BENEMÉRITA UNIVERSIDAD AUTÓNOMA DE PUEBLA

COMPLEJO REGIONAL CENTRO SEDE SAN JOSÉ CHIAPA

Título de la tesis:

Renovación de Infraestructura Tecnológica para la Optimización de Redes usando Telefonía VoIP Segura en un Entorno Industrial

Tesis que para obtener el título de:

Licenciado en Ingeniería en Sistemas y Tecnologías de la Información Industrial

Presenta:

Donaldo Ian López Zacaula

Directores de Tesis:

Dra. Ana Luisa Ballinas Hernández

Dra. María Claudia Denicia Carral

San José Chiapa, Puebla, enero 2026

Agradecimientos

Agradezco a la Benemérita Universidad Autónoma de Puebla por brindarme la oportunidad de cursar mis estudios profesionales y proporcionarme la formación académica necesaria para el desarrollo del presente trabajo.

De manera especial, expreso mi agradecimiento a la Dra. Ana Luisa Ballinas Hernández y Dra. Claudia Denicia Carral asesoras de esta tesis, por su orientación, acompañamiento y valiosas observaciones durante el desarrollo del proyecto, las cuales contribuyeron de manera significativa a la mejora y consolidación del presente trabajo.

Asimismo, agradezco a la empresa Trefilados Inoxidables de México por las facilidades otorgadas, el acceso a la información y el apoyo brindado para la realización del proyecto en un entorno real, lo que permitió aplicar los conocimientos adquiridos durante mi formación académica. De igual forma, expreso mi agradecimiento al Ing. Abdiel García Ramírez, por la constante comunicación, retroalimentación y apoyo técnico brindado durante la implementación del proyecto, los cuales fueron fundamentales para el logro de los objetivos planteados.

Finalmente, a mi padre Delfino, a mi madre Isabel y a mi hermana Diana, mi más profundo agradecimiento por acompañarme en cada etapa de este proceso, por su apoyo constante, su confianza y su comprensión en los momentos más exigentes. Este logro es reflejo de su esfuerzo, su guía y su respaldo incondicional, que han sido una fuente permanente de motivación para alcanzar esta meta con orgullo y gratitud.

Resumen

La presente investigación aborda la renovación de la infraestructura tecnológica de red en un entorno industrial para optimizar las comunicaciones internas mediante la implementación de un sistema de telefonía sobre Protocolo de Internet (Voice over Internet Protocol, VoIP) seguro y eficiente. La problemática identificada se centra en la obsolescencia de la infraestructura existente, la necesidad de optimizar la segmentación de red, limitaciones en la calidad del servicio y vulnerabilidades en materia de videovigilancia, lo cual impacta directamente en la continuidad operativa y la productividad de la organización. El objetivo del trabajo consiste en diseñar e implementar una arquitectura de red modernizada que integre cableado estructurado, redes inalámbricas de alto desempeño y telefonía IP, garantizando calidad de servicio, seguridad y escalabilidad. El alcance del proyecto comprende el diagnóstico de la infraestructura actual, el diseño de la red propuesta, la implementación de VoIP y la evaluación de su desempeño en un entorno industrial real. Para ello, se emplearon técnicas de análisis de red, diseño basado en normas y estándares internacionales, segmentación mediante Redes de Área Local Virtual (Virtual Local Area Network, VLAN), configuración de Calidad de Servicio (Quality of Service, QoS) y pruebas de desempeño. Los resultados obtenidos evidencian una mejora significativa en la calidad de las comunicaciones, reducción de latencia, mayor estabilidad del servicio de voz y un incremento en la optimización general de la red, demostrando que la solución propuesta es viable, eficiente y adaptable a futuros requerimientos tecnológicos.

Índice

Índice de Figuras

Índice de Tablas

CAPÍTULO 1. Introducción

1.1 Antecedentes del Proyecto

En los últimos años, el desarrollo industrial ha estado estrechamente ligado a la adopción de tecnologías de información y comunicación que permitan mejorar la eficiencia operativa, la trazabilidad de procesos y la seguridad de las instalaciones. En este contexto, la infraestructura tecnológica de red se ha convertido en un elemento esencial para sostener la productividad y permitir la integración de nuevas herramientas digitales. No obstante, es común que muchas organizaciones industriales, especialmente aquellas con una trayectoria prolongada, mantengan estructuras tecnológicas que, si bien fueron funcionales en su momento, hoy enfrentan limitaciones frente a las exigencias actuales del entorno digital.

La evolución en el volumen de operaciones, la incorporación de nuevos procesos automatizados y la necesidad de mantener una comunicación continua entre diversas áreas demandan una red más robusta, segura y eficiente. A nivel global, se observa una tendencia creciente hacia la modernización de redes mediante el uso de cableado estructurado conforme a normativas actualizadas, la implementación de telefonía VoIP como solución de comunicación flexible y escalable, y el fortalecimiento de sistemas de videovigilancia para mejorar el control de los espacios físicos.

El presente proyecto surge como respuesta a dicha necesidad, con el propósito de diseñar e implementar una solución tecnológica integral que permita actualizar la infraestructura de red de una instalación industrial, mejorar la cobertura y estabilidad de la conectividad, y modernizar los sistemas de comunicación y monitoreo, alineándose con las mejores prácticas de la transformación digital.

1.2 Planteamiento del Problema

En el presente contexto, numerosas entidades industriales experimentan restricciones considerables en su infraestructura tecnológica, particularmente aquellas cuyo crecimiento ha sido sostenido, pero no se ha acompañado de una actualización equitativa de sus sistemas de red y telecomunicaciones. Es el caso de varias corporaciones que, a pesar de su expansión operativa, continúan empleando estructuras tecnológicas obsoletas, las cuales se distinguen por la utilización de cableado de categoría 5 con longitudes que

superan los 100 metros, lo cual infringe las regulaciones vigentes y pone en riesgo el desempeño de la red.

A lo anterior se añade la existencia de dispositivos obsoletos, conexiones inalámbricas inestables, regiones sin cobertura Wi-Fi, y una telefonía analógica que ya no satisface las demandas de comunicación tanto interna como externa. En realidad, se detectan intermitencias persistentes, una latencia elevada en la transmisión de datos, y un sistema de videovigilancia que no atiende de manera suficiente a todos los aspectos críticos del ambiente industrial, lo que constituye un peligro para la seguridad operativa. Esta situación restringe significativamente la eficiencia de los procesos industriales, impactando tanto en la productividad como en la capacidad de reacción ante contingencias. Aunque la infraestructura fue operativa en su etapa inicial, el desarrollo y la complejidad contemporánea de las operaciones requieren una renovación profunda y estratégica.

Por consiguiente, se hace imprescindible la implementación de una reestructuración tecnológica holística que incorpore la transición hacia sistemas de red optimizados y el aprovechamiento de tecnologías como la telefonía VoIP segura, que proporcionan ventajas significativas en aspectos como conectividad, escalabilidad, velocidad y seguridad. En el presente escenario, la cuestión primordial reside en la renovación y optimización de la infraestructura tecnológica de red para abordar de manera eficiente los desafíos contemporáneos de una industria en expansión.

1.2.1 Objetivos General y Específicos

Objetivo General

Reestructurar la infraestructura tecnológica de red en un entorno industrial mediante cableado estructurado Cat 6A, Wi-Fi 7, videovigilancia IP y telefonía VoIP segura, para optimizar la conectividad en las operaciones innovando las comunicaciones.

Objetivos Específicos

- Realizar un diagnóstico del estado presente de la infraestructura de red a través de mediciones técnicas y evaluación física, con el objetivo de identificar deficiencias críticas, puntos de obsolescencia y riesgos que puedan comprometer la conectividad.

- Elaborar una propuesta de mejora de infraestructura de red de computadoras que incorpore cableado estructurado en conformidad con las regulaciones actuales, la implementación de dispositivos de red actualizados y una cobertura inalámbrica eficaz, con el objetivo de actualizar la red y garantizar su compatibilidad, escalabilidad y rendimiento.
- Implementar un sistema de telefonía segura VoIP y un sistema de videovigilancia con cámaras IP con el objetivo de optimizar la calidad, estabilidad y eficiencia de la comunicación interna y externa de la organización, así como el refuerzo de la seguridad operativa.
- Realizar una evaluación de la mejora de la red anterior a través del examen de indicadores tales como velocidad, latencia y cobertura, así como la aplicación de encuestas al personal operativo, con el objetivo de verificar el rendimiento de la red una vez finalizada su implementación.

1.2.2 Justificación

En un mundo industrial en constante evolución, con una creciente necesidad de servicios eficientes, la infraestructura tecnológica es fundamental para la sostenibilidad y la capacidad de respuesta a los desafíos actuales. Con el tiempo, algunas de estas tecnologías se van quedando obsoletas ante las nuevas tecnologías que la industria actual necesita para mantenerse al día en conectividad, velocidad y seguridad.

Este proyecto es relevante porque aborda una necesidad estratégica: renovar y mejorar la infraestructura tecnológica de red para mejorar las comunicaciones, la conectividad y el monitoreo y, por lo tanto, mejorar la operación, seguridad y eficiencia. En otras instalaciones, puede encontrarse con áreas con poca cobertura inalámbrica, cableado antiguo que ya no cumple con la normativa actual o sistemas de comunicación antiguos que ya no ofrecen el rendimiento que necesitan.

La implementación de telefonía VoIP segura modernizará los canales de comunicación interna y externa, con más funcionalidades y menor costo. Además, la ampliación de la cobertura de red y la implementación de sistemas de videovigilancia más sofisticados mejorarán la seguridad y el control de las operaciones.

A nivel técnico y legal, el proyecto cumple con las mejores prácticas actuales de cableado estructurado, gestión de redes y protección de datos. Por lo tanto, la propuesta es una oportunidad para promover una modernización tecnológica progresiva, de base y orientada

a la eficiencia, escalabilidad y confiabilidad de los sistemas que soportan el crecimiento de la industria.

1.2.3 Preguntas de investigación

¿Cómo puede una empresa industrial mejorar la conectividad, comunicación y seguridad operativa mediante la actualización de su infraestructura tecnológica, integrando soluciones como redes optimizadas y telefonía VoIP segura?

1.2.4 Hipótesis

La modernización de la infraestructura tecnológica con cableado estructurado basado en normas actuales -- además de implementación de telefonía VoIP segura, videovigilancia IP y red inalámbrica de última generación-- mejora la conectividad, la comunicación y la seguridad en las instalaciones industriales traduciéndose en menos fallos de red, más estabilidad en la transmisión de datos y mejor respuesta en los procesos relacionados con las telecomunicaciones.

1.2.5 Alcances y limitaciones

Este proyecto contempla la evaluación, el diseño y la implementación de una infraestructura tecnológica modernizada orientada a mejorar la conectividad y las comunicaciones en un entorno industrial. Entre sus principales alcances se incluye el diagnóstico detallado del estado actual de la red, la actualización parcial del cableado estructurado conforme a normativas vigentes, la incorporación de equipos de red de alto rendimiento, la implementación de un sistema de telefonía VoIP con mecanismos de seguridad y calidad de servicio, así como la optimización del sistema de videovigilancia para lograr una cobertura más eficiente y estratégicamente distribuida.

Es importante señalar que no toda la infraestructura fue sustituida. Parte del cableado existente que cumplía con las condiciones técnicas y normativas necesarias fue conservado y reutilizado, al igual que algunos equipos de red que demostraron ser compatibles con la nueva arquitectura propuesta. Esta decisión permitió optimizar recursos, reducir costos de implementación y asegurar la continuidad operativa durante el proceso de actualización.

Asimismo, el alcance del proyecto incluye la validación de la nueva infraestructura mediante pruebas de conectividad, rendimiento y estabilidad del servicio, especialmente en lo referente a la transmisión de voz sobre IP. Como limitación, no se contempla la capacitación técnica formal del personal una vez concluida la implementación; sin embargo, se proponen

recomendaciones y buenas prácticas que podrán ser adoptadas posteriormente para la correcta operación y mantenimiento de la red.

1.2.6 Impacto Socioeconómico

La actualización de la infraestructura tecnológica en este sector no solo es un avance técnico, sino que también tiene efectos importantes en la economía y la sociedad. Modernizar las redes de comunicación, desde el aspecto social, crea un entorno laboral más conectado, seguro y eficiente, donde los trabajadores pueden realizar sus tareas de manera más fluida y con menos interrupciones. Esto mejora la comunicación dentro de la organización, crea un mejor ambiente de trabajo y fomenta una cultura centrada en la innovación y en el uso responsable de la tecnología.

Desde una perspectiva industrial, la implementación de soluciones como una red de datos sólida y telefonía VoIP segura promueve que las operaciones continúen, disminuye el peligro de errores críticos y optimiza los tiempos de reacción frente a eventualidades. Asimismo, posibilita que la compañía esté en condiciones de implementar nuevas tecnologías o sistemas de automatización en el futuro, lo cual incrementa su habilidad para ajustarse a las demandas del mercado y refuerza su competitividad.

Desde el punto de vista económico, invertir en infraestructura tecnológica produce beneficios que se pueden medir a medio y largo plazo, mencionando algunos de ellos, incluyen la disminución de los gastos relacionados con el mantenimiento de sistemas anticuados, el acortamiento de los periodos de inactividad y la mejora en los recursos de comunicación. Estos avances, a largo plazo, generan una eficiencia operativa más alta y un retorno de inversión positivo, lo cual se ajusta a una perspectiva estratégica de crecimiento sostenible.

1.2.7 Organización de la tesis

Esta tesis presenta una propuesta técnica enfocada en optimizar la infraestructura tecnológica de red en el sector industrial, con un enfoque particular en la puesta en marcha de telefonía VoIP segura, con el fin de mejorar la eficiencia operativa, comunicación y conectividad. En el capítulo II se introduce el marco teórico, que trata los conceptos esenciales vinculados a la telefonía VoIP, las redes de datos, el cableado estructurado, las regulaciones técnicas y los elementos cruciales de seguridad en redes industriales.

De igual modo se presenta una revisión al estado del arte en el Capítulo III, donde se examinan antecedentes, situaciones parecidas y soluciones tecnológicas vigentes que se han puesto en práctica en ambientes industriales de rasgos semejantes, lo cual posibilita contextualizar la propuesta dentro de un marco actualizado. Así mismo durante el Capítulo IV correspondiente a la metodología; se va explicando a fondo los pasos del proyecto, las técnicas de recolección de datos, el análisis técnico que se llevó a cabo y el diseño de la solución en función de criterios como la viabilidad, la normativa y la eficacia.

Los resultados se explican en el Capítulo V, donde se detalla cómo se llevó a cabo la implementación, las mejoras en comunicación y conectividad, y los indicadores que muestran el impacto positivo del proyecto. El capítulo VI, finalmente, presenta las conclusiones y sugerencias. Destaca los beneficios del trabajo realizado, lo que se ha aprendido y las formas posibles de mejorar o ampliar la tecnología en el futuro.

CAPÍTULO 2. Marco Teórico

Este capítulo presenta los principios básicos, técnicos y legales que apoyan el desarrollo del proyecto. Se lleva a cabo un análisis paso a paso de los elementos básicos que forman la infraestructura tecnológica en entornos industriales. Esto se hace desde una visión general hasta detalles específicos, como las redes de datos, el cableado estructurado, la conectividad inalámbrica, la telefonía IP, la seguridad informática, los sistemas de videovigilancia, la transformación digital y las normas relacionadas. Este marco teórico tiene como objetivo ofrecer una base sólida que apoye las decisiones sobre el diseño y la implementación de soluciones tecnológicas para mejorar las redes y la comunicación en entornos industriales.

2.1 Infraestructura tecnológica

La infraestructura tecnológica puede ser conceptualizada como el compendio de recursos físicos, lógicos y organizativos que facilitan la operación, administración y optimización de los sistemas de información y comunicación en un contexto específico. Este término comprende tanto los componentes de hardware y software como los componentes de red, servidores, cableado estructurado, dispositivos de conectividad y plataformas digitales que aseguran la integridad y el flujo eficaz de datos en una entidad.

Dentro de los elementos fundamentales de esta infraestructura se incluyen: los dispositivos informáticos (servidores, estaciones de trabajo, dispositivos móviles), el software de administración y funcionamiento, las redes de comunicación (alámbricas e inalámbricas), el cableado estructurado, los dispositivos de interconexión como los conmutadores y routers, así como los sistemas de suministro, seguridad, monitoreo y respaldo de información. La correcta integración y conservación de estos es esencial para la funcionalidad de los procesos industriales actuales, en especial los que operan bajo estrategias de automatización o digitalización de última generación.

En la industria, la infraestructura tecnológica es esencial porque es la base para los procesos productivos, de control de calidad, logística, trazabilidad y comunicación. Según Zúñiga Vázquez (2022), una infraestructura sólida y estandarizada ayuda a implementar tecnologías relacionadas con la Industria 4.0, que incluyen el Internet de las Cosas (IoT), la inteligencia artificial, los sistemas ciberfísicos y el análisis de grandes cantidades de datos. Además, se destaca que una mala planificación o ejecución de esta infraestructura puede

causar hasta el 80% de los problemas en las redes industriales, lo que resalta la importancia de un diseño cuidadoso y ajustado al contexto en el que se realiza. La Figura 2.1 muestra que una arquitectura virtualizada ayuda a integrar los componentes tecnológicos necesarios para que la operación industrial sea eficiente (Zúñiga Vázquez, 2022).

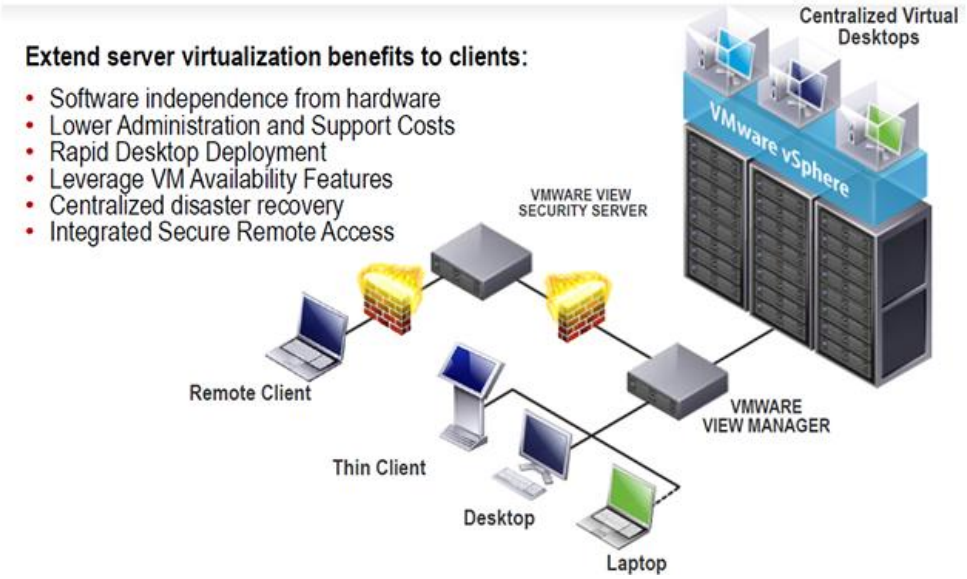


Figura 2.1 Representación gráfica de Arquitectura Virtualizada. Adaptado de Rockwell Automation (2002), citado en (Zúñiga Vázquez, 2022).

La historia de la infraestructura tecnológica ha ido paralela a las revoluciones industriales. En la tercera revolución industrial se incorporaron computadoras y sistemas informáticos a los procesos productivos. Luego, con la Industria 4.0, la transformación digital se profundizó, ahora con hiperconectividad, automatización inteligente y control descentralizado en tiempo real a través de redes de datos y plataformas en la nube (Pangol Lascano, 2022).

Hoy en día las tendencias se dirigen hacia la convergencia entre las tecnologías de la información (TI) y las de operación (OT), creando redes unificadas, seguras y escalables que soporten la gestión empresarial y la producción. Esto implica seguir estándares de diseño, utilizar cableado y equipos industriales certificados, tomar en cuenta factores ambientales como temperatura, vibración o interferencia electromagnética para asegurar la estabilidad y durabilidad de la red (Zúñiga Vázquez, 2022).

2.1.1 Conceptos y componentes de infraestructura de red

La infraestructura de red en entornos industriales se compone de un conjunto de elementos físicos y lógicos que permiten la transmisión segura, eficiente y confiable de la información entre dispositivos, sistemas y servicios. Estos componentes constituyen la base sobre la cual operan tecnologías como redes de datos, telefonía IP, videovigilancia y conectividad inalámbrica, por lo que su correcta comprensión es fundamental para el diseño, implementación y evaluación de soluciones tecnológicas integrales (Tanenbaum & Wetherall, 2011; Kurose & Ross, 2017).

Dentro de este contexto, un Punto de Acceso (Access Point, AP) es un dispositivo de red que permite la conexión inalámbrica de equipos finales a una red cableada, facilitando la movilidad y el acceso a los recursos de red. Una Red de Área Local (Local Area Network, LAN) corresponde a la interconexión de dispositivos dentro de un espacio geográfico limitado, mientras que una Red de Área Local Virtual (Virtual Local Area Network, VLAN) permite segmentar lógicamente la red para mejorar la seguridad, el control del tráfico y el desempeño general del sistema (Kurose & Ross, 2017).

En cuanto a la infraestructura física, el Main Distribution Frame (MDF) es el gabinete principal donde se concentran los equipos centrales de red, como switches principales, servidores o grabadores de video, mientras que los Intermediate Distribution Frame (IDF) funcionan como puntos intermedios de distribución que facilitan la conexión hacia áreas específicas de la instalación. Esta organización jerárquica del cableado estructurado es una práctica ampliamente recomendada para garantizar orden, mantenibilidad y escalabilidad en redes industriales (Tanenbaum & Wetherall, 2011; Zúñiga, 2022).

El cableado estructurado incorpora diversos componentes especializados, entre los que destacan el patch cord, utilizado para interconectar equipos y paneles de parcheo; el pigtail de fibra óptica, que consiste en un cable corto con conector en un extremo empleado para la terminación de enlaces de fibra; y los módulos Mini-GBIC o SFP (Small Form-factor Pluggable), que permiten la conversión de señales eléctricas a ópticas en equipos de red, posibilitando enlaces de fibra óptica de diferentes velocidades y distancias. Asimismo, la fibra óptica monomodo se emplea principalmente en enlaces de larga distancia, mientras que la fibra óptica multimodo es común en interconexiones de corta distancia dentro de instalaciones industriales (Barceló et al., 2004; Zúñiga, 2022).

Desde el punto de vista del desempeño de la red, la latencia se define como el tiempo que tarda un paquete de datos en viajar desde su origen hasta su destino, siendo un parámetro crítico para servicios sensibles al retardo como la telefonía IP. El backbone o red troncal corresponde al conjunto de enlaces principales que interconectan los distintos segmentos de la red, mientras que un uplink es el enlace que conecta un dispositivo de acceso con un equipo de mayor jerarquía, como un switch central (Kurose & Ross, 2017).

En el ámbito de la comunicación y el monitoreo, la Telefonía sobre Protocolo de Internet (Voice over Internet Protocol, VoIP) permite transmitir voz mediante redes IP, integrando los servicios de comunicación con la infraestructura de datos existente. Para asegurar un desempeño adecuado de este tipo de servicios, el Quality of Service (QoS) agrupa un conjunto de mecanismos que permiten priorizar el tráfico crítico dentro de la red. Por su parte, en sistemas de seguridad, el Network Video Recorder (NVR) es el dispositivo encargado de almacenar y gestionar las grabaciones provenientes de cámaras IP, las cuales pueden clasificarse en cámaras domo, bullet o PTZ (Pan-Tilt-Zoom) según su diseño y funcionalidad (Soler, 2009; Caldera & Suazo, 2011).

La comprensión de estos conceptos y componentes permite establecer una base teórica sólida para el análisis, diseño e implementación de infraestructuras tecnológicas de red en entornos industriales, facilitando la integración eficiente de servicios de comunicación, conectividad y videovigilancia desarrollados en los capítulos posteriores (Tanenbaum & Wetherall, 2011; Kurose & Ross, 2017).

2.2 Redes de computadoras

Las redes de computadoras son parte esencial de la infraestructura tecnológica, que permite la interconexión de dispositivos y sistemas para el intercambio de información en entornos corporativos, industriales y domésticos. Estas redes permiten que las computadoras, servidores, impresoras, cámaras IP, dispositivos móviles y más puedan comunicarse entre sí localmente o a distancia, siendo la base para que los sistemas digitales funcionen.

Colocándolo en términos generales, se pueden clasificar en diferentes tipos según su alcance y funcionalidad. Las redes de área local (LAN) conectan dispositivos en un área limitada, como una oficina o una fábrica (véase Figura 2.2), las redes inalámbricas se conectan a través de un punto de acceso y las redes Ethernet se conectan físicamente a un switch (Tanenbaum & Wetherall, 2012).

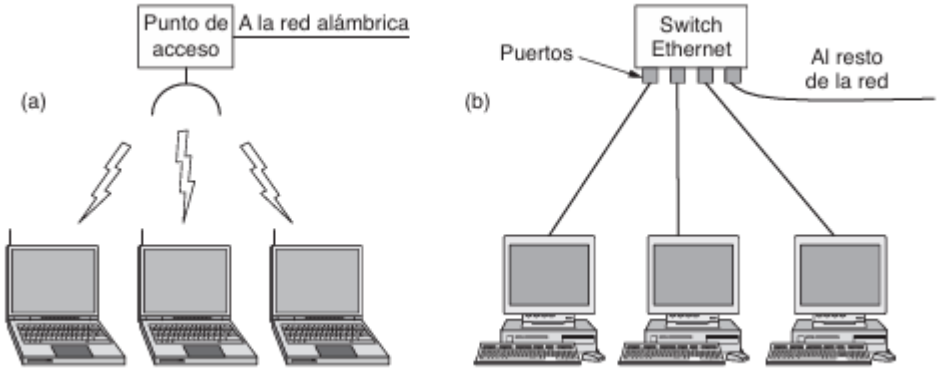


Figura 2.2 Redes LAN inalámbrica y alámbrica (a) Conexión Wi-Fi (802.11), (b) Red Ethernet conmutada. Recuperado de (Tanenbaum & Wetherall, 2012).

Por otro lado, como se puede apreciar en la imagen de la Figura 2.3, las redes de área amplia (WAN) cubren distancias mucho mayores y normalmente interconectan ubicaciones geográficamente dispersas utilizando infraestructuras públicas o privadas. También existen las redes inalámbricas, llamadas WLAN (Wireless Local Area Network), que permiten conectar dispositivos de manera inalámbrica así mismo, por otro lado, las redes virtuales o VLAN (Virtual Local Area Network) son redes lógicas que se configuran dentro de una red física para segmentar y organizar los dispositivos conectados. Estas tecnologías proporcionan más flexibilidad y permiten organizar los datos en las empresas, segmentando la información según los departamentos o niveles de seguridad definidos (Tanenbaum & Wetherall, 2012).

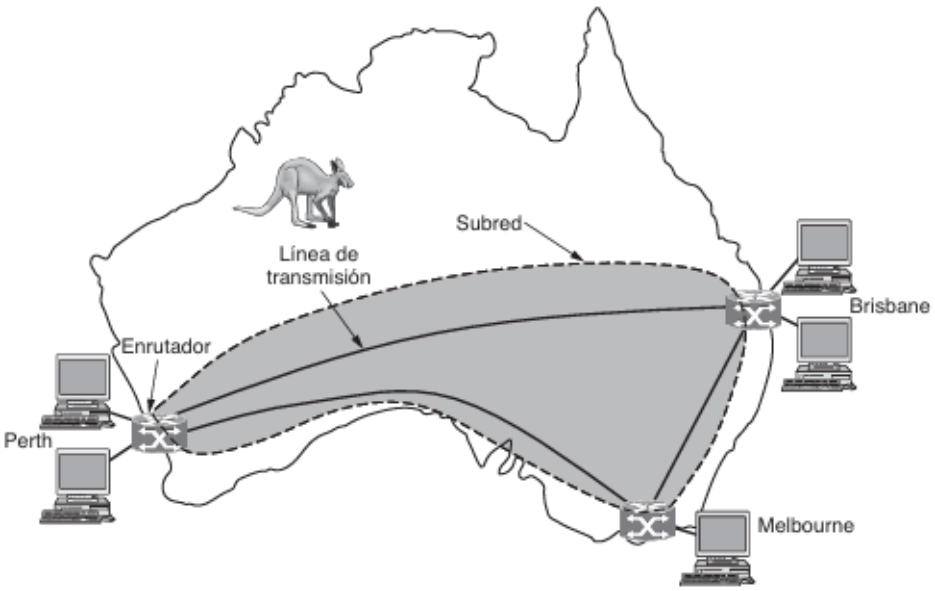


Figura 2.3 Red de área amplia (WAN) conectando varias ciudades. Recuperado de (Tanenbaum & Wetherall, 2012).

En lo que concierne a la arquitectura y el diseño de sistemas informáticos, las redes pueden adoptar diversas topologías, tales como la topología estrella, la topología bus o la topología malla, entre otras alternativas disponibles en el ámbito de las comunicaciones y la conectividad como se puede apreciar en el ejemplo de la Figura 2.4. La topología en estrella, que se utiliza de manera extensiva en las redes locales (LAN) en la actualidad, se basa en la existencia de un nodo central, que generalmente es un conmutador, al cual están conectados todos los dispositivos de la red.

En contraste, la topología en bus se distingue por su estructura lineal y su relativa simplicidad; sin embargo, puede ser considerada menos confiable en comparación con otras configuraciones de red. De otro modo, se debe destacar que la topología en malla proporciona un número superior de rutas de comunicación, lo que da lugar a una arquitectura altamente confiable y resistente a posibles fallos. Estas características la convierten en una opción idónea para entornos en los que la continuidad de las operaciones es fundamental, tal como se indica en el estudio de López Rodríguez (2007).

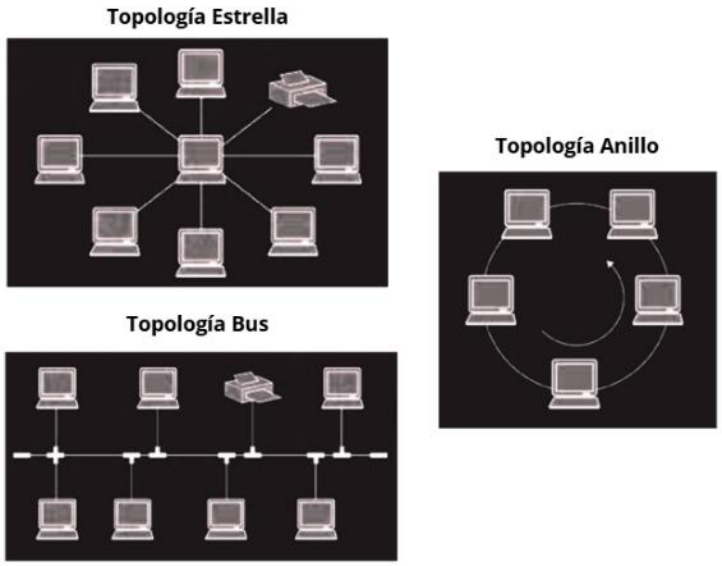


Figura 2.4 Ejemplos de Topología de Red. Adaptado de (Barceló et al., 2004).

En el tema que respecta a los protocolos de comunicación, es fundamental destacar la relevancia del TCP/IP (Protocolo de Control de Transmisión / Protocolo de Internet), el cual se erige como uno de los pilares fundamentales de las comunicaciones contemporáneas. Este protocolo posibilita de manera eficiente y segura la transferencia de información entre dispositivos con diversidad de características y sistemas operativos diversos.

Este protocolo de comunicación asegura una transmisión confiable y segura de datos, estableciendo pautas claras y uniformes para la interacción entre dispositivos conectados, ya sea en entornos de red privados o en entornos de red públicos. Asimismo, el UDP (User Datagram Protocol) también se utiliza en ciertas aplicaciones donde la velocidad es prioritaria frente a la confiabilidad, como sucede en transmisiones de video o voz en tiempo real; a continuación, se presenta un diagrama de ejemplo en la Figura 2.5 para ilustrar este concepto.

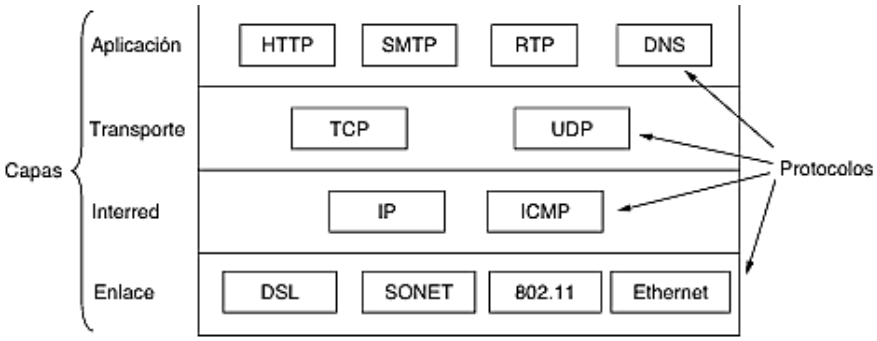


Figura 2.5 Modelo TCP/IP con ejemplos de protocolos por capa. Recuperado de (Tanenbaum & Wetherall, 2012).

Para que estas redes sofisticadas operen de manera eficiente, se necesitan dispositivos de interconexión sofisticados, como switches, routers y puntos de acceso inalámbricos. Estos dispositivos son esenciales para la interconexión y comunicación de todos los dispositivos en la red y permitir así la transmisión de datos e interacción de los usuarios. Los switches (conmutadores) son dispositivos que posibilitan conectar varios equipos en red local y que puedan comunicar entre sí de manera eficiente y segura.

Además, los switches pueden dirigir el tráfico de datos de forma inteligente para evitar conflictos y mantener la red funcionando de manera óptima en todo momento. Los routers, en cambio, son dispositivos cruciales para conectar diferentes redes locales y permitir la comunicación con la red mundial de redes, actuando como intermediarios entre las redes internas y externas. En las redes inalámbricas, los puntos de acceso son los encargados de dar conectividad inalámbrica a varios dispositivos móviles dentro de un área geográfica determinada, lo que permite garantizar la movilidad de los usuarios sin restringir el acceso a los recursos compartidos en la red. En la Tabla 2.1, se explica de manera más detallada la función de los access points y algunos otros componentes antes mencionados.

Tabla 2.1 Principales dispositivos que pueden componer una red

Imagen	***Dispositivo***	***Descripción funcional***
	**Switch**	Permite interconectar varios dispositivos dentro de una red local (LAN), gestionando el tráfico de datos y evitando colisiones. Es esencial en redes con topología en estrella.
	**Router**	Dispositivo que conecta diferentes redes entre sí, permitiendo el acceso a Internet y estableciendo rutas para el tráfico entre redes LAN, WAN o VPN.
	**Punto de Acceso (Access Point)**	Proporciona conectividad inalámbrica a dispositivos móviles en un área determinada, expandiendo el alcance de una red LAN tradicional.
	**Firewall**	Filtra y controla el tráfico entrante y saliente de la red para proteger contra accesos no autorizados, virus o ataques cibernéticos.

	**Servidor de Red**	Centraliza recursos como almacenamiento, aplicaciones o servicios de red (correo, VoIP, bases de datos), facilitando el control y administración.

En este sentido, las complejas redes de datos constituyen el sistema nervioso central de cualquier infraestructura tecnológica moderna, posibilitando una comunicación eficiente, segura y altamente organizada entre los diversos elementos que conforman un entorno digital interconectado. La correcta planificación y ejecución son fundamentales para alcanzar una operación industrial eficiente y perfectamente alineada con las demandas y requerimientos de la actual transformación digital en la que nos encontramos inmersos.

2.3 Modelo de Referencia OSI

El modelo de referencia OSI (Open Systems Interconnection), desarrollado por la Organización Internacional de Normalización (ISO), es uno de los modelos conceptuales más importantes para estudiar, planificar y evaluar infraestructuras de interconexión de datos y sistemas de telecomunicaciones. Su principal objetivo es normalizar y hacer compatibles las funciones necesarias para el proceso de comunicación entre sistemas informáticos diferentes, permitiendo que tecnologías, fabricantes y protocolos diferentes puedan comunicarse entre sí sin problemas (Tanenbaum & Wetherall, 2012).

Este modelo conceptual, muy utilizado en las tecnologías de la información y comunicación, organiza de forma estructurada la manera en que interactúan los dispositivos y sistemas en una red. Las siete capas jerárquicas (véase Figura 2.6), desde la física hasta la de aplicación, definen un marco de referencia para entender y controlar la comunicación de datos en sistemas informáticos complejos y heterogéneos y cada una de estas capas tiene una función específica en el proceso de comunicación, desde la transmisión hasta la recepción de la información, asegurando que la información fluya de manera organizada y segura a través de la red. Esta división en capas permite desarrollar nuevas tecnologías compatibles entre sí y detectar y corregir errores al examinar el sistema por partes aisladas de forma completa (Kurose & Ross, 2017).

