), el Port Forwarding que se configuró con el puerto 1194 apuntaría a una dirección vacía y la red de la constructora quedaría incomunicada.

8.3.5 Conexión de las Sedes Remotas (Sedes 2 y 3)

Para la interconexión: nos trasladamos a la Sede 2 y Sede 3 para la configuración de módem y router, al igual que se hizo en la Sede 1, cambiamos las IPs de acuerdo al proyecto propuesto, *Figura 37, Figura 38, Figura 39 y Figura 40*.

Exceso de velocidad

Estado WAN **LAN** PORT IPv6 WLAN Seguridad Ruteo Reglas de desvío Aplicaciones de red Herramientas

Configuración del puerto LAN LAN > Configuración del Gateway

Configuración del Gateway

Configuración del servidor DHCP

Configuración IP estática DHCP

Esta página permite configurar la dirección IP de administración de LAN. Después de cambiar la dirección IP de administración de LAN, asegúrese de que el pool de direcciones primarias del servidor DHCP esté en la misma subred que la nueva dirección IP de LAN. De lo contrario, el servidor DHCP no funcionará adecuadamente.

Dirección primaria

Dirección IP primaria:

Máscara de subred de dirección primaria:

Figura 37 Configuración módem Sede 2.

Estado WAN **LAN** PORT IPv6 WLAN Seguridad Ruteo Reglas de desvío Aplicaciones de red Herramientas

Configuración del puerto LAN LAN > Configuración del Gateway

Configuración del Gateway

Configuración del servidor DHCP

Configuración IP estática DHCP

Esta página permite configurar la dirección IP de administración de LAN. Después de cambiar la dirección IP de administración de LAN, asegúrese de que el pool de direcciones primarias del servidor DHCP esté en la misma subred que la nueva dirección IP de LAN. De lo contrario, el servidor DHCP no funcionará adecuadamente.

Dirección primaria

Dirección IP primaria:

Máscara de subred de dirección primaria:

Figura 38 Configuración módem Sede 3.

Network Map Internet Wireless HomeShield Advanced

Quick Setup

Network

Status

Internet

LAN

IPTV/VLAN

DHCP Server

Dynamic DNS

Routing

LAN

View and configure LAN settings.

MAC Address: 3C-64-71-A9-B2-7E

IP Address:

Subnet Mask:

Link Aggregation

Combine two LAN ports together to make a single high-bandwidth data path.

Figura 39 Configuración Router Sede 2

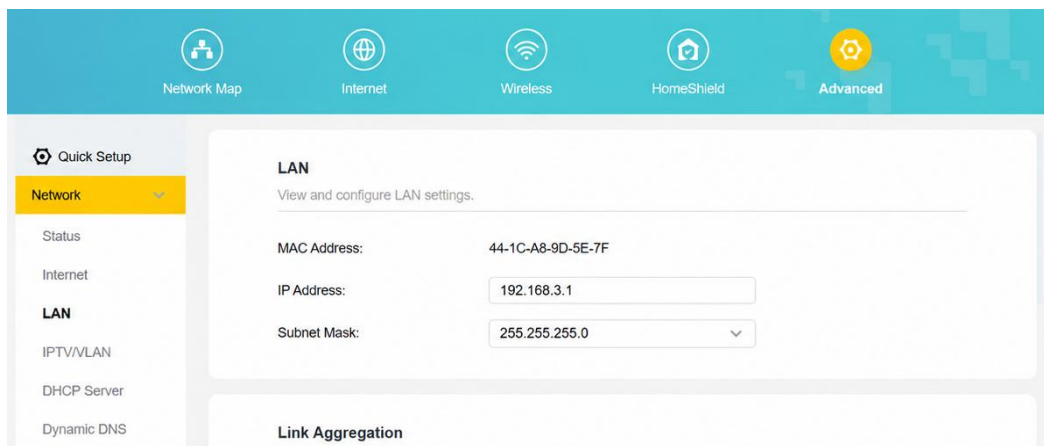


Figura 40 Configuración de Router Sede 3

Para finalizar se vinculan los routers para que se tenga el enlace a la Sede 1, esto se logra accediendo en Advanced > VPN Merge > Server List > Add, damos nombre y subimos el archivo (.ovpn) que generamos en el router de la Sede 1. *Figura 41.*

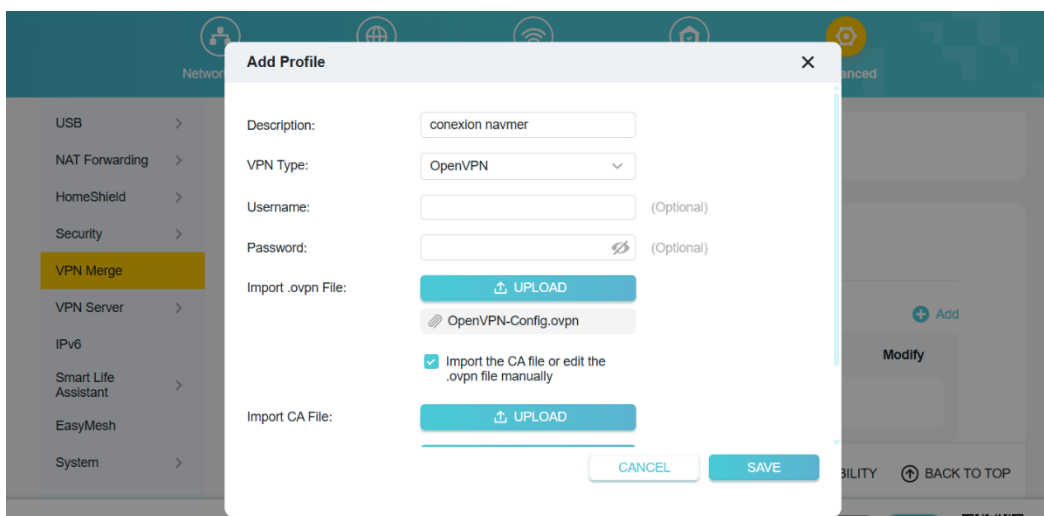


Figura 41 Vinculación VPN en Sede 2 y 3

Finalmente, se verifica que se conecta a la VPN, por lo cual se puede empezar a trabajar en la red. *Figura 42*

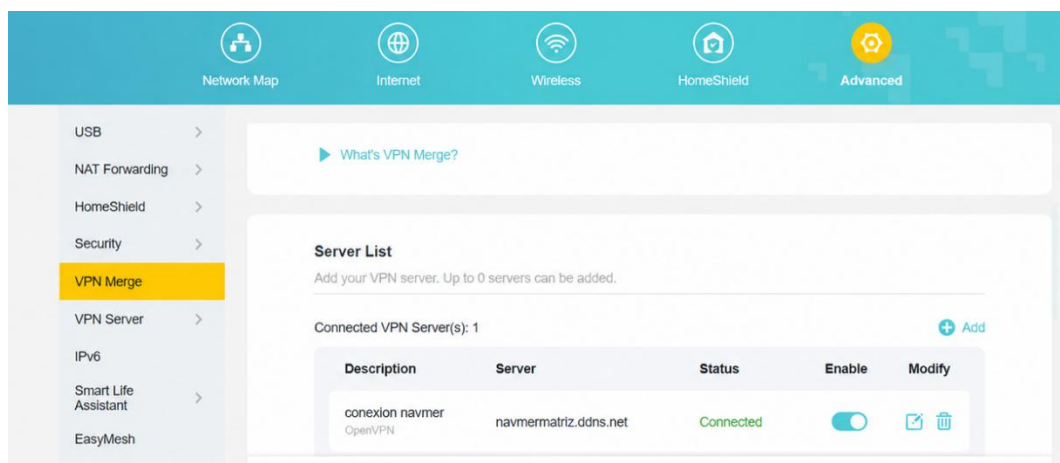


Figura 42 VPN Conectada

8.4 Pruebas de conectividad y seguridad

La fase de validación técnica constituyó un paso crítico para garantizar que la infraestructura de red implementada cumpliera con los estándares de rendimiento, estabilidad y seguridad requeridos por la operación multisede de Constructora NAVMER.

En esta sección se documentan las pruebas de conectividad y los protocolos de seguridad ejecutados, los cuales abarcaron desde la verificación lógica del tráfico y los tiempos de respuesta entre sedes, hasta la aplicación de controles de ciberseguridad perimetral y de acceso. A través de esta evaluación, se comprobó la eficacia de la arquitectura diseñada, asegurando que los flujos de información y la integridad de los datos corporativos operaran de manera óptima y confiable en un entorno de producción real.

8.4.1 Pruebas lógicas

Mediante la consola de comandos del sistema operativo Windows (Command Prompt - CMD), se ejecutan distintos comandos con la finalidad de comprobar la comunicación entre dispositivos, analizar los tiempos de respuesta en la transmisión de datos y verificar la configuración y el funcionamiento de la red. Estas pruebas permitieron identificar el estado de conexión y las rutas de comunicación existentes entre los equipos.

A continuación, se presenta una breve descripción de algunos de los comandos utilizados

durante el desarrollo de las pruebas: *ping*, *ipconfig /all*, *netstat* y *tracert*.