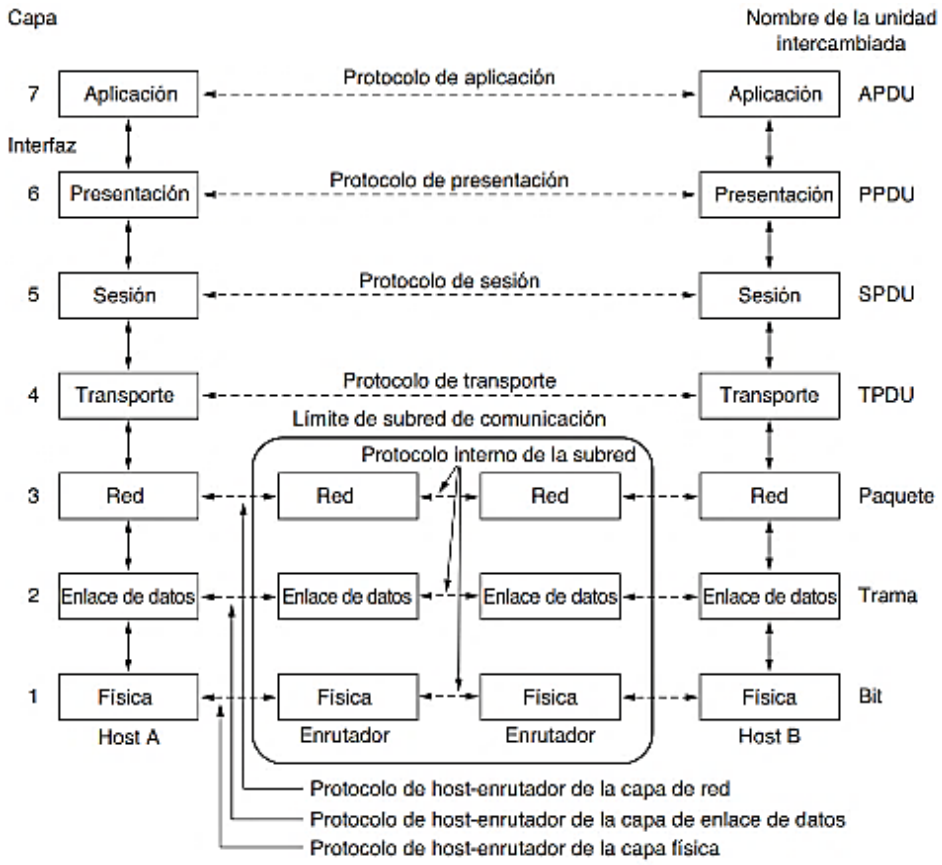


Figura 2.6 Modelo OSI. Recuperado de (Tanenbaum & Wetherall, 2012).

Desde el punto de vista práctico, este modelo es muy útil para entender cómo interactúan entre sí las diferentes capas que componen una red de comunicaciones; por ejemplo, la capa física define cómo se transmiten señales eléctricas u ópticas a través de medios de comunicación como cables UTP, fibra óptica o inalámbricos. Estos puntos son bien discutidos por el autor Castellón Arenas (2014) en su libro sobre la norma EIA/TIA-568 para cableado estructurado. En la capa de enlace de datos, tecnologías tan conocidas como Ethernet o Wi-Fi son las responsables de la forma en que se organiza la información en tramas y se controla la presencia de errores. Estas tecnologías son fundamentales para garantizar la integridad y fiabilidad de los datos, sobre todo en entornos industriales, donde el ruido y las condiciones adversas son comunes. En consecuencia, como indica el experto Zúñiga Vázquez en su estudio de 2022, es necesario tener en cuenta estas tecnologías en el diseño de infraestructuras de red para dar respuesta a las necesidades de la industria 4.0.

Por otro lado, la capa de red se encarga de interconectar dispositivos y establecer la

comunicación entre ellos a través de direcciones IP y la mejor ruta para enviar paquetes a través de redes interconectadas. En la capa de transporte, el Protocolo de Control de Transmisión (TCP) y el Protocolo de Datagramas de Usuario (UDP) aseguran la integridad y la entrega correcta de los datos entre los sistemas finales. En aplicaciones como telefonía IP o videovigilancia IP, estas capas de seguridad son vitales y estratégicas. Por ejemplo, como lo señalan Soler Palacín (2009) y Caldera Palma y Suazo Sequeira (2011), la telefonía IP utiliza múltiples protocolos, tales como SIP (Session Initiation Protocol) en la capa de aplicación y RTP (Real-time Transport Protocol) en la capa de transporte, para establecer y mantener las comunicaciones de voz. Estos protocolos certifican la calidad de audio por medio de mecanismos de control de flujo y detección y corrección de errores.

En las capas altas del modelo, la capa de sesión gestiona el establecimiento, mantenimiento y finalización de sesiones entre aplicaciones, lo cual es valioso en entornos donde la comunicación segura y confiable es crítica; por otro lado, la capa de presentación es responsable de funciones como el cifrado, la compresión y la conversión de datos, esenciales para las aplicaciones actuales que requieren la transmisión segura y eficiente de datos multimedia, como video o audio. Finalmente, la capa de aplicación es la que directamente interactúa con el usuario y sus aplicaciones; en ella trabajan protocolos tales como HTTP, FTP, SMTP, DNS, ONVIF o RTSP, estos últimos imprescindibles para los servicios de videovigilancia IP. Como indican Jinez Granja y Pantoja Prado (2020), esta capa es la encargada de la comunicación y transmisión de datos en las capas de vigilancia digital.

El modelo OSI, más allá de su importancia teórica, es ampliamente aplicado en la práctica en la industria y la tecnología; como indican los autores Salimbeni y Bianchi (2019), una planificación adecuada de infraestructura tecnológica implica la integración de diversos servicios y dispositivos, lo que exige conocimiento sobre la forma en que interactúan las capas de red. Es importante considerar la complejidad e interdependencia de los componentes tecnológicos para asegurar que la infraestructura funcione de manera óptima. Asimismo, autores como Jaimes, García y Rodríguez (2011) mencionan que la alineación estratégica entre la visión de la empresa y la arquitectura de red se debe basar en modelos técnicos fuertes como el Modelo OSI para garantizar la escalabilidad, redundancia y eficiencia del sistema.

2.4 Cableado estructurado

El cableado estructurado siempre que se encuentre bien diseñado e instalado será la mejor base de cualquier sistema de comunicaciones moderno ya que este tipo de infraestructura, al estar diseñada y seguir estándares, asegura una transmisión eficiente y confiable de información digital, ya sean datos, voz o video. Su arquitectura permite integrar fácilmente todo tipo de servicios en una única infraestructura, simplificando la expansión y el mantenimiento del sistema sin interrumpir las conexiones existentes.

El cableado estructurado es la solución estandarizada para resolver la complejidad de las infraestructuras de red empresarial y de telecomunicaciones. Su propósito es hacer que los diferentes equipos y sistemas tecnológicos puedan trabajar juntos de manera eficiente. Como indica la investigación de Joskowicz (2006), antes de estos estándares comunes, cada fabricante de hardware tenía que desarrollar sus propios sistemas de cableado, lo que hacía muy difícil actualizar o integrar nuevas tecnologías.

Desde 1985, se inició el proceso de instauración de regulaciones particulares, tal como la normativa TIA/EIA-568, que estipula de forma exhaustiva una serie de parámetros técnicos y topologías a aplicar en la instalación de sistemas de cableado en edificios destinados a uso comercial, tal como se ilustra en la Figura 2.7. Según la investigación de Joskowicz (2006), existe una correlación entre las variables estudiadas.

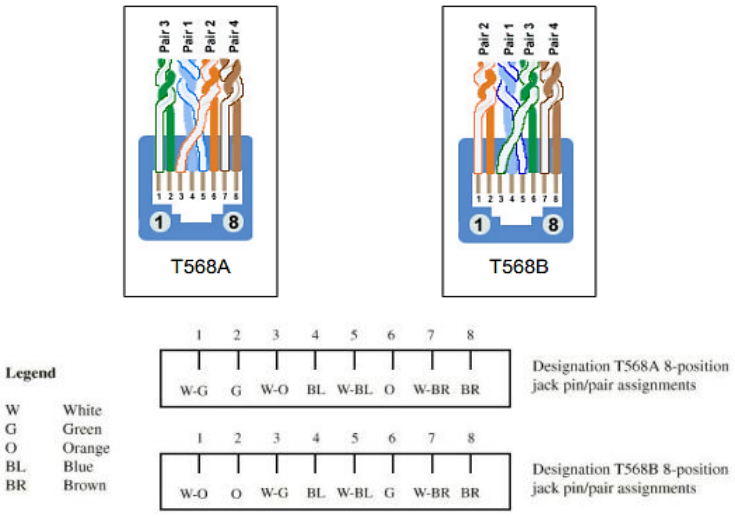


Figura 2.7 Asignación de pines y colores de los pares trenzados para conectores RJ-45 según estándares T568A y T568B. Recuperado de (Joskowicz, 2006).

Actualmente los estándares más reconocidos y utilizados en la industria para diseñar y certificar el cableado estructurado son los de la Asociación Nacional de Estándares

Americanos (ANSI), la Asociación de la Industria de Telecomunicaciones (TIA) y la Asociación de la Industria Electrónica (EIA); estos estándares especifican en detalle las características técnicas y los requisitos para los sistemas de comunicación en cobre (par trenzado) y en fibra óptica, incluyendo la transmisión de datos, la calidad de la señal, la inmunidad al ruido y la compatibilidad con diversas tecnologías. Además, definen normas específicas para la instalación de equipos, interconexión de dispositivos, canalización y ubicación de puntos de acceso para asegurar un rendimiento óptimo y un fácil mantenimiento de la red.

Uno de los estándares más importantes en este campo es el TIA/EIA-568B, que especifica la forma correcta de ordenar los cables en los conectores RJ-45 mediante los esquemas 568A y 568B. Cabe mencionar que el esquema 568B es el más utilizado en las infraestructuras de red, tal como menciona Castellón Arenas (2014) en su estudio. Hablando de las categorías de cable más comunes hoy en día, existe la categoría 5e, capaz de transmitir datos a 1 Gbps y 100 MHz; también está la Categoría 6, pensada para redes Gigabit Ethernet y capaz de funcionar hasta 250 MHz y con protección extra contra interferencias y diafonía; por otro lado, existen las categorías 6A y superiores, muy utilizadas en entornos industriales exigentes o redes de alto rendimiento.

Estas categorías pueden soportar velocidades de transmisión de hasta 10 Gbps en distancias de hasta 100 metros, lo que las hace adecuadas para aplicaciones que exigen un alto rendimiento (Castellón Arenas, 2014). Pero también hay que saber que los cables de red pueden venir en diferentes estructuras y materiales. Por ejemplo, el cable UTP (sin protección), el cable FTP (cubierto en general) o el cable STP (blindado por pares), que ofrece mayor protección contra interferencias eléctricas externas. Debe elegirse el tipo de cable apropiado al nivel de interferencia electromagnética del lugar en el que se vaya a utilizar.

La instalación adecuada y correcta del cableado estructurado requiere tomar en cuenta ciertos aspectos importantes y necesarios para que funcione de manera correcta, entre ellas, en primer lugar, el respeto riguroso de la distancia máxima permitida para los tramos horizontales, que en el caso de los cables de cobre no debe superar los 100 metros. También es importante la distancia apropiada entre las fuentes de interferencias electromagnéticas y la canalización y etiquetado preciso de los cables. Además, es crucial seguir al pie de la letra las normas en cuanto a curvatura, tensión y radio de curvatura de los cables, factores críticos para garantizar el rendimiento y la longevidad del sistema de

cableado ya que, en aplicaciones exigentes, además, es necesario evaluar en detalle la resistencia del material a condiciones extremas de temperatura, humedad o vibración para asegurar la máxima durabilidad y continuidad de la comunicación (Zúñiga Vázquez, 2022).

Finalmente, una vez instalados los elementos, es fundamental realizar pruebas certificadas para verificar que el sistema cumpla con los parámetros de atenuación, diafonía y pérdida por retorno definidos en los estándares internacionales de calidad y desempeño más exigentes por lo que este proceso riguroso asegura la más alta calidad del cableado estructurado, la máxima confiabilidad de la red y su capacidad para soportar cualquier aplicación de comunicación y automatización en ambientes empresariales y comerciales exigentes.

2.4.1 Conexión Vertical y Horizontal

En el diseño e instalación de un sistema de cableado estructurado se debe tener en cuenta la forma en que se organizan físicamente las conexiones, que básicamente son de dos tipos: horizontal, que conecta el área de trabajo con el cuarto de telecomunicaciones, y vertical, también llamado backbone o troncal, que interconecta los cuartos de telecomunicaciones. Ambos tipos de enlaces son necesarios para la red de comunicaciones de una organización y así asegurar su buen funcionamiento. Las dos son partes esenciales para garantizar el mejor rendimiento, escalabilidad y facilidad de mantenimiento de una red de comunicaciones, sobre todo en las redes industriales y empresariales, donde la fiabilidad y la continuidad son imprescindibles.

La conexión horizontal (cableado horizontal) es la parte del cableado estructurado que va desde el punto de distribución intermedio (IDF) hasta el área de trabajo del usuario final en un edificio o instalación. Esta parte de cableado es fundamental para asegurar una conectividad de red y comunicación entre los dispositivos y equipos en el área de trabajo. Aquí se incluyen los cables de par trenzado categorías 5e, 6 o 6A, los paneles de parcheo, las tomas de red y los distintos componentes de canalización o charolas del cableado estructurado. De acuerdo con la norma TIA/EIA-568B, la longitud máxima para este tendido no debe superar los 100 metros lineales. Normalmente, en la mayoría de los casos, se elige una topología en estrella, donde todos los puntos de la red convergen al panel de parcheo central localizado en el rack del IDF.

Para garantizar la integridad y confiabilidad de la señal de red, el cableado horizontal debe mantenerse alejado de fuentes potenciales de interferencia electromagnética, como

motores eléctricos, transformadores de potencia y otros equipos industriales que generen campos electromagnéticos no deseados. Además, es fundamental respetar los radios mínimos de curvatura, emplear canalizaciones identificadas y elegir accesorios que ayuden a evitar la atenuación o degradación de la señal ya que de acuerdo con el estudio de Zúñiga Vázquez (2022), en los ambientes industriales se debe considerar el uso de cableado blindado STP o FTP, ya que estos cables ofrecen una protección adicional contra interferencias electromagnéticas generadas por equipos o instalaciones eléctricas cercanas.

Por otra parte, la conexión vertical (backbone) es la que interconecta de manera eficiente y segura los diferentes cuartos de telecomunicaciones, desde el distribuidor principal (MDF) a los distribuidores intermedios (IDF). Este subsistema es, sin duda, el corazón del sistema de cableado estructurado, ya que de su desempeño depende la eficacia, eficiencia y confiabilidad de toda la red.

El backbone de una red generalmente se construye con fibra óptica monomodo o multimodo de alta calidad, o en su defecto con cableado de cobre de alta categoría, en función de las necesidades de ancho de banda, distancia y complejidad de la topología del edificio. Además de permitir la comunicación de datos, voz y videovigilancia entre localizaciones o edificios diferentes, este trozo se ha de diseñar en términos de redundancia que aseguren el servicio ante fallos físicos. Para realizar una instalación adecuada se deben considerar todos los elementos estructurales del edificio (escaleras de acceso entre plantas, conductos verticales de comunicación, canalizaciones homologadas) para garantizar su integridad física y la trazabilidad de las conexiones.

Como señala Joskowicz (2006), el backbone es el esqueleto que soporta y estructura la red de telecomunicaciones debe ser diseñado con visión de futuro, capaz de soportar el crecimiento tecnológico y la incorporación de nuevos servicios sin tener que sustituir la infraestructura ya instalada. De este modo, un diseño bien estructurado garantiza que la conectividad horizontal y vertical trabajen juntas en armonía para proporcionar una base confiable, escalable y de alto rendimiento para las infraestructuras de comunicación actuales; en la Figura 2.8, presentada por López (2023), se exponen algunos de los subsistemas básicos pertenecientes al cableado estructurado que se ha discutido anteriormente.

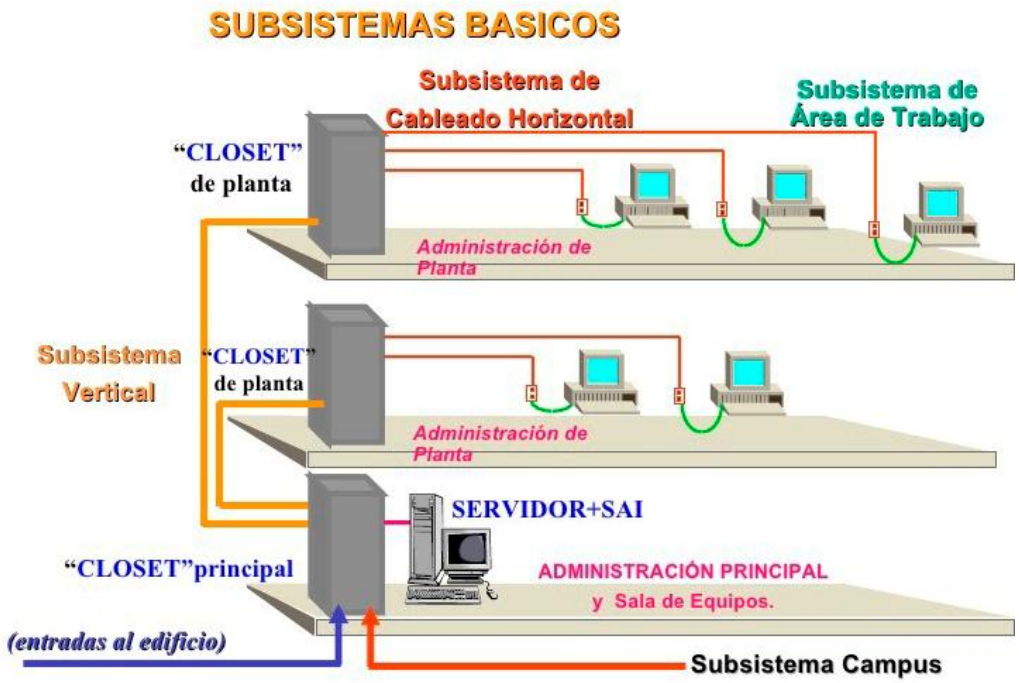


Figura 2.8 Subsistemas básicos del cableado estructurado en redes. Recuperado de (López, 2023).

2.5 Conectividad inalámbrica

Hoy en día, en el mundo de la infraestructura tecnológica, la conectividad inalámbrica es un elemento esencial para asegurar la flexibilidad, movilidad y escalabilidad de los sistemas de comunicación; por lo anterior este tipo de conexión inalámbrica es capaz de crear enlaces entre dispositivos sin cables físicos, lo que es muy útil en entornos como los industriales, educativos o corporativos. Su uso se ha extendido por ser muy rentable económicamente y por las posibilidades operativas que permite en lugares donde sería difícil o estaría prohibido por las leyes locales instalar cableado (López Rodríguez, 2007).

Las redes inalámbricas se basan en los estándares IEEE 802.11 (véase Figura 2.9), que especifican detalles técnicos para diferentes niveles de rendimiento, alcance y frecuencia, por ejemplo, el estándar 802.11b funciona en la banda de 2.4 GHz y alcanza un máximo de 5 Mbps en condiciones reales, mientras que el estándar 802.11g puede llegar hasta los 24 Mbps en la misma banda; por otro lado, el 802.11a opera en la banda de 5 GHz y puede alcanzar velocidades teóricas de hasta 54 Mbps, pero su alcance es menor que el de otras tecnologías inalámbricas. Más tarde, la 802.11n adoptó la técnica MIMO (multiple-input multiple-output), capaz de lograr velocidades reales superiores a 100 Mbps y una mayor estabilidad en entornos con interferencia electromagnética (Tanenbaum & Wetherall, 2012).

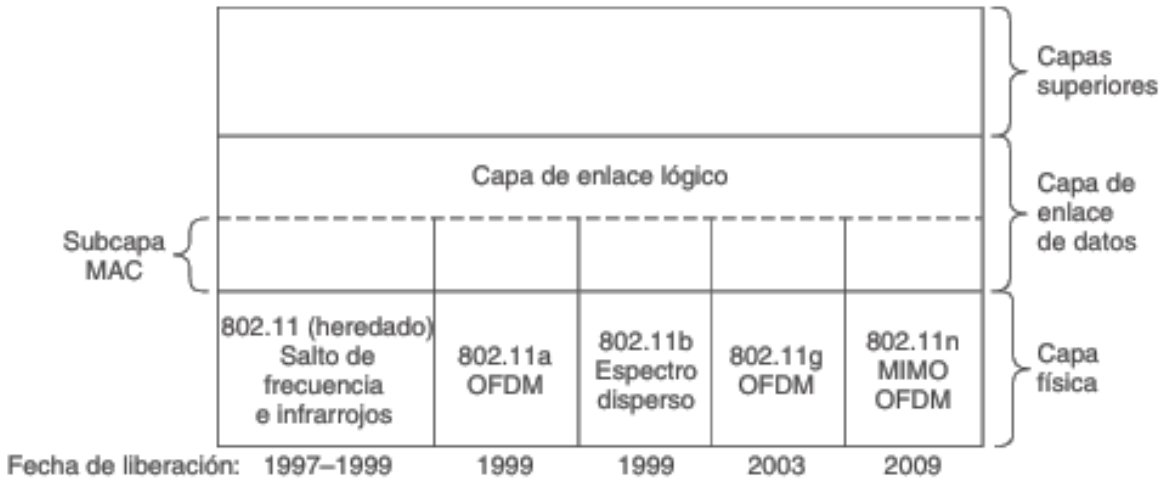


Figura 2.9 Evolución de los protocolos IEEE 802.11 en la pila de capas. Recuperado de (Tanenbaum & Wetherall, 2012).

En tiempos recientes, han emergido los estándares 802.11ac y 802.11ax, conocido también como Wi-Fi 6, los cuales ofrecen mejoras significativas en la capacidad de transmisión, la gestión simultánea de múltiples dispositivos y la optimización del consumo energético, además; se suma a esto el emergente estándar Wi-Fi 7 (802.11be), que introduce innovaciones tales como la implementación de canales de 320 MHz, la modulación 4096-QAM y la tecnología de operación multienlace (MLO). Estas características permiten alcanzar velocidades que superan un gigabit por segundo, reduciendo la latencia y mejorando la eficiencia en la transferencia de información en entornos de gran relevancia, según Cisco Systems (2025).

Con el propósito de llevar a cabo un análisis exhaustivo y detallado de las características más relevantes de los distintos estándares de conectividad inalámbrica, se presenta a continuación la Tabla 2.2. En esta tabla se resumen aspectos fundamentales, tales como la frecuencia de operación, el ancho de banda disponible, la velocidad máxima teórica y la capacidad de conexión simultánea de múltiples dispositivos.

Tabla 2.2 Principales características de los diferentes estándares Wi-Fi

Estándar Wi-Fi	***Frecuencia***	***Velocidad Máxima Teórica***	***Modulación***	***Canal Máximo***	***Año***	***Características Destacadas***
802.11b	2.4 GHz	11 Mbps	DSSS	20 MHz	1999	Alta compatibilidad, bajo rendimiento
802.11g	2.4 GHz	54 Mbps	OFDM	20 MHz	2003	Mejora de velocidad sobre 802.11b
802.11n	2.4 / 5 GHz	600 Mbps	MIMO-OFDM	40 MHz	2009	MIMO, mayor alcance y velocidad
802.11ac (Wi-Fi 5)	5 GHz	1.3 Gbps	256-QAM	80/160 MHz	2013	Alta velocidad, mejor rendimiento multimedia
802.11ax (Wi-Fi 6)	2.4 / 5 GHz	9.6 Gbps	1024-QAM	160 MHz	2019	Eficiencia en entornos densos, OFDMA
802.11be (Wi-Fi 7)	2.4 / 5 / 6 GHz	hasta 46 Gbps	4096-QAM	320 MHz	2024	Alta velocidad, baja latencia, MLO (Multi-Link Operation), múltiples enlaces simultáneos

En términos de seguridad cibernética, las redes Wi-Fi de hoy en día deben usar protocolos de encriptación fuertes y modernos, como WPA3 ya que este protocolo viene a sustituir a sus antecesores, WEP y WPA2, para proporcionar una mayor seguridad gracias a un cifrado más robusto, resistencia ante ataques de fuerza bruta y una mejor gestión de claves. Esto es crítico en los ambientes industriales más especializados, donde la integridad de la información y la disponibilidad del sistema son prioridades ineludibles, como ya advierte el informe de (Cisco Systems, 2025).

Sin embargo, el desempeño de una red inalámbrica está sujeto a muchos factores diferentes y complicados, como la interferencia electromagnética de otros dispositivos, la

ubicación de los puntos de acceso, la saturación del canal de datos y la gran cantidad de dispositivos que intentan conectarse simultáneamente y permanentemente; por lo cual es de vital importancia realizar estudios de cobertura, análisis de espectro y pruebas de rendimiento antes de la implementación real para garantizar su óptimo y continuo funcionamiento durante el proyecto (López Rodríguez, 2007).

En definitiva, la conectividad inalámbrica ya no es una opción, sino un elemento necesario en la estructura de red, sobre todo en organizaciones con necesidades de gran flexibilidad, crecimiento y optimización de sus procesos, así como la implementación adecuada, combinada con la adopción y aplicación de buenas prácticas de seguridad y planificación, puede establecer altos niveles de conectividad incluso en los entornos más exigentes.

2.6 Telefonía IP / VoIP

La telefonía IP, voz sobre protocolo de internet (VoIP por sus siglas en inglés), es una tecnología que permite transmitir señales de voz sobre redes con protocolo IP, que, a diferencia de la telefonía analógica, que utiliza circuitos conmutados, la telefonía VoIP codifica la voz en paquetes de datos que se transmiten por la red; esta técnica aprovecha mejor el ancho de banda y reduce drásticamente los costos de comunicación (Caldera Palma & Suazo Sequeira, 2011).

Entre los beneficios de la VoIP industrial destacan la escalabilidad, la interoperabilidad con otros servicios digitales, la integración con aplicaciones como videollamadas, correo electrónico y CRM, y la reducción de la infraestructura para líneas telefónicas, además; posibilita la administración centralizada del sistema de comunicaciones y la movilidad, ya que no están ligadas a una ubicación física.

Técnicamente, la telefonía por Internet (VoIP) necesita protocolos específicos para funcionar. Uno de los protocolos más importantes es el Protocolo de Inicio de Sesión (SIP, por sus siglas en inglés), que se encarga de iniciar, modificar y finalizar las sesiones de comunicación entre los usuarios. Este protocolo es un protocolo de señalización y se basa en un modelo cliente-servidor; usa habitualmente el puerto 5060 para establecer sesiones. Cabe destacar que el Protocolo de Inicio de Sesión (SIP) no transporta la voz, sino que negocia la sesión de datos (Caldera Palma & Suazo Sequeira, 2011).

El transporte de la voz se realiza mediante el protocolo RTP (Real-time Transport Protocol), que encapsula trozos de audio y video e incluye información como marcas de tiempo y

números de secuencia para garantizar la sincronización y el orden correcto de los datos en tiempo real; el protocolo es ampliamente empleado por las aplicaciones multimedia, gracias a su eficiencia y compatibilidad con códecs de audio y video (Kurose & Ross, 2017). Pero para que la telefonía IP funcione correctamente, se necesita una infraestructura de red con ciertas características. Debe de asegurarse una QoS adecuada en términos de ancho de banda, latencia, jitter y pérdida de paquetes.

En las redes industriales, donde la comunicación debe ser permanente y confiable, estos aspectos son determinantes para evitar cortes o degradación de la llamada (Caldera Palma & Suazo Sequeira, 2011). Aunque más allá de los beneficios económicos y de escalabilidad que ofrece la Telefonía IP, es importante conocer la tecnología que hace posible su funcionamiento; como ya se ha comentado, una de las piedras angulares en este mundo es el Protocolo de Inicio de Sesión (SIP), estandarizado por el Grupo de Trabajo de Ingeniería de Internet (IETF). Su propósito es negociar, cambiar y cerrar sesiones multimedia interactivas entre usuarios, como llamadas de voz, videollamadas, mensajería instantánea y conferencias. (Caldera Palma y Suazo Sequeira, 2011).

SIP sólo trabaja en la capa de señalización y delega en otros protocolos (como RTP) el transporte del flujo real de audio/video entre los puntos finales. Así, mientras que SIP negocia y gestiona la sesión, RTP transporta el contenido. Este protocolo está basado en un modelo cliente-servidor (véase Figura 2.10); los terminales SIP pueden ser tanto clientes como servidores, siendo Agentes de Usuario (User Agents) que se dividen en dos roles: UAC (User Agent Client), que inicia la llamada, y UAS (User Agent Server), que la recibe. Además, la comunicación se basa en direcciones SIP, similares a las URL, lo que permite al usuario ser localizable independientemente de su ubicación física mencionado en (Kurose & Ross, 2017).

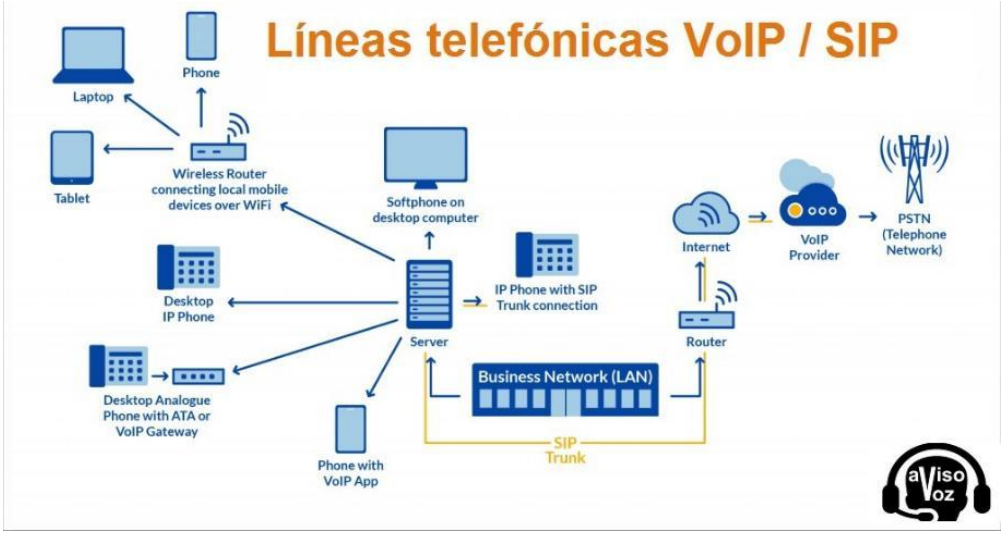


Figura 2.10 Algunos componentes para integrar llamadas SIP sobre VOZ IP. Recuperado de (Redacción Avisovozl, 2018).

Además, la seguridad y el control de las llamadas generalmente se refuerzan con componentes dedicados, tales como los SBC (Session Border Controllers), que protegen los bordes de la red y realizan funciones esenciales como transcodificación, control de tráfico y autenticación de usuarios. (Caldera Palma & Suazo Sequeira, 2011) realizaron un estudio sobre el efecto del cambio climático sobre la biodiversidad en bosques lluviosos tropicales.

Otro elemento esencial en las soluciones VoIP es el PBX IP (Private Branch Exchange), una central telefónica digital, esencial para las comunicaciones empresariales, estas modernas PBX, como Asterisk, permiten gestionar de forma eficiente las comunicaciones internas y externas de una empresa; más allá de la llamada, estos sistemas suelen incluir correo de voz, audioconferencias, menús interactivos (IVR), entre otras funciones.

Aunque lo mejor es que estas soluciones se pueden integrar perfectamente tanto con teléfonos IP físicos como con softphones, para una comunicación eficiente y flexible en la empresa; Asterisk, en particular, es un software de código abierto muy popular en el mundo de las telecomunicaciones, por su flexibilidad y bajo costo. (Caldera Palma & Suazo Sequeira, 2011) hicieron una revisión completa.

Finalmente, es importante considerar las medidas de seguridad que se deben implementar en las redes de voz sobre protocolo de internet (VoIP), la voz sobre redes IP puede ser vulnerable a amenazas como interceptación de datos, denegación de servicio o manipulación maliciosa por lo que es importante establecer medidas de seguridad fuertes

para garantizar la integridad y confidencialidad de la información que se está transmitiendo; para establecer una comunicación segura y confiable en la industria, se deben utilizar protocolos de encriptación robustos como el SRTP (Secure Real-time Transport Protocol).

También es recomendable implementar firewalls, sistemas de autenticación fuertes y segmentación de red para proteger la confidencialidad e integridad de las comunicaciones. Su correcta implementación y engranaje con una infraestructura sólida y bien planificada permite revolucionar la manera en que se gestiona y coordina la comunicación interna de una organización.

2.7 Seguridad en redes

La seguridad en las redes informáticas es esencial para asegurar la integridad, confidencialidad y disponibilidad de la información en entornos digitales que son cada vez más interconectados. Representa un aspecto fundamental que demanda la implementación de estrategias proactivas y medidas preventivas con el fin de mitigar posibles amenazas cibernéticas y salvaguardar los activos digitales de las organizaciones y los usuarios; su relevancia se fundamenta en la necesidad de implementar controles sólidos, políticas de seguridad eficaces y mecanismos de monitoreo continuo que faciliten la detección y respuesta oportuna ante incidentes de seguridad que pudieran comprometer la operatividad y la reputación de una red.

A medida que las organizaciones empresariales y productivas progresan hacia entornos interconectados y digitalizados, es esencial considerar que los riesgos asociados a vulnerabilidades, accesos no autorizados y posibles filtraciones de datos confidenciales aumentan de manera considerable. Por consiguiente, garantizar la confidencialidad, integridad y disponibilidad de la información se ha convertido en una prioridad esencial para todas las entidades, especialmente en entornos industriales que operan bajo los principios de la Cuarta Revolución Industrial.

En este contexto, es fundamental considerar que los principios esenciales de la seguridad en redes comprenden un conjunto de medidas y protocolos destinados a asegurar la protección de la información sensible y confidencial; entre estas medidas se encuentran el cifrado de la información, que consiste en codificar los datos de manera que solo puedan ser interpretados por aquellos autorizados a acceder a ellos, la autenticación de usuarios, que verifica la identidad de las personas que intentan ingresar a la red, y el control de

acceso a los recursos, que regula qué usuarios tienen permiso para utilizar determinados servicios o información.

Estas prácticas son esenciales para evitar vulnerabilidades y ciberataques que comprometan la integridad y confidencialidad de los datos, como por ejemplo el cifrado de extremo a extremo, una medida de seguridad imprescindible para garantizar la confidencialidad de la información transmitida, ya que evita que terceros no autorizados accedan a la información incluso si logran interceptar y capturar los paquetes de información mientras están en tránsito; por otra parte, la autenticación constituye un proceso esencial que asegura la veracidad de la identidad de los individuos o dispositivos que intentan acceder al sistema, previniendo de esta manera posibles intrusiones o suplantaciones de identidad.

Por otro lado, el control de acceso tiene la responsabilidad de establecer las políticas y restricciones que determinan las acciones que los usuarios autorizados pueden llevar a cabo sobre los recursos del sistema, garantizando así un uso adecuado y seguro de la información almacenada. De acuerdo con lo expuesto por Kurose y Ross en su obra publicada en 2017, dichos mecanismos son fundamentales para preservar la integridad y la confidencialidad de los datos en entornos informáticos.

En el ámbito de los sistemas VoIP y las redes industriales la implementación de protocolos como SRTP (Secure Real-time Transport Protocol) y TLS (Transport Layer Security) garantiza la seguridad de las sesiones de voz y de los canales de señalización por lo que estas tecnologías cifran tanto los datos de audio como los metadatos, lo que previene la escucha no autorizada, la suplantación de identidad y la manipulación de las llamadas (López Rodríguez, 2007).

No obstante, además de las técnicas defensivas es fundamental identificar las principales amenazas que enfrentan las redes, entre estas destacan los ataques de denegación de servicio (DoS y DDoS) que buscan saturar un sistema para impedir su funcionamiento normal además de la interceptación de datos, donde se accede de forma pasiva a información confidencial; y la suplantación de identidad (spoofing), mediante la cual un atacante finge ser un usuario legítimo para obtener privilegios o robar datos (Tanenbaum & Wetherall, 2012).