1. El comando **ping** se emplea para verificar la conectividad entre dispositivos de red, además de medir el tiempo que tardan los paquetes de datos en enviarse y recibirse.
2. El comando **tracert** permite visualizar la ruta que siguen los paquetes de información desde un equipo hasta su destino, mostrando cada uno de los saltos y el tiempo de respuesta correspondiente.
3. El comando **ipconfig (/all)** proporciona información detallada sobre la configuración de red del equipo, incluyendo direcciones IP, adaptadores de red, configuración DNS y demás parámetros de conexión.
4. El comando **netstat** se utiliza para consultar las conexiones activas del equipo, así como el estado de los puertos y servicios de red en funcionamiento

En la *Figura 43* se ilustra una prueba de comunicación entre equipos de la misma LAN mediante el comando **ping**. En la constructora NAVMER existen sedes, diferenciadas por su LAN. En la *Figura 44* se ilustra una prueba **ping** de la sede 1 a la sede 2 con excelente tiempo de respuesta.

```
C:\Users\Equipo1>ping 192.168.1.17

Haciendo ping a 192.168.1.17 con 32 bytes de datos:
Respuesta desde 192.168.1.17: bytes=32 tiempo=53ms TTL=64
Respuesta desde 192.168.1.17: bytes=32 tiempo=40ms TTL=64
Respuesta desde 192.168.1.17: bytes=32 tiempo=52ms TTL=64
Respuesta desde 192.168.1.17: bytes=32 tiempo=51ms TTL=64

Estadísticas de ping para 192.168.1.17:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
        (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 40ms, Máximo = 53ms, Media = 49ms

C:\Users\Equipo1> ■
```

Figura 43 prueba ping misma LAN.

```

Adaptador desconocido Conexión de área local:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Conexión de área local* 1:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Conexión de área local* 2:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Wi-Fi:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :

Adaptador de Ethernet Conexión de red Bluetooth:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :

Adaptador de Ethernet Ethernet:

    Estado de los medios. . . . . : medios conectados
    Sufijo DNS específico para la conexión. . :
    Vínculo: dirección IPv6 local. . . . : fe80::4b77:f4e3:ccf9:2a61%11
    Dirección IPv4. . . . . : 192.168.1.169
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . : 192.168.1.1

C:\Users\Equipo1>ping 192.168.2.114

Haciendo ping a 192.168.2.114 con 32 bytes de datos:
Respuesta desde 192.168.2.114: bytes=32 tiempo=6ms TTL=64
Respuesta desde 192.168.2.114: bytes=32 tiempo=10ms TTL=64
Respuesta desde 192.168.2.114: bytes=32 tiempo=12ms TTL=64
Respuesta desde 192.168.2.114: bytes=32 tiempo=33ms TTL=64

Estadísticas de ping para 192.168.2.114:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 6ms, Máximo = 33ms, Media = 15ms

```

Figura 44 Prueba de conexión a Sede 2.

En la *Figura 45* se muestra ahora la comunicación con la sede 3, con resultados positivos similares. Posteriormente, se ejecuta el comando **ipconfig all** (*Figura 46*) donde se muestran los datos principales de la configuración de red del equipo

```

Adaptador de Ethernet Ethernet:

Estado de los medios. . . . . : medios conectados
Sufijo DNS específico para la conexión. . :
Vínculo: dirección IPv6 local. . . . . : fe80::4b77:f4e3:ccf9:2a61%11
Dirección IPv4. . . . . : 192.168.1.169
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . : 192.168.1.1

C:\Users\Equipo 1>ping 192.168.3.68

Haciendo ping a 192.168.3.68 con 32 bytes de datos:
Respuesta desde 192.168.3.68: bytes=32 tiempo=4ms TTL=64
Respuesta desde 192.168.3.68: bytes=32 tiempo=17ms TTL=64
Respuesta desde 192.168.3.68: bytes=32 tiempo=29ms TTL=64
Respuesta desde 192.168.3.68: bytes=32 tiempo=3ms TTL=64

Estadísticas de ping para 192.168.3.68:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
        (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 3ms, Máximo = 29ms, Media = 13ms

C:\Users\Equipo 1>

```

Figura 45 Prueba de conexión a Sede 3.

```

Adaptador de Ethernet Ethernet:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . :
Descripción . . . . . : Realtek Gaming GbE Family Controller
Dirección física. . . . . : 14-13-33-29-6F-79
DHCP habilitado. . . . . : sí
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . . . : fe80::4b77:f43:ccf9:2a61%11(Preferido)
Dirección IPv4. . . . . : 192.168.1.169(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : lunes, 25 de mayo de 2026 05:53:31 p. m.
La concesión expira . . . . . : domingo, 4 de julio de 2162 12:48:03 a. m.
Puerta de enlace predeterminada . . . . . : 192.168.1.1
Servidor DHCP . . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 118756147
DUID de cliente DHCPv6. . . . . : 00-01-01-00-31-32-E7-CB-84-69-93-68-57-01
Servidores DNS. . . . . : 192.168.1.1
NetBIOS sobre TCP/IP. . . . . : habilitado

Adaptador de LAN inalámbrica Wi-Fi:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . :
Descripción . . . . . : MediaTek MT7921 Wi-Fi 6 802.11ax PCIe Adapter
Dirección física. . . . . : 84-69-93-68-57-01
DHCP habilitado. . . . . : sí
Configuración automática habilitada . . . : sí

Adaptador de Conexión de red Bluetooth:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . :
Descripción . . . . . : Bluetooth Device (Personal Area Network)
Dirección física. . . . . : 14-13-33-29-6F-78
DHCP habilitado. . . . . : sí
Configuración automática habilitada . . . : sí

C:\Users\abima>

```

Figura 46 Prueba ipconfig all.

La *Figura 47* y *Figura 48* muestran las pruebas de rastreo efectuada con el comando **tracert**, empleada para monitorizar cronológicamente cada uno de los saltos y puertas de enlace que intervienen en el trayecto hacia cada una de las sedes.

```
C:\Users\Equipo 1>tracert 192.168.2.1

Traza a la dirección 192.168.2.1 sobre un máximo de 30 saltos:

  1    <1 ms    <1 ms    <1 ms    192.168.1.169
  2     2 ms     2 ms     2 ms    192.168.254.254
  3     6 ms     6 ms     5 ms    10.0.0.1
  4     8 ms     7 ms     7 ms    10.0.0.2
  5    12 ms    11 ms    12 ms    192.168.253.254
  6    15 ms    14 ms    15 ms    192.168.2.1

Traza completa.

C:\Users\Equipo 1>
```

Figura 47 Prueba tracert de conexión a Sede 2.

```
C:\Users\Equipo 1>tracert 192.168.3.1

Traza a la dirección 192.168.3.1 sobre un máximo de 30 saltos:

  1    <1 ms    <1 ms    <1 ms    192.168.1.169
  2     2 ms     2 ms     2 ms    192.168.254.254
  3     6 ms     6 ms     6 ms    10.0.0.1
  4     9 ms     8 ms     8 ms    10.0.0.3
  5    13 ms    12 ms    13 ms    192.168.252.254
  6    16 ms    15 ms    17 ms    192.168.3.1

Traza completa.

C:\Users\Equipo 1>
```

Figura 48 Prueba tracert de conexión a Sede 3.

8.4.2 Pruebas de aplicación (base de datos)

Constructora NAVMER cuenta con un sistema de inventarios que gestiona la información

de productos, materiales, ventas, existencias y operaciones internas. Este sistema permite concentrar los registros generados en la sede principal, facilitando el control administrativo de los recursos que intervienen en las actividades comerciales y operativas.

Aunque el sistema ya se encontraba implementado previamente dentro de la organización, fue necesario analizar su funcionamiento general para determinar la forma en que podía integrarse a la infraestructura de red propuesta. El sistema permite llevar el control de usuarios autorizados, registrar movimientos de inventario, consultar existencias, generar reportes administrativos y apoyar procesos relacionados con ventas, facturación y control de materiales tal como se muestra en la *Figura 49*.



Figura 49 Interfaz del sistema de inventarios NAVMER.

De manera general, el sistema funciona mediante una base de datos implementada en Microsoft Access donde se almacenan los registros principales de operación. Estos registros pueden incluir productos, claves de artículos, cantidades disponibles, precios, movimientos de entrada y salida, ventas realizadas, datos de usuarios y reportes generados por el personal autorizado. A partir de esta información, el sistema permite mantener un control más ordenado de las existencias y reducir errores derivados de registros manuales o información dispersa.

Entre las funciones principales del sistema se encuentran el registro de productos,

actualización de inventarios, generación de reportes, control de ventas, emisión de documentos administrativos y consulta de existencias. Asimismo, puede gestionar alertas por niveles bajos de inventario, lo que permite anticipar las necesidades de abastecimiento y mejorar la toma de decisiones en la empresa. Para el análisis de funcionamiento y determinar la mejor manera de conectividad entre las sedes se puede acceder a el diseño de relaciones *Figura 50*.

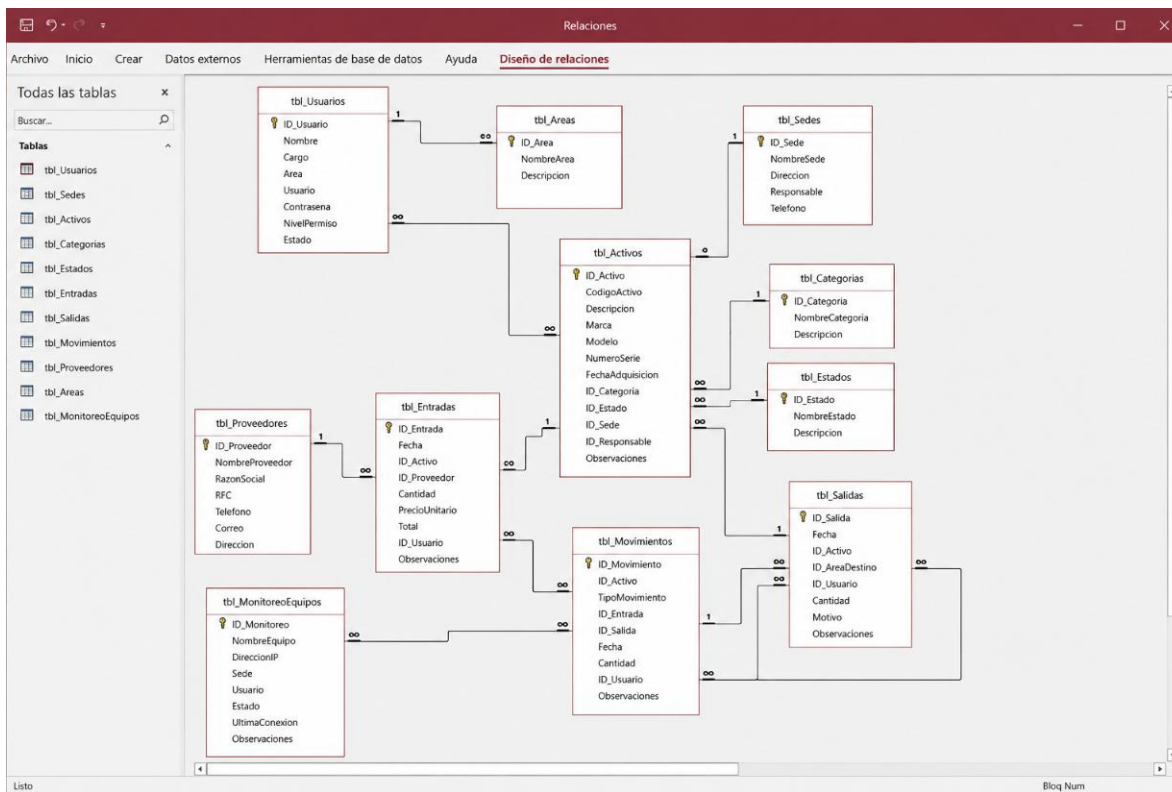


Figura 50 Entidad Relación Sistema de Inventarios NAVMER.

En su estado inicial, el sistema se utilizaba principalmente en la sede 1, por lo que la información generada en las sedes 2 y 3 no podía registrarse de inmediato en la misma base de datos. Esta situación provocaba dependencia de la sede principal para actualizar las ventas, existencias o movimientos realizados en otras ubicaciones.

Por esta razón, la intervención técnica del proyecto se centró en habilitar las condiciones de conectividad necesarias para que el sistema pudiera operar desde las tres sedes de la empresa. El objetivo fue permitir que al menos un equipo por sede tuviera acceso al sistema de

inventarios, de modo que las ventas, consultas y registros realizados en las sedes remotas pudieran integrarse directamente a la base de datos principal.

8.4.3 Conectividad para operación multisede

Como resultado del análisis del sistema de inventarios utilizado por Constructora NAVMER, se identificó que una de las alternativas más adecuadas para su operación en un entorno multisede era implementar una arquitectura basada en la separación de componentes Front-End y Back-End. Este esquema permite centralizar la información en una única base de datos y, al mismo tiempo, facilita el acceso de múltiples usuarios desde diferentes ubicaciones geográficas.

La arquitectura propuesta fue diseñada para aprovechar la infraestructura de red implementada entre las sedes de Jiquipilco e Ixtlahuaca mediante una conexión VPN Site-to-Site, garantizando el acceso seguro a la información almacenada en la base de datos central. Gracias a esta estructura, los usuarios pueden consultar y actualizar registros desde cualquiera de las sedes sin necesidad de duplicar información o generar múltiples versiones de la base de datos.

De acuerdo con (Microsoft, 2026) Back-End corresponde al componente encargado del almacenamiento centralizado de la información del sistema de inventarios. Este archivo contiene todas las tablas necesarias para el registro y administración de los activos, materiales y movimientos realizados dentro de la empresa. Por otra parte, el Front-End corresponde a la interfaz mediante la cual los usuarios interactúan con el sistema de inventarios. Este componente fue distribuido en los equipos autorizados de cada una de las sedes para permitir el acceso a la información almacenada en la base de datos central.

A diferencia del Back-End, el Front-End no almacena información crítica, sino que contiene los formularios, consultas, reportes y demás elementos necesarios para la operación diaria del sistema. De esta manera, los usuarios pueden registrar movimientos, consultar existencias, generar reportes y realizar búsquedas sin interactuar directamente con las tablas de la base de datos.

Se procede a la generar Back-End, y Front-End, esto lo logramos gracias a la herramienta

con la que cuenta Microsoft Access Database Splitter tal como se muestra en la *Figura 51*.

Una vez generados los archivos de la separación de datos los ubicamos en la carpeta de registros del sistema de inventarios, los cuales son fundamentales para el trabajo entre sedes, en la *Figura 52* vemos los archivos generados.

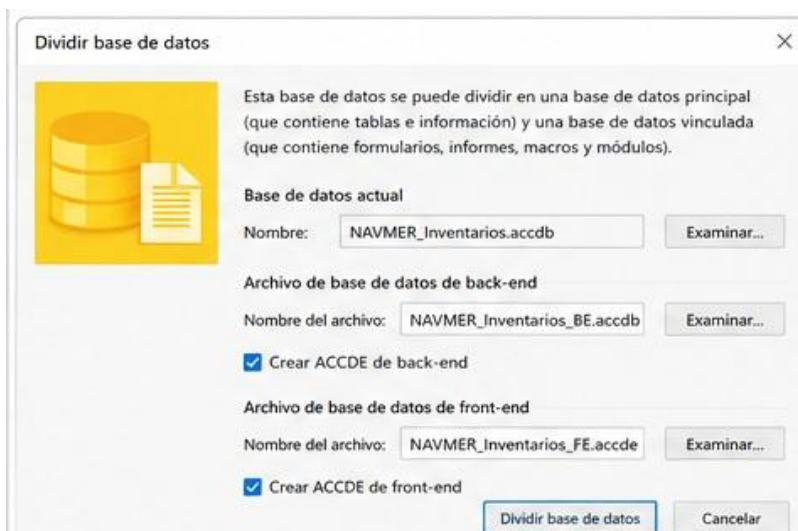


Figura 51 Database Splitter, dividir Base de Datos.

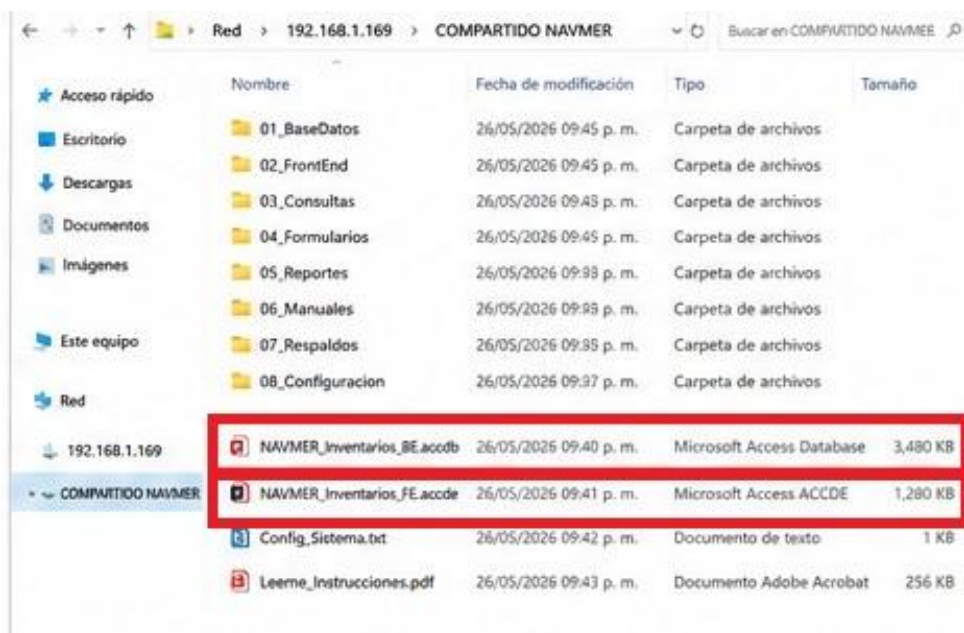


Figura 52 Archivos Back-End y Front-End

8.4.4 Creación de unidad de red

Para la implementación propuesta, el archivo Back-End fue ubicado en una carpeta compartida dentro de la Sede 1 de Jiquipilco, considerada como sede principal debido a que concentra los recursos administrativos y tecnológicos de la organización. Al centralizar la información en una sola ubicación se garantiza que todos los usuarios trabajen sobre los mismos datos, evitando inconsistencias o duplicidad de registros.

Se crea la unidad de red en el equipo de la sede principal donde se tiene acceso a la base de datos de la constructora, creamos una carpeta en la unidad C del equipo con el nombre de COMPARTIDO NAVMER, damos clic derecho y nos vamos a propiedades→ Uso compartido → Uso compartido avanzado → Permisos → se selecciona Everyone y damos todos los permisos → Aceptar, por último, en el apartado de Seguridad otorgamos los permisos necesarios y damos Aplicar. Figura, y para la organización y control de información de sedes se crea carpetas para cada una *Figura 53 y Figura 54*.

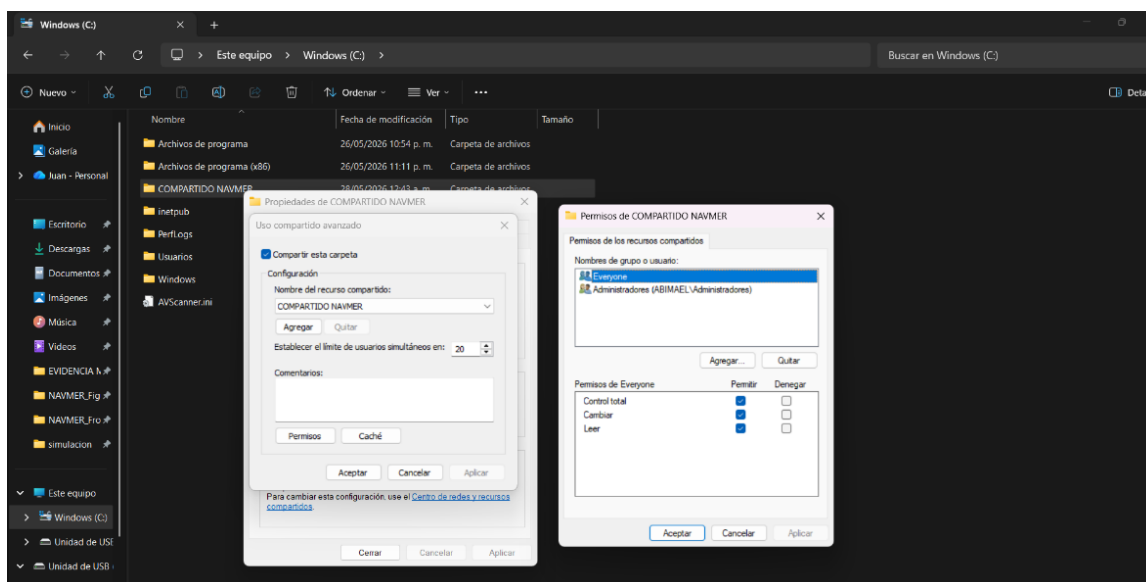


Figura 53 Creación de carpeta compartida para la unidad de red.