Por otro lado, en entornos industriales conectados al Internet de las Cosas (IoT), los dispositivos pueden ser blancos fáciles de ataques si no cuentan con configuraciones seguras desde su instalación como señala Barros Losada (2017), en el contexto de la Industria 4.0, la ciberseguridad se establece como uno de los principales desafíos tecnológicos y esto se debe a que la creciente dependencia de conexiones digitales, servicios en la nube y sensores distribuidos incrementa el número de puntos vulnerables dentro de una red.

Para abordar estas amenazas, las prácticas recomendadas comprenden la implementación de cortafuegos, sistemas de detección y prevención de intrusiones (IDS/IPS), autenticación multifactor, segmentación de redes, actualizaciones periódicas de software y la capacitación del personal; asimismo, el diseño de la red debe incluir la estrategia de defensa en profundidad, lo que implica la implementación de múltiples capas de seguridad, de manera que, en caso de que una de ellas falle, las demás puedan contener o mitigar el impacto del ataque.

Adicionalmente, es esencial tener en cuenta mecanismos específicos de protección en los puntos más vulnerables de la red, tales como los puertos de comunicación. Una práctica recomendada consiste en deshabilitar aquellos puertos que no están en uso y monitorear constantemente el tráfico hacia los que permanecen activos. Esta medida disminuye la superficie de ataque, lo que complica el acceso no autorizado desde el exterior (Tanenbaum & Wetherall, 2012).

El filtrado por puertos y protocolos debe ser complementado por una política de firewall que sea rigurosa y adecuadamente configurada. Estos dispositivos, ya sean físicos o virtuales, funcionan como barreras que regulan el flujo de datos entre diferentes áreas de la red, estableciendo normas fundamentadas en direcciones IP, servicios y aplicaciones. Un firewall de próxima generación (NGFW) tiene la capacidad de inspeccionar el contenido de los paquetes con el fin de identificar patrones maliciosos que van más allá del encabezado del protocolo (Kurose & Ross, 2017).

En cuanto al cifrado, no solo debe aplicarse en la transmisión de datos sino también en el almacenamiento ya que, para tal fin, se dispone de algoritmos avanzados, como el Estándar de Cifrado Avanzado (AES, por sus siglas en inglés), que aseguran la confidencialidad de la información, incluso en situaciones de acceso físico a los dispositivos; asimismo, se sugiere la utilización de conexiones VPN (Red Privada Virtual) al acceder de manera remota

a los recursos de la red, lo cual proporciona una capa adicional de seguridad a través de túneles cifrados (Caldera & Suazo, 2011).

Una medida esencial es la segmentación de redes. Esta estrategia implica la segmentación de la infraestructura en subredes distintas, con el propósito de limitar el movimiento lateral de un atacante en caso de que se produzca una intrusión; de este modo, los sistemas críticos, tales como servidores VoIP, cámaras IP o bases de datos industriales, pueden permanecer aislados de áreas menos seguras o susceptibles al acceso externo (UIT, 2003). Como se resume en la Tabla 2.3, estos mecanismos y herramientas constituyen una base sólida para la implementación de una política integral de seguridad en redes, asegurando la protección lógica de los activos tecnológicos.

Tabla 2.3 *Principales herramientas y mecanismos de seguridad en redes*

Herramienta	***Descripción***	***Función principal***	***Aplicación en redes industriales***
Firewall	Dispositivo o software que filtra el tráfico de red según reglas definidas.	Restringir accesos no autorizados entre redes o zonas.	Segmentación de red, control de tráfico entre áreas críticas.
VPN	Red privada virtual que cifra la conexión entre dos puntos remotos.	Garantizar conexiones seguras sobre redes públicas.	Acceso remoto seguro a sistemas SCADA o servidores empresariales.
IDS/IPS	Sistemas de detección (IDS) y prevención (IPS) de intrusos.	Identificar y bloquear intentos de ataque.	Supervisión continua del tráfico interno y externo.
Cifrado AES	Algoritmo de cifrado simétrico de alta seguridad.	Proteger la confidencialidad de los datos.	Encriptación de archivos, correos, VoIP y conexiones inalámbricas.
Autenticación multifactor (MFA)	Requiere más de una credencial para verificar la identidad del usuario.	Reforzar el acceso seguro a sistemas críticos.	Control de acceso a redes y paneles de configuración de dispositivos.

Segmentación de red (VLANs)	División lógica de la red en subredes independientes.	Limitar el alcance de ataques y facilitar la gestión.	Aislamiento de cámaras, servidores, VoIP, etc.
Actualización de firmware	Práctica de mantener actualizado el software embebido de dispositivos.	Corregir vulnerabilidades conocidas.	Seguridad en switches, APs, routers, cámaras y terminales industriales.
Monitoreo continuo	Vigilancia activa del estado de la red y comportamiento del tráfico.	Detección temprana de anomalías o amenazas.	Herramientas como Wireshark o software SIEM.

En casos más sofisticados, como por ejemplo en entornos industriales con dispositivos IoT, es recomendable establecer protocolos seguros de configuración remota, autenticación fuerte en dispositivos embebidos y registros de auditoría para todo acceso o cambio al sistema así como la actualización continua del firmware y el monitoreo en tiempo real completan el conjunto de acciones preventivas para garantizar la seguridad en estos ambientes dinámicos y altamente conectados como lo expone (Barros Losada, 2017).

Finalmente, no hay que olvidar el factor humano; la capacitación regular del personal en ciberseguridad, el establecimiento de políticas claras de uso de recursos informáticos y la realización de simulacros de respuesta ante incidentes refuerzan la cultura de la organización ante nuevas amenazas. Por lo tanto, la seguridad de la red no es solo una cuestión de herramientas, sino de estrategia, prevención y colaboración.

2.8 Videovigilancia en redes

Antes de hablar de videovigilancia IP, primero debemos saber qué significa "IP", ya que son las siglas de Protocolo de Internet; este protocolo forma parte del conjunto de reglas que permiten la comunicación a través de redes informáticas, asignando una dirección única a cada dispositivo (como una "dirección postal digital").

En términos de cámaras IP, significa que cada cámara tiene su propia dirección y puede ser gestionada individualmente a través de la red, comunicándose con servidores de almacenamiento, software de gestión de vídeo y otros dispositivos de la misma red expuesto por (Tanenbaum & Wetherall, 2011; López Rodríguez, 2007).

La videovigilancia es un componente esencial en los sistemas de seguridad física de infraestructuras tecnológicas; su asociación con redes de datos ha revolucionado su uso y alcance. Históricamente, los sistemas de videovigilancia se han apoyado en circuitos cerrados de televisión (CCTV) analógicos, sin embargo, las tecnologías de Protocolo de Internet han dado lugar a las soluciones de videovigilancia en red (también llamada videovigilancia IP), que superan ampliamente a sus predecesoras en capacidad técnica y funcionalidad.

Básicamente, un sistema de videovigilancia IP envía el flujo de video a través de una red, ya sea cableada o inalámbrica. Esto posibilita el monitoreo remoto, la administración centralizada y la escalabilidad del sistema. Las partes que normalmente componen este sistema son cámaras IP, servidores de almacenamiento, software VMS (Video Management Software), switches de red y enlaces de comunicación, todos funcionando de manera interoperable sobre una misma infraestructura (García Mata, 2011). Una de las mayores diferencias entre los sistemas IP y los sistemas CCTV analógicos es la forma en que se transmiten y procesan las señales.

En los CCTV analógicos, cada cámara necesita un cable individual hasta el punto de visionado o grabación. Por otro lado, en los sistemas protocolo de Internet (IP), la señal es digital desde el principio y se puede transmitir, controlar y almacenar en redes de área local (LAN), redes de área amplia (WAN) o incluso por Internet, lo que permite la supervisión desde cualquier parte del mundo (García Mata, 2011).

Además, las cámaras IP tienen grandes beneficios funcionales, como la alta calidad de imagen por los sensores megapíxel y de barrido progresivo, el acceso remoto para usuarios múltiples, la integración con sistemas de alarma y software inteligente de video análisis; también posibilitan ajustes avanzados como detección de movimiento, alarmas de sonido, notificaciones automatizadas y administración de eventos, características inviables en sistemas analógicos tradicionales como se menciona en el trabajo del autor (García Mata, 2011).
Podemos resumir los principales tipos de cámaras y sus características como se muestra en la Tabla 2.4 del siguiente apartado:

Tabla 2.4 *Principales tipos de cámaras IP y sus características*

Tipo de cámara IP	***Imagen***	***Descripción***	***Aplicación común***
Domo fija		Cámara de forma semiesférica, discreta, se instala en techos. Vista fija, resistente a vandalismo.	Interiores, oficinas, accesos controlados
Bala (Bullet)		Cámara con carcasa alargada. Alta visibilidad, ideal para exteriores. Buena protección ambiental.	Perímetro, fachadas, estacionamientos
Bala 180° (Panorámica)		Variante de cámara bala con lente ultra gran angular. Cubre un ángulo de hasta 180° con una sola unidad.	Vigilancia perimetral, muros largos
PTZ (Pan-Tilt-Zoom)		Controlable remotamente. Gira horizontal y verticalmente, con zoom óptico. Supervisa áreas amplias y dinámicas.	Áreas extensas, patios, parques
Ojo de pez (360°)		Captura en ángulo completo desde un solo punto. Cubre toda el área sin necesidad de movimiento.	Almacenes, vestíbulos, interiores abiertos
Cámara térmica		Detecta el calor emitido por objetos/personas. Funciona en total oscuridad o condiciones adversas.	Seguridad industrial, vigilancia nocturna

Nota. Imágenes obtenidas de (Hikvision, 2025).

A nivel técnico, la videovigilancia IP requiere de ciertos requisitos en la infraestructura: ancho de banda suficiente, servidores de video con buen procesamiento, almacenamiento suficiente (local o en red) y seguridad para el tráfico de video. Según (López Rodríguez, 2007), es aconsejable usar estaciones de trabajo para el almacenamiento de video y

sistemas de compresión como MPEG4 o H.264 para aprovechar el espacio y el tráfico de red (López Rodríguez, 2007).

Además, se usa PoE (Power over Ethernet) para alimentar cámaras IP directamente a través del cable de red, lo que ahorra en costos de instalación y simplifica la infraestructura. Además, sistemas como NAS o SAN se pueden utilizar para el almacenamiento en masa y seguro de grabaciones (López Rodríguez, 2007).

Por otra parte, como se detalla en la Tabla 2.5, existen diversos equipos y componentes complementarios indispensables en un sistema de videovigilancia IP, tales como grabadores NVR, switches PoE, UPS y controladores KVM, cuya función es garantizar una operación segura, continua y centralizada del sistema.

Tabla 2.5 *Componentes complementarios indispensables en un CCTV IP*

Componente	***Imagen de Referencia***	***Función principal***	***Aplicación común***
NVR (Network Video Recorder)		Dispositivo encargado de grabar, almacenar y gestionar las imágenes de cámaras IP.	Centro de control de videovigilancia.
Switch PoE (Power over Ethernet)		Conecta cámaras IP a la red y les suministra energía eléctrica a través del mismo cable de red.	Instalaciones con múltiples cámaras IP.
KVM (Keyboard Video Mouse)		Permite controlar múltiples servidores, NVRs o computadoras desde un solo teclado, monitor y mouse.	Cuartos de control, racks de servidores.
UPS (Sistema de alimentación ininterrumpida)		Suministra energía de respaldo ante fallos eléctricos, protegiendo los sistemas críticos.	Soporte energético para NVR y switches.
Gabinete de red (Rack)		Aloja de forma ordenada y segura equipos como NVR, switches, routers y organizadores de cableado.	Cuartos de comunicaciones o salas técnicas.

Servidor de almacenamiento		Complemento al NVR para almacenamiento de largo plazo o respaldo en sistemas de gran escala.	Vigilancia continua o almacenamiento masivo.
Router/firewall		Controla el acceso externo/interno y protege la red del sistema de videovigilancia.	Seguridad perimetral de red.

En términos de rentabilidad, la videovigilancia IP resulta más económica a largo plazo gracias a su flexibilidad, capacidad de actualización e integración con los sistemas de seguridad ya existentes y su menor necesidad de infraestructura específica en comparación con el cableado coaxial tradicional de los sistemas analógicos (Calani, 2010).

La videovigilancia IP es el siguiente paso en seguridad, ofreciendo una forma más eficiente, escalable y confiable de vigilancia por lo que su correcta implementación no solo protege físicamente los espacios, sino que también se integra con el ecosistema digital de una organización.

2.9 Transformación digital en la industria

En el mundo actual, cada vez más competitivo, la transformación digital se ha convertido en un pilar para el fortalecimiento de las empresas manufactureras y más allá de la simple adopción de tecnologías, implica una transformación profunda de los modelos de negocio, los procesos y la cultura, potenciada por la integración de tecnologías disruptivas como el Internet de las Cosas (IoT), Big Data, Inteligencia Artificial y sistemas ciberfísicos (Barros Losada, 2017).

Aquí es donde la llamada Industria 4.0 representa una nueva revolución en la industria. Según Yandar Lobón y Moreno Ospina (2019), este término, nacido en Alemania, busca la digitalización completa de los procesos productivos mediante la interconexión de dispositivos, sensores y sistemas inteligentes por lo que esta revolución impacta no solo cómo se fabrican las cosas, sino cómo las empresas interactúan con sus clientes y gestionan su cadena de valor.

Adicionalmente, Salimbeni y Bianchi (2019) indican que la Industria 4.0 no solo implica automatización de tareas, sino que impacta en la planificación estratégica, la toma de

decisiones en tiempo real y la integración de procesos de extremo a extremo, así mismo, esta evolución exige, por tanto, una fuerte inversión en infraestructura tecnológica, capacitación de personal y reorganización estructural.

Además, la digitalización ha probado ser beneficiosa para las industrias que la implementan. Entre los beneficios están la mejora de la eficiencia operativa, la reducción de costos, la mayor flexibilidad para responder a las necesidades del mercado y la mejora de la capacidad de innovación. Esto se logra a través de sistemas conectados que pueden producir y analizar grandes cantidades de datos en tiempo real (Zúñiga Vázquez, 2022). Pero también es cierto que uno de los principales retos de esta transformación es la brecha digital que existe, sobre todo en las pequeñas y medianas empresas (pymes). Como señalan Salimbeni y Bianchi (2019), muchas de estas instituciones tienen carencias de infraestructura y limitaciones de financiamiento y de personal capacitado que impiden que inicien su proceso de modernización.

Además, la transformación digital implica un cambio cultural, donde la capacitación continua del personal y la adquisición de nuevas habilidades técnicas y digitales son esenciales, esta transformación requiere un liderazgo comprometido con la innovación y la sostenibilidad a largo plazo. En definitiva, la transformación digital en el sector no es solo una necesidad tecnológica, sino una estrategia integral para garantizar la competitividad, la resiliencia y la sostenibilidad de las empresas en un mundo en constante cambio y cada vez más interconectado.

2.10 Normativas y estándares aplicables

La adhesión a normas y estándares internacionales es parte integral del diseño, implementación y mantenimiento de infraestructuras tecnológicas confiables y seguras porque mediante la estandarización se asegura la interoperabilidad de los dispositivos y sistemas, la calidad, eficiencia y sostenibilidad de las soluciones tecnológicas en entornos industriales.

Entre las principales organizaciones que generan estándares en esta área están la Organización Internacional de Normalización (ISO), la Comisión Electrotécnica Internacional (IEC), el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) y la Asociación de la Industria de las Telecomunicaciones (TIA); cada una desarrolla manuales técnicos que detallan desde el cableado estructurado hasta los protocolos de comunicación y los estándares eléctricos y mejores prácticas de instalación (Tanenbaum & Wetherall,

2012).

El estándar TIA/EIA-568 se usa más comúnmente para diseñar y certificar redes de datos., esta norma define los requisitos para los sistemas de cableado de telecomunicaciones en edificios comerciales, incluyendo configuraciones de conectores, códigos de color, longitudes máximas y especificaciones de rendimiento, por ejemplo, la norma TIA/EIA-568-B.2 se refiere a los cables de par trenzado, y la norma TIA/EIA-568-B.3 al cableado de fibra óptica (Zúñiga Vázquez, 2022).

Adicionalmente, la ISO/IEC 11801 en sus partes variables define los estándares internacionales para la infraestructura genérica de telecomunicaciones en edificios, lo que permite la uniformidad de las instalaciones en todo el mundo. Esta norma se adapta también a entornos industriales con la guía M.I.C.E., que tiene en cuenta factores mecánicos, de acceso, químicos y electromagnéticos que pueden afectar el desempeño del sistema (Zúñiga Vázquez, 2022).

En las redes inalámbricas y Ethernet, el IEEE 802.3 (Ethernet) y el IEEE 802.11 (Wi-Fi) son los estándares más importantes. Estos estándares garantizan la compatibilidad entre dispositivos de diferentes fabricantes, la eficiencia en la transmisión de datos y el cumplimiento de especificaciones técnicas como velocidad, frecuencia, modulación y seguridad (López Rodríguez, 2007).

Por otra parte, para el cableado de fibra óptica se deben tener en cuenta las recomendaciones del estándar TIA-568.3-D, el cual define las prácticas para la instalación y medición de rendimiento de sistemas ópticos, incluyendo criterios de conectorización, pérdida por inserción y reflectancia, entre otros. Además, la UIT-T G.671 define las características ópticas y mecánicas de los conectores y la IEC 61300-3-35, los criterios para la inspección visual de superficies ópticas (Veloz Pérez, 2019).

2.11 Síntesis

En este capítulo se han definido de manera explícita los constructos y teorías que respaldan la ejecución de la presente investigación; se ha definido la infraestructura tecnológica como la infraestructura subyacente y fundamental que soporta y estructura las redes de comunicación en los entornos industriales, especificando sus componentes principales como hardware, software, cableado, conectividad y demás dispositivos. También se han estudiado en profundidad las características y especificaciones técnicas de las infraestructuras de comunicación, se han analizado en detalle los beneficios y

requisitos para la implementación de voz sobre IP y se ha hecho hincapié en la importancia de contar con un cableado estructurado y certificado según las normas técnicas actuales. También se ha explicado en profundidad cómo funcionan y evolucionan las redes inalámbricas hacia estándares más avanzados como Wi-Fi 6 y 7; además, se han tratado en detalle las bases de seguridad informática necesarias para proteger estas infraestructuras tecnológicas.

CAPÍTULO 3. Estado del Arte

En este capítulo se hace una revisión bibliográfica sistemática y crítica de la literatura académica, técnica y de práctica sobre la infraestructura tecnológica en ambientes industriales; a través de la revisión de diferentes fuentes expertas, como tesis de grado, artículos científicos, informes técnicos y casos reales de implementación, se busca conocer el estado actual de las soluciones de conectividad, comunicación y monitoreo que se han planteado e implementado en contextos similares al del presente proyecto. Para justificar la solución planteada, se analizan diferentes enfoques relacionados con la modernización de redes de datos, la migración a Voz sobre Protocolo de Internet (VoIP), la migración a redes inalámbricas de alta eficiencia, los sistemas de videovigilancia sobre Protocolo de Internet (IP), el cumplimiento de normativas técnicas, entre otros.

3.1 Trabajos relacionados con infraestructura tecnológica en entornos empresariales

En los últimos años, la renovación y modernización de la infraestructura tecnológica en entornos industriales se ha convertido en una necesidad estratégica para las organizaciones que buscan mejorar su competitividad y eficiencia; muchos autores lo han abordado desde diferentes enfoques, pero todos coinciden en que la evolución tecnológica no solo requiere la adopción de nuevas herramientas, sino una transformación completa de los sistemas de red actuales.

En ese sentido, el estudio de Zúñiga Vázquez (2022) hace una revisión detallada de la infraestructura física de red Ethernet para industria 4.0, haciendo énfasis en el diseño estructurado de cableado, la elección de estándares —ANSI/TIA e ISO/IEC— y las soluciones escalables y seguras. En su propuesta, el autor define parámetros técnicos específicos para garantizar un rendimiento óptimo en contextos industriales, teniendo en cuenta elementos como el ruido electromagnético, la redundancia de enlaces y la compatibilidad con tecnologías en desarrollo.

Adicionalmente, Salimbeni y Bianchi (2019) subrayan que la transición de la industria doméstica hacia un modelo 4.0 demanda no solo una infraestructura física sólida, sino también una estrategia de integración digital que tenga en cuenta componentes como sensores, dispositivos inteligentes, redes de alta disponibilidad y plataformas de gestión en

tiempo real. De acuerdo con los autores, uno de los retos primordiales para las organizaciones radica en superar la fragmentación tecnológica y adoptar modelos de conectividad interoperables.

Según Odremán (2014), la administración tecnológica se presenta como un elemento crucial para la transferencia de innovación en el sector industrial, enfatizando que cualquier proceso de transformación debería iniciarse con un diagnóstico técnico y organizacional que facilite la identificación de las capacidades actuales y las áreas prioritarias de intervención. Jaimes, Núñez y Rojas (2011) abogan por una perspectiva sistémica de la infraestructura tecnológica, en la que el diseño de redes debe alinearse con los objetivos estratégicos de la organización.

Por el contrario, varias investigaciones recientes aplicadas en contextos específicos reafirman la relevancia de estos conceptos; como ejemplo, Benites Cruz (2023) realiza un proyecto de diseño de red estructurada en una institución educativa, ajustando normativas industriales a un entorno académico, demostrando que los principios de escalabilidad, redundancia y eficiencia energética se pueden aplicar en diferentes contextos. Similarmente, Becerra Aldeán (2024) diseña una red de datos moderna en una planta industrial, con fibra óptica, cableado estructurado y puntos de acceso inalámbrico para mejorar la conectividad interna y la gestión de procesos.

De la revisión de los estudios para esta sección, existe un acuerdo en que la modernización de la infraestructura tecnológica no debe limitarse al cambio de equipos obsoletos, sino que debe ser un proceso integral que abarque la planificación, normatividad, interoperabilidad, sostenibilidad y un enfoque estratégico, estos antecedentes justifican la idea planteada en este proyecto, además de evidenciar las mejores prácticas, deficiencias y oportunidades de mejora en casos similares del sector industrial.

3.2 Proyectos similares de diseño de redes o videovigilancia

En los últimos años, colegios, asociaciones locales y empresas han dado el paso para modernizar sus infraestructuras tecnológicas con redes cableadas, inalámbricas o sistemas de videovigilancia IP; estos casos de estudio permiten identificar enfoques, metodologías y resultados, lo cual es relevante para comparar y contextualizar la presente propuesta. Un ejemplo más representativo es el proyecto de Jinez Granja y Pantoja Prado (2020), quienes desarrollaron un sistema de videovigilancia comunitaria para el barrio La

Herradura, cantón Pasaje. Su propuesta consistió en colocar cámaras IP y un servidor de vigilancia para hacer más segura a la ciudadanía. Las conclusiones subrayan la relevancia de una planificación eficaz de la red, la elección apropiada de cámaras y la integración eficaz del sistema de almacenamiento. A pesar de que el contexto es residencial, las directrices técnicas y las decisiones de diseño son extrapolables a contextos industriales, particularmente en lo concerniente a la distribución de puntos de captura, suministro eléctrico y control de acceso a distancia.

Cortés Altamiranda y Castellar Jiménez (2024) elaboraron una red de monitoreo de video fundamentada en el Internet de las Cosas (IoT), que fue implementada en una institución educativa. Contrariamente a otros proyectos, esta metodología implicó la implementación de microcontroladores, sensores y conectividad inalámbrica para integrar el sistema de videovigilancia con una plataforma de visualización centralizada; la propuesta subraya la importancia de la modularidad y la escalabilidad, atributos esenciales en contextos industriales con demandas fluctuantes.

Alcarraz Díaz y Escobar Díaz (2021) también diseñaron un sistema de videovigilancia y control a través del Internet de las Cosas (IoT) en instituciones educativas de Colombia, empleando tecnologías como Raspberry Pi, cámaras IP, sensores PIR y conexiones Wi-Fi; este proyecto enfatiza la factibilidad técnica y económica de la implementación de soluciones de bajo costo con un impacto significativo, siempre y cuando se efectué una evaluación adecuada de riesgos, análisis de cobertura y dimensionamiento del sistema. A pesar de que su entorno es educativo, los principios de diseño y selección tecnológica también se aplican a instalaciones industriales que demandan soluciones eficaces y adaptables.

Además, ciertas investigaciones recientes centradas en el diseño de redes en contextos institucionales subrayan la importancia de una planificación estructurada. Se puede citar el caso de Benites Cruz (2023), que elaboró una propuesta de cableado estructurado en una institución académica, tomando en cuenta estándares TIA/EIA, disposición lógica y física, así como las necesidades de expansión futura. Esta perspectiva estratégica se encuentra en consonancia con las prácticas óptimas para la implementación de redes en instalaciones industriales, donde la continuidad operativa y la escalabilidad son elementos fundamentales.

Se puede inferir que los proyectos examinados coinciden en enfatizar la necesidad de incorporar criterios técnicos, operativos y económicos para alcanzar soluciones funcionales,

seguras y sostenibles por lo que demuestran que, tanto en contextos educativos como comunitarios, la infraestructura de red y videovigilancia debe ser concebida desde una perspectiva holística, capaz de responder a las circunstancias reales del entorno, lo cual se alinea plenamente con los propósitos de este estudio.

3.3 Trabajos relacionados con Telefonía IP y virtualización en redes empresariales

La telefonía IP (VoIP) y la virtualización de redes se han consolidado como tecnologías clave en las estrategias de modernización tecnológica de las empresas actuales; estas nuevas tecnologías no solo optimizan los recursos existentes, sino que también permiten mayor flexibilidad operativa, escalabilidad y reducción de costos en comparación con las infraestructuras tradicionales y obsoletas. En este contexto, muchos casos de estudio y proyectos han detallado su aplicación en el mundo real, lo que sirve como ejemplo para diseñar y desarrollar soluciones similares en otros contextos de la industria y los negocios.

Una de las mayores contribuciones en este campo es el trabajo de Altamirano Hernández (2013), quien desarrolló un sistema completo de telefonía IP para una empresa privada con el objetivo de mejorar la comunicación interna y reducir los costos de telefonía tradicional. Su proyecto abarcó desde la planificación e implementación de un servidor Asterisk, software de código abierto reconocido en el mundo de las telecomunicaciones, hasta la implementación estratégica de extensiones IP para permitir la comunicación eficiente y segura entre las áreas y departamentos de la organización.

Como resultado de las acciones tomadas, se logró mejorar el servicio, pero sobre todo se logró una optimización en la gestión de los recursos de infraestructura de red. Este caso en particular demuestra que la tecnología de Voz sobre Protocolo de Internet (VoIP) es una alternativa totalmente viable y eficiente incluso en organizaciones con pocos recursos tecnológicos. Todo esto, por supuesto, siempre y cuando se realice una correcta planificación de la red de comunicaciones y se implementen mecanismos que permitan garantizar la calidad de servicio (QoS) a los usuarios finales.

Por otro lado, el documento desarrollado por la Unión Internacional de Telecomunicaciones (UIT) en el año 2003 da una mirada completa sobre los beneficios, retos y directrices técnicas asociadas con la implementación y adopción de la telefonía IP en diversos contextos. El informe señala que, aunque esta tecnología es una evolución natural de las

redes de comunicación, su implantación debe considerar factores críticos como la interoperabilidad, la ciberseguridad, la compatibilidad con los sistemas existentes y el cumplimiento de la normativa actual. Estas preocupaciones son especialmente pertinentes en los entornos industriales altamente especializados, donde la continuidad del servicio y la integridad y confiabilidad de la información son esenciales para el éxito y la eficiencia de las empresas.

Además, en el estudio de Caldera Palma y Suazo Sequeira (2011) se profundiza en los aspectos técnicos de la tecnología VoIP, describiendo a detalle protocolos como SIP, H.323 y RTP, así como los componentes necesarios para su configuración e implementación exitosa en redes locales. Su metodología altamente práctica y detallada muestra de manera clara y precisa todos los pasos para realizar una implementación escalonada y exitosa, desde el levantamiento exhaustivo de requerimientos del proyecto hasta las pruebas exhaustivas de funcionalidad para asegurar un resultado óptimo.

Por otra parte, el estudio de Soler Palacín (2009) describe el proceso de planificación e implementación de una infraestructura de comunicaciones VoIP en un entorno académico, mencionando los beneficios económicos que se pueden obtener, pero también los desafíos técnicos que deben abordarse, como garantizar la calidad de voz, los tiempos de respuesta y la adquisición de equipos específicos para garantizar una transmisión fluida y confiable.

Hablando de virtualización, Casierra, Casanova y Guapi (2018) profundizan en la virtualización como una manera de simular infraestructuras tecnológicas complejas sin incurrir en altos costos. Su propuesta consiste en crear laboratorios virtuales usando software de código abierto para simular infraestructuras de redes, servidores y aplicaciones empresariales en un entorno seguro y controlado.

Estas soluciones tecnológicas de vanguardia simplifican el diseño, las pruebas exhaustivas y la capacitación en las tecnologías de red más avanzadas sin necesidad de tener los equipos en el sitio, lo cual es conveniente y eficiente, especialmente en las etapas iniciales de implementación o en entornos de prueba y experimentación.

En conjunto, los estudios analizados reafirman que tanto la telefonía IP como la virtualización son tecnologías maduras, confiables y ampliamente desplegadas en diferentes sectores productivos a nivel mundial de igual modo, los datos confirman que su integración no solo mejora significativamente la eficiencia operativa, sino que también

refuerza la seguridad, la flexibilidad y la sostenibilidad de las redes empresariales, características imprescindibles para cualquier entorno industrial que desee adaptarse a la transformación digital.

3.4 Trabajos relacionados con redes inalámbricas modernas

Con la creciente digitalización en la industria y el desarrollo de los modelos de Industria 4.0 y 5.0, las infraestructuras de comunicación inalámbrica se han vuelto esenciales como habilitadores para conectar dispositivos, sensores y sistemas distribuidos; en el mundo actual, tecnologías de última generación como Wi-Fi 6 y Wi-Fi 7, así como las arquitecturas IoT, han sido ampliamente estudiadas por su potencial para mejorar la eficiencia energética, reducir la latencia, soportar altas densidades de dispositivos simultáneos y garantizar comunicaciones confiables incluso en entornos electromagnéticamente desafiantes.

En esa misma línea, Martínez Tello (2025) diseñó toda una red inalámbrica para conectar dispositivos IoT en un entorno industrial complejo. Para ello, realizó simulaciones extensivas en NetSim, analizando el comportamiento de métricas cruciales como el consumo de energía, la tasa de pérdida de paquetes y la ubicación óptima de nodos en la red; su enfoque innovador incorpora modelos de propagación realistas y técnicas avanzadas de optimización energética, cruciales para escenarios donde los dispositivos operan de forma autónoma y sostenible en el tiempo. Más allá de lo ya expuesto, el autor destaca la necesidad de establecer gateways de alto rendimiento y desarrollar topologías resilientes y adaptables que aseguren la continuidad del servicio ante interferencias o restricciones de cobertura.

Además, el estudio de John et al. (2024) ofrece una visión completa de cómo las tecnologías emergentes como Wi-Fi 7, las redes 5G y TSN se combinan para transformar la industria manufacturera. A través de una revisión comparativa, los autores muestran cómo la tecnología Wi-Fi 7 basada en el protocolo IEEE 802.11be logra mejoras sustanciales en la velocidad de transmisión, latencia ultrabaja y sincronización precisa, haciéndola adecuada para aplicaciones críticas como robótica, control de maquinaria y análisis en tiempo real. Estas capacidades son fundamentales para establecer una conectividad industrial totalmente determinista y compatible con los exigentes requisitos de tiempo real de las aplicaciones de misión crítica en entornos dinámicos.

Por otro lado, en un artículo bien interesante, Murad et al. (2024) hacen una revisión completa y detallada de la evolución histórica y técnica de la familia Wi-Fi desde sus inicios hasta las capacidades futuras que se esperan en Wi-Fi 7. En su análisis explora en profundidad tanto los beneficios como los retos técnicos de esta nueva generación de tecnología, como la compatibilidad con tecnologías anteriores, el uso de canales de 320 MHz, la modulación 4096-QAM o el soporte multibanda (MLO), para entender completamente lo que esta evolución puede significar. El estudio concluye que la tecnología Wi-Fi 7 es una excelente solución para entornos industriales complejos, pero una planificación técnica y una configuración adecuada del entorno son determinantes para garantizar su funcionamiento y rendimiento.

Desde un punto de vista práctico y de implementación, la guía técnica actualizada de Cisco Systems para 2025 proporciona una serie de recomendaciones detalladas y específicas para implementar con éxito la tecnología Wi-Fi 7 en entornos empresariales e industriales. Entre las recomendaciones que proporciona, se incluyen medidas para aumentar la densidad de puntos de acceso, controlar la convivencia con otras tecnologías inalámbricas y garantizar la calidad del servicio mediante una configuración avanzada de QoS y segmentación del tráfico de datos. Este documento es de gran interés para aquellas organizaciones que desean migrar de arquitecturas tecnológicas legadas a soluciones inalámbricas flexibles y adaptables sin comprometer la estabilidad e integridad de sus comunicaciones internas y externas.

Finalmente, el análisis técnico que George y su equipo desarrollaron en 2023 viene a reforzar y ampliar los conocimientos anteriores mostrando de forma detallada las mejoras tecnológicas que la nueva generación de Wi-Fi, denominada Wi-Fi 7, ofrece sobre sus predecesoras; entre sus características más destacadas están la multiplexación multienlace (MLO), la capacidad de funcionar simultáneamente en las bandas de 2.4, 5 y 6 GHz y su plena compatibilidad con entornos densos de dispositivos IoT; estas características hacen de Wi-Fi 7 una tecnología idónea para aplicaciones industriales de alto rendimiento, baja latencia y máxima fiabilidad.

En conclusión, todos los estudios analizados coinciden en que las infraestructuras de comunicación inalámbrica de nueva generación son un habilitador clave para los sistemas automatizados, la monitorización continua y el control de procesos en la industria, pero, llevar a cabo este proceso implica un análisis profundo de las condiciones del entorno y una evaluación exhaustiva de las normas de seguridad, calidad y eficiencia energética que

deben cumplirse. Esta evidencia apoya totalmente la estrategia de este proyecto, que desde un principio apostó por la integración de soluciones inalámbricas de alta tecnología como base de una infraestructura tecnológica robusta, flexible y totalmente en línea con los principios de la transformación digital actual.

3.5 Trabajos alineados con normativas, estándares y buenas prácticas aplicadas a redes de computadoras

La implementación de soluciones tecnológicas en entornos industriales exige un estricto cumplimiento de normativas y estándares técnicos específicos que garanticen la interoperabilidad, la seguridad, la calidad del servicio y la sostenibilidad a largo plazo de la infraestructura establecida; en este contexto, diversos expertos han llevado a cabo un análisis exhaustivo sobre la importancia de implementar prácticas adecuadas y efectivas, respaldadas por organismos internacionales de renombre, tales como la Asociación Nacional de Estándares de Estados Unidos (ANSI), el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), la Organización Internacional de Normalización (ISO) y el Grupo de Trabajo de Ingeniería de Internet (IETF). El objetivo de estas prácticas es establecer directrices comunes que regulen desde la infraestructura física de cableado hasta los complejos protocolos de comunicación utilizados en redes, tanto cableadas como inalámbricas.

Una de las referencias fundamentales en el ámbito del cableado estructurado es la investigación llevada a cabo por Castellón Arenas en el año 2014. En su estudio, el autor lleva a cabo un análisis exhaustivo de los elementos constitutivos, las configuraciones de red, los subsistemas implicados y los criterios establecidos en la normativa EIA/TIA-568. Este documento detallado no solo describe de manera minuciosa las configuraciones adecuadas de cables, conectores, canalizaciones y puntos de terminación, sino que también enfatiza la importancia de la planificación, organización y documentación exhaustiva de la red como un elemento fundamental e indispensable en el diseño técnico. De acuerdo con el autor de la publicación, la planificación e implementación adecuadas de un sistema de cableado estructurado son fundamentales para asegurar la eficiencia operativa, la facilidad de mantenimiento y la capacidad de escalabilidad de la red, aspectos esenciales en cualquier entorno industrial o empresarial.

Adicionalmente, Joskowicz (2006) proporciona una orientación exhaustiva para el desarrollo y análisis de infraestructuras de cableado estructurado, considerando los

lineamientos establecidos en las normativas ANSI/TIA/EIA y su adaptación a las diversas exigencias de las organizaciones; en su propuesta se destacan principios y estrategias significativas, tales como la segmentación lógica de redes, que garantiza un funcionamiento eficiente y seguro; la creación de rutas seguras, que optimiza la conectividad; la planificación anticipada del crecimiento, que asegura la escalabilidad del sistema; y la protección efectiva contra posibles interferencias electromagnéticas que podrían afectar el desempeño de la red. Estos lineamientos son de suma importancia y constituyen un elemento esencial en el diseño de redes industriales que deben funcionar de manera continua y confiable en entornos que presentan altas exigencias físicas, mecánicas y eléctricas.

Desde una perspectiva académica y científica, los significativos aportes teóricos de autores reconocidos como Tanenbaum y Wetherall en su obra de 2012, así como los fundamentos presentados por Kurose y Ross en su publicación de 2017, proporcionan marcos conceptuales sólidos y exhaustivos sobre el funcionamiento complejo y la interconexión de redes de computadoras, estos expertos analizan de manera exhaustiva y detallada tanto los modelos de referencia OSI y TCP/IP, como los diversos protocolos que regulan el intercambio de información en cada una de las capas que integran dichos modelos. Sus trabajos destacan la importancia de cumplir con las normativas técnicas ampliamente reconocidas en la implementación de infraestructuras de red, tales como el Protocolo de Configuración Dinámica de Hosts (DHCP), el Sistema de Nombres de Dominio (DNS), el Protocolo de Internet (IP), el Protocolo de Control de Transmisión (TCP), el Protocolo de Datagramas de Usuario (UDP), el Protocolo de Transferencia de Hipertexto (HTTP) y el Protocolo de Inicio de Sesión (SIP).

Estos protocolos son esenciales para asegurar el rendimiento óptimo de los sistemas de Comunicación de Voz sobre Protocolo de Internet (VoIP), los sistemas de videovigilancia basados en IP, las soluciones de monitoreo a distancia y los procesos de automatización en entornos industriales; asimismo, en este contexto se deben considerar aspectos fundamentales tales como la gestión del ancho de banda, la priorización del tráfico, la protección contra intrusiones y la fiabilidad de las comunicaciones en entornos empresariales que requieren altos niveles de exigencia. Todo lo mencionado es fundamental para asegurar un rendimiento óptimo y una operatividad eficiente en las redes de comunicación de última generación.

Es fundamental señalar que, en los entornos industriales altamente especializados, la aplicación de estas directrices no solo garantiza un rendimiento técnico sobresaliente, sino que también cumple una función esencial en el ámbito de las inspecciones, las acreditaciones de excelencia, como ISO 9001 o ISO/IEC 27001, y en el cumplimiento de normativas legales específicas del sector. Asimismo, es fundamental considerar que la adherencia a las recomendaciones y directrices establecidas por entidades y organizaciones reconocidas, como BICSI, IEEE y otras asociaciones de prestigio en el ámbito técnico y profesional, es esencial para asegurar la implementación exitosa de sistemas de infraestructura que satisfagan los estándares de seguridad, eficiencia y flexibilidad exigidos en el actual entorno industrial dinámico.

En su totalidad, las obras literarias analizadas coinciden en señalar que una implementación tecnológica adecuada y eficiente debe estar necesariamente vinculada al contexto normativo y legal que la regula en la actualidad; la adopción de estándares técnicos no solo responde de manera directa a la necesidad de garantizar la compatibilidad e interoperabilidad entre diversos sistemas y dispositivos, sino que también se establece como una herramienta estratégica de gran importancia para asegurar la sostenibilidad, escalabilidad y confiabilidad a largo plazo de los sistemas tecnológicos. Esto es especialmente relevante en entornos industriales que operan en condiciones críticas y requieren una continuidad operativa ininterrumpida y sin interrupciones.

3.6 Discusión del estado del arte

A partir del análisis de las obras estudiadas en los apartados previos, se puede distinguir una variedad de perspectivas, métodos y soluciones aplicadas en situaciones reales y simuladas. Sin embargo, el presente proyecto es relevante también porque se detectan vacíos temáticos y limitaciones que se repiten; en general, la mayor parte de las investigaciones analizadas se enfocan en elementos particulares de la infraestructura tecnológica, ya sea desde el punto de vista del cableado estructurado, la implementación de telefonía IP, el establecimiento de redes sin cables o el montaje de sistemas para videovigilar.

No obstante, no es común que estos elementos se integren en una solución única, escalable y adecuada para los ambientes industriales, como ejemplo, la investigación de Jinez Granja y Pantoja Prado (2020) y la de Alcarraz Díaz y Escobar Díaz (2021) se enfocan en crear sistemas de videovigilancia IP para ser utilizados en entornos educativos o comunitarios,

dejando fuera temas esenciales como el diseño estructurado de la red y el manejo energético de los dispositivos, en la misma línea, las investigaciones de Soler Palacín (2009) y Altamirano Hernández (2013) proporcionan soluciones prácticas en el campo de la telefonía IP. No obstante, no tocan el tema de su integración con otros servicios de red, como por ejemplo la videovigilancia o la conexión inalámbrica.

Asimismo, los autores John et al. (2024) y Martínez Tello (2025), a pesar de que estudian en profundidad el diseño de redes IoT inalámbricas en ambientes industriales, se enfocan casi únicamente en la optimización energética y la efectividad del canal de transmisión, sin tratar el tema de la integración con otros subsistemas de infraestructura. Aun en estudios más amplios, como el de Zúñiga (2022), que estudia la modernización física de redes Ethernet dentro del marco de la industria 4.0, no se evalúan simultáneamente los requerimientos para virtualización de servicios, vigilancia por video o comunicación unificada.

Desde el punto de vista técnico y normativo, los estándares revisados ofrecen una base firme para la elaboración individual de cada subsistema. No obstante, si se implementa de forma fragmentada, se pueden generar problemas de interoperabilidad al tratar de integrar diferentes servicios en una sola infraestructura, así como duplicación de recursos o inconsistencias; una de las dificultades más grandes que el proyecto actual tiene la intención de tratar es la diferencia entre la teoría normativa y su implementación práctica integrada.

En este marco, el valor agregado de esta propuesta radica en su perspectiva integral, articulada y contextualizada, este proyecto, a diferencia de las investigaciones previas que se centran en un solo aspecto del problema, trata simultáneamente la actualización del cableado estructurado, la implementación de redes inalámbricas sofisticadas, el uso de telefonía IP, el cumplimiento normativo según normas técnicas reconocidas y la inclusión de videovigilancia IP. Todo lo anteriormente mencionado se adapta a las circunstancias y requerimientos reales de una instalación industrial, teniendo en cuenta criterios como la eficiencia, la sostenibilidad y la escalabilidad.

Para concluir esta sección, el análisis comparativo muestra que hay una necesidad no cubierta en los estudios analizados: la integración coherente de diferentes tecnologías en un solo diseño técnico funcional. Esta restricción se convierte en una oportunidad porque

posibilita que se posicione el proyecto actual como una solución innovadora, que es capaz de fusionar en un solo esquema lo que hasta ahora se ha abordado de forma separada.

3.7 Síntesis

Se ha hecho en este capítulo un examen minucioso de los proyectos, antecedentes e investigaciones más relevantes que tienen relación con el diseño, la modernización y la puesta en marcha de infraestructuras tecnológicas en ámbitos industriales; se han tratado temas fundamentales mediante el análisis de varias fuentes, incluyendo la infraestructura física de red, la telefonía IP, las redes inalámbricas avanzadas, la virtualización de servicios, los sistemas de videovigilancia IP y las normas técnicas pertinentes.

Los análisis revisados han hecho posible reconocer tendencias, prácticas adecuadas y soluciones que ya se han aplicado, además de las limitaciones frecuentes en términos de cobertura funcional, escalabilidad o integración. La mayoría de los proyectos evaluados suelen concentrarse en áreas concretas del diseño de red, sin tratar simultáneamente todos los subsistemas que integran una infraestructura tecnológica integral.

CAPÍTULO 4. Metodología

En este capítulo se describe de manera explícita el camino metodológico que se siguió para la elaboración del presente proyecto; en las siguientes secciones se detalla el tipo de investigación, el modelo utilizado y las fases que orientaron el análisis, diagnóstico, diseño e implementación de la solución tecnológica. Además, se muestran las herramientas de captura de información, los criterios que guiaron las decisiones técnicas y los procesos de validación que determinaron la efectividad de las soluciones propuestas.

4.1 Marco contextual del caso de estudio

Como parte del enfoque de diseño de este proyecto, es importante contextualizar el ambiente organizacional en el cual se piensa implementar la solución tecnológica; en este capítulo se aborda el caso de estudio elegido: la empresa Trefilados Inoxidables de México (TIM), para conocer sus características operativas, tecnológicas y organizacionales, así como los desafíos que abren la oportunidad para proponer una mejora en su infraestructura de red.

4.1.1 Información general de la empresa

Trefilados Inoxidables de México (TIM), empresa productora de aceros inoxidables, líder en la fabricación de alambres, barras de acero inoxidable y aleaciones de níquel para las industrias automotriz, de la construcción y electrónica; siendo los mejores en su ramo por mejorar continuamente los niveles de calidad de sus productos y servicios, siempre bajo estándares internacionales de producción y control de calidad; información recuperada de (Trefilados Inoxidables de México, 2024).

Forma parte de Grupo Novametal, una red mundial con empresas hermanas como NOVAMETAL S.A. (Suiza), NOVAMETAL do Brasil Ltda. (Brasil), WPSS (Pty) Ltd (Sudáfrica), TDV (Francia), entre muchas otras, alcanzando presencia global con canales de distribución en Europa y Estados Unidos; la misma red lo consolida como el único productor en México de barras de acero inoxidable de alta calidad y excelencia, con tecnología de vanguardia en todos sus procesos; datos recuperados de (Trefilados Inoxidables de México, 2024).

4.1.2 Entorno organizacional y tecnológico

Cuando se inicia el proyecto, la empresa cuenta con una infraestructura tecnológica en funcionamiento, pero con ciertos problemas y fallos parciales por antigüedad, con ciertas limitaciones de escalabilidad, seguridad, alcance, redundancia y velocidad de transmisión de datos; sus redes internas se sostienen principalmente en cableado tradicional y algunos puntos de acceso Wifi sin segmentar ni documentar, lo que dificulta el monitoreo, la trazabilidad y el mantenimiento de sus sistemas.

También hay fallas de conectividad en algunas áreas claves de la planta que afectan directamente procesos como control de producción, registro de trazabilidad, cámaras de seguridad y acceso al servidor local en diferentes áreas. Además, la planta ha crecido más allá de la capacidad de la red actual, creando cuellos de botella y puntos de falla repetitivos, entre otros.

4.2 Justificación del proyecto en el contexto empresarial

La digitalización industrial de hoy en día necesita infraestructuras tecnológicas robustas, escalables y seguras; en ese sentido, el presente proyecto es una propuesta integral para modernizar, optimizar y unificar la red de datos de la organización, implementando elementos que fortalezcan la conectividad, el monitoreo y la comunicación interna.

Entre las soluciones planteadas se encuentra la implementación de un sistema de cableado estructurado TIA/EIA-568, la migración a una telefonía IP basada en servidores VoIP, la implementación de una red inalámbrica de última generación Wi-Fi 7, un sistema de videovigilancia IP con grabación centralizada y la segmentación lógica de la red en VLANs con mecanismos básicos de ciberseguridad; esta solución integrada sienta las bases para una infraestructura resiliente, eficiente y en línea con la Industria 4.0.

4.3 Tipo y enfoque de investigación

Para este proyecto se eligió un enfoque metodológico aplicado y cuantitativo, ya que busca resolver un problema tecnológico específico a través de soluciones prácticas y medibles. A diferencia de la investigación básica, que busca generar conocimiento teórico, aquí se puede manipular la infraestructura tecnológica de un entorno industrial, mejorando sus redes de comunicación y sistemas relacionados; por su diseño, la investigación es no experimental, ya que no se manipulan intencionalmente las variables del entorno, sino que se estudian tal como ocurren naturalmente. A través de la observación en campo, toma de

información técnica y documentación existente, se determinan las fallas actuales y se proponen soluciones específicas de mejora.

Asimismo, la investigación es descriptiva y diagnóstica, porque permite describir la situación actual de la infraestructura tecnológica de la empresa, medir su rendimiento e identificar los factores que restringen su eficiencia, seguridad y escalabilidad, posteriormente se pasa a la fase propositiva, donde se crea una solución técnica basada en buenas prácticas, leyes actuales y tecnologías emergentes.

4.4 Diseño metodológico

Para la elaboración de este proyecto se siguió una metodología en etapas bien definidas, las cuales permitieron dar solución de manera organizada a la problemática encontrada en la infraestructura tecnológica de la organización. Mediante este diseño metodológico se aseguró la coherencia entre el diagnóstico inicial, la propuesta de soluciones técnicas y la verificación de resultados; en la Figura 4.1 se presentan las principales fases que orientaron la realización del estudio:

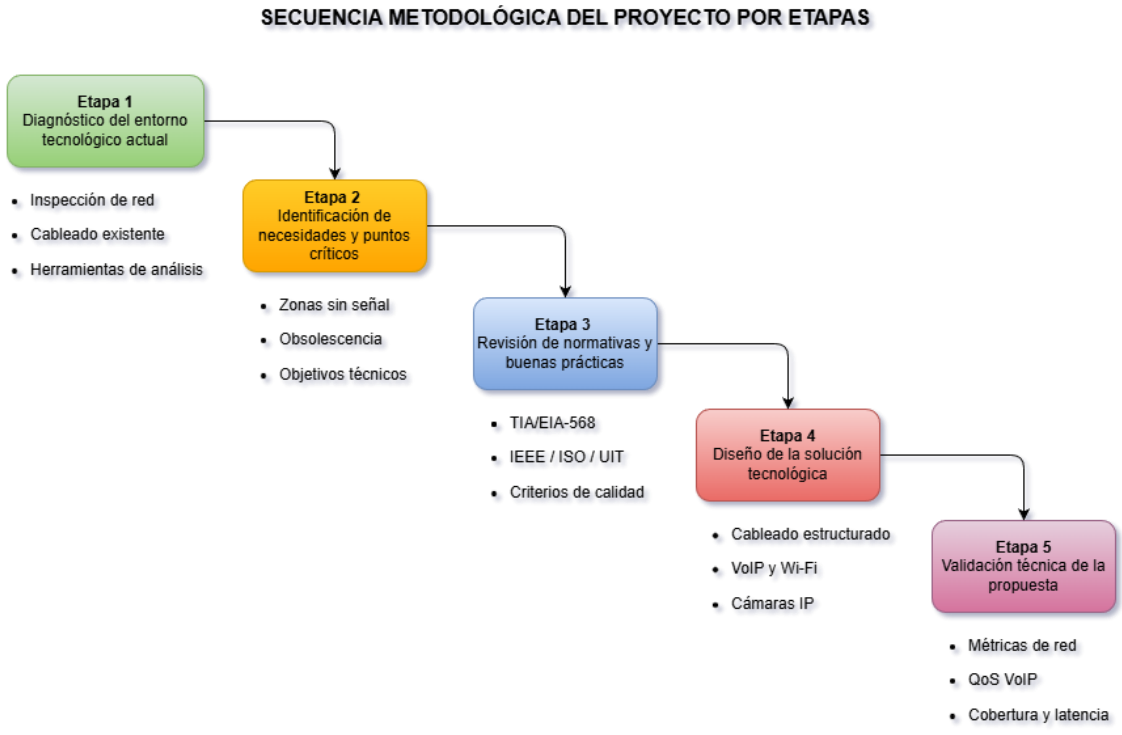


Figura 4.1 Diagrama de secuencia metodológica del proyecto por etapas.

En la primera etapa, diagnóstico del entorno tecnológico actual, se realizó un relevamiento del estado actual de la red de datos y los sistemas que la componen, considerando el tipo y antigüedad del cableado, la antigüedad de los equipos, la cobertura inalámbrica, la existencia de telefonía analógica y la densidad de cámaras de videovigilancia. Los datos se recopilaron a través de inspección física, revisión documental, entrevistas técnicas y herramientas de análisis de red.

A partir de esta información, en la etapa de identificación de necesidades y puntos críticos, se identificaron las limitaciones más relevantes que afectan la infraestructura, entre las que destacan problemas de conectividad que obstaculizan la eficiencia operativa, señal débil en áreas estratégicas, carencia de escalabilidad, obsolescencia de componentes y escasa integración entre sistemas de comunicación y seguridad. Durante esta fase se definieron los objetivos técnicos que la propuesta de renovación debía satisfacer.

Posteriormente, en la revisión de normativas y buenas prácticas se consultaron los estándares técnicos y regulatorios relevantes, como TIA/EIA-568 para cableado estructurado, IEEE para redes inalámbricas y criterios de seguridad para redes IP. Este análisis constituyó la base para asegurar que el diseño técnico fuera de calidad, compatible y sostenible en el tiempo.

Con base en estos hallazgos, se procedió al diseño de la solución tecnológica, desarrollando una propuesta integral que abarca la reorganización del cableado, la implementación de redes inalámbricas de alto rendimiento, la migración a telefonía IP segura y la actualización del sistema de videovigilancia con cámaras IP. El diseño técnico se adaptó a las necesidades reales del entorno, priorizando la eficiencia operativa, la escalabilidad futura y la facilidad de mantenimiento.

Finalmente, en la etapa de validación técnica de la propuesta se establecieron mecanismos para medir el impacto de la solución planteada mediante métricas como velocidad de transmisión, estabilidad de conexión, disminución de latencia, calidad de servicio (QoS) en telefonía IP y cobertura de vigilancia. Estos criterios de validación permiten verificar si la infraestructura renovada satisface los estándares de rendimiento esperados.

4.5 Metodología empleada

Para la elaboración del proyecto se utilizó la metodología de mejora continua del ciclo PHVA (Planear, Hacer, Verificar, Actuar), muy utilizada en la industria para controlar procesos de manera sistemática, eficiente y en cumplimiento de estándares de calidad (véase Figura 4.2).

Esta metodología estructuró el proceso en pasos lógicos y secuenciales que facilitaron su ejecución técnica y la evaluación objetiva de los resultados por lo que la elección de este enfoque se justifica en la necesidad de instaurar una forma de trabajo flexible, que permita reconocer oportunidades de mejora, aplicar medidas correctivas, verificar resultados y adaptar la propuesta al contexto específico.

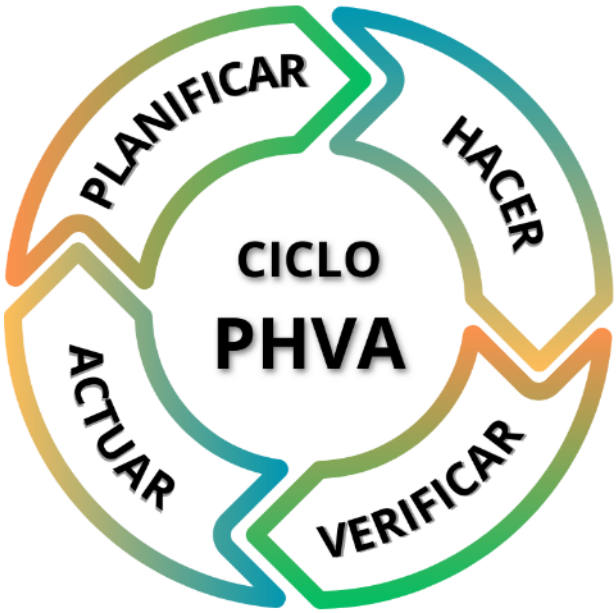


Figura 4.2 Representación del ciclo PHVA. Elaboración propia.

Planear (P)

En esta etapa se realizó un diagnóstico detallado de la infraestructura tecnológica existente, identificando debilidades, riesgos y áreas de oportunidad. Se recopilaron datos sobre el cableado, los dispositivos de red, la cobertura inalámbrica, la telefonía analógica y los sistemas de videovigilancia, para establecer los requerimientos técnicos que guiarían el diseño de la solución.

Hacer (H)

Con base en los hallazgos obtenidos, se procedió a diseñar una propuesta integral de renovación tecnológica que incluye: cableado estructurado conforme a normativas vigentes, implementación de redes inalámbricas eficientes, migración a telefonía VoIP segura y reconfiguración del sistema de videovigilancia IP. Esta etapa contempla tanto el diseño conceptual como la implementación técnica, real según el alcance definido.

Verificar (V)

En esta fase se evaluó el desempeño de la solución propuesta mediante métricas clave como la velocidad de transmisión, estabilidad de la red, calidad del servicio (QoS) en telefonía IP, cobertura de señal Wi-Fi y alcance de los sistemas de videovigilancia. Los resultados obtenidos se compararon con la situación inicial, con el fin de comprobar la mejora efectiva en términos de conectividad, comunicación y seguridad.

Actuar (A)

Finalmente, con base en los resultados de la verificación, se definieron ajustes y recomendaciones para optimizar la implementación, garantizando la escalabilidad, sostenibilidad y adaptabilidad de la solución a largo plazo. Esta fase asegura que los aprendizajes derivados del proyecto se traduzcan en acciones correctivas o preventivas para futuras intervenciones tecnológicas.

4.2 Etapas del proyecto aplicadas

Como se ha mencionado anteriormente, el desarrollo del proyecto se estructuró en diversas fases sucesivas que permitieron abordar de manera sistemática cada una de las áreas clave relacionadas con la renovación de la infraestructura tecnológica. Estas etapas respondieron a una lógica de mejora continua, considerando desde la caracterización del entorno hasta la validación del diseño propuesto.

4.5.1 Diagnóstico de la infraestructura actual

En una primera fase, se llevó a cabo un diagnóstico técnico completo de la infraestructura tecnológica en el entorno industrial de estudio. Esta etapa permitió conocer el estado actual de los sistemas de red, comunicación y seguridad para definir una línea base confiable sobre la cual se formuló la propuesta de renovación tecnológica.

El levantamiento de información se realizó en conjunto con el Ingeniero en Sistemas, actual encargado del área de tecnología de la empresa.

A través de sesiones de revisión documental y entrevistas técnicas, el ingeniero fue compartiendo la información existente y resolviendo las preguntas que iban surgiendo sobre la forma en que operaba y estaba estructurada actualmente la red. Es importante mencionar que, según su testimonio, él no participó en la fase inicial de implementación de la infraestructura tecnológica hace más de 20 años. En ese tiempo, varios ingenieros han pasado por el área; por lo tanto, hoy en día es un sistema legado y parcialmente documentado.

Tras su colaboración e inspección física, se pudo determinar que la empresa dispone de la siguiente infraestructura tecnológica de red:

- Site principal centralizado, desde donde se distribuía la conectividad a las distintas áreas de la planta.
- Dos enlaces de conectividad a internet: uno provisto por Bestel y otro por Telmex, configurados como respaldo mutuo.
- Firewall Fortinet 101F, encargado de la gestión de la seguridad perimetral de la red.
- Cuatro servidores físicos con distintos propósitos, entre los que se incluían:
    - Un servidor con el sistema NAVISION versión 5
    - Un segundo servidor con NAVISION 2018
    - Un servidor destinado a MasterWeb
    - Y un servidor principal de control general
- Un dispositivo NAS (Network Attached Storage) para almacenamiento en red.
- Un sistema de KVM (Keyboard Video Mouse switch) para gestión remota de servidores.
- Un grabador de video en red (NVR) marca Hikvision, que centralizaba la videovigilancia.

- Un total de 33 cámaras de seguridad, de las cuales varias presentaban fallas o estaban fuera de operación.
- Un conmutador telefónico analógico, ya obsoleto, con una sola línea funcional conectada al teléfono del área de ventas.
- Un switch PoE dedicado para cámaras IP y cuatro switches adicionales: tres destinados a nodos de red cableados y uno para redes inalámbricas (Wi-Fi).
- Diversos No-Breaks, cuya capacidad resultaba insuficiente para garantizar la continuidad operativa de los equipos críticos durante cortes de energía.
- Presencia de cableado estructurado desorganizado tipo Cat 5 desactualizado, con tramos enredados, sin etiquetado ni identificación clara, lo que dificultaba tareas de mantenimiento o reconfiguración.
- Cuatro IDF (Intermediate Distribution Frame) distribuidos en puntos estratégicos de la planta industrial:
    - Uno ubicado en la subestación eléctrica
    - Otro en la parte superior del edificio exterior, en el área de calidad
    - Un tercero encima de un baño en la zona de embarques
    - Y un cuarto en el área de seguridad e higiene

En estos IDF se hallaron switches planos y conexiones por cable UTP, e incluso algunos tramos que utilizaban antiguos convertidores de fibra óptica para llegar a los puntos más distantes del site principal.

- La conectividad inalámbrica estaba soportada por dos antenas Wi-Fi 5 en oficinas administrativas y cuatro adicionales distribuidas en la planta, las cuales ofrecían cobertura limitada y desigual.
- Existían también múltiples nodos con pequeños switches intermedios, instalados en tramos largos para extender la conectividad a computadoras, impresoras y equipos de control.

- Finalmente, se detectó que solo había una entrada telefónica activa y ya no se mantenía un sistema de telefonía fija funcional a nivel general.

En este chequeo también se descubrió que no había documentación técnica legada que explicara la topología, configuración o estado actual de la red. No existían planos estructurales ni fichas técnicas, por lo que el conocimiento del sistema se había ido generando de forma empírica, por inmersión operativa y experiencia del personal actual. Además, como parte del análisis técnico, se desarrollaron diagramas lógicos del estado actual de la red de datos y CCTV. Estos diagramas se elaboraron tras un recorrido físico por las instalaciones, la documentación existente y la información del personal de TI para tener una representación visual de la forma en que se distribuyen, conectan y segmentan los dispositivos en la infraestructura tecnológica actual.

En la Figura 4.3 se muestra el diagrama lógico de la red principal, la 192.168.1.x, donde se puede apreciar el site principal, los IDF distribuidos, los enlaces a internet, servidores, antenas Wi-Fi, impresoras y equipos de usuario, así como los switches intermedios que daban soporte a cada área de la planta. Se observan varios saltos de red, falta de jerarquía y sobrecarga de nodos en ciertos puntos.

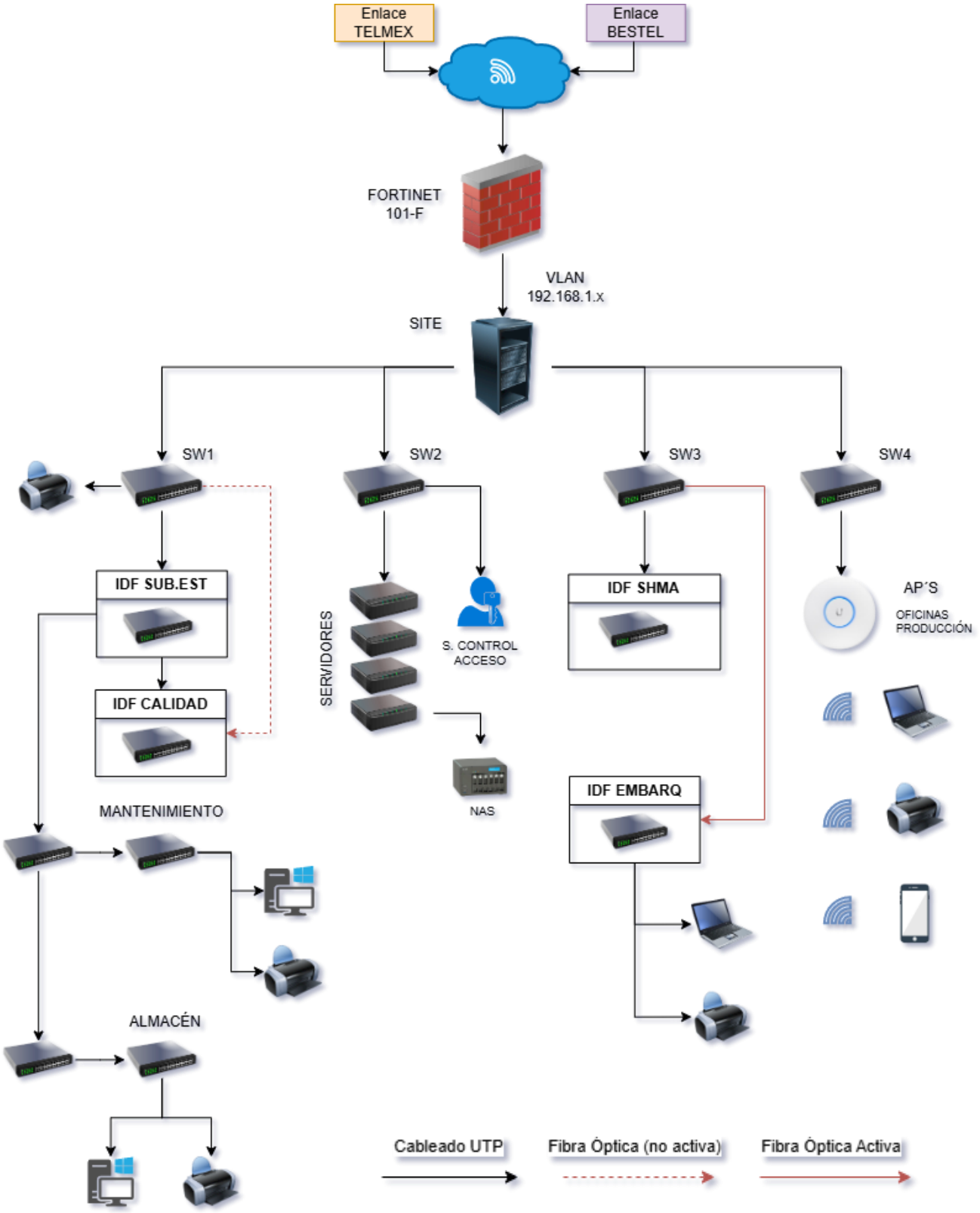


Figura 4.3 Diagrama lógico de la red principal inicial. Elaboración propia.

La Figura 4.4 muestra el diagrama de la red de videovigilancia, correspondiente al segmento 192.168.30.x, en el cual se conectaban las cámaras IP, el NVR y los IDF utilizados para alimentar o redistribuir la señal de video. A pesar de contar con convertidores de fibra óptica en algunos tramos, toda la red operaba efectivamente sobre cableado Ethernet, y muchas cámaras dependían de tomas eléctricas convencionales, sin un esquema unificado de PoE ni gestión centralizada.

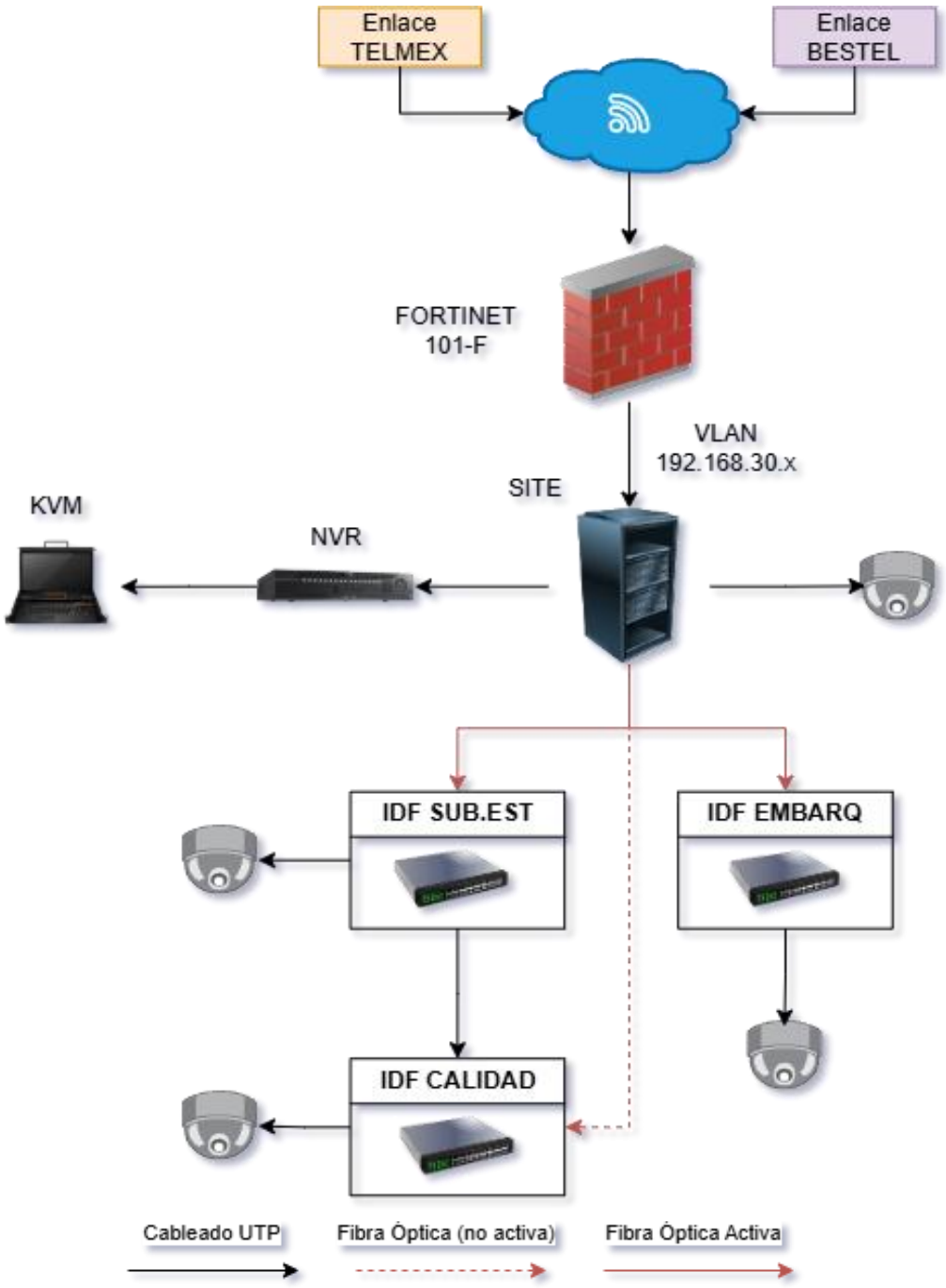


Figura 4.4 Diagrama de red del sistema de videovigilancia. Elaboración propia.

Ambos diagramas hicieron posible reconocer de forma gráfica y exacta algunas problemáticas que serán solucionadas en las siguientes fases del proyecto.

4.5.2 Identificación de necesidades y puntos críticos en la empresa

Además del levantamiento lógico de la red, se mapeó físicamente la ubicación de los puntos de acceso inalámbricos (APs) desplegados en la planta industrial. Esta evaluación determinó la cobertura actual, la dispersión de la señal Wi-Fi y las posibles zonas con restricciones de conectividad.

El resultado de dicha inspección se refleja en los siguientes planos (véase Figuras 4.5 y 4.6), en los que se identifican dos antenas Wi-Fi en la zona de oficinas y cuatro antenas repartidas por toda la zona de producción. Es importante mencionar que estos equipos contaban con configuraciones no estandarizadas e incluso se instalaban sin tener en cuenta las mejores prácticas de cobertura ni un diseño de celdas que evitara interferencias o zonas muertas.

El estudio mostró que, si bien existían puntos de acceso en ubicaciones estratégicas, la cobertura no era suficiente para dar abasto con el tráfico actual, sobre todo en horas pico o en lugares con alta densidad de dispositivos móviles o inalámbricos; esta dispersión, aunada a la ausencia de un sistema de control centralizado y la saturación del segmento de red 192.168.1.x, generaba una experiencia poco confiable para los usuarios operativos y administrativos.

4.5.2.1 Antenas en oficinas

Figura 4.5 Ubicación de APs en oficinas administrativas. Elaboración propia con base en planos internos de la empresa.

4.5.2.2 Antenas en planta productiva

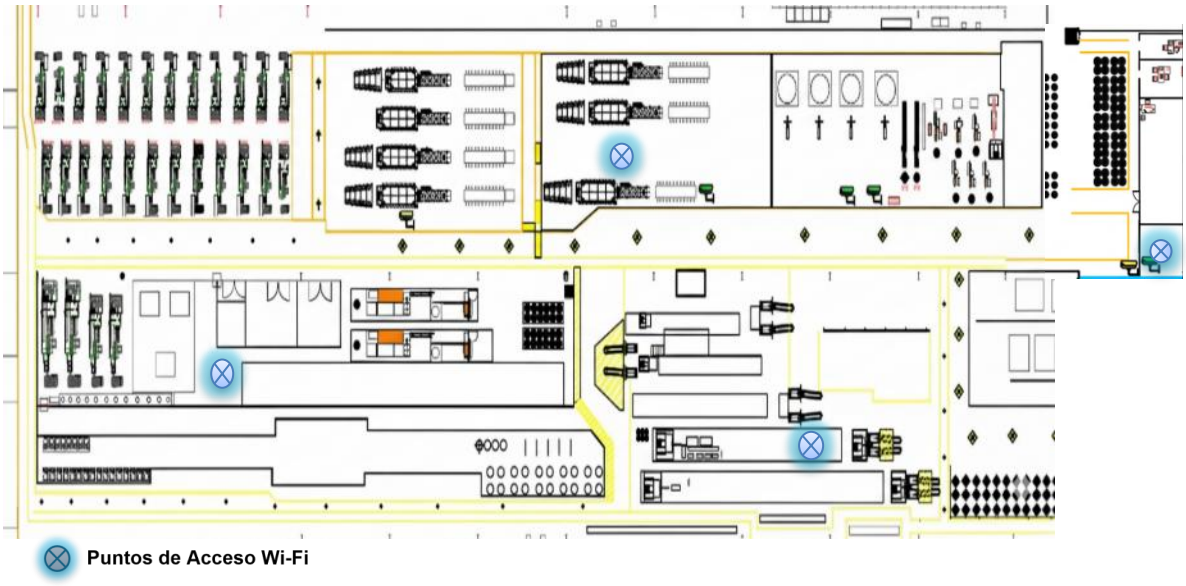


Figura 4.6 Ubicación de APs en áreas productivas. Elaboración propia con base en planos internos de la empresa.