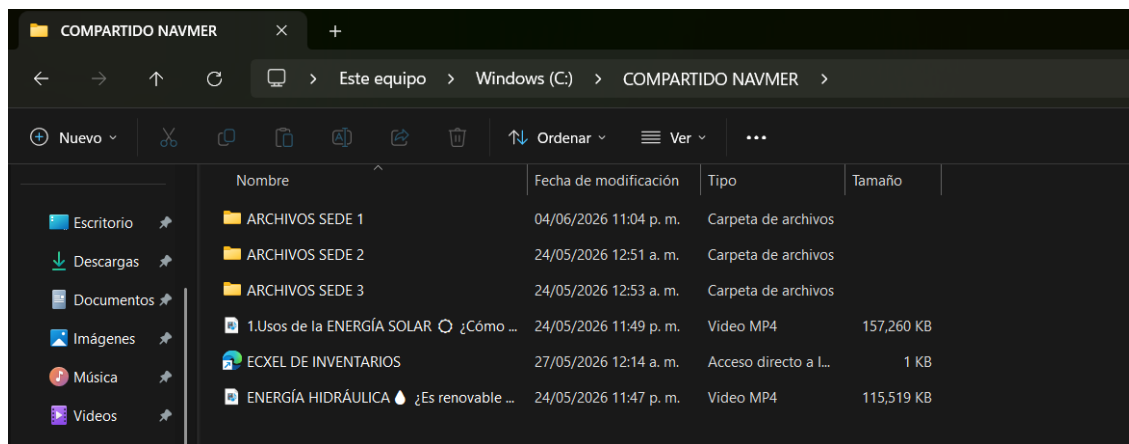


Figura 54 Creación de carpetas por sede en unidad de red.

Ahora se conecta a la unidad de red a los equipos que así se requiera, se configura la conexión, en Equipo damos clic derecho y se selecciona *Conectar a una unidad de red*, se despliega una ventana como en la figura, se coloca el nombre de la carpeta junto con la IP del equipo que comparte la carpeta, este equipo funge como servidor. *Figura 55.*

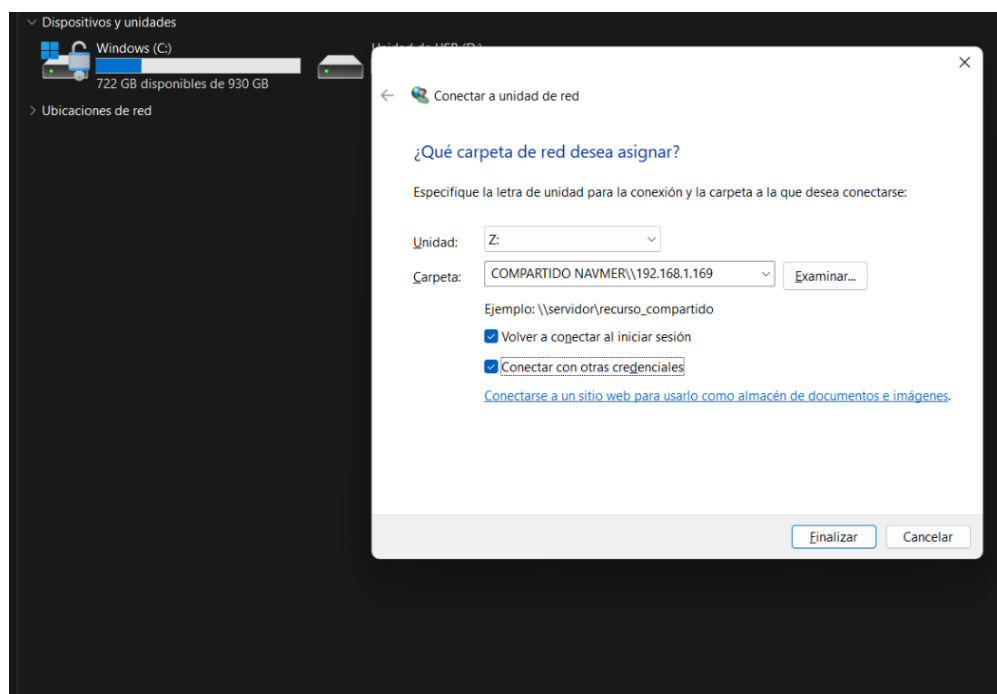


Figura 55 Conectar a la unidad de red.

Una vez conectada la unidad de red en los equipos enlazados se crea la unidad con la descripción de la ruta de origen como se muestra en la figura, comprobando el funcionamiento de la red. *Figura 56*

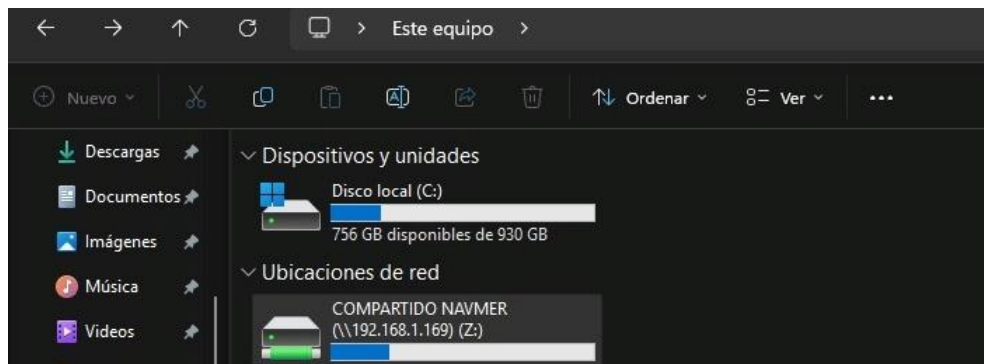


Figura 56 Unidad de red vinculada.

Con la unidad conectada en los equipos, se procede a la integración del sistema de inventarios en esta unidad, como se muestra en la *Figura 57*.

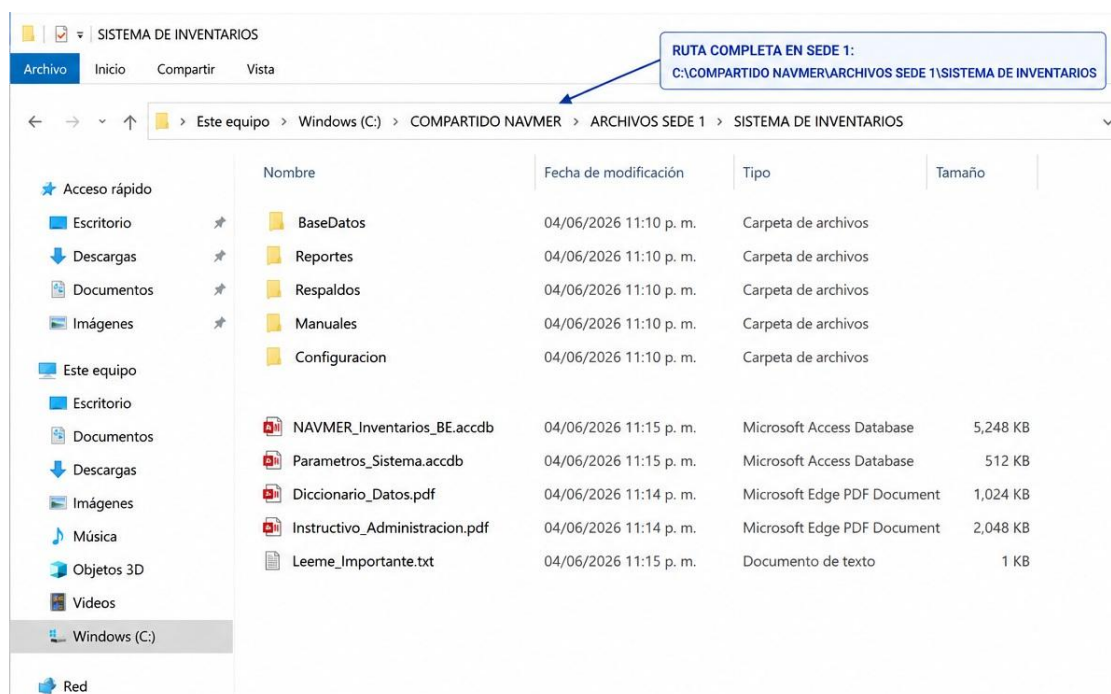


Figura 57 Archivos de Sistema de Inventarios NAVMER.

Dentro de este componente se almacenan las tablas relacionadas con el catálogo de activos, entradas y salidas de materiales, responsables de resguardo, ubicaciones físicas, historial de movimientos y demás información requerida para el control de inventarios. Debido a la importancia de estos datos, el acceso directo al archivo fue restringido únicamente al personal autorizado, reduciendo el riesgo de modificaciones accidentales o pérdidas de información.

Asimismo, la ubicación centralizada del Back-End facilita la realización de respaldos periódicos, tareas de mantenimiento y procesos de recuperación ante posibles fallas, lo que fortalece la seguridad y la disponibilidad de la información empresarial.

Como parte fundamental para que se pueda trabajar simultáneamente entre las sedes, utilizamos el archivo Front-End que generamos y lo colocamos en la unidad de la siguiente manera (*Figura 58*).