Para tener una mejor idea de la cobertura inalámbrica real en el ambiente industrial, se generaron mapas de calor Wi-Fi sobre los planos físicos de la planta y las oficinas administrativas (véase Figuras 4.7 y 4.8). Estos mapas muestran gráficamente las áreas de señal fuerte, media y débil según la ubicación actual de los puntos de acceso (APs) y las obstrucciones arquitectónicas que afectan la señal.

El estudio mostró que las áreas con señal alta (rojo/naranja) se localizaban en las proximidades de los APs, como pasillos centrales, áreas de oficinas colindantes y ciertas líneas de producción. Pero había grandes áreas con cobertura media o mala (amarillo/verde y azul/púrpura), sobre todo en los extremos de las instalaciones, en cuartos cerrados o en áreas donde había maquinaria pesada o racks metálicos. Estos resultados reafirman la ubicación inadecuada de los APs y la necesidad de un rediseño de la red inalámbrica, apoyándose en estudios de sitio más exactos.

Las tablas descriptivas anexas a cada plano (Tablas 4.1 y 4.2) resumen los principales puntos analizados: situación de los APs, áreas de cobertura por nivel de señal y atenuantes (muros, mobiliario metálico, densidad de equipos industriales, etc.).

4.5.2.2.1 Mapa de calor en oficinas

Figura 4.7 Mapa de calor Wi-Fi en oficinas administrativas. Elaboración propia con base en planos internos de la empresa.

Tabla 4.1 Explicación de los elementos del mapa de calor en oficinas

Elemento	***Descripción***
Ubicación de APs	2 puntos de acceso (círculos con X azul) ubicados en el pasillo central, aprox. a 1/3 y 2/3 de la longitud del edificio.
Zonas de señal fuerte (Rojo/Naranja)	Pasillo principal y oficinas adyacentes inmediatas.
Zonas de señal media (Amarillo/Verde)	Oficinas periféricas, salas de reunión laterales y esquinas de los pasillos.
Zonas de señal débil (Azul/Púrpura)	Extremos del edificio (por ejemplo, la gran sala de reuniones en el lado derecho y la esquina inferior izquierda).
Factores de atenuación	Muros divisorios de tablaroca o block, mobiliario denso, equipos de oficina metálicos.

4.5.2.2.2 Mapa de calor en producción

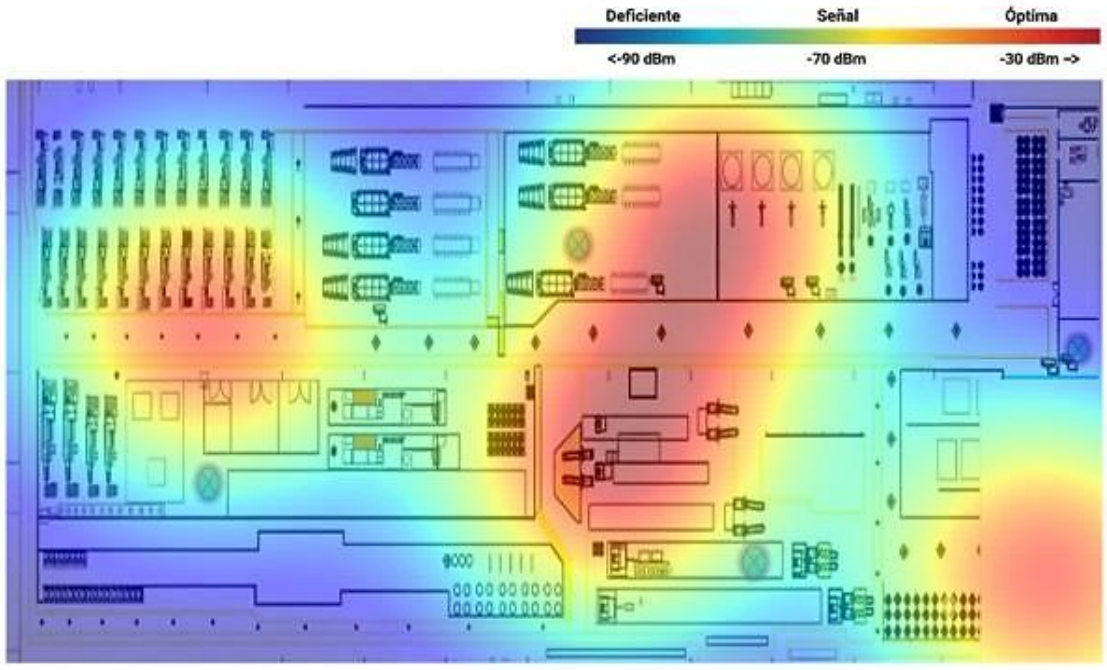


Figura 4.8 Mapa de calor Wi-Fi en área productiva. Elaboración propia con base en planos internos de la empresa.

Tabla 4.2 Explicación de los elementos del mapa de calor en producción

Elemento	***Descripción***
Ubicación de APs	4 puntos de acceso (círculos con X azul/violeta) distribuidos: 1) inferior-izquierdo, 2) superior-central, 3) inferior-central/derecha, 4) extremo superior-derecho.
Zonas de señal fuerte (Rojo/Naranja)	Áreas cercanas a cada AP: pasillos centrales, líneas de producción inmediatas y oficinas anexas.
Zonas de señal media (Amarillo/Verde)	Secciones intermedias entre APs, algunas áreas de máquinas y pasillos laterales.
Zonas de señal débil (Azul/Púrpura)	Esquinas más alejadas, cuartos cerrados, zonas con racks metálicos o maquinaria pesada.

Factores de atenuación	Muros de block, estanterías metálicas, equipos industriales de gran volumen, racks eléctricos.

Como parte del diagnóstico técnico de la infraestructura, se tomaron más de 30 mediciones independientes de velocidad de red utilizando la herramienta SpeedTest by Ookla; las pruebas se realizaron en dos zonas principales: zona de oficinas y zona de producción, a ciertas distancias del punto de acceso Wi-Fi más cercano.

Para una mejor interpretación, los resultados se tabularon por bloques de distancia:

- Oficinas: 5, 10 y 15 metros
- Producción: 10, 20 y 30 metros

Cada tabla muestra los datos tomados de ping (latencia), velocidad de descarga y velocidad de subida en diferentes localizaciones físicas y niveles de saturación.

Los resultados muestran un degradado de señal a medida que se aleja la señal, siendo más notorio en la zona de producción, donde el ambiente industrial crea interferencias adicionales, estructuras metálicas y mayor densidad de usuarios. Por otro lado, las oficinas tienen un comportamiento más constante, aunque también con signos de saturación en horas pico; en las Tablas 4.3 - 4.8, se muestran los resultados obtenidos en términos de velocidad de descarga (Mbps), velocidad de carga (Mbps) y latencia promedio (Ping en ms).

La Tabla 4.3 presenta los resultados obtenidos en el área de oficinas administrativas a una distancia aproximada de 5 metros del punto de acceso Wi-Fi. En este escenario se observan velocidades de descarga estables, con valores superiores a los 55 Mbps en la mayoría de las mediciones, así como velocidades de subida consistentes y niveles de latencia bajos, inferiores a los 25 ms. Estos resultados reflejan un desempeño adecuado de la red en condiciones cercanas al punto de acceso y con mínima atenuación de la señal.

Tabla 4.3 Mediciones en oficinas administrativas 5 metros de distancia

#	Descarga (Mbps)	Subida (Mbps)	Ping (ms)
1	58.88	44.26	23
2	62.83	36.87	24
3	55.00	38.31	23
4	65.61	32.58	17
5	63.73	35.62	19
6	59.71	33.67	24
7	59.84	30.76	15
8	65.64	40.49	17
9	62.20	47.89	25
10	67.51	31.11	21

En la Tabla 4.4 se muestran las mediciones realizadas en oficinas administrativas a 10 metros de distancia. Aunque las velocidades de descarga y subida se mantienen relativamente estables, se comienza a notar una ligera variabilidad en los valores, así como un incremento moderado en la latencia. Este comportamiento sugiere el inicio de una degradación natural de la señal conforme aumenta la distancia, aunque sin afectar de forma crítica la experiencia del usuario, pero con oportunidad de mejora.

Tabla 4.4 Mediciones en oficinas administrativas 10 metros de distancia

#	Descarga (Mbps)	Subida (Mbps)	Ping (ms)
11	58.58	31.38	20
12	53.97	41.09	25
13	64.87	41.42	19
14	61.93	43.67	21
15	55.41	30.01	24
16	56.84	36.06	24
17	62.42	31.35	23
18	62.20	41.00	23
19	66.62	44.32	23
20	56.38	38.12	20

La Tabla 4.5 evidencia un mayor impacto de la distancia sobre el desempeño de la red inalámbrica en oficinas administrativas. Las velocidades de descarga presentan una disminución más marcada y la latencia muestra valores más elevados y variables. Estos resultados indican una pérdida progresiva de calidad de la señal, atribuible tanto a la distancia como a posibles obstáculos físicos y a la saturación del canal inalámbrico.

Tabla 4.5 Mediciones en oficinas administrativas 15 metros de distancia

#	Descarga (Mbps)	Subida (Mbps)	Ping (ms)
21	46.46	30.10	25
22	48.71	25.34	30
23	52.89	34.94	21
24	57.04	34.40	27
25	48.95	37.89	28
26	51.30	35.19	23
27	43.63	35.20	22
28	47.73	39.10	26
29	54.61	27.61	30
30	58.57	28.97	29

Los resultados mostrados en la Tabla 4.6 corresponden a mediciones realizadas en la planta de producción a una distancia de 10 metros del punto de acceso. A diferencia del área administrativa, se observan velocidades de descarga y subida considerablemente menores, así como valores de latencia más elevados. Este comportamiento podría estar asociado a las condiciones propias del entorno industrial, como maquinaria en operación, estructuras metálicas e interferencias electromagnéticas.

Tabla 4.6 Mediciones en planta de producción 10 metros de distancia

#	Descarga (Mbps)	Subida (Mbps)	Ping (ms)
1	38.68	27.84	36
2	35.88	28.41	42
3	33.80	23.89	43
4	38.83	31.82	32
5	43.14	26.12	28
6	31.56	22.40	38

7	34.73	24.62	29
8	48.47	21.63	44
9	33.44	26.47	34
10	48.68	25.90	40

La Tabla 4.7 muestra un deterioro adicional en el desempeño de la red al incrementar la distancia a 20 metros dentro de la planta de producción. Las velocidades presentan una mayor inestabilidad y la latencia se incrementa de forma más consistente.

Tabla 4.7 Mediciones en planta de producción 20 metros de distancia

#	*Descarga (Mbps)*	*Subida (Mbps)*	*Ping (ms)*
11	39.30	24.72	39
12	37.36	21.21	39
13	38.91	26.21	40
14	37.49	22.77	34
15	30.67	30.62	29
16	45.88	28.16	32
17	40.20	22.50	35
18	33.66	29.14	30
19	36.57	31.24	31
20	40.32	29.60	39

Finalmente, la Tabla 4.8 refleja el escenario más desfavorable evaluado durante el diagnóstico, con mediciones realizadas a 30 metros en la planta de producción. En este caso se observan las velocidades de descarga y subida más bajas, así como los valores de latencia más altos del conjunto de pruebas. Este comportamiento evidencia claramente las limitaciones de la infraestructura inalámbrica actual para cubrir distancias mayores en este tipo de entornos, reforzando la necesidad de una redistribución y modernización de los puntos de acceso.

Tabla 4.8 Mediciones en planta de producción 30 metros de distancia

#	*Descarga (Mbps)*	*Subida (Mbps)*	*Ping (ms)*
21	37.60	23.22	29

22	25.00	16.41	50
23	29.73	19.59	38
24	36.32	24.39	31
25	26.48	21.09	46
26	35.36	19.96	32
27	25.00	18.34	35
28	34.22	26.77	41
29	30.64	21.69	39
30	30.85	22.12	43

Observaciones generales

En oficinas a 5 y 10 metros, los valores de descarga son buenos (superiores a 50 Mbps en la mayoría de los casos) con ping inferior a 20 ms, pero con caídas. A 15 metros, el enlace ya se degrada, con latencias de hasta 60 ms y velocidades erráticas. En producción, incluso a 10 metros, se alcanzaron velocidades por debajo de 30 Mbps en algunos puntos, empeorando a 20 y 30 metros, donde el ping supera los 70 ms en algunos casos, lo que certifica una mala experiencia de conectividad.

Se observó también la presencia de pequeños switches intermedios para extender la red a lugares distantes, incrementando los saltos y degradando el rendimiento. La saturación de la VLAN principal (192.168.1.x), en la que conviven servicios críticos y usuarios de oficina/planta, es otro elemento que afecta la estabilidad de la red.

Esta evaluación proporciona una línea base técnica del estado de la conectividad inalámbrica que se comparará con los resultados posteriores a la implementación del rediseño de infraestructura propuesto en este proyecto.

Documentación técnica previa sobre la red de videovigilancia

En el proceso de diagnóstico también se encontró una ficha técnica antigua del sistema CCTV de la planta, que contenía un mapa con la ubicación de cámaras y diagramas de arquitectura de red y descripciones de equipos. Este material sirvió como una referencia general, pero se encontró que no representaba el estado actual del sistema.

En concreto, se detectaron cámaras ya no operativas, equipos retirados o sustituidos sin quedar registro, así como direcciones IP ya no activas en el segmento original. Esta desactualización documental dificultó el seguimiento y control de los recursos instalados.

El mapa que se muestra en la Figura 4.9 (muy desactualizado) muestra 40 ubicaciones de cámaras, categorizadas por tipo (PTZ, domo/bullet, ojo de pez), así como la ubicación de IDFs y el NVR.

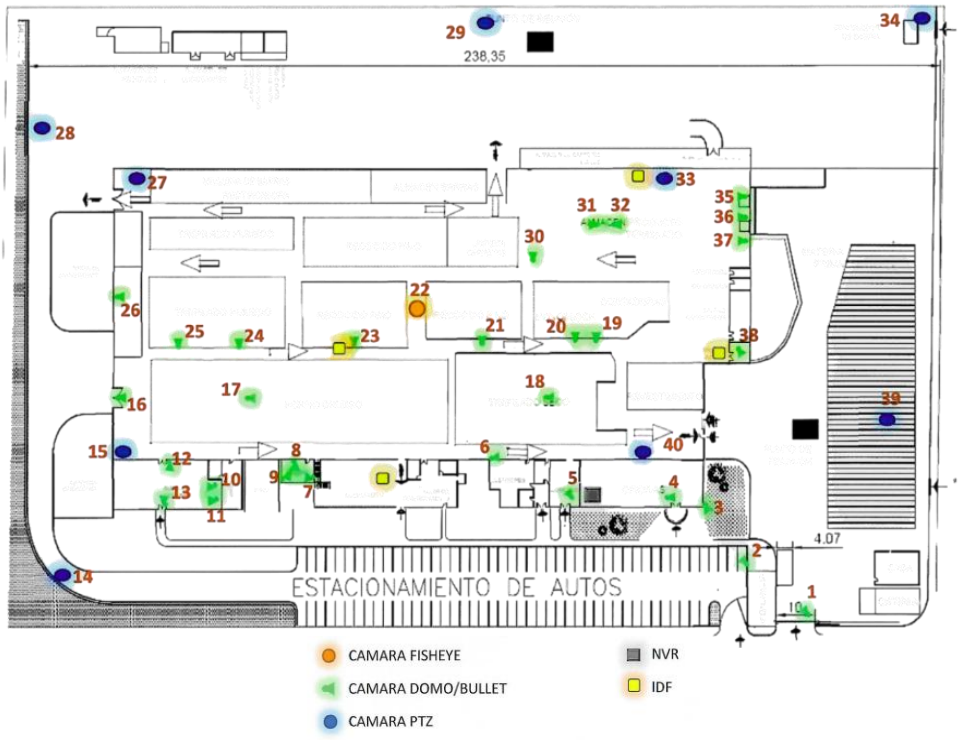


Figura 4.9 Plano general de ubicación de cámaras en planta. Recuperado del archivo proporcionado por la empresa.

Junto con dicho plano, se localizó un resumen técnico de instalación inicial que formaba parte de los archivos de documentación de la empresa, el cual incluye información sobre el MDF (gabinete principal), la distribución de equipos en los IDF, los tipos de cámaras instaladas por área (interior, perímetro y oficinas), así como una lista de equipos de respaldo como UPS, monitores y conversores de medios (ver Anexo A).

Asimismo, se encontraron planos de arquitectura de red donde se representa la interconexión entre los NVR, switches, cámaras IP y enlaces de fibra óptica hacia los IDF, incluyendo el uso de conversores de medios y esquemas de alimentación eléctrica. No obstante, estos documentos no reflejaban con precisión el estado actual de la

infraestructura, ya que presentaban configuraciones que ya no se encontraban en operación (ver Anexo B).

Adicionalmente, se identificaron registros históricos de direccionamiento IP correspondientes al NVR-01, en el rango 192.168.1.x, los cuales evidencian que varias direcciones asignadas originalmente a cámaras ya no se encontraban activas o habían sido reutilizadas para otros dispositivos. Esta situación confirmó que el sistema había sido modificado sin una actualización documental formal (ver Anexo C).

Debido a que la documentación existente no era fiel a la infraestructura real, se realizó un levantamiento físico completo de la red de videovigilancia, a partir del cual se elaboró un nuevo diagrama lógico actualizado, presentado en la Figura 4.2. Dicho diagrama se construyó con base en recorridos presenciales, revisión de cableado, identificación de equipos funcionales y entrevistas con personal del área de TI, estableciendo una base confiable para la fase de rediseño de la infraestructura tecnológica.

4.5.3 Revisión de normativas y lineamientos técnicos

Como parte del diagnóstico, se hizo una revisión exhaustiva de normativas, estándares técnicos y guías de mejores prácticas internacionales para el diseño, instalación y administración de redes industriales modernas. Este ejercicio sirvió para reconocer fallas técnicas en la infraestructura actual, medir su obsolescencia y definir criterios para la futura propuesta de renovación.

Entre los marcos de referencia consultados se encuentran:

- **Cableado estructurado (EIA/TIA-568)**

La norma EIA/TIA-568 especifica los criterios técnicos para sistemas de cableado estructurado, incluyendo categorías de cable, distancias máximas, jerarquía de distribución (MDF/IDF), organización de racks y etiquetado (Castellón, 2014). El resultado del diagnóstico evidenció que la infraestructura actual viola varios de estos principios, como por ejemplo el caos en el cableado, los saltos innecesarios por switches y la falta de etiquetado, lo que dificulta la trazabilidad y el mantenimiento.

- **Redes inalámbricas (IEEE 802.11)**

Las redes Wi-Fi hoy en día se desvían de lo que establece el estándar IEEE 802.11 en términos de diseño de celdas, control de canales, balanceo de carga, roaming y

redundancia (de Miguel et al., s.f.). No existen controladores ni arquitectura definida, lo que causa saturación e inestabilidad, como demostraron los mapas de calor.

- **Videovigilancia IP (recomendaciones de fabricantes)**

De acuerdo con Hikvision (Caldera & Suazo, 2011), una red de videovigilancia IP debe correr en una VLAN exclusiva, con switches PoE, almacenamiento en red y cableado dedicado. Pero en la red actual se encontró tráfico compartido, cámaras alimentadas desde tomas de corriente, múltiples dispositivos fuera de línea, lo que afecta la eficiencia y escalabilidad del sistema.

- **Fibra óptica (TIA-568.3-D y mejores prácticas)**

En cuanto a la conectividad troncal, se identificaron convertidores fibra-Ethernet, pero sin sacar provecho del medio óptico; de acuerdo con la norma TIA-568.3 y casos como el de Zúñiga (2022), una red actual debe usar enlaces troncales de fibra para obtener más ancho de banda, menos latencia y más inmunidad al ruido. No hacer uso de la fibra es un desperdicio.

- **Seguridad y segmentación de red (recomendaciones de fabricantes)**

La segmentación actual de la red, que separa el tráfico general (192.168.1.x) del CCTV (192.168.30.x), no tiene políticas de control de acceso, monitoreo de tráfico, etc., contradiciendo las buenas prácticas de seguridad de fabricantes como Cisco, Fortinet, entre otros, (Cisco, 2025). Necesita una arquitectura más sólida, con VLANs por función y reglas de acceso explícitas.

- **Migración tecnológica y VoIP (UIT, 2003)**

Finalmente, se revisó el Informe fundamental sobre telefonía IP de la Unión Internacional de Telecomunicaciones (UIT, 2003), donde se discuten los desafíos técnicos y organizacionales para migrar de conmutadores analógicos a sistemas IP convergentes. El uso hoy en día de un conmutador analógico obsoleto refuerza la necesidad de implementar nuevas tecnologías como VoIP bajo protocolos estándares como SIP o H.323 (Caldera & Suazo, 2011).

4.6 Propuesta de mejora a la infraestructura tecnológica

En base a lo que se descubrió en la etapa de diagnóstico, se diseñó una solución tecnológica completa para solucionar las carencias encontradas en la infraestructura de red, comunicación y videovigilancia. Esta etapa permitió transformar las necesidades

identificadas en una propuesta técnica factible y en concordancia con estándares regulatorios, criterios de eficiencia operativa y potencial de escalabilidad. Como resultado, se creó una nueva arquitectura lógica de red, que define una estructura jerárquica, organizada y segmentada de los recursos tecnológicos, para una gestión más eficiente y segura del tráfico de datos en todo el entorno industrial.

En la Figura 4.10 se muestra el diseño planteado, el cual incluye enlaces redundantes de Internet provistos por Telmex y Bestel, ambos canalizados a través de un firewall Fortinet 101-F, que actúa como dispositivo de seguridad perimetral. A partir de aquí el tráfico se dirige a la data center principal (SITE), donde se encuentra el switch core de distribución, servidores internos, NAS, switch IP y control de accesos. Desde el switch core se extienden enlaces troncales a seis IDF ubicados en puntos estratégicos: calidad, subestación eléctrica, vigilancia, SHMA, envíos y almacén, cubriendo así toda la red física a lo largo de la planta. Estos enlaces, diseñados para funcionar sobre cableado estructurado y fibra óptica, para mejorar drásticamente el ancho de banda, la latencia y la fiabilidad de la transmisión de datos.

Esta propuesta es una reformulación de la arquitectura tecnológica actual, impactando directamente en el ordenamiento físico y lógico de la red, disminuyendo cuellos de botella, mejorando la administración de tráfico y aplicando mejores prácticas de seguridad y escalabilidad. Además, cumple con las directrices de normativas como la TIA/EIA-568 para cableado estructurado, IEEE 802.11 para redes inalámbricas y las mejores prácticas de segmentación segura de fabricantes líderes como Cisco y Fortinet.

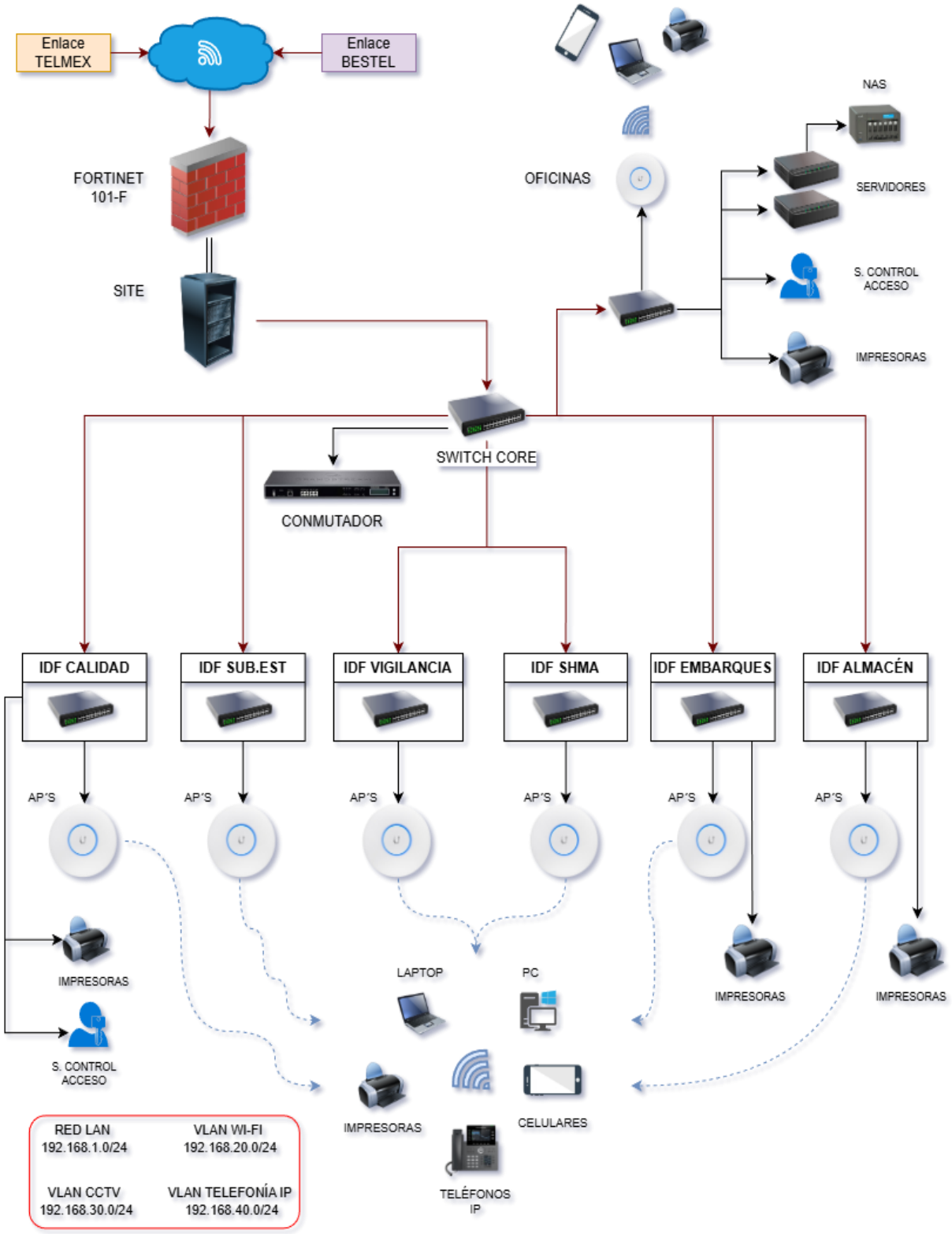


Figura 4.10 Diseño de la infraestructura de red propuesta. Elaboración propia.

El nuevo diseño contempla la instalación de puntos de acceso inalámbricos (APs) de alta densidad en áreas clave, tanto en las oficinas como en la planta; estos dispositivos se conectan directamente a switches PoE o nodos distribuidos para proporcionar cobertura inalámbrica más robusta, estable y con mayor capacidad de usuarios simultáneos; además, se implementó una segmentación lógica de la red en cuatro VLAN dedicadas para aislar el tráfico de red por función, mejorando la seguridad, el rendimiento y la capacidad de administración como se muestra en la Tabla 4.9.

Tabla 4.9 Segmentación de red por VLAN

VLAN ID	***Nombre***	***Máscara subred***	***Dirección de red***	***Gateway***	***Dirección de broadcast***	***Rango por VLAN (hosts válidos)***
1	VLAN LAN	255.255.255.0 (/24)	192.168.1.0	192.168.1.1	192.168.1.255	192.168.1.1 – 192.168.1.254
20	VLAN Wi-Fi	255.255.255.0 (/24)	192.168.20.0	192.168.20.1	192.168.20.255	192.168.20.1 – 192.168.20.254
30	VLAN CCTV	255.255.255.0 (/24)	192.168.30.0	192.168.30.1	192.168.30.255	192.168.30.1 – 192.168.30.254
40	VLAN Telefonía IP	255.255.255.0 (/24)	192.168.40.0	192.168.40.1	192.168.40.255	192.168.40.1 – 192.168.40.254

La primera corresponde a la red LAN común (192.168.1.0/24), en donde se conectan servidores, estaciones de trabajo, impresoras y demás dispositivos de oficina; la segunda es la VLAN Wi-Fi (192.168.20.0/24), destinada a dispositivos móviles, laptops y tabletas que se conectan a través de los puntos de acceso inalámbricos. Por otra parte, la tercera corresponde a la VLAN de CCTV (192.168.30.0/24), la cual permite aislar el tráfico de videovigilancia y asegurar ancho de banda y estabilidad para las cámaras IP y los NVR. Finalmente, la VLAN de telefonía IP (192.168.40.0/24) está dedicada al tráfico de voz, permitiendo aplicar políticas de calidad de servicio (QoS) sin interferir con el tráfico de datos.

Esta segmentación por función crítica es una gran mejora sobre el diseño anterior, ya que ahora se pueden implementar políticas de control de tráfico, zonificación entre redes, priorización de servicios y una administración más limpia y segura, en cumplimiento con estándares como TIA/EIA-568, IEEE 802.1Q, IEEE 802.11 y las mejores prácticas de fabricantes como Cisco, Fortinet, Hikvision, entre otros.

4.6.1 Cobertura WIFI 7

Como parte del fortalecimiento de la infraestructura de red para soportar servicios de voz, video, datos y movilidad, también se planteó la sustitución del cableado estructurado existente por cableado nuevo categoría Cat 6A. Esta mejora se hace eco de la necesidad de aumentar la velocidad, la capacidad de transmisión y la inmunidad al ruido electromagnético, especialmente en un entorno industrial con muchas fuentes de ruido. El nuevo cableado Cat 6A es capaz de certificar enlaces de 10 Gbps hasta 100 metros, mejorando el rendimiento de los servicios críticos como telefonía IP, videovigilancia, servidores y red inalámbrica.

En concreto, todas las antenas Wi-fi se incluyeron en este nuevo esquema de cableado, garantizando su alimentación a través de PoE y conexión directa al backbone de red. Para asegurar una cobertura robusta y a prueba del futuro, se sugirió usar Wi-Fi 7 (802.11be), simulando primero su comportamiento y alcance con el software de planificación de red de Ruijie Networks. Las simulaciones afinaron la ubicación de antenas en puntos óptimos, teniendo en cuenta materiales de edificación, obstáculos y densidad de usuarios.

Se planificó la ubicación de las antenas Wi-Fi en puntos estratégicos, tales como oficinas administrativas, calidad, embarques, seguridad e higiene, así como la ampliación del sistema a áreas donde antes no llegaba, como vigilancia, almacén y mantenimiento. En todos los casos se eligieron dispositivos de alto rendimiento modelo Huawei AirEngine 5773-23H con Wi-Fi 7 de doble banda y múltiples flujos espaciales (4x4 MU-MIMO) y funciones avanzadas de control de tráfico, optimización automática y acceso seguro. La cobertura proyectada se puede observar en las siguientes simulaciones gráficas, que muestran el estimado de señal en cada zona mencionada. Estas simulaciones serán la base para la validación en campo y futura optimización dinámica de canales y potencias.

4.6.1.1 Simulación Wifi 7 en oficinas administrativas

La Figura 4.11 muestra la simulación de cobertura Wi-Fi 7 en el área de oficinas administrativas. En el mapa de calor se observa una predominancia de zonas en color verde, lo que indica niveles de señal óptimos para el uso intensivo de aplicaciones de datos, voz y videoconferencia. La ubicación de los puntos de acceso permite cubrir adecuadamente estaciones de trabajo, salas de juntas y áreas comunes, manteniendo niveles de potencia adecuados y baja atenuación, aun considerando muros divisorios y mobiliario de oficina.

Figura 4.11 Simulación de cobertura Wi-Fi 7 en oficinas administrativas. Elaboración propia con base en planos internos de la empresa.

4.6.1.2 Simulación Wifi 7 en producción

En la Figura 4.12 se presenta la simulación correspondiente a la planta de producción, un entorno caracterizado por maquinaria, estructuras metálicas y mayor interferencia electromagnética. A pesar de estas condiciones, la cobertura proyectada muestra una señal mayoritariamente estable, con áreas verdes y amarillas que garantizan conectividad suficiente para dispositivos móviles, terminales industriales y equipos de supervisión. Las zonas de atenuación leve se concentran en áreas con mayor densidad de equipos, sin comprometer la operación general de la red.

Figura 4.12 Simulación de cobertura Wi-Fi 7 en planta de producción. Elaboración propia con base en planos internos de la empresa.

4.6.1.3 Simulación Wifi 7 en vigilancia

La Figura 4.13 muestra la cobertura estimada para el área de vigilancia. La ubicación del punto de acceso permite cubrir de manera eficiente tanto los espacios interiores como las zonas cercanas a accesos y perímetros. Aunque se observan áreas con señal media en los extremos del plano, la intensidad resultante es suficiente para el funcionamiento continuo de sistemas de monitoreo, dispositivos móviles del personal de seguridad y aplicaciones críticas asociadas a esta área.

Figura 4.13 Simulación de cobertura Wi-Fi 7 en área de vigilancia. Elaboración propia con base en planos internos de la empresa.

4.6.1.4 Simulación Wifi 7 en mantenimiento

La Figura 4.14 corresponde a la simulación de cobertura en el área de mantenimiento, donde existen múltiples obstáculos físicos, muros y equipos de gran tamaño. El mapa de calor refleja una combinación de zonas verdes y amarillas, indicando una cobertura adecuada para labores operativas. Las áreas de mayor atenuación se localizan en zonas extremas, sin afectar la conectividad en los puntos de trabajo principales.

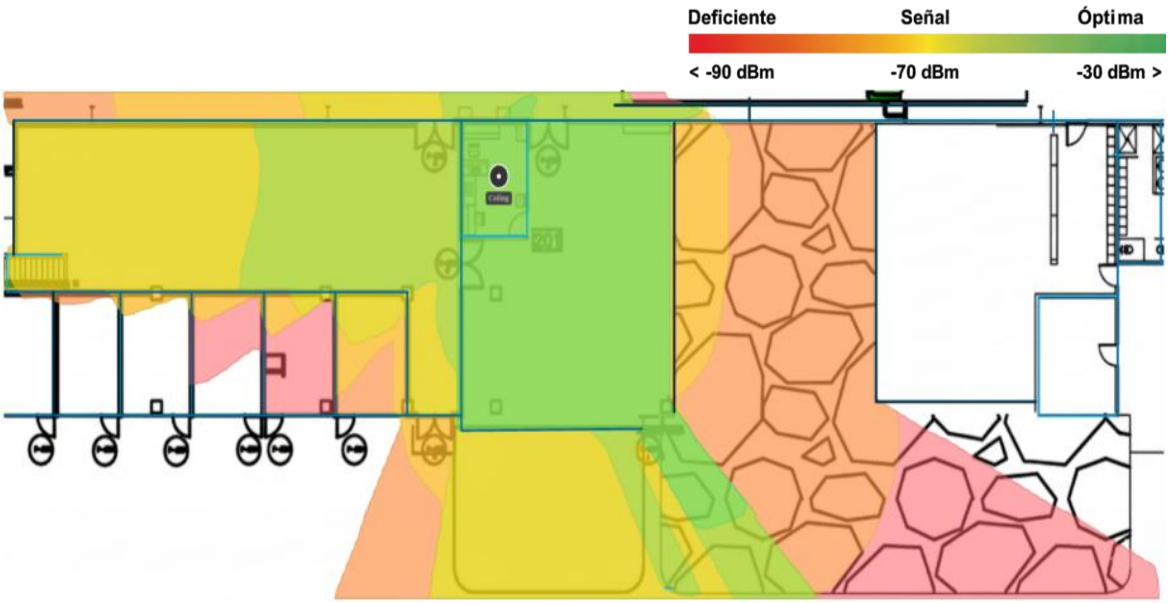


Figura 4.14 Simulación de cobertura Wi-Fi 7 en área de mantenimiento. Elaboración propia con base en planos internos de la empresa.

4.6.1.5 Simulación Wifi 7 en almacén y compras

Finalmente, la Figura 4.15 presenta la simulación de cobertura en el área de almacén y compras. En este escenario, la señal se mantiene estable y uniforme, a pesar de la presencia de estanterías y materiales almacenados que pueden generar reflexión o absorción de la señal. La cobertura proyectada garantiza conectividad confiable para sistemas de inventario, dispositivos móviles, lectores y estaciones de trabajo, contribuyendo a una operación eficiente y continua del área.

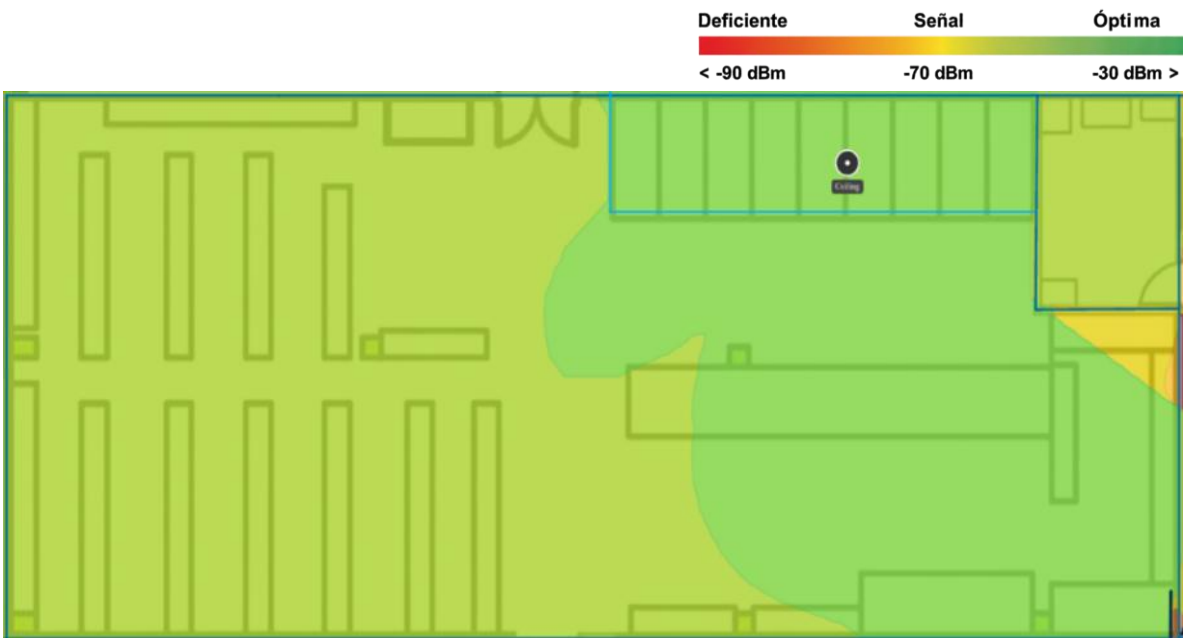


Figura 4.15 Simulación de cobertura Wi-Fi 7 en almacén y área de compras. Elaboración propia con base en planos internos de la empresa.

Las simulaciones de cobertura anteriores, utilizando la herramienta Ruijie Networks, confirmaron el diseño y la ubicación de los puntos de acceso Wi-Fi 7 (Huawei AirEngine 5773-23H) en las diferentes áreas de la planta industrial.

En términos generales, en todas las áreas analizadas (oficinas administrativas, planta productiva, vigilancia, almacén, mantenimiento y compras) se tiene un buen desempeño de señal, ya que predominan las zonas de color verde en los mapas de calor, lo que es señal de una excelente intensidad y calidad de señal inalámbrica. Las áreas amarillas/naranjas de atenuación leve se localizan mayormente en perímetros distantes o en áreas de muros divisorios, estanterías metálicas o equipos industriales grandes. Pero a pesar de estas condiciones estructurales, la cobertura continúa siendo viable para las necesidades operativas de los usuarios móviles.

La decisión de instalar nuevo cableado estructurado categoría Cat 6A hasta cada punto de acceso y la alimentación PoE garantizó la estabilidad y continuidad del servicio con un buen rendimiento. Adicionalmente, la segmentación en VLANs (192.168.20.x para Wi-Fi, entre otras) mejora el tráfico, refuerza la seguridad lógica y simplifica la administración de la red. Con este análisis se verifica que el nuevo diseño de red inalámbrica soluciona las fallas encontradas en el diagnóstico inicial y crea una infraestructura preparada para soportar servicios de alta demanda y nuevas tecnologías en el entorno industrial.

Como parte de la propuesta de mejora integral, se propuso además la reorganización del SITE principal para hacer un mejor uso del espacio físico, aumentar la eficiencia y disminuir los riesgos de falla eléctrica, saturación de cableado o desorden de infraestructura.

En el momento del diagnóstico inicial, se detectó cableado antiguo, dispositivos abandonados y hardware inoperativo que entorpecía la visibilidad en la gestión de red y creaba un riesgo para la continuidad del negocio. Ante esta situación, se planteó el retiro de cableado en desuso, la remoción de dispositivos innecesarios y el traslado de los equipos activos a una estructura organizada, etiquetada y en cumplimiento de las buenas prácticas de cableado estructurado.

También se recomendó colocar sistemas de respaldo de energía UPS (Uninterruptible Power Supply) en cada gabinete de distribución (IDF y MDF) con capacidad suficiente para mantener en funcionamiento los switches, convertidores de medios y equipos de comunicación ante fallas en el suministro eléctrico.

En la Tabla 4.10 se resumen los principales equipos que componen la nueva infraestructura de red:

Tabla 4.10 Equipos necesarios para cumplir con la infraestructura propuesta

Modelo / Nombre	***Descripción técnica***	***Cantidad***	***Imagen (referencial)***
AirEngine 5773-23H	Access Point Wi-Fi 7 de alto rendimiento, montaje en techo, tecnología híbrida óptico-eléctrica, doble banda 2.4/5 GHz.	17	
Patch Panel 24p	Panel de parcheo de 24 puertos para redes Cat 6A, con etiquetado e identificación frontal.	2	
Organizadores de cables	Organizadores horizontales y verticales de 1U para racks de 19", optimizan la gestión del cableado estructurado.	6	

Pigtails y Minigbic (LinkedPro)	Pigtails SC/APC multimodo y monomodo para fibra óptica, compatibles con módulos SFP LinkedPro.	12	
RJ45 LinkedPro	Conectores RJ45 categoría 6A blindados, aptos para terminación profesional en paneles y faceplates.	100	
CloudEngine S5731-H	Switch de capa 3 con 48 puertos Gigabit Ethernet + 4 uplinks 10GE, administrable, ideal para distribución en IDF.	4	
Grandstream UCM6208	IP PBX con 8 puertos FXO, hasta 800 usuarios, 50 llamadas simultáneas, soporte para SIP, voz, buzón y grabación.	1	
CloudEngine S6730-H	Switch core 10GE de alto rendimiento, 24 puertos 10GE, 4 uplinks 40GE, alta disponibilidad, redundancia y QoS.	1	
Bobinas UTP Cat 6A	Bobinas de cable UTP Cat 6A blindado de 305 metros, para cableado estructurado horizontal y backbone.	6	
APC Smart-UPS X 2000VA	UPS de 2000VA, línea interactiva, pantalla LCD, monitoreo inteligente, protección crítica para servidores y red.	2	
UPS 700VA	UPS de respaldo básico para IDFs, con regulación de voltaje y protección ante picos eléctricos.	5	

Gabinete mural 6U	Gabinete de pared con 6 unidades de rack, puerta de cristal templado, profundidad 479.5 mm, estructura reforzada color negro.	6	

4.6.2 Renovación de sistema CCTV

Por otra parte, dentro de la iniciativa de modernización tecnológica, otro de los puntos que se trató fue la renovación total del sistema de videovigilancia IP, que presentaba varias deficiencias relacionadas con la forma de gestionar el flujo de datos, el estado físico de los equipos y la sobrecarga en la red principal; como parte de la mejora y optimización, se diseñó una arquitectura dedicada y totalmente aislada para el sistema CCTV, soportada en una VLAN separada (192.168.30.x). Esta solución se desplegó con el objetivo de garantizar que siempre exista el ancho de banda necesario para permitir la transmisión continua de video y evitar cualquier interferencia con otros servicios de red. Además, esta estrategia busca facilitar la administración y el control de este sistema CCTV.

La nueva solución planteada en la Figura 4.16, donde se crea una arquitectura centralizada en la que todo el tráfico de las cámaras IP se dirige a un switch principal (SW1), el cual se conecta directamente al switch core del SITE. Desde este mismo punto de enlace se interconectan los grabadores NVR, un KVM para monitoreo y control y los enlaces de distribución hacia los diferentes IDFs ubicados en puntos estratégicos de la planta: control de calidad, subestación eléctrica, vigilancia, sala de máquinas, área de embarques y bodega. Cada IDF soporta una gran cantidad de cámaras IP alimentadas por switches PoE, simplificando enormemente el cableado y haciendo una instalación más limpia y reduciendo el número de fuentes de alimentación externas para cada dispositivo.

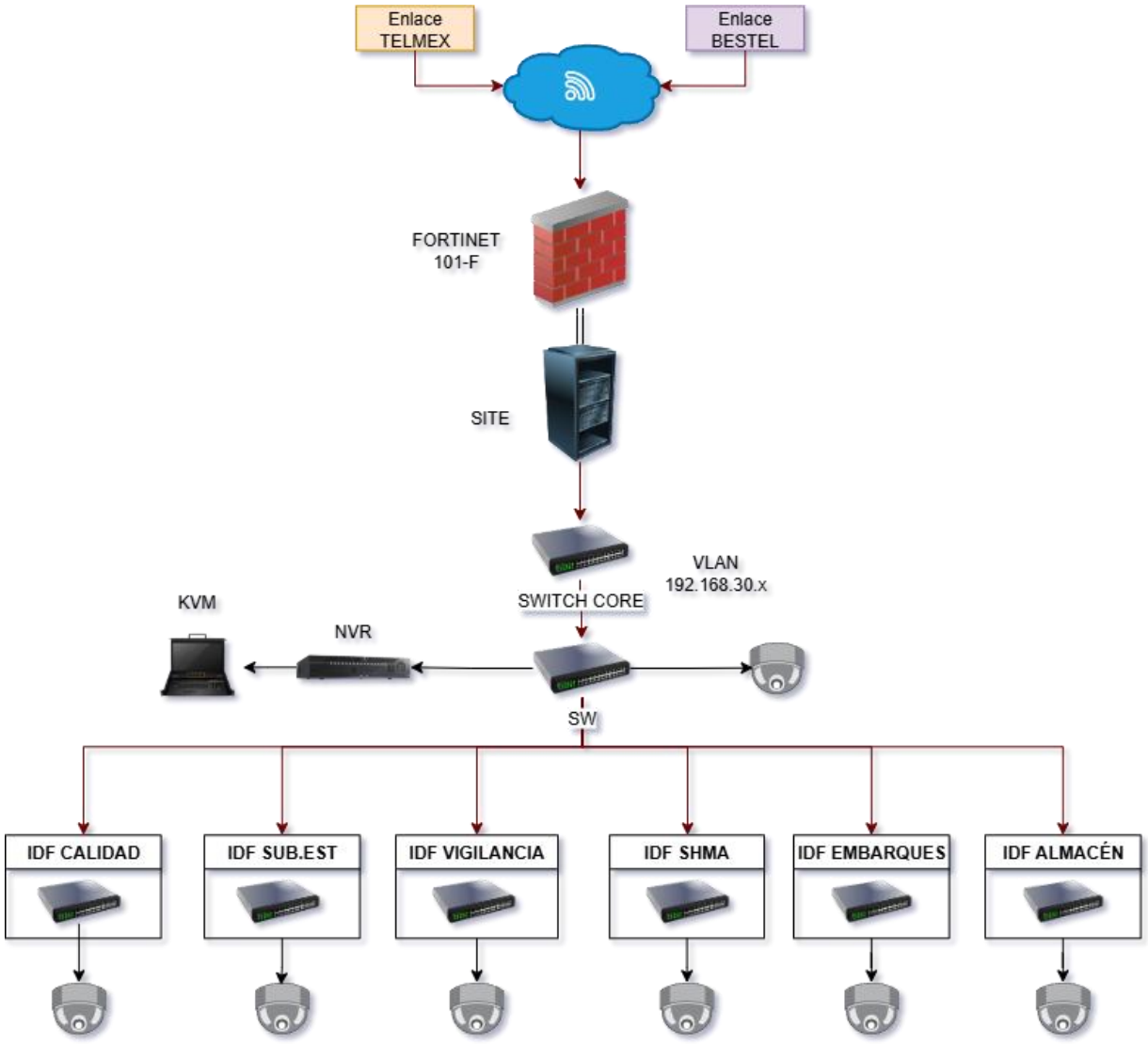


Figura 4.16 Diagrama de CCTV propuesto. Elaboración propia.

Es importante mencionar que esta red CCTV se apoya en el tendido de fibra óptica ya existente en la planta, pero que no se encontraba en uso. La solución propone su uso a través de enlaces dedicados con transceptores de medios, según la distancia del recorrido: fibra óptica multimodo para distancias cortas (menores a 550 m) y monomodo para distancias largas entre edificios o zonas de difícil acceso, garantizando alta velocidad, baja latencia y alta confiabilidad en la transmisión; esta infraestructura proporciona la capacidad para soportar cámaras de alta resolución, videovigilancia en vivo y grabación continua sin impactar el rendimiento de la red en general.

4.6.3 Propuesta VoIP

Por otro lado, en una propuesta completa de renovación tecnológica, se propuso además la renovación del sistema de telefonía, pasando de un sistema analógico obsoleto a uno moderno basado en Voz sobre IP (VoIP). Para ello se consideró la implementación de un conmutador IP Grandstream de última generación, el cual será capaz de controlar las comunicaciones internas y externas de la planta de manera eficiente, escalable y con múltiples funcionalidades avanzadas. Así mismo, esta solución se complementó con la contratación de troncales SIP que ofrece el operador Telmex, conectándose directamente a la red pública telefónica a través de enlaces digitales, mejorando la calidad de audio y reduciendo costos de llamadas, además de eliminar las restricciones físicas de la red analógica anterior.

El sistema está diseñado para asignar 39 extensiones internas, entre oficinas administrativas, operativas y puntos estratégicos de la planta. Para los teléfonos se eligieron dispositivos marca Grandstream, desde los modelos GRP2634 (teléfonos básicos de escritorio) hasta los modelos GXV3470 y GXV3480 (teléfonos multimedia con pantalla táctil para jefaturas y gerencia) y GAC2570 (teléfono para conferencias en salas de juntas), todos compatibles con SIP y totalmente compatibles con el conmutador Grandstream UCM.

El sistema está preparado para soportar tanto llamadas internas como externas, así como funcionalidades avanzadas tales como buzón de voz (correo de voz), desvíos automáticos, reglas de entrada/salida, grabación DVR de llamadas, presencia y agenda compartida. Esta solución permite controlar las comunicaciones de manera centralizada, mejorar la atención al cliente, la coordinación interna y permite futuras expansiones sin realizar cambios en la infraestructura física, ya que todo funciona sobre la red de datos y en una VLAN exclusiva para telefonía IP (192.168.10.x) con QoS, evitando interferencia con otras aplicaciones de red.

Para satisfacer las necesidades de comunicación interna y externa de las diferentes áreas de la organización, se determinó una distribución de teléfonos IP de acuerdo con la jerarquía operativa, la frecuencia de uso, las necesidades de movilidad y el tipo de interacción funcional. Para ello se definió un modelo escalonado, proporcionando terminales en función del perfil de usuario y el puesto que desempeñe: teléfonos básicos con múltiples líneas para personal operativo y administrativo; terminales multimedia para supervisores y jefaturas; equipos ejecutivos con cámara y pantalla táctil para dirección; y equipos especializados

para salas de juntas o entornos colaborativos. En la Tabla 4.12 se muestra la distribución de teléfonos IP por área y tipo de dispositivo, y en la Tabla complementaria 4.13 se especifican las características técnicas más relevantes de cada modelo, justificando su elección según sus capacidades funcionales.

Tabla 4.11 Modelos y distribución de los teléfonos IP

Área	***Tipo de Teléfono***	***Cantidad***
Dirección General	GXV3480	3
Vicedirección	GXV3470	1
Planeación y Logística	GXV3470	1
	GRP2634	3
Comercio Exterior	GXV3470	1
	GRP2634	2
Finanzas y Contabilidad	GXV3470	2
	GRP2634	2
Recursos Humanos	GXV3470	1
	GRP2634	1
Seguridad, Higiene y MA	GXV3470	1
	GRP2634	2
Calidad	GXV3470	1
	GRP2634	2
Mantenimiento	GXV3470	1
	GRP2634	1

Producción	GXV3470	1
	GRP2634	1
Almacén	GXV3470	1
	GRP2634	2
Comercial / Ventas	GXV3470	1
	GRP2634	3
Tecnologías de la Información	GXV3470	1
Salas de juntas / capacitación	GAC2570	4
	TOTAL	**39**

Tabla 4.12 Características técnicas de teléfonos IP seleccionados

Modelo	***Descripción***	***Características Técnicas Relevantes***	***Imagen***
GRP2634	Teléfono IP profesional de escritorio con 8 líneas.	✓ 8 líneas / 4 cuentas SIP ✓ 32 teclas BLF programables ✓ Pantalla LCD a color de 2.8" ✓ Audio HD con cancelación de eco ✓ PoE (IEEE 802.3af) y 2 puertos Gigabit ✓ Soporte para aprovisionamiento automático	
GXV3470	Teléfono multimedia IP para supervisores con pantalla táctil.	✓ Android 11 ✓ Pantalla táctil de 7" IPS (1280x800 px) ✓ Soporte para aplicaciones Android ✓ Wi-Fi de doble banda (2.4/5GHz), Bluetooth ✓ Cámara frontal 2 MP para videollamadas ✓ Soporte PoE y 2 puertos Gigabit RJ45 ✓ Salida HDMI	
GXV3480	Teléfono IP ejecutivo avanzado con capacidades de	✓ Android 11 ✓ Pantalla táctil de 8" (1280x800 px) ✓ Cámara frontal 2 MP ✓ Soporte para múltiples cuentas SIP	

	video y colaboración.	✓ Wi-Fi, Bluetooth, PoE ✓ Altavoces duales con cancelación de ruido ✓ Salida HDMI ✓ Soporte para apps Android profesionales	
GAC2570	Teléfono de conferencia IP para salas de juntas.	✓ Pantalla táctil de 7" (1024x600 px) ✓ 12 micrófonos 360° hasta 5 m ✓ Cancelación automática de eco (AEC) y supresión de ruido ✓ Wi-Fi, Bluetooth, PoE ✓ Puerto HDMI y USB-C ✓ - Soporte Android 10	

4.2.1 Definición y validación de los criterios de evaluación

Para verificar la efectividad del rediseño de la infraestructura tecnológica en la planta industrial, se definieron unos criterios de evaluación que permitirán medir el impacto real de la propuesta, desde un punto de vista técnico y desde el punto de vista del usuario; así mismo, la evaluación utiliza métricas tanto cuantitativas como cualitativas para analizar el rendimiento de la red, la telefonía IP y el sistema de videovigilancia. Además, se propone un enfoque comparativo, utilizando como línea base los valores obtenidos en la etapa de diagnóstico para compararlos antes vs. después de la implementación.

Desde el punto de vista técnico, se emplearán herramientas como NetSpot, SpeedTest e iPerf para determinar la velocidad, latencia, pérdida de paquetes y fuerza de señal (dBm) en una red inalámbrica. Estas pruebas se llevarán a cabo en áreas clave como oficinas, planta, vigilancia, mantenimiento, envíos y almacén. Además, se medirá la continuidad del sistema a través de la disponibilidad (uptime) posterior a la integración de sistemas UPS y la calidad funcional del sistema de videovigilancia (cobertura real, resolución, visión nocturna, PTZ y almacenamiento). Para telefonía IP se revisarán indicadores de calidad de llamada (QoS), latencia, jitter, servicios como correo de voz, desvíos y el uso de extensiones distribuidas en todas las áreas.

Adicional a los elementos técnicos, se realizarán encuestas de percepción a usuarios administrativos para recopilar su experiencia sobre la mejora que han sentido en la conectividad, calidad de llamadas, Wi-Fi, sistema de videovigilancia y confiabilidad en general; importante mencionar que estas encuestas se diseñaron en dos cuestionarios específicos: Encuesta de Evaluación de la Red Industrial y Telefonía IP y Encuesta de

Evaluación del Sistema de Videovigilancia IP. Ambas emplean escalas tipo Likert y preguntas abiertas para recolectar datos métricos y cualitativos. Los resultados que arrojen estos instrumentos serán analizados en el capítulo siguiente.

4.7 Síntesis

En este capítulo presentó de manera estructurada la propuesta metodológica que se siguió para el desarrollo del proyecto, desde el diagnóstico inicial hasta el diseño de una solución tecnológica integral. Mediante el estudio del entorno organizacional y la evaluación de la infraestructura tecnológica existente, se determinaron carencias significativas en términos de conectividad, segmentación lógica, seguridad, cobertura inalámbrica y videovigilancia. Sobre la base de estos resultados, se elaboró una propuesta de renovación integral, basada en estándares internacionales (TIA/EIA-568, IEEE 802.11, UIT, entre otros), que incorpora cableado estructurado categoría 6A, Wi-Fi 7, videovigilancia IP centralizada y telefonía VoIP; además, se definieron métricas objetivas de evaluación técnica y perceptual, apoyadas en herramientas especializadas (NetSpot, SpeedTest, iPerf) y encuestas a usuarios, que permitirán comparar el antes y el después de la intervención.

CAPÍTULO 5. Resultados

En este capítulo se presentan de forma organizada los resultados que se fueron obteniendo durante la renovación de la infraestructura tecnológica, optimizando la red y desplegando un sistema de telefonía VoIP segura; tras el diagnóstico y diseño planteado, se llevaron a cabo múltiples acciones técnicas por fases, las cuales fueron documentadas en campo con registros fotográficos, diagramas de red, mediciones de señal, comparativas antes/después.

Todos los resultados que se muestran a continuación dan respuesta a los objetivos planteados en la presente investigación, enmarcado en la metodología descrita en capítulos anteriores. Se utilizaron herramientas como NetSpot para mediciones de señal inalámbrica, pruebas de conectividad en VLANs y nodos críticos, pruebas de rendimiento en servicios de telefonía IP, priorizando la calidad de servicio (QoS), latencia, cobertura, estabilidad de red y seguridad.

Además, se adjuntan evidencias fotográficas de los procesos de instalación, cableado, montaje de racks, configuración de equipos, segmentación de red y puesta en marcha de servicios para certificar técnicamente cada etapa del proyecto, además, se hace una comparación entre el estado inicial diagnosticado y el estado posterior a la implementación, con encuestas a usuarios para medir la percepción de mejora y satisfacción general.

5.1 Resultados de la implementación tecnológica

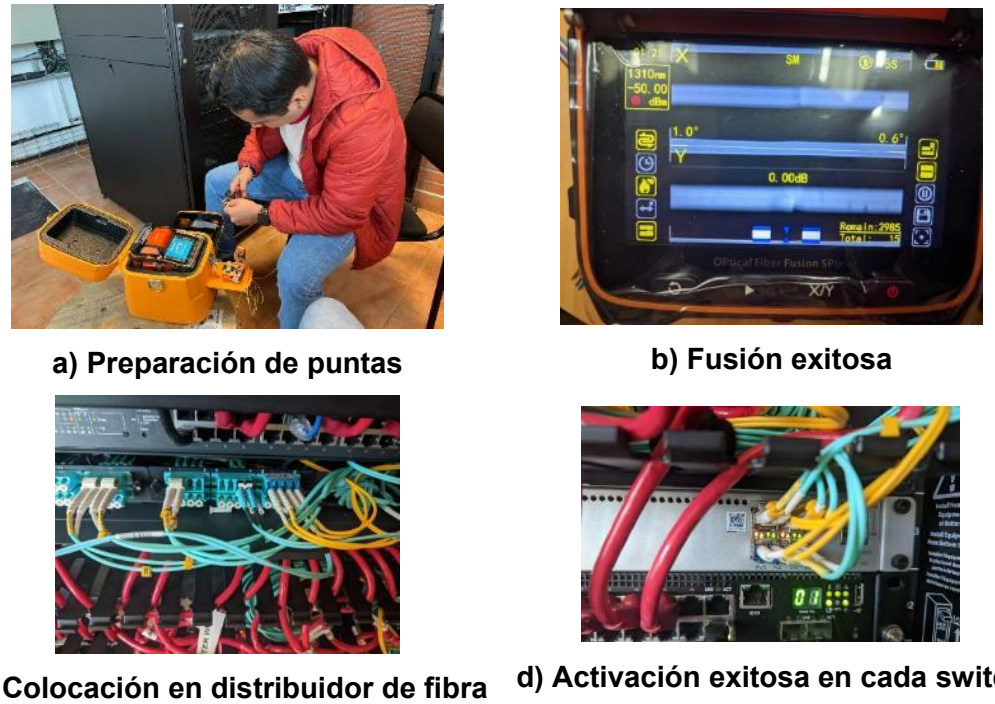
5.1.1 Red inalámbrica (Wi-Fi)

Como parte esencial para garantizar el funcionamiento óptimo de la nueva red inalámbrica basada en Wi-Fi 7, se llevó a cabo la activación de los tramos de fibra óptica monomodo y multimodo, según el tipo de infraestructura existente en cada recorrido, conectando el site principal con los IDF (Intermediate Distribution Frames) ubicados en oficinas y áreas de producción.

La Figura 5.1 (a) muestra la preparación de las puntas de fibra previo al proceso de empalme, mientras que en la Figura 5.1 (b) se observa la fusión exitosa realizada mediante una fusionadora especializada, garantizando enlaces con baja atenuación y alta confiabilidad. Posteriormente, los extremos fusionados fueron organizados y alojados en distribuidores ópticos, como se aprecia en la Figura 5.1 (c), permitiendo una gestión

ordenada y segura del cableado de fibra. Finalmente, en la Figura 5.1 (d) se evidencia la activación correcta de los enlaces ópticos en cada switch administrable mediante módulos Mini-GBIC (SFP), confirmando la comunicación efectiva entre el site principal y los nodos remotos.

Esta estructura de conexión punto a punto por fibra óptica asegura una transmisión estable y de alta velocidad, indispensable para soportar la operación de los nuevos puntos de acceso inalámbricos, así como los servicios críticos de datos, voz y video en toda la infraestructura.



a) Preparación de puntas

b) Fusión exitosa

c) Colocación en distribuidor de fibra

d) Activación exitosa en cada switch

Figura 5.1 Proceso de activación de fibras ópticas.

Resultados de cableado e instalación de puntos de acceso

Una vez concluida la activación de los tramos de fibra óptica, se procedió a la instalación de los switches de acceso marca Huawei en cada uno de los IDF, con el objetivo de recibir la señal de red proveniente del site principal a través de módulos Mini-GBIC (SFP). Estos switches funcionan como nodos de distribución, permitiendo la alimentación de red y energía PoE necesaria para la operación de los puntos de acceso Wi-Fi 7.

En la Figura 5.2 (a) se muestra la instalación y organización del cableado dentro de los IDF, donde se observa la correcta gestión de fibras y enlaces UTP, asegurando orden, accesibilidad y facilidad de mantenimiento. Posteriormente, desde cada switch se realizó el

tendido de cableado estructurado UTP categoría 6A hacia las áreas operativas, como se aprecia en la Figura 5.2 (b), garantizando enlaces de alto desempeño y baja susceptibilidad al ruido electromagnético propio del entorno industrial.

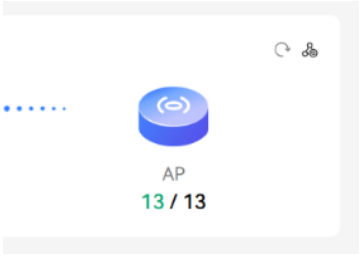
La Figura 5.2 (c) evidencia la instalación física de los Access Points, los cuales fueron montados estratégicamente en techo o pared conforme al diseño de cobertura definido en la etapa de planeación. Cada dispositivo fue alimentado mediante PoE y correctamente etiquetado según su ubicación. Finalmente, en la Figura 5.2 (d) se muestra la administración y validación exitosa de los puntos de acceso desde la plataforma Huawei eKit, confirmando la correcta detección, configuración y operación de los equipos instalados.

Este procedimiento estandarizado fue replicado en todos los IDF de la planta, asegurando una cobertura inalámbrica uniforme, estable y de alto rendimiento, acorde a los requerimientos operativos y a la infraestructura Wi-Fi 7 propuesta.

a) Instalación y organización en IDF

b) Tendido de cable en producción

c) Instalación de los AP



d) Administración exitosa en el panel Huawei Ekit

Figura 5.2 Proceso de instalación de los puntos de acceso Wifi.

Validación de cobertura inalámbrica – Mapas de calor

Como parte del proceso de validación de la red Wi-Fi implementada, se generaron mapas de calor con la herramienta especializada WiFi Heat Map, los cuales permiten visualizar gráficamente la intensidad de señal en diferentes zonas del sitio. Esta técnica se empleó para contrastar los resultados reales obtenidos en campo contra las simulaciones de cobertura previamente realizadas en el software Ruijie, corroborando que ambas concordaban de forma altamente precisa.

Se presentan a continuación los dos mapas de calor más representativos, correspondientes a las zonas con mayor densidad de usuarios: oficinas administrativas (véase Figura 5.3) y área de producción (véase Figura 5.4).

Figura 5.3 Resultado del mapa de calor en oficinas administrativas. Elaboración propia con base en planos internos de la empresa.

En esta imagen se observa una distribución uniforme y óptima de la señal inalámbrica, con intensidad mayor a -50 dBm en prácticamente la totalidad del espacio. La colocación estratégica de los Access Points en pasillos centrales permitió una cobertura eficiente para todos los cubículos, oficinas privadas, salas de juntas y recepción, manteniendo márgenes seguros de señal incluso en las esquinas del edificio.

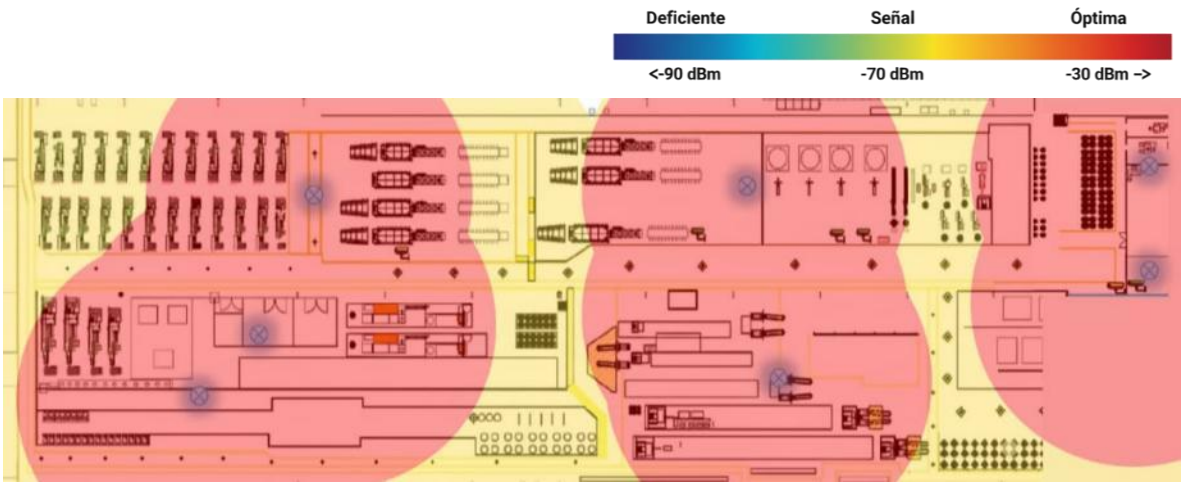


Figura 5.4 Mapa de calor en planta de producción. Elaboración propia con base en planos internos de la empresa.

En el área industrial, a pesar de las posibles interferencias electromagnéticas y estructuras metálicas, el mapa muestra una cobertura adecuada, predominando áreas de señal “óptima” y “estable” (entre -30 y -70 dBm), con muy pocos puntos en nivel “deficiente”. La correcta ubicación de los Access Points en intersecciones principales y zonas abiertas aseguró un alcance efectivo en líneas de producción, oficinas, almacenes y zonas de inspección.

Ambos mapas evidencian el cumplimiento de los criterios de diseño y validan la calidad de implementación. Esta validación gráfica se complementa con las mediciones técnicas de velocidad y latencia, que se presentan en el siguiente apartado.

Resultados de pruebas de velocidad y rendimiento inalámbrico

Después de la instalación de los Access Points Wi-Fi 7 y la activación de la red de fibra óptica y switches de acceso, se realizaron mediciones técnicas con herramientas especializadas como Speedtest, documentadas en tablas y analizadas individualmente según la distancia entre el punto de medición y el AP más cercano. A continuación, se presentan los resultados comparando la situación previa (diagnóstico inicial) con el desempeño posterior a la implementación; se midieron tres parámetros clave: velocidad de descarga, velocidad de subida y latencia (ping) dentro de las siguientes dos zonas principales.

Mediciones en oficinas administrativas

5 metros de distancia

Los resultados obtenidos en la Tabla 5.1 reflejan un desempeño sobresaliente. Las velocidades de descarga oscilan entre los 151.5 Mbps y 170.0 Mbps, mientras que las de subida varían entre 121.7 Mbps y 129.9 Mbps. El ping se mantiene en valores muy bajos, con un promedio de apenas 4.5 ms, lo cual es ideal para aplicaciones en tiempo real como llamadas VoIP, videoconferencias o transferencia de archivos pesados.

Tabla 5.1 Resultados de mediciones en oficinas 5 metros de distancia

#	Descarga (Mbps)	Subida (Mbps)	Ping (ms)
1	169.4	126.2	3
2	166.2	122.5	5
3	158.8	124.1	6
4	151.5	121.7	5
5	165.3	127.8	6
6	160.6	124.4	4
7	162.7	126.5	3
8	159.2	123.8	4
9	168.6	128.6	5
10	170.0	129.9	4

10 metros de distancia

En esta Tabla 5.2, se aprecia una leve disminución respecto a los 5 metros, como es natural por la propagación de señal. Las velocidades de descarga van de 138.0 Mbps a 158.9 Mbps, y las de subida entre 110.8 Mbps y 122.7 Mbps. La latencia promedio sube ligeramente, con valores entre 6 y 10 ms, pero sigue siendo completamente aceptable y funcional para todos los servicios digitales.

Tabla 5.2 Resultados de mediciones en oficinas 10 metros de distancia

#	Descarga (Mbps)	Subida (Mbps)	Ping (ms)
1	158.9	120.4	7
2	145.2	118.3	9
3	149.8	122.7	6
4	151.3	117.0	7
5	154.7	120.6	8
6	139.4	115.3	7
7	143.2	110.8	9
8	138.0	116.4	10
9	147.8	118.5	8
10	140.5	114.1	6

15 metros de distancia

En esta última Tabla 5.3 se puede notar una mayor degradación natural de la señal, pero aún dentro de parámetros aceptables. Las velocidades de descarga fluctúan entre 119.5 Mbps y 138.0 Mbps, y las de subida entre 100.4 Mbps y 114.5 Mbps. El ping oscila entre 9 y 12 ms.

Tabla 5.3 Resultados de mediciones en oficinas 5 metros de distancia

#	Descarga (Mbps)	Subida (Mbps)	Ping (ms)
1	134.7	112.3	9
2	123.6	108.8	10
3	126.1	105.5	11
4	120.9	100.4	12
5	130.2	110.6	9
6	138.0	114.5	10
7	119.5	106.7	11
8	125.4	104.1	12
9	133.7	109.0	10
10	122.5	102.6	11

5.1.1.1 Mediciones en producción

Las siguientes mediciones se realizaron en la planta de producción, donde las condiciones ambientales son más exigentes debido a la presencia de maquinaria, estructuras metálicas, equipos eléctricos y otras fuentes de interferencia. Aun así, los resultados muestran un rendimiento robusto gracias a la correcta planificación de los puntos de acceso y a la infraestructura de red implementada en alturas adecuadas.

10 metros de distancia

Como se observa en la Tabla 5.4, las velocidades de descarga se mantienen entre 134.5 Mbps y 152.6 Mbps, mientras que las velocidades de subida oscilan entre 107.8 Mbps y 120.5 Mbps. El ping, aunque ligeramente más alto que en oficinas, permanece entre 8 y 12 ms, valores completamente funcionales para servicios industriales conectados.