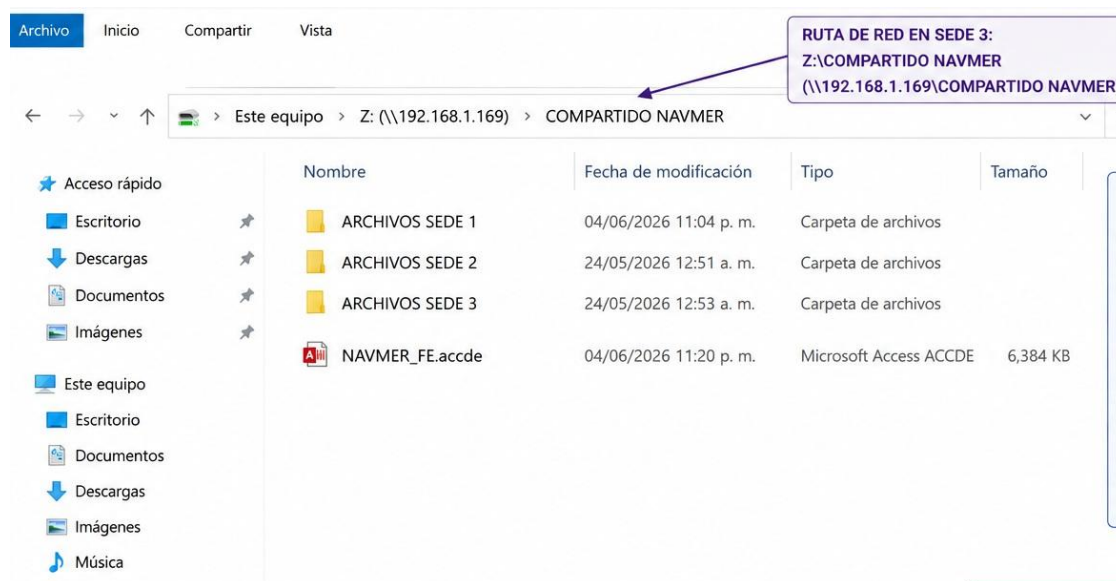


Figura 58 Ubicación de archivo Front-End.

Además, cada instancia del Front-End mantiene una vinculación permanente con las tablas alojadas en el Back-End mediante las rutas de acceso configuradas en la red privada virtual. Gracias a esta vinculación, cualquier modificación realizada por un usuario se refleja de

inmediato para los demás usuarios conectados al sistema, lo que permite una gestión de inventarios más eficiente y coordinada entre las tres sedes de la empresa.

La infraestructura diseñada permite que la sede principal actúe como punto central de administración, mientras que las sedes remotas acceden a los recursos compartidos mediante los mecanismos de comunicación establecidos. De esta forma se logra una operación coordinada sin necesidad de duplicar bases de datos o generar múltiples versiones de la información.

8.4.5 Seguridad de la red

La implementación de la infraestructura tecnológica del sistema de inventarios de Proyectos y Construcciones NAVMER requirió adoptar diversas medidas de seguridad orientadas a proteger la información y garantizar la continuidad de las operaciones. Debido a que el sistema opera en tres sedes ubicadas en diferentes localidades, fue necesario establecer mecanismos que permitieran asegurar la comunicación entre ellas, así como resguardar los equipos, la base de datos y los recursos compartidos utilizados en la operación diaria.

La aplicación de estas medidas contribuyó a mejorar la confiabilidad de la infraestructura implementada, a reducir los riesgos asociados a la pérdida o alteración de la información y a proporcionar un entorno de trabajo más seguro para los usuarios del sistema.

La comunicación entre las sedes es un elemento fundamental para el funcionamiento del sistema de inventarios, ya que permite acceder a la información centralizada desde diferentes ubicaciones. Con el propósito de garantizar una conexión segura entre las sucursales, se implementó una red privada virtual (VPN Site-to-Site), mediante la cual se estableció la comunicación entre las sedes de Jiquipilco e Ixtlahuaca.

Esta solución integra las redes locales de cada sede en una infraestructura lógica única, facilitando el acceso a los recursos compartidos y a la base de datos central, sin exponer los servicios internos a Internet. De esta manera, los usuarios pueden trabajar con la información almacenada en la Sede 1 como si estuvieran conectados a la misma red local. Además de mejorar la seguridad de las comunicaciones, la VPN simplificó la administración de la red al concentrar los recursos en un punto central, lo que facilitó las labores de mantenimiento, supervisión y atención de incidencias relacionadas con la conectividad entre sedes.

8.4.6 Seguridad en los equipos de cómputo

Los equipos de cómputo constituyen el principal medio de acceso al sistema de inventarios, por lo que se consideraron medidas orientadas a preservar tanto el funcionamiento de los dispositivos como la integridad de la información que procesan.

Cada estación de trabajo fue configurada de acuerdo con las necesidades operativas de los usuarios, limitando el acceso únicamente a las funciones requeridas para el desempeño de sus actividades. Esta práctica reduce la posibilidad de modificaciones accidentales sobre componentes críticos del sistema y contribuye a mantener un entorno de trabajo más controlado.

Asimismo, el uso de cuentas de usuario permite identificar a las personas que acceden a los recursos compartidos, facilitando la administración de permisos y el seguimiento de las actividades realizadas dentro de la infraestructura tecnológica. Esto favorece una mejor gestión de los accesos y fortalece el control sobre los recursos institucionales.

Por otra parte, la utilización de configuraciones similares en los equipos de las distintas sedes facilita las tareas de soporte técnico, mantenimiento y actualización, contribuyendo a mantener condiciones adecuadas para la operación continua del sistema.

8.4.7 Seguridad de la base de datos

La base de datos concentra la información relacionada con los activos, materiales, movimientos y registros operativos de la empresa, por lo que su protección constituye un aspecto prioritario de la infraestructura implementada.

Para su administración, se adoptó una arquitectura Front-End/Back-End que permite separar la interfaz utilizada por los usuarios del almacenamiento de la información. Bajo este esquema, el archivo Back-End se ubicó en la unidad compartida de la Sede 1 y funcionó como repositorio central para todas las sucursales conectadas a la red. Esta configuración evita la generación de múltiples copias independientes de la base de datos y reduce el riesgo de inconsistencias derivadas de la duplicidad de información. Al mismo tiempo, facilita la administración y el mantenimiento de los datos al concentrarlos en un único lugar.

Por su parte, el archivo Front-End fue distribuido en los equipos autorizados de cada sede, lo que permitió a los usuarios realizar consultas, registros y actualizaciones mediante

formularios y reportes, sin necesidad de acceder directamente a las tablas que contienen la información crítica. Esta separación mejora el control de la estructura de la base de datos y reduce la posibilidad de modificaciones no autorizadas.

falla o incidente operativo.

8.4.8 Seguridad de la unidad compartida

Como parte de la infraestructura implementada, se habilitó una unidad compartida destinada a almacenar los recursos necesarios para la operación del sistema de inventarios. Esta unidad está alojada en el equipo principal de la Sede 1 y actúa como punto central de acceso para las demás sedes conectadas a través de la VPN.

La organización de los archivos en esta unidad permitió mantener una estructura ordenada de la base de datos, los formularios de acceso, los reportes, los respaldos y la documentación relacionada con el sistema. Esta distribución facilita la gestión de los recursos y mejora la localización de la información cuando se requiere.

Adicionalmente, se configuraron permisos de acceso para restringir la modificación de archivos sensibles únicamente al personal autorizado (*Figura 59*). Con ello se reduce el riesgo de alteraciones accidentales y se contribuye a preservar la integridad de la información almacenada.

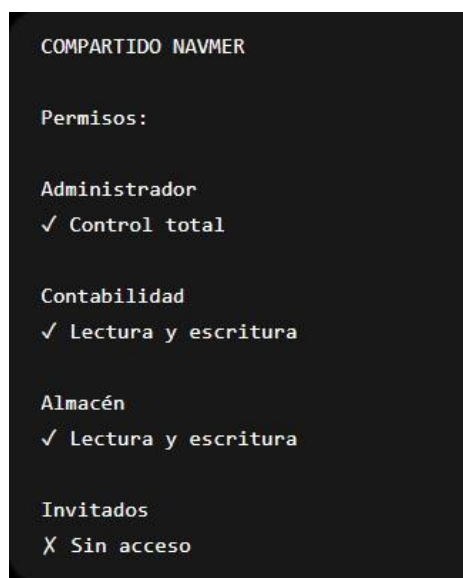


Figura 59 Permisos para la unidad de red.

8.4.9 Seguridad mediante respaldos de información

La disponibilidad de la información es un factor esencial para garantizar la continuidad de las operaciones del sistema de inventarios. Por esta razón, se contempló realizar respaldos periódicos de los archivos que conforman la base de datos y de los recursos asociados a su funcionamiento. Las copias de seguridad permiten recuperar información ante situaciones como fallas de hardware, errores de configuración, daños en los equipos o eliminación accidental de archivos. Asimismo, ofrecen la posibilidad de restaurar versiones anteriores de la información cuando sea necesario.

La implementación de una estrategia de respaldo contribuye a mitigar el impacto de posibles incidentes y ofrece un mecanismo de recuperación que favorece la continuidad operativa de la organización.

8.4.10 Monitoreo y disponibilidad de los recursos

Como complemento de las medidas de seguridad adoptadas, se realizaron actividades de monitoreo orientadas a verificar el estado y la disponibilidad de los equipos y servicios involucrados en la operación del sistema de inventarios.

Estas actividades permiten detectar oportunamente problemas de conectividad, interrupciones en la comunicación entre sedes o fallas en los dispositivos conectados a la red. La información obtenida facilita las labores de soporte técnico y contribuye a la atención temprana de incidencias antes de que afecten de manera significativa la operación del sistema.

Asimismo, el monitoreo permite verificar que los recursos compartidos permanezcan disponibles para los usuarios autorizados y que los equipos de la infraestructura funcionen adecuadamente.

En conjunto, las medidas implementadas fortalecieron la seguridad y estabilidad de la infraestructura tecnológica de NAVMER, proporcionando un entorno confiable para la operación del sistema de inventarios y para el intercambio de información entre las distintas sedes de la empresa.

9. CAPACITACIÓN

Como parte del proceso del proyecto en Constructora NAVMER, fue necesario desarrollar un programa de capacitación dirigido a los diferentes perfiles operativos y administrativos de la empresa, ya que la organización cuenta con personal de diversas áreas, entre ellas administración, contabilidad, ingeniería civil, arquitectura, almacén, auxiliares y personal operativo de campo.

Para el propósito mencionado, se identificó la necesidad de establecer un proceso de transferencia de conocimientos que permitiera facilitar la adaptación tecnológica de los colaboradores y garantizar el correcto uso y a su vez, considerar las funciones específicas de cada área, el nivel de interacción con los sistemas informáticos y las necesidades operativas.

La capacitación tuvo como finalidad fortalecer el uso adecuado del sistema de inventarios, reducir las incidencias derivadas de errores operativos y mejorar la continuidad de los procesos administrativos y técnicos en la empresa.

9.1 Personal de nuevo ingreso

Objetivo de la capacitación

Proporcionar al personal de nuevo ingreso los conocimientos básicos necesarios para el uso adecuado de los equipos de cómputo y de los recursos tecnológicos implementados en la empresa, promoviendo el cuidado de la infraestructura y la correcta utilización de los sistemas institucionales.

Temario desarrollado

Módulo 1. Introducción a los recursos tecnológicos de la empresa

- Equipos de cómputo utilizados en NAVMER.
- Equipos All-In-One y estaciones de trabajo.
- Impresoras y dispositivos periféricos.
- Reguladores de voltaje y protección eléctrica.
- Infraestructura básica de red.

Durante este módulo se explicó la función de cada dispositivo dentro de las actividades diarias de la empresa, permitiendo que el personal identificara los componentes tecnológicos con los que interactuaría durante su jornada laboral.



Figura 60 Capacitación nuevo ingreso.

Módulo 2. Uso básico de equipos de cómputo

- Encendido correcto del equipo.
- Inicio de sesión mediante credenciales personales.
- Navegación básica en Windows.
- Uso de carpetas institucionales.
- Apagado seguro del sistema.

Se capacitó al personal sobre los procedimientos adecuados para operar los equipos, evitando daños al sistema operativo y pérdidas de información ocasionadas por apagados incorrectos.

Módulo 3. Buenas prácticas de uso tecnológico

- Conservación física de los equipos.

- Manejo adecuado de cables y conexiones.
- Restricción de alimentos y líquidos.
- Uso responsable de cuentas institucionales.
- Protección de contraseñas.

Este módulo tuvo como finalidad fomentar una cultura de cuidado y responsabilidad sobre los recursos tecnológicos proporcionados por la empresa.

Módulo 4. Reporte de incidencias

- Identificación de fallas eléctricas.
- Identificación de problemas de red.
- Procedimiento de reporte.
- Escalamiento de incidencias al área responsable.

Se establecieron mecanismos de comunicación para reportar fallas oportunamente y evitar manipulaciones incorrectas que pudieran afectar la infraestructura instalada.

Justificación del bloque

La capacitación del personal de nuevo ingreso resulta fundamental debido a que gran parte de las incidencias tecnológicas se originan por desconocimiento en el uso de los equipos. La formación impartida permitió reducir riesgos operativos, fortalecer el cuidado de la infraestructura tecnológica y promover el uso adecuado de los recursos implementados durante el proyecto.

9.2 Encargados de almacén, materiales y ferretería

Objetivo de la capacitación

Capacitar al personal responsable del control de inventarios para utilizar correctamente la infraestructura tecnológica y el sistema de inventarios implementado en la empresa.



Figura 61 Capacitación área de almacén, materiales y ferretería.

Temario desarrollado

Módulo 1. Introducción al sistema de inventarios

- Objetivos del sistema.
- Beneficios de la operación en red.
- Comunicación entre sedes.
- Flujo de información institucional.

Se explicó la importancia del sistema dentro de la operación diaria y su papel en la administración de materiales y herramientas.

Módulo 2. Operación del sistema de inventarios

- Inicio de sesión.
- Consulta de existencias.
- Registro de entradas.

- Registro de salidas.
- Búsqueda de productos.
- Consulta de movimientos.

Los participantes realizaron ejercicios prácticos relacionados con los procesos cotidianos de control de materiales.

Módulo 3. Infraestructura tecnológica de apoyo

- Uso de equipos All-In-One.
- Funcionamiento de impresoras.
- Uso de reguladores de voltaje.
- Procedimientos ante fallas eléctricas.

Se abordaron aspectos preventivos para proteger la continuidad de la operación del almacén.

Módulo 4. Conectividad y continuidad operativa

- Indicadores de red.
- Verificación de acceso al sistema.
- Identificación de fallas básicas.
- Procedimiento de reporte.

El personal aprendió a identificar situaciones que podrían afectar la sincronización de la información entre sedes.

Justificación del bloque

Debido a que el almacén concentra el control de materiales, herramientas y recursos utilizados en obra, fue indispensable garantizar que los responsables comprendieran el funcionamiento del sistema y de la infraestructura tecnológica implementada, fortaleciendo la precisión de los registros y la continuidad operativa.

9.3 Arquitectos, ingenieros civiles, administradores y contadores

Objetivo de la capacitación

Capacitar al personal técnico y administrativo en el uso de la infraestructura multisede, los recursos compartidos y las medidas de seguridad implementadas para la protección de la información institucional.

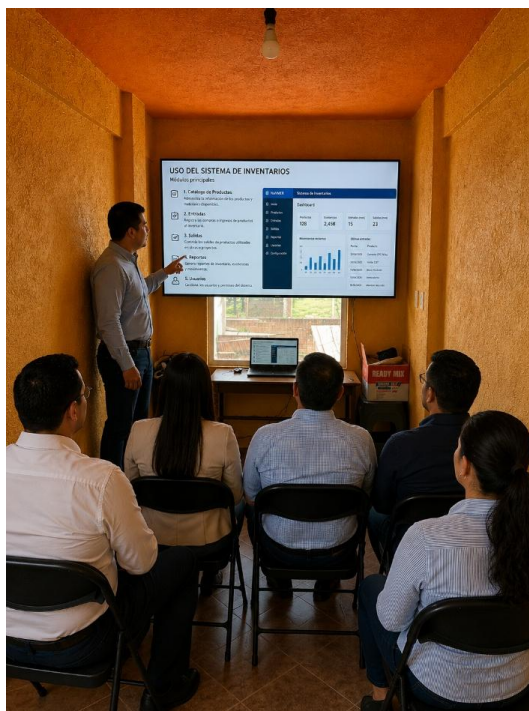


Figura 62 Capacitación de arquitectos, contadores y administradores.

Temario desarrollado

Módulo 1. Infraestructura de comunicación multisede

- Concepto de red privada virtual (VPN).
- Comunicación entre sedes.
- Acceso remoto a recursos compartidos.
- Beneficios de la centralización de información.

Se explicó el funcionamiento general de la infraestructura implementada y su impacto en la productividad organizacional.

Módulo 2. Administración de carpetas y recursos compartidos

- Acceso a unidades de red.
- Estructura de carpetas institucionales.
- Organización documental.
- Almacenamiento centralizado.

Los participantes aprendieron a utilizar correctamente los recursos compartidos y a mantener organizada la documentación institucional.

Módulo 3. Administración concurrente de información

- Edición colaborativa de archivos.
- Control de versiones.
- Prevención de duplicidad documental.
- Procedimientos de almacenamiento.

Este módulo permitió mejorar la gestión de documentos técnicos, financieros y administrativos.

Módulo 4. Seguridad de la información

- Gestión segura de contraseñas.
- Bloqueo de equipos.
- Protección contra correos fraudulentos.
- Respaldo de información.
- Uso responsable de recursos tecnológicos.

Se fortalecieron las buenas prácticas relacionadas con la protección de información crítica de la empresa.

Módulo 5. Respaldo y recuperación de información

- Importancia de los respaldos.
- Procedimientos establecidos por la empresa.
- Almacenamiento seguro de evidencia documental.
- Recuperación básica de archivos.

Se promovió la protección de la información estratégica generada durante la operación de la empresa.

Justificación del bloque

Las áreas técnicas y administrativas gestionan información crítica relacionada con proyectos de obra, presupuestos, contratos, documentación fiscal y evidencia operativa. La capacitación permitió fortalecer la seguridad de la información, mejorar la colaboración entre sedes y aprovechar de manera eficiente la infraestructura tecnológica implementada.

CONCLUSIONES

El desarrollo del proyecto “Mejora de la infraestructura de red y comunicación de base de datos en Constructora NAVMER” permitió atender una necesidad real de la organización, relacionada con la comunicación entre sus diferentes sedes y con la administración eficiente de la información institucional. A partir del diagnóstico realizado, fue posible identificar las principales limitaciones en materia de conectividad, acceso a la información y gestión de recursos tecnológicos, que afectaban la operación diaria de la empresa y dificultaban la coordinación entre las distintas áreas de trabajo.

La implementación de la infraestructura de red propuesta permitió establecer una comunicación segura y estable entre las tres sedes de la constructora mediante el uso de redes privadas virtuales (VPN), lo que permitió compartir la información de manera más eficiente y confiable. Asimismo, la centralización de la base de datos del sistema de inventarios facilitó el acceso a la información en tiempo real, redujo la duplicidad de registros, mejoró el control de los recursos y fortaleció la disponibilidad de los datos para la toma de decisiones.

Respecto a la simulación realizada, el uso de Cisco Packet Tracer versión 8.2.2 permitió validar previamente el funcionamiento de la topología diseñada antes de su implementación física. Mediante esta herramienta fue posible comprobar la conectividad entre las tres sedes, verificar el correcto direccionamiento IP, el funcionamiento del enrutamiento, la comunicación entre equipos y el intercambio de información dentro de la red propuesta. La simulación redujo riesgos de implementación y permitió identificar oportunamente posibles inconsistencias en la configuración de la infraestructura, así mismo ofreció una perspectiva clara al momento de proponerla con la empresa, disipando dudas y visualizando los alcances.