Tabla 5.4 Resultados de mediciones en producción 10 metros de distancia

#	Descarga (Mbps)	Subida (Mbps)	Ping (ms)
1	152.6	118.3	9
2	142.3	120.5	10
3	138.0	111.2	12
4	150.1	115.7	8
5	145.8	116.4	11
6	134.5	107.8	12
7	139.3	112.5	10
8	141.6	113.0	9
9	147.2	119.1	8
10	137.8	108.9	12

20 metros de distancia

En esta distancia intermedia, las velocidades de descarga se encuentran entre 118.2 Mbps y 138.0 Mbps, y las de subida entre 93.7 Mbps y 110.7 Mbps. El ping se encuentra en el rango de 11 a 16 ms, aún dentro de valores aceptables para el entorno industrial (Tabla 5.5).

Aunque se comienza a notar una ligera degradación natural por la distancia, las velocidades siguen siendo superiores a los 100 Mbps y permiten la operación de cámaras IP, terminales

de escaneo, acceso a sistemas internos y otras aplicaciones típicas del entorno de producción.

Tabla 5.5 Resultados de mediciones en producción 20 metros de distancia

#	Descarga (Mbps)	Subida (Mbps)	Ping (ms)
1	132.2	105.1	12
2	125.6	104.3	14
3	138.0	110.7	13
4	129.9	101.8	11
5	130.7	102.5	14
6	118.2	95.4	16
7	124.4	98.3	13
8	121.6	93.7	15
9	135.3	108.4	12
10	119.7	97.1	13

30 metros de distancia

Este escenario representa una gran distancia dentro del entorno productivo. Las velocidades de descarga se mantienen entre 102.4 Mbps y 115.3 Mbps, y las de subida entre 80.8 Mbps y 94.6 Mbps. El ping sube ligeramente, oscilando entre 14 y 18 ms (Tabla 5.6).

A pesar de tratarse de la distancia más crítica, los valores medidos se mantienen completamente operativos. La red conserva una cobertura adecuada y sin interrupciones, lo cual demuestra la correcta ubicación de los Access Points y la potencia de la tecnología Wi-Fi 7.

Tabla 5.6 Resultados de mediciones en producción 30 metros de distancia

#	Descarga (Mbps)	Subida (Mbps)	Ping (ms)
1	115.3	93.4	14
2	108.7	88.3	15
3	110.5	90.1	18
4	113.2	94.6	17
5	111.9	89.9	14

6	104.6	84.2	17
7	109.8	86.3	15
8	105.7	83.6	18
9	107.6	87.1	16
10	102.4	80.8	17

Los resultados obtenidos muestran mejoras significativas respecto a las condiciones iniciales en la fase de diagnóstico, en las que las velocidades promedio apenas superaban los 50 Mbps y se registraban pérdidas de señal y latencias superiores a 20 ms en varios sectores. En el siguiente apartado se presentará la comparativa completa entre las condiciones previas y las actuales, para evidenciar la mejora lograda con esta implementación.

5.1.2 Comparativa de resultados promedio (antes vs después)

Oficinas administrativas

A 5 metros de distancia

Como se muestra en la Tabla 5.7, existe un incremento de más del 160% en velocidad de descarga y más del 230% en subida, además de una reducción de latencia del 78%, alcanzando un rendimiento óptimo. Esta mejora garantiza fluidez en videollamadas, transferencia de archivos pesados, navegación y uso de sistemas internos en tiempo real.

Tabla 5.7 Comparativa a 5 metros de distancia en oficinas

	ANTES (DIAGNÓSTICO)	DESPUÉS (IMPLEMENTACIÓN)
Velocidad promedio de descarga	62.10 Mbps	163.7 Mbps
Velocidad promedio de subida	37.16 Mbps	125.5 Mbps
Ping promedio	20.80 ms	4.5 ms

A 10 metros de distancia

Por otra parte, la Tabla 5.8 muestra que las velocidades se duplicaron en descarga y triplicaron en subida, mientras que la latencia fue reducida a menos de un tercio. Esta mejora representa una conectividad más estable para usuarios a distancia intermedia, que suelen presentar problemas en redes mal diseñadas. En este caso, se garantiza un servicio de calidad.

Tabla 5.8 Comparativa a 10 metros de distancia en oficinas

	ANTES (DIAGNÓSTICO)	DESPUÉS (IMPLEMENTACIÓN)
Velocidad promedio de descarga	59.92 Mbps	148.9 Mbps
Velocidad promedio de subida	37.84 Mbps	118.0 Mbps
Ping promedio	22.20 ms	7.1 ms

Si bien hay una leve reducción respecto a los 5 metros, el rendimiento sigue siendo excelente. La señal mantiene una alta calidad, sin presencia de latencias críticas ni degradaciones importantes.

A 15 metros de distancia

A pesar de ser la distancia más lejana en oficina, los datos muestran un incremento del 150% en descarga y del 227% en subida, con una latencia reducida en más de 15 ms, lo cual representa una mejora decisiva (Tabla 5.9). Esta zona, que en el diagnóstico presentaba riesgo de saturación, ahora se comporta dentro de parámetros óptimos.

Se observa una disminución proporcional por la distancia, sin embargo, se mantienen velocidades por encima de los 100 Mbps y una latencia aún adecuada para aplicaciones en tiempo real. La red sigue siendo estable y confiable para tareas administrativas y de comunicación.

Tabla 5.9 Comparativa a 15 metros de distancia en oficinas

	ANTES (DIAGNÓSTICO)	DESPUÉS (IMPLEMENTACIÓN)
Velocidad promedio de descarga	50.99 Mbps	127.5 Mbps
Velocidad promedio de subida	32.87 Mbps	107.5 Mbps
Ping promedio	26.10 ms	10.5 ms

Las comparativas demuestran que la implementación de Wi-Fi 7 ha mejorado de forma drástica y comprobable el rendimiento de la red en oficinas administrativas, logrando velocidades superiores a 100 Mbps en todos los casos, y latencias por debajo de los 11 ms incluso a mayores distancias.

Área de producción

A 10 metros de distancia

En la Tabla 5.10 se comparan las velocidades de descarga y subida, las cuales se multiplicaron por más de tres veces, y el ping fue reducido en un 72%. Esta mejora garantiza conectividad estable para aplicaciones como cámaras IP, ERP, terminales industriales y servicios en tiempo real. A pesar del entorno con maquinaria pesada y posibles interferencias, los resultados fueron sobresalientes.

Tabla 5.10 Comparativa a 10 metros de distancia en producción

	ANTES (DIAGNÓSTICO)	DESPUÉS (IMPLEMENTACIÓN)
Velocidad promedio de descarga	38.72 Mbps	143.9 Mbps
Velocidad promedio de subida	25.91 Mbps	114.3 Mbps

Ping promedio	36.60 ms	10.1 ms

Este entorno, con mayor interferencia electromagnética y presencia de maquinaria, aún logra mantener una señal robusta. Las velocidades superan el doble del rendimiento anterior, que rondaba los 60 Mbps en las mejores condiciones.

A 20 metros de distancia

Incluso en zonas intermedias, la mejora fue notable. La velocidad de descarga se triplicó y la de subida se cuadruplicó. La latencia se mantuvo por debajo de los 14 ms, un valor adecuado para ambientes productivos donde se requiere precisión y estabilidad (Tabla 5.11). Esto demuestra que la red mantiene su eficiencia con distancias medias y barreras físicas presentes.

Tabla 5.11 Comparativa a 20 metros de distancia en producción

	ANTES (DIAGNÓSTICO)	DESPUÉS (IMPLEMENTACIÓN)
Velocidad promedio de descarga	38.04 Mbps	127.6 Mbps
Velocidad promedio de subida	26.62 Mbps	101.7 Mbps
Ping promedio	34.80 ms	13.3 ms

Aunque hay una degradación por distancia, las métricas siguen siendo superiores a los estándares previos. La subida se mantiene por encima de 100 Mbps.

A 30 metros de distancia

La Tabla 5.12 muestra la comparativa en la zona más lejana del AP, donde importa que la señal aún sea perceptible, y aun así la red logró velocidades superiores a 100 Mbps en descarga y más de 85 Mbps en subida. El ping fue reducido en más de 20 ms.

Tabla 5.12 Comparativa a 30 metros de distancia en producción

	ANTES (DIAGNÓSTICO)	DESPUÉS (IMPLEMENTACIÓN)
Velocidad promedio de descarga	31.12 Mbps	109.0 Mbps
Velocidad promedio de subida	21.36 Mbps	87.8 Mbps
Ping promedio	38.40 ms	16.1 ms

Incluso en el peor escenario de distancia dentro de planta, las velocidades se mantienen de forma óptima. La latencia se acerca a los 17 ms, límite aceptable para servicios interactivos. Este comportamiento valida la correcta ubicación de los Access Points y la eficiencia de la red Wi-Fi 7 frente a entornos exigentes.

La implementación de la nueva red inalámbrica ha resultado en una mejora sustancial de la cobertura, velocidad y latencia en toda la empresa. Las oficinas administrativas experimentan un servicio prácticamente sin pérdida de calidad a lo largo de 15 metros. En el caso de la planta, incluso con obstáculos físicos y mayor interferencia, la red mantiene una operación superior a los 100 Mbps, algo que era imposible con la infraestructura anterior.

Esto representa un aumento de más del 150% en velocidad promedio y una reducción de la latencia a menos de la mitad, mejorando la productividad, el acceso a sistemas como Business Central, el desempeño de llamadas internas VoIP y la experiencia del usuario en general.

5.1.2 Sistema de videovigilancia IP (CCTV)

Resultados de activación de fibra óptica

Paralelamente a la implementación de la red inalámbrica, se llevó a cabo la activación de la infraestructura necesaria para el correcto funcionamiento del sistema de videovigilancia IP (CCTV). Este proceso contempló la habilitación de enlaces de fibra óptica dedicados exclusivamente para la red de videovigilancia, garantizando el aislamiento del tráfico, la

estabilidad de la transmisión y el desempeño requerido para el envío continuo de video en tiempo real.

En la Figura 5.5 (a) se muestra la activación de fibras ópticas existentes en los IDF, donde se realizaron las fusiones correspondientes con pigtails y su correcta organización dentro de los distribuidores ópticos. De manera complementaria, en la Figura 5.5 (b) se observa la activación de los enlaces de fibra en el site principal, los cuales permiten concentrar el tráfico de videovigilancia proveniente de las diferentes áreas de la planta.

Los enlaces ópticos fueron conectados a switches de acceso dedicados para CCTV mediante módulos Mini-GBIC (SFP), como se aprecia en la Figura 5.5 (c), donde los indicadores de estado confirman la correcta activación y operación de los enlaces. Esta arquitectura permite asegurar una comunicación confiable entre las cámaras IP, los equipos de grabación y los sistemas de monitoreo centralizados.

Cabe destacar que, para futuras ampliaciones del sistema, se dispone de fibra óptica adicional, pigtails, adaptadores y módulos GBIC en stock, lo que facilita la expansión de la red CCTV sin afectar la infraestructura existente.

a) Activación de fibras existentes IDF

b) Activación de fibras en el SITE

c) Indicadores de señal exitosa en switch principal SITE

Figura 5.5 Resultados de activación de fibras ópticas para CCTV.

5.1.3 Resultados de simulación, cableado e instalación de cámaras POE

Además, como parte del rediseño completo de la infraestructura tecnológica, se simuló con la herramienta Ruijie Planner la instalación de cámaras de videovigilancia para confirmar la cobertura visual en las áreas críticas de la planta industrial por lo que estas simulaciones optimizaron la ubicación de los dispositivos en términos de ángulos de visión, obstrucciones estructurales, distancias focales y objetivos de vigilancia específicos.

Las áreas principales que abarcaron el diseño fueron: oficinas administrativas, nave de producción, zona de embarques, vigilancia perimetral, área lateral de básculas y estacionamiento exterior. En algunos casos se planteó la sustitución a modo de "uno por uno" de cámaras ya existentes, en otros se plantearon relocalizaciones tácticas o la adición de nuevos puntos de control, en respuesta a puntos negros o zonas de riesgo identificadas en el análisis inicial.

La solución incluye 64 cámaras IP de distintos tipos en función de la necesidad de cobertura: bullet para pasillos y accesos, domos motorizados (PTZ) para áreas extensas con necesidad de paneo y zoom, y ojo de pez (eyefish 180°) para interiores o salas de control donde se necesita visión panorámica; este nuevo diseño proporciona una cobertura total, minimizando los puntos ciegos y mejorando la capacidad de vigilancia continua en horario laboral y nocturno.

Simulación CCTV

La Figura 5.6 muestra la simulación de cobertura de videovigilancia en las oficinas administrativas. El diseño prioriza la supervisión de accesos, pasillos principales y áreas de circulación interna, garantizando una cobertura visual continua sin puntos ciegos relevantes. La distribución de cámaras permite un control efectivo del flujo de personal y visitantes, así como la protección de activos y áreas sensibles, manteniendo ángulos de visión adecuados aun en espacios cerrados y con divisiones arquitectónicas.

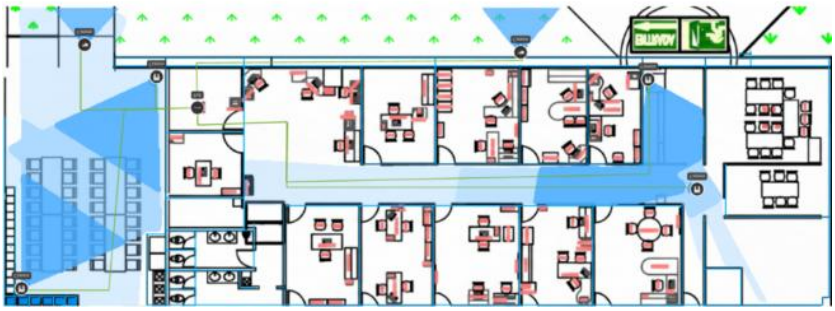


Figura 5.6 Simulación de cobertura de videovigilancia en oficinas administrativas. Elaboración propia con base en planos internos de la empresa.

En la Figura 5.7 se presenta la simulación de videovigilancia en la nave de producción, una de las áreas críticas por su tamaño, densidad operativa y valor de los activos. La ubicación estratégica de las cámaras permite una cobertura amplia de líneas de proceso, zonas de operación y pasillos industriales, considerando la presencia de maquinaria, estructuras metálicas y obstáculos visuales. Este diseño facilita la supervisión operativa, el análisis de incidentes y el reforzamiento de la seguridad laboral.

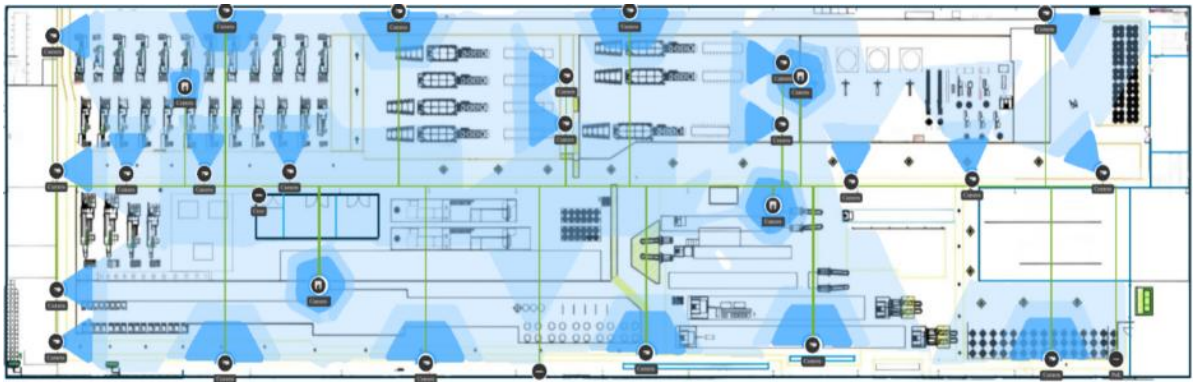


Figura 5.7 Simulación de cobertura de videovigilancia en planta de producción. Elaboración propia con base en planos internos de la empresa.

La Figura 5.8 corresponde a la simulación de cobertura en el área de embarques. En esta zona, la videovigilancia se enfocó en la supervisión de maniobras de carga y descarga, control de mercancía, accesos a andenes y circulación de montacargas. La cobertura proyectada permite un monitoreo efectivo de procesos logísticos, reduciendo riesgos de pérdidas, errores operativos o incidentes durante la manipulación de productos.

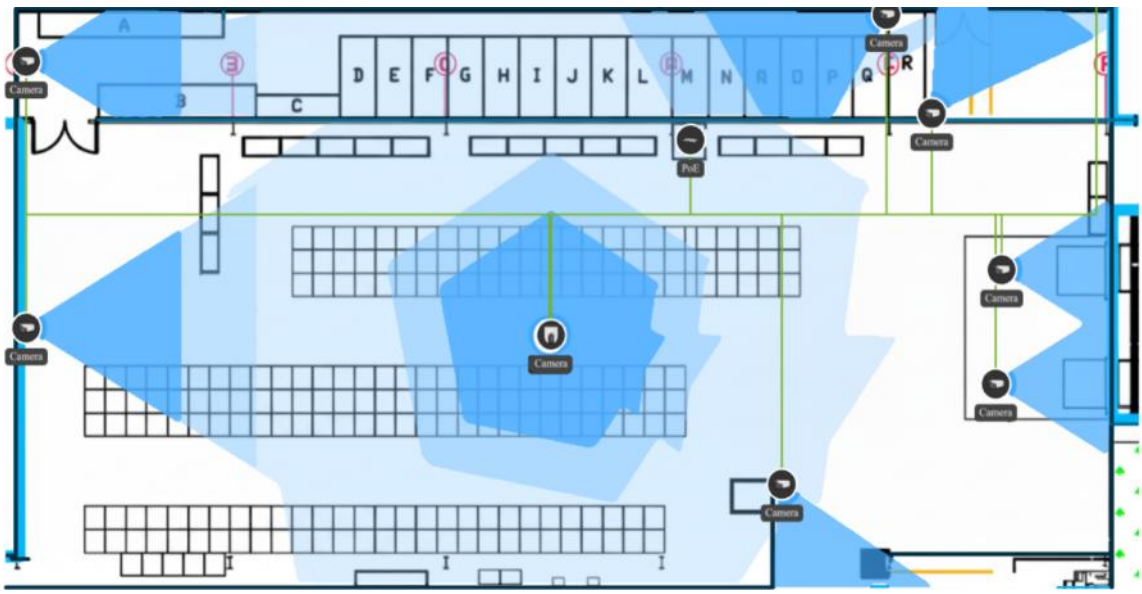


Figura 5.8 Simulación de cobertura de videovigilancia en zona de embarques. Elaboración propia con base en planos internos de la empresa.

La Figura 5.9 muestra la simulación de cobertura en el área de vigilancia y accesos principales. El diseño prioriza el control visual de entradas, salidas y zonas de control de personal y visitantes, permitiendo una identificación clara de movimientos y eventos relevantes. La disposición de las cámaras asegura una supervisión continua tanto en interiores como en zonas de transición hacia el exterior, fortaleciendo la seguridad perimetral de la instalación.

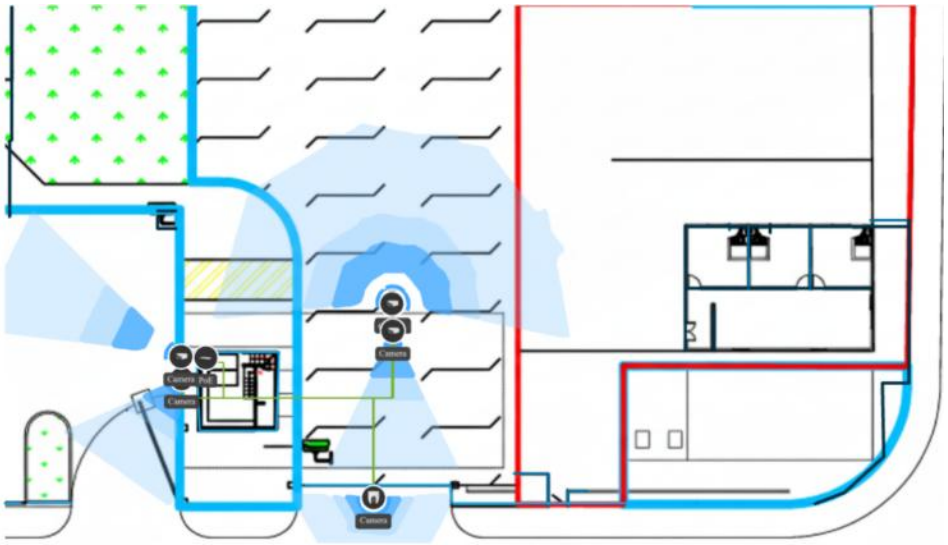


Figura 5.9 Simulación de cobertura de videovigilancia en zona de caseta y entradas. Elaboración propia con base en planos internos de la empresa.

La Figura 5.10 presenta la simulación de videovigilancia en el área lateral y de báscula. En esta zona, la cobertura se orienta a la supervisión de pesaje, tránsito vehicular y movimientos de carga, garantizando visibilidad completa de las operaciones. La ubicación de las cámaras permite registrar eventos clave relacionados con el ingreso y salida de unidades, aportando evidencia visual para control operativo y auditorías internas.

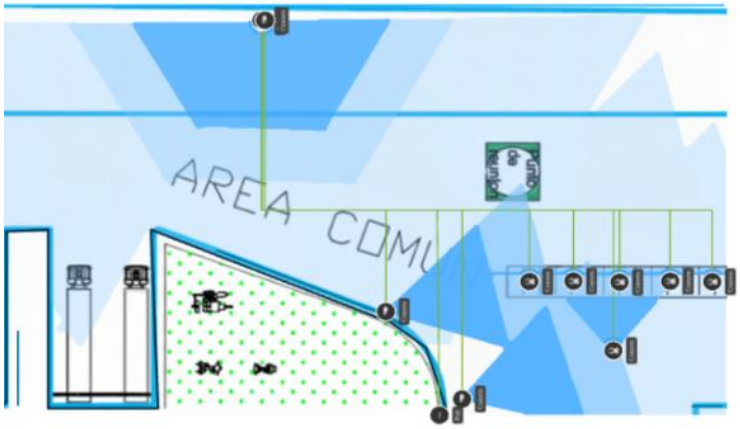


Figura 5.10 Simulación de cobertura de videovigilancia en básculas. Elaboración propia con base en planos internos de la empresa.

Finalmente, la Figura 5.11 muestra la simulación de cobertura en la parte frontal del complejo y el estacionamiento exterior. El diseño asegura una cobertura amplia de áreas abiertas, accesos vehiculares y zonas comunes, permitiendo la detección temprana de incidentes, control de vehículos y apoyo a la seguridad patrimonial. La cobertura proyectada reduce significativamente los puntos ciegos en zonas exteriores, tanto en condiciones diurnas como nocturnas.

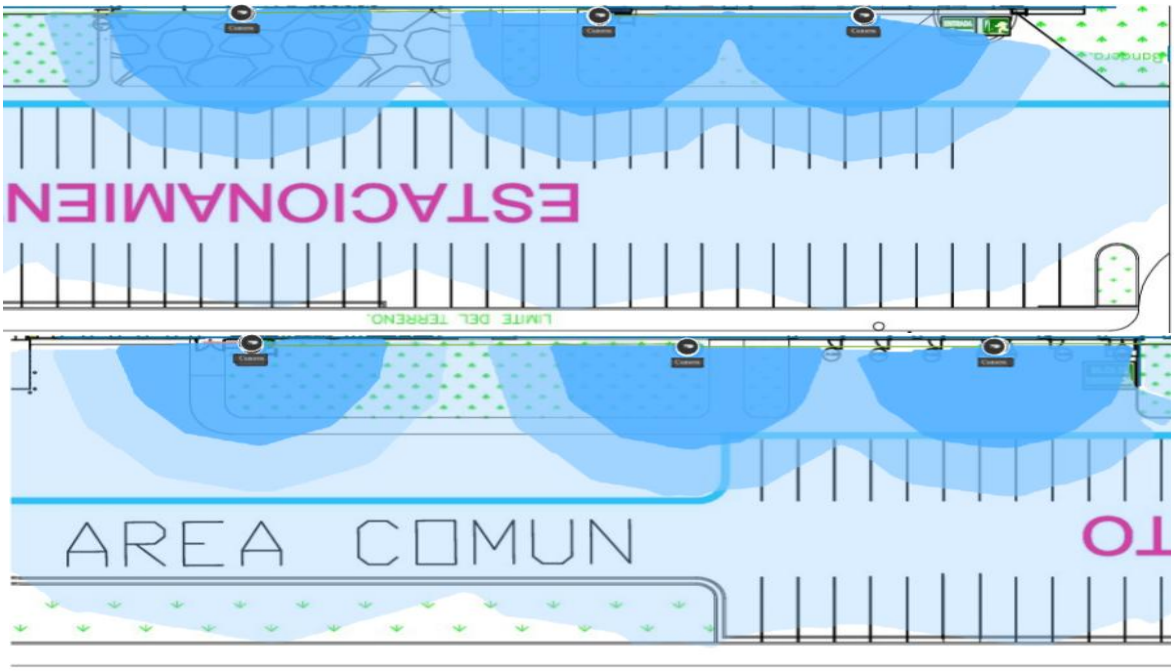


Figura 5.11 Simulación de cobertura de videovigilancia en estacionamiento. Elaboración propia con base en planos internos de la empresa.

Por otra parte, en la Tabla 5.13 se resumen los modelos de cámaras IP elegidos para el nuevo sistema de videovigilancia, agrupándolas por tipo, función y especificaciones técnicas de interés, por lo que, cada modelo se seleccionó en función de especificaciones como resolución, ángulo de visión, tipo de lente, resistencia a la intemperie (IP66), funciones inteligentes (seguimiento automático o detección por IA) y compatibilidad nativa con grabadores Hikvision y software de administración remota. Esta combinación de dispositivos puede dar solución a necesidades perimetrales, interiores, grandes áreas, accesos críticos y puntos ciegos preexistentes.

Tabla 5.13 Distribución de cámaras IP propuestas por tipo funcional

Tipo de cámara	Modelo / Nombre	Descripción técnica	Cantidad	Imagen (referencial)
Bullet (visión fija)	DS-2CD1T83G2-LIU(F)	Cámara IP tipo bullet de 8MP (4K), lente fija de 4 mm, dual light, micrófono integrado, visión en color día/noche, carcasa exterior resistente.	24	
Bullet 180° (dual lens)	DS-2CD2T87G2P-LSU/SL	Cámara bullet IP con doble lente y visión panorámica de 180°, resolución 5120x1440, IR, ColorVu, micrófono y luz estroboscópica, IP67.	16	
Domo 180° (dual lens)	DS-2CD2T87G2P-LSU/SL	Cámara domo IP con doble lente panorámica 180°, idénticas capacidades al modelo bullet pero en formato antivandálico para interiores o accesos.	6	
Fisheye 360°	Fisheye IP 8 MP Exterior	Cámara IP ojo de pez de 8 MP con cobertura de 360°, PoE, visión envolvente para interiores o áreas amplias, carcasa exterior.	8	
PTZ (motorizada)	ColorVu PTZ 8 MP 12X	Cámara domo IP PTZ de 8MP con zoom óptico 12X, IR, luz blanca, seguimiento automático, alarma sonora, luz estroboscópica, resistencia IK10/IP66.	10	

El planteamiento de rediseño del sistema de videovigilancia garantiza una cobertura completa, eficiente y técnicamente respaldada. La disponibilidad de diferentes tipos de cámaras, como bullet, domo panorámicas, fisheye, PTZ, permite dar respuesta exacta a las necesidades operativas y de seguridad de cada área en particular. Esta diversidad de dispositivos no solo amplía la capacidad de vigilancia en tiempo real,

sino que también permite optimizar el uso de recursos, utilizando lentes panorámicos en áreas abiertas y funciones de auto seguimiento inteligente en puntos de acceso clave; de igual modo importante destacar que la estandarización de equipos y dispositivos en el ecosistema Hikvision permite una gestión centralizada, escalabilidad a futuro y una integración transparente con los sistemas de almacenamiento, red y respaldo ya considerados en la propuesta inicial.

Posteriormente, se llevó a cabo la instalación del cableado estructurado desde cada switch TP-Link ubicado en los IDF hasta la ubicación específica de cada cámara IP, conforme al plan de despliegue definido en las etapas previas del proyecto. El proceso inició con el canalizado del cableado mediante sistemas de sujeción adecuados, como se observa en la Figura 5.12 (a), garantizando protección mecánica, orden y cumplimiento de criterios de seguridad.

El tendido del cable UTP categoría 6A se realizó en áreas productivas y de difícil acceso utilizando escalerillas y apoyos elevados, tal como se aprecia en la Figura 5.12 (b), asegurando que ningún tramo excediera los 100 metros lineales establecidos por el estándar de cableado horizontal. Esta práctica permitió mantener la calidad de transmisión de datos y la correcta alimentación PoE de las cámaras IP instaladas.

La Figura 5.12 (c) muestra la instalación física de las cámaras IP en sus ubicaciones finales, considerando ángulos de visión, cobertura efectiva y reducción de puntos ciegos en áreas críticas. Finalmente, en la Figura 5.12 (d) se presenta un ejemplo de visualización exitosa desde el sistema NVR, confirmando la correcta comunicación entre las cámaras, los switches de borde y los sistemas de monitoreo centralizados.

La aplicación sistemática de este procedimiento en todos los puntos de instalación permitió asegurar una cobertura integral en accesos, perímetro, almacenes, líneas de producción, oficinas y áreas de seguridad, fortaleciendo el control visual y la capacidad de respuesta ante eventos operativos y de seguridad.

a) Proceso de cableado tubería interna

b) Tendido de cable en producción

c) Instalación de cámaras

d) Ejemplo de vista exitosa desde NVR

Figura 5.12 Proceso y resultado de instalación de cámaras IP.

5.1.1 Telefonía IP (VoIP)

Resultados de la configuración e instalación de la telefonía IP

De igual forma que en las etapas anteriores del proyecto, se procedió a la instalación de un nuevo conmutador IP (PBX), el cual fue configurado desde cero para operar con las troncales SIP proporcionadas por el proveedor de servicios de voz. El equipo fue montado en el site principal, como se observa en la Figura 5.13 (a), integrándose a la infraestructura central de red y garantizando alta disponibilidad del servicio.

Posteriormente, el PBX y los dispositivos asociados fueron configurados dentro de la VLAN destinada exclusivamente a la telefonía IP, asegurando el aislamiento del tráfico de voz respecto a los servicios de datos, tal como se aprecia en la Figura 5.13 (b). Esta segmentación permite aplicar políticas de seguridad y calidad de servicio (QoS) adecuadas para la transmisión de voz sobre IP.

La Figura 5.13 (c) muestra la instalación física de los teléfonos IP en las distintas áreas operativas y administrativas, los cuales fueron conectados a la red mediante enlaces PoE desde los switches de acceso. Finalmente, en la Figura 5.13 (d) se evidencia la configuración exitosa de red en cada terminal, incluyendo la asignación de dirección IP, máscara de subred y parámetros de comunicación necesarios para su correcta operación.

Con esta implementación se logró habilitar un sistema de telefonía IP funcional, escalable y alineado a la infraestructura de red propuesta, garantizando comunicación interna eficiente, reducción de costos operativos y facilidad de administración centralizada.

a) Conmutador instalado en el SITE

b) Configurado en VLAN 40

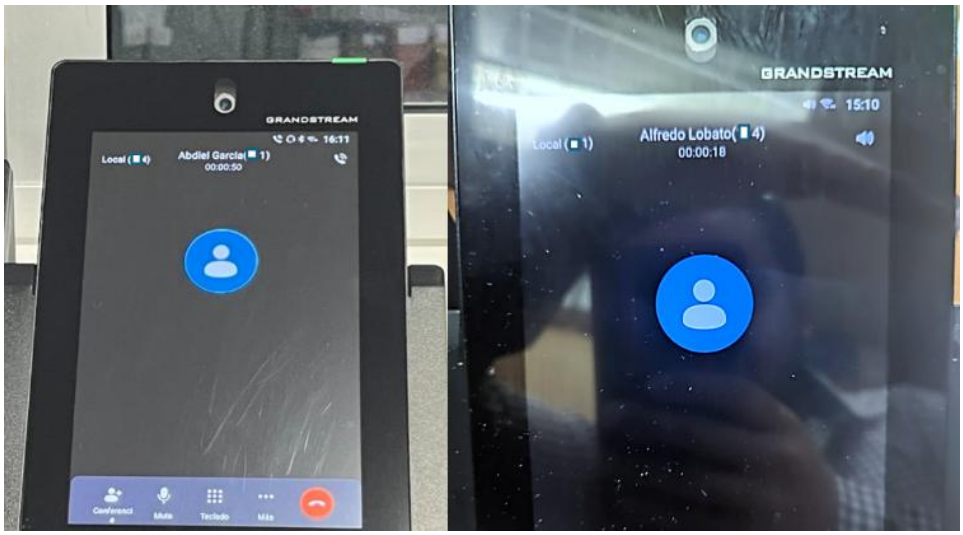
c) Instalación de teléfonos

d) Configuración de red exitosa

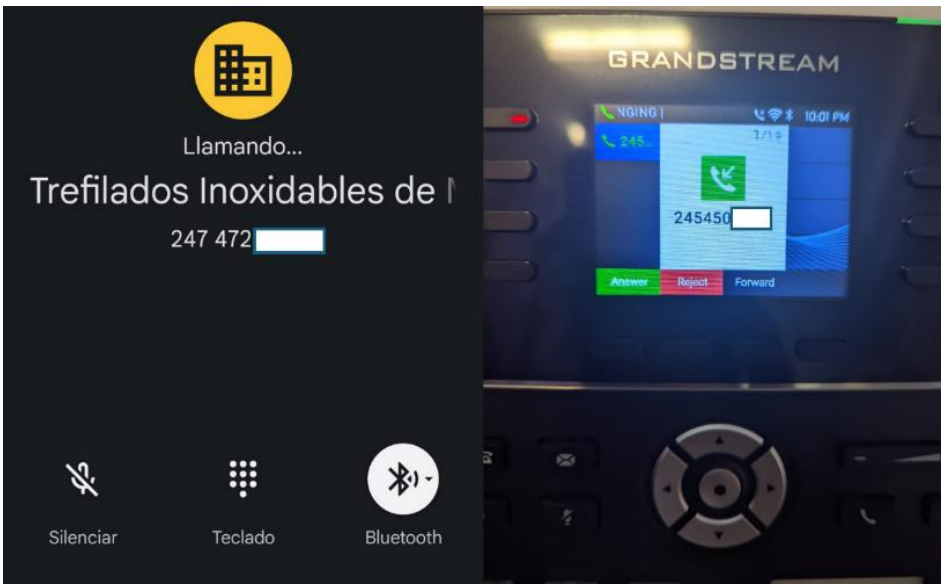
Figura 5.13 Proceso de instalación de telefonía IP.

Una vez concluida la instalación y configuración del sistema de telefonía IP, se llevaron a cabo pruebas funcionales de llamadas internas y externas con el objetivo de validar la correcta operación de la plataforma. Las pruebas incluyeron la verificación de comunicación entre extensiones, calidad de audio, tiempos de establecimiento de llamada, así como la funcionalidad de servicios adicionales como buzón de voz y transferencia de llamadas.

En la Figura 5.14 (a) se observa una llamada exitosa entre extensiones internas, confirmando la correcta asignación de extensiones y el funcionamiento del conmutador IP. De igual forma, la Figura 5.14 (c) muestra una llamada exitosa hacia y desde el exterior, validando la correcta integración de las troncales SIP con el proveedor de servicios de voz.



a) Llamada exitosa entre extensiones



c) Llamada exitosa del exterior

Figura 5.14 Resultados de pruebas de llamadas.