De igual manera, las pruebas de conectividad realizadas demostraron el correcto funcionamiento de la infraestructura implementada, validando la comunicación entre sedes, el acceso a los recursos compartidos y la operación del sistema de inventarios en un entorno multisede. Complementariamente, la incorporación de medidas de seguridad, respaldos periódicos y controles de acceso contribuyó a fortalecer la protección de la información institucional y a reducir los riesgos asociados a la pérdida o alteración de datos.

En materia de seguridad, el proyecto incorporó diversos mecanismos orientados a proteger

la disponibilidad, la integridad y la confidencialidad de la información. La utilización de una VPN Site-to-Site permitió establecer un canal de comunicación seguro entre las sedes mediante el cifrado del tráfico de datos, lo que redujo la exposición de la información durante su transmisión. Además, se propusieron medidas complementarias como el uso de credenciales individuales, la administración de permisos de acceso, el respaldo periódico de la información, el empleo de reguladores de voltaje para proteger los equipos, así como generar buenas prácticas de seguridad por parte de los usuarios en el uso de los equipos y sistema de inventarios.

La capacitación impartida al personal constituyó un elemento indispensable para garantizar el aprovechamiento adecuado de la infraestructura implementada. La formación diferenciada dirigida al personal de nuevo ingreso, encargados de almacén, arquitectos, ingenieros, administradores y contadores permitió desarrollar las competencias necesarias para utilizar adecuadamente el sistema de inventarios, los recursos compartidos, la infraestructura de red y las medidas de seguridad establecidas. Con ello se favorece la continuidad operativa de la constructora y se reduce la probabilidad de incidencias derivadas de errores operativos o del desconocimiento de las herramientas tecnológicas.

Este proyecto representó una oportunidad para aplicar de manera práctica los conocimientos adquiridos durante la formación profesional en las áreas de redes de computadoras, bases de datos y seguridad informática. La experiencia permitió desarrollar habilidades en el análisis de requerimientos, el diseño de soluciones, la implementación de redes empresariales y la resolución de problemas en entornos de trabajo reales.

Finalmente, puede concluirse que la mejora de la infraestructura de red y de la comunicación de la base de datos contribuyó significativamente al fortalecimiento tecnológico de Constructora NAVMER, proporcionando una plataforma más eficiente, segura y preparada para atender las necesidades actuales y futuras de la empresa. Este proyecto demuestra que la adecuada integración de las tecnologías de la información constituye un elemento estratégico para incrementar la productividad, optimizar los procesos internos y favorecer el crecimiento organizacional en un entorno cada vez más digitalizado.

REFERENCIAS

- Acosta, M. G. (2022). Gestión y control de inventario en pequeñas y medianas empresas (pymes) como herramienta de información para la toma de decisiones en tiempos de crisis. *Revista de Investigación Académica sin Fronteras*. Recuperado el 12 de 05 de 2026, de <https://goo.su/ARcIN>
- Almazán Galeno, E. (2007). Proyecto de una red privada virtual (VPN) a la empresa Proyección y Administración Empresarial de Mexico S.A. de C.V. *Tesis UNAM*. (U. A. México, Ed.) México. Recuperado el 15 de 04 de 2026, de <https://goo.su/IOW7h>
- Andrés F. Betancur-Pérez¹, J. J.-T. (2015). Redes elásticas del futuro: beneficios para la red internade telecomunicaciones de colombia. *Tecno Lógicas*, 18, 125-136. Recuperado el 24 de febrero de 2026, de <https://biblat.unam.mx/hevila/Tecnologicas/2015/vol18/no34/10.pdf>
- Ariganello, E. (2025). *Redes Cisco, Guía de estudio para la certificación CCNA 200-301*. RA-MA Editorial. Recuperado el 29 de agosto de 2025, de <https://lc.cx/HuoZxg>
- Cabello, G. J. (2025). *Almacenamiento de la información e introducción a los SGBD*. IC Editorial. Recuperado el 28 de agosto de 2025, de <https://goo.su/8lodk>
- Calume, R. C. (2015). *Informatica partes de un PC*. RCGCalume. Recuperado el 20 de febrero de 2026, de <https://n9.cl/ao6xk>
- Cisco Systems, Inc. (21 de agosto de 2024). *Cisco Catalyst SD-WAN Design Guide*. (cisco.com, Editor) Recuperado el 28 de agosto de 2025, de Cisco Design Zone: <https://goo.su/x0YpxD>
- Citys. (27 de 06 de 2024). *Diferentes tipos de routers en las redes*. Obtenido de CONSULTORIA INTEGRAL EN TECNOLOGÍA Y SISTEMAS: <https://goo.su/tMrWyj>
- Corella-Parra, L. M. (2023). Desarrollo de un sistema de control de inventario para una empresa comercial. *Revista Científica. Scielo*. Recuperado el 07 de 04 de 2026, de <https://goo.su/cVyZMz>
- Dordoigne, J. (2015). *Redes Informaticas-Nociones Fundamentales* (2015 ed.). Barcelona,

- España: ENI. Recuperado el febrero de 2026, de <https://goo.su/c3gbY>
- Escobar Hernández, H. (22 de 11 de 2019). Sistema de información que controla y administra el inventario y las ventas de una pequeña empresa comercial. *Tesis UAEMex*. (U. A. México, Ed.) México. Recuperado el 11 de 05 de 2026, de <http://hdl.handle.net/20.500.11799/105321>
- Evila, M. C. (2026). Seguridad en redes LAN implementando VLAN. *Articulo, Universidad Autonoma del Esatdo de Hidalgo*. (U. A. Hidalgo, Ed.) México. Recuperado el 18 de 04 de 2026, de <https://www.uaeh.edu.mx/scige/boletin/sahagun/n8/a5.html#refe1>
- García, C. J. (2021). *Operaciones auxiliares con Tecnologías de la Información y la Comunicación*. IC Editorial. Recuperado el 28 de agosto de 2025, de <https://goo.su/klos8qU>
- García, J. M. (2025). *Planificación de proyectos de implantación de infraestructuras de redes*. IC Editorial. Recuperado el 28 de agosto de 2025, de <https://lc.cx/r5pqjf>
- Gil Vázquez Pablo, P. B. (2010). *Redes y Transmisión de datos*. (U. d. Publicaciones, Ed.) San Vicente, España: Universidad de Alicante. Servicio de Publicaciones. Recuperado el 28 de agosto de 2025, de <https://goo.su/DPSY5>
- González Morales, A. (2006). Redes Privadas Virtuales (VPN). *Tesis UAEH*. (U. A. Hidalgo, Ed.) México. Recuperado el 17 de 05 de 2026, de <https://chatgpt.com/c/6a1cf7c6-45d4-83e8-8547-150fccaaa7c4>
- Hernández, R. E. (2025). Implementación y evaluación del comportamiento dinámico de una red celular 5G standalone basada en SDR con fronthaul activo DWDM. *Tesis de Ingeniería en Computación, UNAM*, 34-47. Ciudad de México, México. Recuperado el 28 de agosto de 2025, de https://tesiunamdocumentos.dgb.unam.mx/ptd2025/jul_sep/0871529/Index.html
- Iglesias Mouteira, R. (05 de mayo de 2004). *Instalación de redes informaticas e ordenadores* (2004 ed.). Madrid, España: Ideaspropias Editorial. Recuperado el 28 de agosto de 2025, de The Network Installers: <https://goo.su/6AZD2>
- link, O. t. (2023). ¿Cuál es la diferencia entre el switch no administrable, switch Web Smart y switch administrable? *Tp link*, 1. Recuperado el 15 de 03 de 2026, de

- <https://support.omadanetworks.com/es/document/12881/?app=deco>
- Microsoft. (20 de 05 de 2026). *Microsoft*. Obtenido de <https://support.microsoft.com/en-us/access/split-an-access-database>
- Miranda, V. C. (2020). *Sistemas Informáticos y Redes locales*. Madrid, España: Ediciones Paraninfo S. A. Recuperado el 26 de agosto de 2025, de <https://goo.su/wzBDyJP>
- Molina, C. S. (2022). Seguridad en bases de datos. *Revista Iberoamericana de Tecnología Educativa*. Recuperado el 12 de 04 de 2026, de <https://unimeso.edu.mx/ojs/index.php/RITE/article/view/10?utm>
- noip. (7 de 04 de 2026). *noip.com*. Obtenido de <https://www.noip.com/login>
- Osorno Saavedra, S. (2003). Implementacion de una red privada virtual (VPN); basada en protocolo MPLS, sobre un red IP. *Tesis UNAM*. (U. A. México, Ed.) Ciudad de México, México. Recuperado el 12 de 04 de 2026, de <https://goo.su/pivQp3S>
- Pérez, G. M. (2021). Diseño e implementación de una red LAN para la empresa SOFTEL. 123-142. Recuperado el 28 de agosto de 2025, de <https://revistas.unesum.edu.ec/index.php/unesumciencias/article/view/582>
- PlanNet. (19 de septiembre de 2024). *Guía para implementar redes empresariales escalables y fáciles de administrar*. Recuperado el 29 de agosto de 2025, de Blog PlanNet: <https://blog.plannet.mx/implementar-redes-empresariales-escalable>
- Postigo, P. A. (2022). *Gestión de base de datos*. Madrid, Sierra de guadarrama, España: Ediciones Paraninfo, S.A. Recuperado el 28 de agosto de 2025, de <https://goo.su/pAO6>
- Poveda, N. M. (2014). Tecnologías de comunicación para redes de potencia inteligentes de media y alta tensión. *Prisma Tecnológico*, 29-32. Recuperado el 13 de Febrero de 2026, de <https://revistas.utp.ac.pa/index.php/prisma/article/view/520>
- QuickTechie, A career growth machine. (28 de 08 de 2025). *Palo Alto Networks Network Certified Security Generalist Certification Exam*. QuickTechie. Recuperado el 28 de agosto de 2025, de <https://goo.su/ml24L>
- Reyes Felipe, M. G. (2007). Informe del proyecto de un sistema de inventarios basado en el

- diplomado de administración de base de datos. *Tesis UNAM*. (F. d. UNAM, Ed.) México. Recuperado el 12 de 05 de 2026, de <https://goo.su/Z7zXemh>
- Stokes, H. (4 de febrero de 2025). *The Network Installer*. Obtenido de The Network Installer: <https://thenetworkinstallers.com/es/blog/dispositivos-de-instalaci%C3%B3n-de-red/>
- Varela, G. M. (2023). Diseño, Implementación y Factibilidad Técnica de una red de Telecomunicaciones para proveer el servicio de Internet en localidades pequeñas de Baja California. *Tesis de ingeniería en Computación, UNAM*, 74-80. Ciudad de México, México: UNAM. Recuperado el 28 de agosto de 2025, de <https://tesiunamdocumentos.dgb.unam.mx/ptd2023/septiembre/0847377/Index.html>
- Zone, R. (24 de Febrero de 2026). *Redes zone*. Obtenido de <https://www.redeszone.net/tutoriales/redes-cable/programas-simular-red/>

GLOSARIO

Access (Microsoft Access)

Sistema de Gestión de Bases de Datos (SGBD) relacional desarrollado por Microsoft que permite crear y administrar bases de datos mediante interfaces gráficas, formularios, consultas e informes.

Ancho de banda

Capacidad máxima de transmisión de datos de un medio de comunicación en un período determinado, generalmente medido en bits por segundo (bps), Mbps o Gbps.

Back-End

Componente de una base de datos que contiene el almacenamiento centralizado de la información, incluyendo las tablas con los datos críticos del sistema. En arquitecturas distribuidas, se ubica en un servidor central accesible desde múltiples ubicaciones.

Base de datos

Colección organizada de datos estructurados por temas que permite su gestión, almacenamiento, consulta y modificación eficiente, facilitando el mantenimiento y estableciendo relaciones lógicas entre la información almacenada.

Buffer

Zona de memoria temporal donde se almacenan las tramas (unidades de envío de datos) antes de ser reenviadas al puerto correspondiente en un switch o dispositivo de red.

Cableado estructurado

Sistema estandarizado de cableado que integra diversos componentes (cables, conectores, paneles, etc.) para crear una infraestructura de telecomunicaciones capaz de soportar múltiples servicios como datos, voz y video.

Cliente

Dispositivo o estación de trabajo que solicita servicios o recursos a un servidor dentro de una red. También conocido como nodo o estación de trabajo.

DBaaS (Database as a Service)

Modelo de implementación de bases de datos en la nube donde el proveedor se encarga de las tareas operativas de mantenimiento, gestión y administración en tiempo real, con alta disponibilidad y procesos de automatización.

DHCP (Dynamic Host Configuration Protocol)

Protocolo de red que permite la asignación automática de direcciones IP y otros parámetros de configuración a los dispositivos conectados a una red, facilitando su administración.

DNS (Domain Name System)

Sistema que traduce nombres de dominio legibles por humanos (como www.ejemplo.com) en direcciones IP numéricas que las computadoras utilizan para identificarse en la red.

Enrutamiento

Proceso de seleccionar la ruta más adecuada para enviar paquetes de información desde una red de origen hasta su destino en otra red, utilizando protocolos de comunicación establecidos.

Ethernet

Estándar de red de área local (LAN) que define las especificaciones técnicas para la transmisión de datos mediante cableado, incluyendo tipos de cables, conectores y velocidades de transmisión.

Firewall

Dispositivo o software de seguridad de red que controla y filtra el tráfico entrante y saliente según reglas de seguridad predefinidas, protegiendo la red contra accesos no autorizados y amenazas externas.

Front-End

Componente de una base de datos que contiene la interfaz mediante la cual los usuarios interactúan con el sistema, incluyendo formularios, consultas, reportes y otros elementos de acceso a los datos, sin almacenar información crítica.

FTP (File Transfer Protocol)

Protocolo de red utilizado para la transferencia de archivos entre sistemas conectados a una

red TCP/IP.

Gateway (Puerta de enlace)

Dispositivo o dirección IP que sirve como punto de acceso para que los dispositivos de una red local se comuniquen con otras redes, como Internet. En una LAN, generalmente corresponde a la dirección IP del router.

Gigabit Ethernet

Estándar de transmisión de datos que permite velocidades de hasta 1000 Mbps (1 Gbps) a través de cableado de red, siendo significativamente más rápido que el Ethernet tradicional de 100 Mbps.

HTTP/HTTPS (Hypertext Transfer Protocol / Secure)

Protocolos de aplicación para la transferencia de información en la web. HTTPS es la versión segura que utiliza cifrado TLS/SSL para proteger los datos transmitidos.

IP (Internet Protocol)

Protocolo que define el formato de los paquetes de datos y el sistema de direccionamiento utilizado para identificar dispositivos en una red. Cada dispositivo tiene una dirección IP única.

Jack

Conector hembra diseñado para ajustarse a placas de pared, paneles de conexión y cajas de conexión en instalaciones de cableado estructurado, permitiendo la conexión rápida de dispositivos.

LAN (Local Area Network)

Red de área local que conecta computadoras y dispositivos en un área geográfica limitada (como una oficina o edificio), permitiendo compartir archivos, recursos e impresoras.

Latencia

Tiempo que tarda un paquete de datos en viajar desde su origen hasta su destino a través de una red, generalmente medido en milisegundos (ms). Una baja latencia indica una red más rápida y responsiva.

MAC (Media Access Control)

Dirección física única asignada a cada interfaz de red por el fabricante, utilizada para identificar dispositivos en una red local a nivel de hardware.

Módem

Dispositivo que modula y demodula señales para permitir la comunicación entre redes digitales y analógicas, facilitando la conexión a Internet a través de diferentes medios de transmisión.

Patch Cord

Cable de conexión flexible, generalmente UTP, terminado en conectores plug en ambos extremos, utilizado para interconectar dispositivos en una red o conectar equipos a tomas de red.

Ping

Comando de red utilizado para verificar la conectividad entre dispositivos y medir el tiempo de respuesta en la transmisión de paquetes de datos, enviando mensajes ICMP de eco.

Plug

Conector macho físico que se inserta en un jack o enchufe hembra para transmitir datos o electricidad, como los conectores RJ-45 utilizados en cables de red.

Puerto

Interfaz física o lógica en un dispositivo de red (switch, router, computadora) que permite la conexión de otros dispositivos o la comunicación mediante protocolos específicos.

QoS (Quality of Service)

Conjunto de tecnologías y mecanismos que priorizan ciertos tipos de tráfico de red sobre otros, garantizando un rendimiento adecuado para aplicaciones críticas como voz sobre IP o videoconferencias.

Red de computadoras

Conjunto de dispositivos interconectados mediante medios físicos o inalámbricos cuyo objetivo es compartir recursos e información entre sí.

Router (Enrutador)

Dispositivo de red cuya función principal es interconectar redes diferentes y dirigir el tráfico de datos entre ellas, determinando la ruta más eficiente para enviar paquetes de información a su destino.

SD-WAN (Software-Defined Wide Area Network)

Tecnología de red que utiliza principios de redes definidas por software para gestionar y optimizar el rendimiento de redes WAN, permitiendo conectar de forma segura múltiples ubicaciones con mayor rendimiento, confiabilidad y escalabilidad.

Servidor

Computadora o sistema que proporciona recursos, datos, servicios o programas a otros dispositivos (clientes) a través de una red. Generalmente tiene mayor capacidad de procesamiento y almacenamiento que los clientes.

STP (Spanning Tree Protocol)

Protocolo de red que previene la formación de bucles en redes con topologías redundantes, asegurando que exista un único camino activo entre dos nodos de la red.

Subneteo (Subnetting)

Proceso de dividir una red IP en subredes más pequeñas y manejables, optimizando el uso del espacio de direcciones y mejorando la seguridad y el rendimiento de la red.

Switch (Conmutador)

Dispositivo de red que interconecta equipos dentro de una red local, permitiendo la comunicación y el intercambio de datos entre ellos mediante la conmutación de tramas hacia los puertos correspondientes.

TCP/IP (Transmission Control Protocol/Internet Protocol)

Conjunto de protocolos de comunicación que permiten la interconexión de dispositivos en redes locales y en Internet, definiendo cómo se transmiten y reciben los datos.

Topología de red

Distribución física o lógica de los dispositivos y conexiones en una red. Las topologías

comunes incluyen estrella, anillo, bus y malla.

Tracert (Trace Route)

Comando de red que muestra la ruta completa que siguen los paquetes de datos desde el origen hasta el destino, indicando cada salto (router) intermedio y los tiempos de respuesta.

UTP (Unshielded Twisted Pair)

Tipo de cable de par trenzado no blindado utilizado comúnmente en redes Ethernet, compuesto por pares de hilos de cobre trenzados para reducir interferencias electromagnéticas.

VLAN (Virtual Local Area Network)

Red de área local virtual que permite segmentar lógicamente una red física en múltiples redes independientes, mejorando la seguridad, el rendimiento y la administración del tráfico de red.

VPN (Virtual Private Network)

Red privada virtual que establece una conexión segura y cifrada a través de una red pública (como Internet), permitiendo la comunicación protegida entre sedes remotas o usuarios móviles.

WAN (Wide Area Network)

Red de área extensa que conecta dispositivos o redes locales geográficamente dispersas, utilizando enlaces de telecomunicaciones de larga distancia para la transmisión de datos.

Wi-Fi

Tecnología de red inalámbrica que permite la conexión de dispositivos a una red local sin necesidad de cableado físico, utilizando ondas de radiofrecuencia según los estándares IEEE 802.11.