Así mismo se verificó que dentro de la administración del conmutador se logre monitorear todas las llamadas realizadas como se muestra en la Figura 5.15:

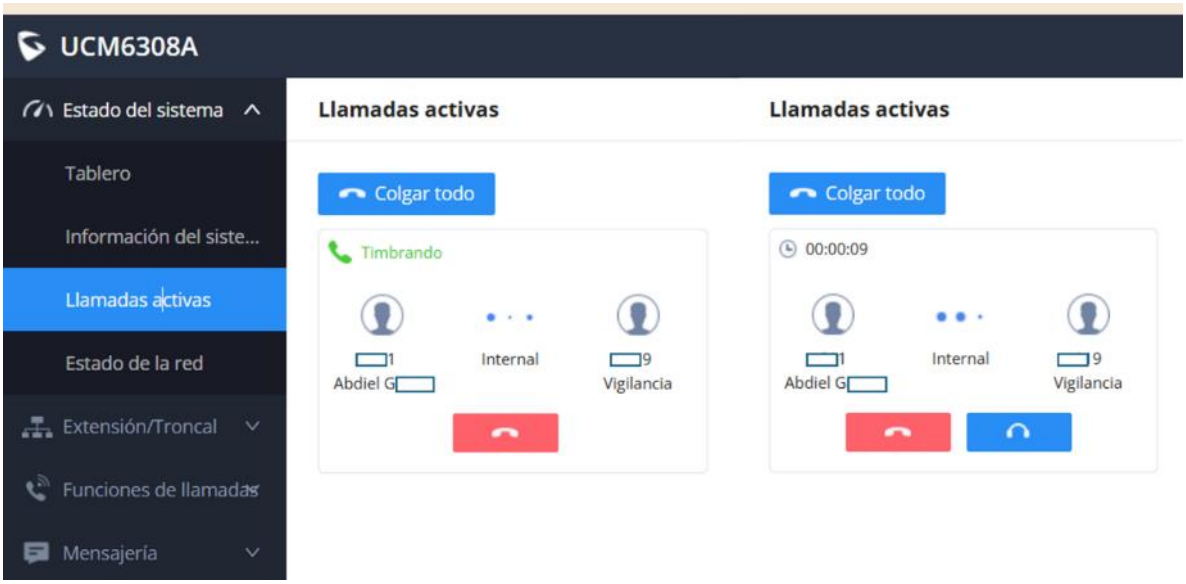


Figura 5.15 Pruebas de llamadas entre extensiones en el conmutador.

5.1.1.1 Validación de calidad de servicio – Telefonía IP

Una vez concluida la instalación física de los teléfonos IP, así como la configuración del conmutador, troncales y red interna, se procedió a realizar pruebas de validación funcional entre áreas estratégicas de la empresa.

Estas pruebas consistieron en la realización de llamadas internas simuladas entre extensiones IP de distintas áreas, a fin de evaluar la calidad del audio, la latencia en el establecimiento de llamadas, y la estabilidad general del servicio como se mostró en la imagen anterior.

Los parámetros medidos fueron:

- Latencia de establecimiento de llamada (ms): tiempo desde que se marca hasta que se inicia la conexión.
- Calidad de voz (MOS): "Mean Opinion Score", escala de 1 a 5 donde >4.0 se considera excelente.
- Estabilidad de conexión: sin cortes, retardo, eco ni interrupciones.

Los datos mostrados en la Tabla 5.14, fueron recopilados directamente desde el conmutador IP, el cual registra métricas clave en cada sesión de llamada: latencia de establecimiento, calidad de voz (MOS) y estado de conexión.

Tabla 5.14 Resultados de llamadas internas entre áreas

Área origen	Área destino	Latencia (ms)	MOS promedio	Resultado general
Dirección General	Planeación y Logística	118 ms	4.5	☑ Excelente
Finanzas y Contabilidad	Recursos Humanos	123 ms	4.4	☑ Excelente
Comercial / Ventas	Almacén	110 ms	4.6	☑ Excelente
Producción	Mantenimiento	125 ms	4.3	☑ Excelente
Seguridad e Higiene	Calidad	115 ms	4.5	☑ Excelente
Sala de Juntas	Dirección General	130 ms	4.4	☑ Excelente
Tecnologías de la Información	Vicedirección	119 ms	4.6	☑ Excelente
Recursos Humanos	Comercio Exterior	117 ms	4.5	☑ Excelente
Planeación y Logística	Producción	122 ms	4.4	☑ Excelente
Almacén	Calidad	113 ms	4.5	☑ Excelente

Los resultados obtenidos a partir de las diez llamadas simuladas entre áreas clave de la organización evidencian un comportamiento altamente satisfactorio del sistema de Telefonía IP. En todas las pruebas, la latencia de establecimiento de llamada se mantuvo en un rango de 110 a 130 milisegundos, valores considerados óptimos para entornos VoIP internos. Asimismo, el puntaje MOS (Mean Opinion Score), indicador de calidad de voz percibida por el usuario, fue consistentemente superior a 4.3 en una escala de 1 a 5, lo cual se traduce en una calidad de audio clara, sin distorsiones, retardos, eco ni interrupciones.

Los datos recopilados validan que la solución de Telefonía IP instalada es completamente funcional y estable. La calidad de voz, el bajo tiempo de establecimiento de llamadas y la correcta integración de los teléfonos IP por modelo y área confirman una implementación exitosa y lista para operación continua.

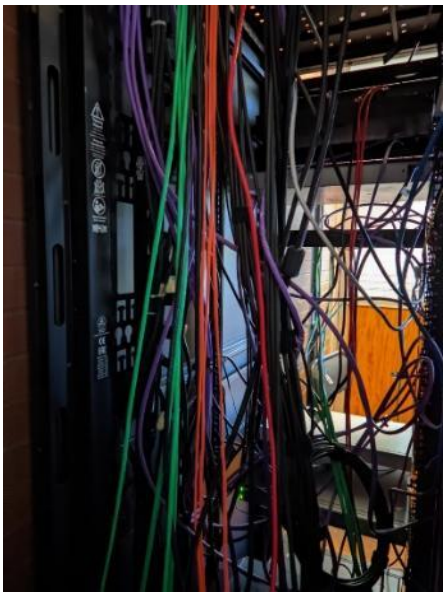
Organización y depuración del Site principal

Una vez finalizada la instalación de todos los equipos de red y telefonía requeridos —incluyendo switches, puntos de acceso, cámaras, servidores y teléfonos IP— se procedió a una etapa crítica para asegurar la eficiencia operativa y el orden del entorno tecnológico: la organización integral del site principal.

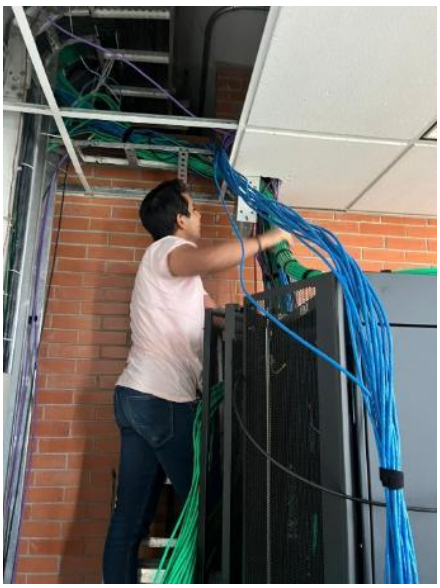
Durante esta fase se realizó una revisión exhaustiva de la infraestructura existente, identificando equipos obsoletos, dañados o en desuso, los cuales fueron retirados de manera controlada para liberar espacio físico, reducir riesgos eléctricos y disminuir el consumo energético innecesario. De forma paralela, se integraron adecuadamente los nuevos dispositivos, tales como el router principal, los sistemas de respaldo UPS para servidores y equipos críticos, así como los nuevos paneles de conexión y switches centrales.

Para optimizar la gestión del cableado, se implementaron organizadores horizontales y verticales, eliminando enredos, rutas cruzadas y puntos de tensión en los enlaces. Asimismo, se llevó a cabo un proceso sistemático de identificación, etiquetado y reubicación de cables, descartando aquellos que ya no cumplían función alguna y consolidando conexiones previamente dispersas o sin orden lógico. Esta actividad incluyó la estandarización del etiquetado de puertos, equipos y tramos de red, facilitando futuras labores de mantenimiento, diagnóstico y ampliación de la infraestructura.

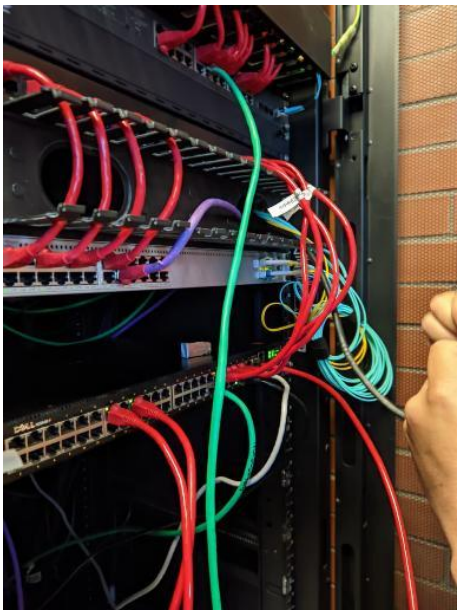
En la Figura 5.16 (a) se observa el estado inicial del cableado, caracterizado por enlaces enredados y desorganizados; mientras que en la Figura 5.16 (b) se muestra el proceso de reorganización llevado a cabo dentro del site. La Figura 5.16 (c) evidencia la correcta identificación y etiquetado del cableado funcional, y finalmente, en la Figura 5.16 (d) se aprecia parte del cableado retirado tras el proceso de depuración. Estas acciones permitieron lograr una distribución más lógica, segura y alineada con las mejores prácticas de infraestructura tecnológica.



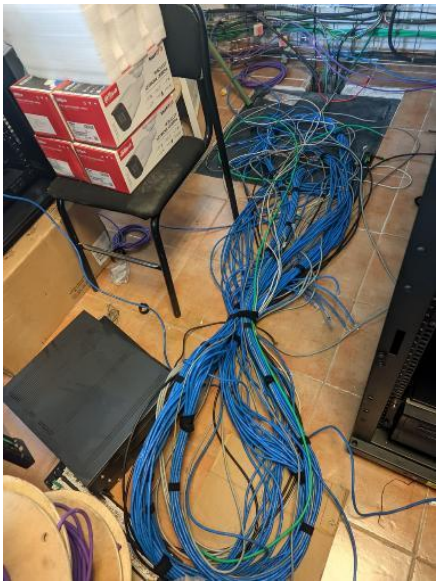
a) Cableado enredado y desorganizado



b) Proceso de organización



c) Identificación y etiquetado

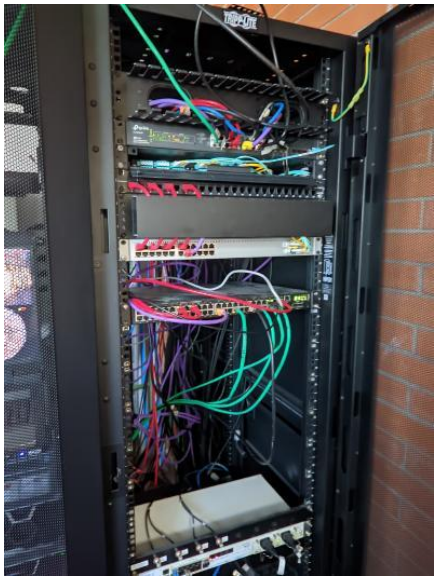


d) Parte del cableado retirado

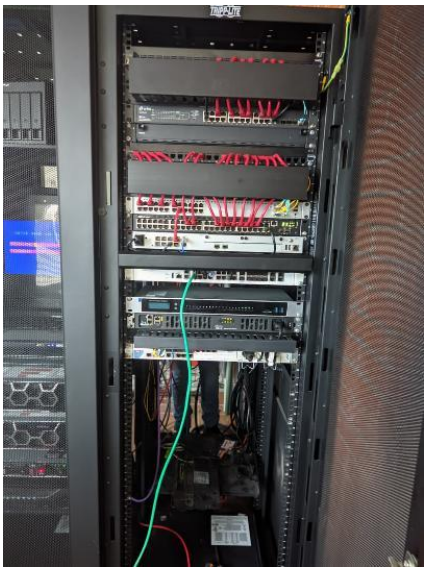
Figura 5.16 Proceso de organización de cableado de SITE.

En la Figura 5.17 se muestran las evidencias del proceso de organización de los principales componentes del site, incluyendo switches, distribuidores de red, enlaces de fibra y cobre, servidores, sistemas de grabación NVR, dispositivos KVM, conmutador IP y organizadores de cableado.

En la Figura 5.17 (a) se observa el inicio del proceso de organización en los switches, mientras que la Figura 5.17 (b) muestra los avances finales tras la correcta gestión y acomodo del cableado. La Figura 5.17 (c) evidencia la migración de enlaces y la instalación de sistemas UPS para respaldo eléctrico, y finalmente, en la Figura 5.17 (d) se presenta la organización final de servidores, NVR y equipos KVM, reflejando una distribución ordenada, segura y alineada con las mejores prácticas de infraestructura tecnológica.



a) Inicio de organización en switches



b) Avances finales en la organización

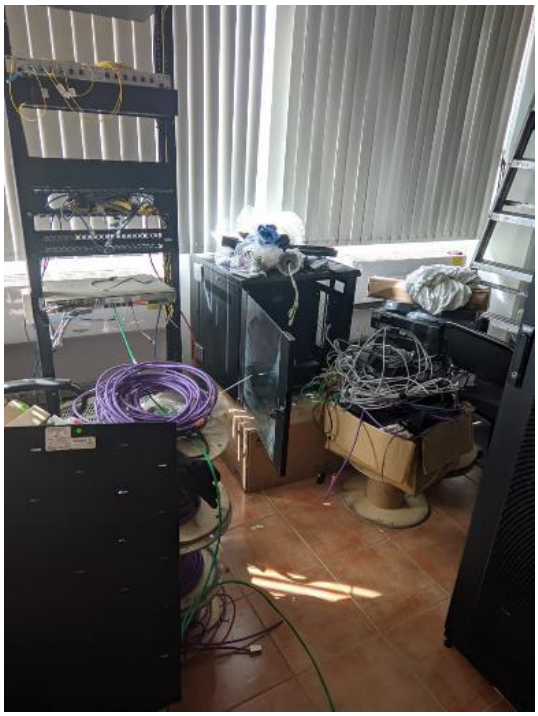
c) Migración de enlaces e instalación de UPS

d) Organización de servidores, NVR y KVM

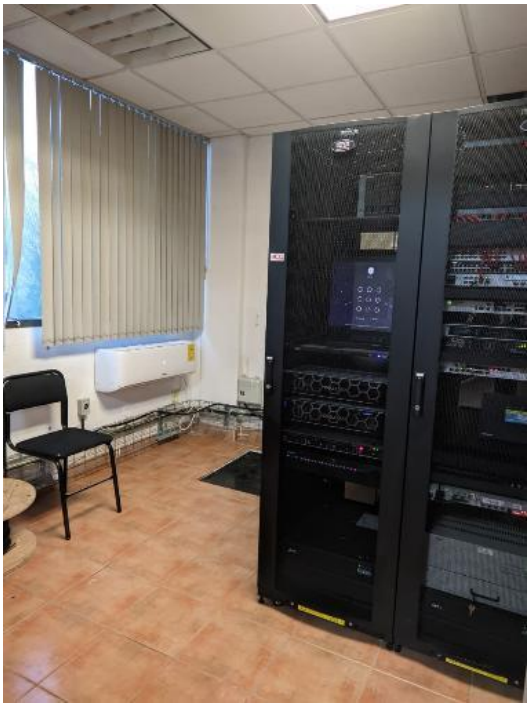
Figura 5.17 Proceso de organización de SITE.

A continuación, se presenta una comparación del estado original del site, mostrado en la Figura 5.18 (a), y el resultado final tras las labores de organización y limpieza, ilustrado en

la Figura 5.18 (b), lo que permite observar de manera clara el impacto visual y técnico de las acciones de mejora implementadas.



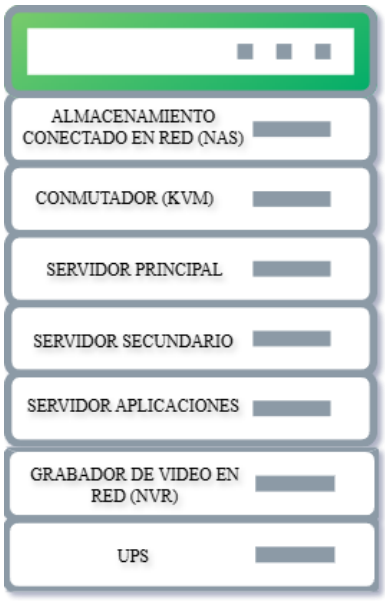
a) Vista de SITE antes



b) Vista de SITE actual

Figura 5.18 Resultado de organización de SITE.

En la Figura 5.19 se muestra la disposición del rack de servidores, en el cual se integran los principales elementos de procesamiento, almacenamiento y respaldo del sistema. Este rack alberga el servidor principal, el servidor secundario y el servidor de aplicaciones, así como el sistema de almacenamiento conectado en red (NAS) destinado al respaldo de información. Adicionalmente, se incluyen el conmutador KVM para la administración centralizada de los servidores, el grabador de video en red (NVR) del sistema de videovigilancia y la unidad UPS, encargada de proporcionar respaldo eléctrico y protección ante fallas de energía.



5.19 Resultado de organización de SITE. Elaboración propia.

Por su parte, la Figura 5.20 presenta la organización del rack de red y comunicaciones, donde se agrupan de manera estructurada los componentes responsables de la distribución, control y seguridad de la red empresarial. En este rack se localizan los patch panels, organizadores de cableado, switches dedicados para cámaras, distribuidores de fibra óptica, switches administrativos, el switch core, el firewall Fortinet, el conmutador de troncales IP, así como los enlaces troncales de comunicación y una unidad UPS adicional para respaldo eléctrico. Esta disposición facilita la administración, el mantenimiento y la escalabilidad de la infraestructura de red.

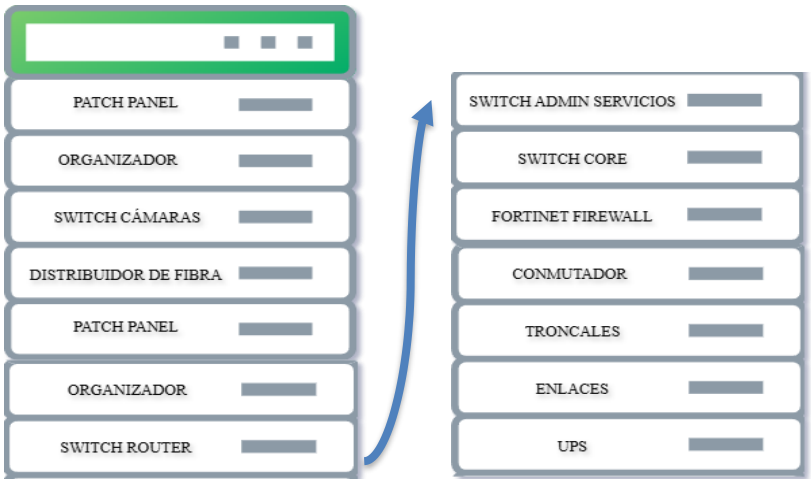


Figura 5.20 Organización general en el segundo rack. Elaboración propia.

5.2 Resultados de encuestas de validación y percepción del usuario

5.1.2 Generalidades de la aplicación de encuestas

Como parte del proceso de validación del proyecto de renovación de la infraestructura tecnológica, se aplicaron encuestas de percepción a los usuarios finales con el objetivo de evaluar el desempeño, confiabilidad y aceptación de los servicios implementados, específicamente la red de datos, la red inalámbrica Wi-Fi, la telefonía IP y el sistema de videovigilancia IP.

La aplicación de las encuestas se realizó de manera presencial y dirigida, considerando únicamente al personal administrativo, ya que este grupo es el principal usuario de los servicios de conectividad, telefonía IP y videovigilancia dentro de la organización. La selección de la población encuestada respondió a criterios de disponibilidad, uso constante de los sistemas y relevancia operativa.

Para la encuesta de evaluación de la red industrial y servicios de telefonía IP, la población total considerada fue de 50 colaboradores administrativos. De este grupo, se obtuvo una muestra efectiva de 42 personas, quienes se encontraban laborando al momento de la aplicación y utilizan de manera directa y cotidiana los servicios de red y telefonía IP para el desarrollo de sus actividades.

Por su parte, la encuesta de evaluación del sistema de videovigilancia IP se aplicó exclusivamente al personal autorizado con acceso a las cámaras y al sistema NVR. En este caso, la población estuvo conformada por 8 usuarios, todos ellos pertenecientes al área administrativa y con responsabilidades directas en tareas de supervisión, seguridad y monitoreo, por lo que su opinión resulta representativa para evaluar el funcionamiento y utilidad del sistema.

Las encuestas incluyeron preguntas orientadas a medir aspectos clave como velocidad y estabilidad de la red, calidad del servicio Wi-Fi, desempeño de la telefonía IP, confiabilidad del sistema, tiempos de respuesta del soporte técnico, percepción de seguridad de la información y nivel de satisfacción general. En el caso del sistema de videovigilancia, se evaluaron adicionalmente la calidad de imagen, facilidad de acceso a grabaciones, cobertura, tiempos de respuesta ante fallas y utilidad operativa del sistema.

A continuación, se presentan y analizan los resultados obtenidos de ambas encuestas, los cuales permiten complementar los resultados técnicos del proyecto con la percepción

directa del usuario final, proporcionando una visión integral del impacto de la implementación.

5.1.3 Encuesta de Evaluación de la Red Industrial y Servicios de Telefonía IP

Pregunta 1: ¿La velocidad de la red es suficiente para realizar sus actividades?

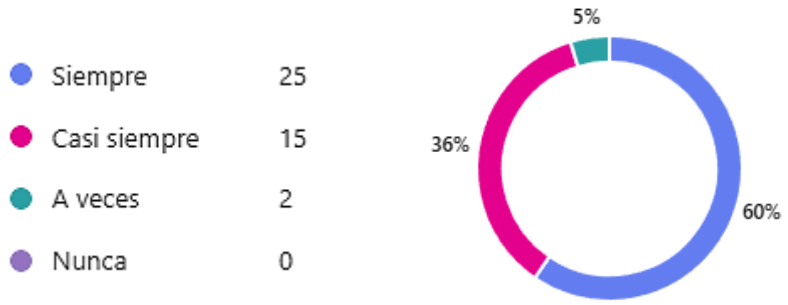


Figura 5.21 Resultados de la primera pregunta (Encuesta de red). Elaboración propia.

Los resultados muestran una alta satisfacción en cuanto a la velocidad de la red implementada (véase Figura 5.21). El 60% de los usuarios indicó que siempre cuentan con una velocidad adecuada para realizar sus actividades, y un 36% adicional afirmó que casi siempre. Solo un 5% manifestó que a veces ha percibido deficiencias, mientras que ningún usuario reportó una experiencia negativa constante.

Interpretación

Estos datos reflejan que la red cumple con los estándares operativos esperados en un entorno industrial, permitiendo a la mayoría de los usuarios ejecutar sus tareas sin interrupciones ni lentitud. La mejora sustancial observada en las pruebas técnicas se ve respaldada por la percepción del usuario final, lo que valida el éxito de la implementación desde un enfoque práctico y funcional.

Pregunta 2: ¿Con qué frecuencia experimenta interrupciones o caídas de la red?

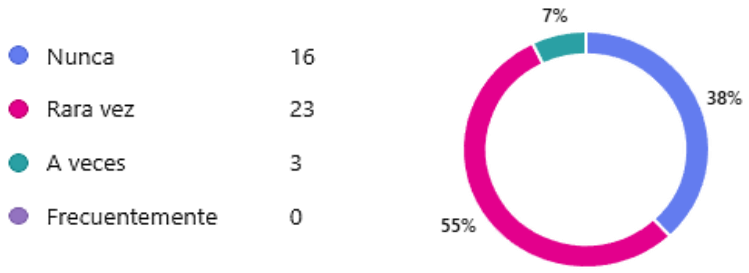


Figura 5.22 Resultados de la segunda pregunta (Encuesta de red). Elaboración propia.

Análisis

Se muestra en la Figura 5.22 que más del 90% de los usuarios encuestados reporta que nunca o rara vez experimenta interrupciones en el servicio de red, lo cual es un indicador muy positivo de estabilidad y confiabilidad del sistema. Solo el 7% manifestó haber tenido caídas ocasionales, y ningún usuario señaló que estas fallas ocurran de forma frecuente.

Interpretación

Estos datos confirman que la infraestructura implementada no solo es rápida, sino también estable y robusta, cumpliendo con los requerimientos de continuidad operativa en un entorno industrial. La baja incidencia de caídas (complementada con la percepción de velocidad adecuada en la pregunta anterior) consolida la evidencia de que la red se encuentra correctamente dimensionada y configurada para soportar el volumen y criticidad de los servicios actuales.

Pregunta 3: ¿Cómo califica la calidad de conexión Wi-Fi en su área de trabajo?

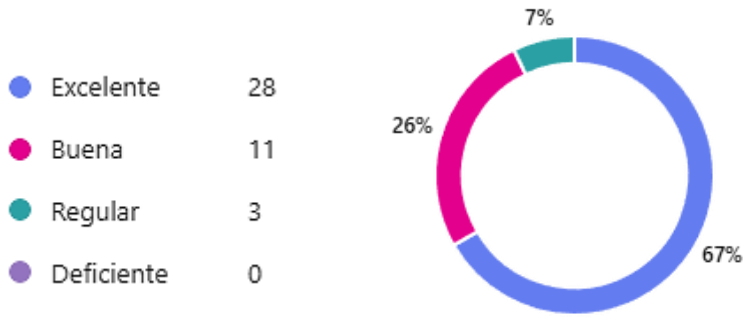


Figura 5.23 Resultados de la tercera pregunta (Encuesta de red). Elaboración propia.

Análisis

Un 67% de los encuestados calificó la calidad de la conexión Wi-Fi como excelente, mientras que un 26% adicional la consideró buena, lo que representa un 93% de satisfacción positiva. Solo un pequeño grupo (7%) la evaluó como regular y nadie señaló una calidad deficiente (véase Figura 5.23).

Interpretación

Estos resultados reflejan el éxito de la nueva infraestructura inalámbrica implementada, validando tanto el diseño de cobertura como la correcta colocación de los puntos de acceso (APs). La percepción de calidad coincide con las mediciones técnicas realizadas y los mapas de calor presentados anteriormente, consolidando la percepción de una red moderna, estable y funcional, incluso en zonas de alta demanda.

Pregunta 4: ¿Experimenta retrasos al acceder a aplicaciones críticas (ERP, correo, sistemas de producción)?

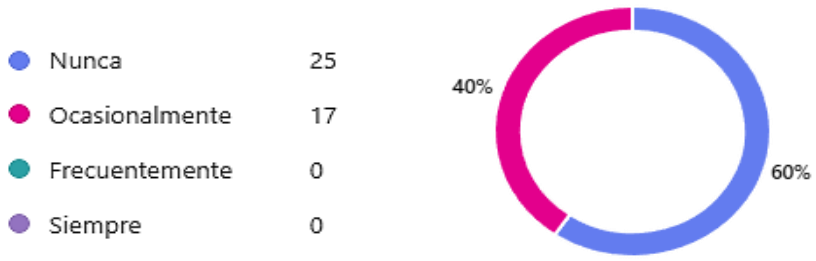


Figura 5.24 Resultados de la cuarta pregunta (Encuesta de red). Elaboración propia.

Análisis

La Figura 5.24 expone que el 100% de los encuestados reporta no experimentar retrasos constantes al acceder a aplicaciones críticas. De ese total, un 60% indica que nunca ha percibido lentitud, mientras que el 40% restante solo de forma ocasional. Es relevante destacar que ningún usuario declaró experimentar problemas frecuentes o permanentes.

Interpretación

Estos resultados refuerzan la idea de que la red y los servicios asociados (incluyendo los servidores, switches y enlaces) están correctamente dimensionados y optimizados para soportar las aplicaciones empresariales clave. La ausencia total de respuestas negativas o

críticas frecuentes sugiere una experiencia fluida y eficiente en el uso de herramientas de negocio, contribuyendo directamente a la productividad operativa.

Pregunta 5: ¿Qué tan confiable considera la red de la empresa en general?

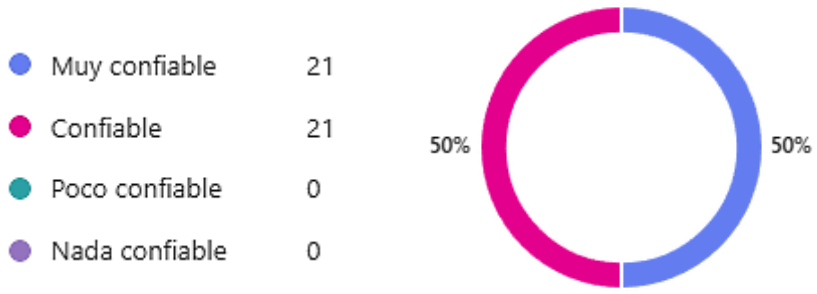


Figura 5.25 Resultados de la quinta pregunta (Encuesta de red). Elaboración propia.

Análisis

El 100% de los encuestados considera que la red es confiable o muy confiable, distribuidos equitativamente entre ambas opciones (véase Figura 5.25). No se registraron respuestas negativas, lo cual demuestra una percepción uniforme y sólida sobre la fiabilidad de la infraestructura de red instalada.

Interpretación

Esta respuesta reafirma el impacto positivo del proyecto de renovación tecnológica. La red no solo cumple con los requerimientos técnicos y operativos, sino que ha logrado generar una percepción generalizada de confianza entre los usuarios. Esta percepción se alinea con los resultados de las preguntas anteriores, y representa uno de los objetivos clave de cualquier implementación en entornos industriales: garantizar continuidad, seguridad y estabilidad.

Pregunta 6: Cuando ocurre un problema en la red, ¿qué tan rápido se soluciona?

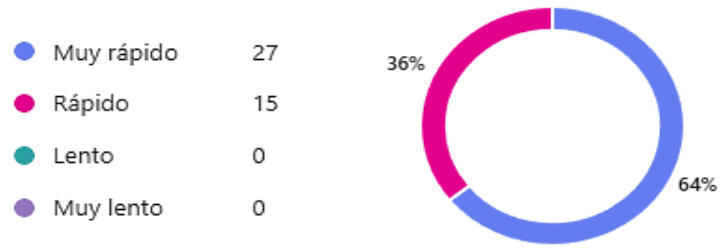


Figura 5.26 Resultados de la sexta pregunta (Encuesta de red). Elaboración propia.

Análisis

El 100% de los encuestados considera que los problemas en la red se resuelven con rapidez, y la mayoría (64%) incluso califica el tiempo de respuesta como “muy rápido” (véase Figura 5.26). No se reportaron percepciones negativas (ni lentitud ni demoras), lo cual refleja una respuesta eficiente por parte del área de soporte técnico o sistemas ante cualquier eventualidad.

Interpretación

Este resultado refuerza la eficiencia operativa de la infraestructura tecnológica y del equipo responsable del mantenimiento y soporte. No solo se logró implementar una red estable y de alto rendimiento, sino que también se estableció un sistema de atención ágil y eficaz, reduciendo tiempos de inactividad y mejorando la experiencia del usuario final.

Pregunta 7: ¿Recibe apoyo oportuno del área de TI cuando reporta fallas de red?

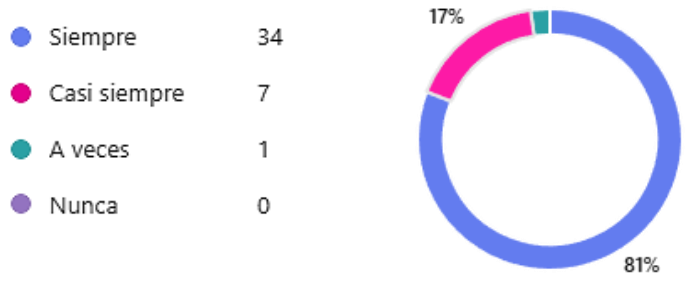


Figura 5.27 Resultados de la séptima pregunta (Encuesta de red). Elaboración propia.

Análisis

Se muestra en la Figura 5.27 que la mayoría absoluta de los usuarios (98%) reporta que recibe apoyo oportuno siempre o casi siempre cuando se presentan fallas de red. El 81% menciona que siempre tiene respuesta inmediata, mientras que el 17% indica que ocurre en la mayoría de los casos. Solo un 2% expresó que el apoyo es ocasional, y nadie reportó falta total de atención.

Interpretación

Estos resultados reflejan una percepción altamente positiva sobre el desempeño del área de TI, confirmando su compromiso con la atención eficaz a incidentes de red. La capacidad de respuesta, disponibilidad y resolución de problemas son reconocidas por la mayoría de los usuarios, lo cual fortalece la confianza en el equipo técnico y en la infraestructura

instalada. Este nivel de atención también es coherente con la mejora observada en los tiempos de solución de fallas (pregunta anterior).

Pregunta 8: ¿Con qué frecuencia sus llamadas VoIP presentan cortes o retrasos (jitter)?

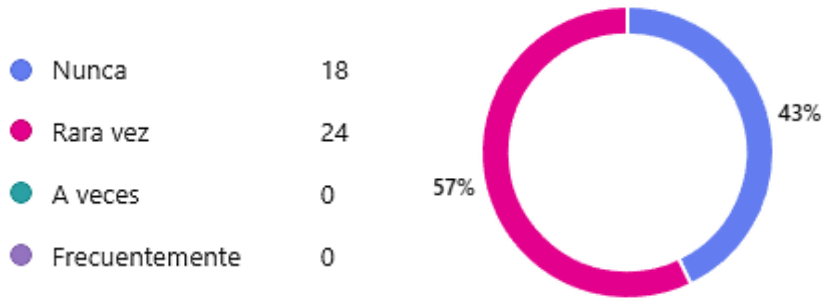


Figura 5.28 Resultados de la octava pregunta (Encuesta de red). Elaboración propia.

Análisis

El 100% de los usuarios encuestados indicó que nunca o rara vez ha experimentado cortes o retrasos en sus llamadas VoIP (véase Figura 5.28). Ningún usuario reportó problemas recurrentes o frecuentes, lo cual es un indicador clave de calidad en servicios VoIP.

Interpretación

Estos resultados reflejan una implementación exitosa y estable del sistema de telefonía IP. El hecho de que ningún usuario haya reportado interrupciones frecuentes sugiere que los parámetros técnicos como latencia, jitter y pérdida de paquetes están dentro de los márgenes aceptables, lo que garantiza una calidad de audio clara y sin interrupciones. Además, este dato valida la correcta configuración de las troncales, QoS y segmentación de red (VLAN VoIP) que fueron consideradas durante el diseño de la nueva infraestructura.

Pregunta 9: ¿La calidad de audio en llamadas internas y externas es...?

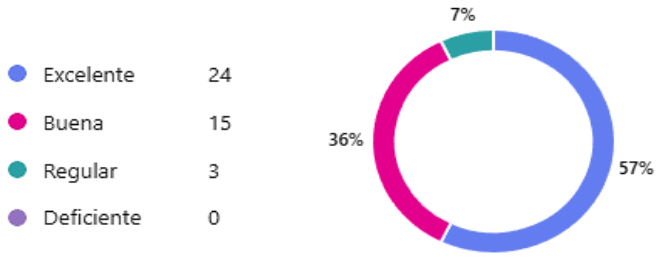


Figura 5.29 Resultados de la novena pregunta (Encuesta de red). Elaboración propia.

Análisis

La gran mayoría de los usuarios considera que la calidad de audio en las llamadas es satisfactoria como se expone en la Figura 5.29, con un 93% calificándola como excelente o buena. Solo un 7% la percibe como regular, y ningún usuario la considera deficiente.

Interpretación

Estos resultados refuerzan el éxito de la implementación del sistema de telefonía IP, indicando que las llamadas, tanto internas como externas, se desarrollan con una calidad sonora adecuada, sin distorsión, eco o cortes. Esto implica que la infraestructura de red brinda el ancho de banda suficiente, los teléfonos IP están correctamente configurados, y los dispositivos de red como conmutadores y gateways funcionan sin cuellos de botella.

Pregunta 10: ¿Se interrumpen las llamadas por fallos de red?

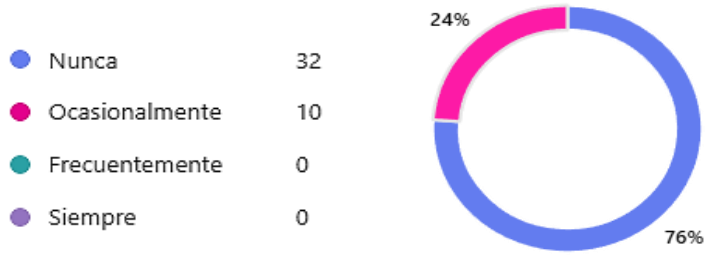


Figura 5.30 Resultados de la décima pregunta (Encuesta de red). Elaboración propia.

Análisis

El 76% de los usuarios reporta que nunca se interrumpen las llamadas por fallos de red, mientras que el 24% indica que esto ocurre de forma ocasiona (véase Figura 5.30). No hubo registros de interrupciones frecuentes o constantes.

Interpretación

Esta respuesta evidencia un comportamiento estable de la red respecto a la continuidad de las llamadas IP. Las interrupciones ocasionales pueden estar relacionadas con factores externos o casos aislados, pero el hecho de que no existan reportes de interrupciones frecuentes o permanentes refuerza la confiabilidad del sistema de comunicación implementado.

Pregunta 11: ¿Se siente seguro al manejar información sensible a través de la red?

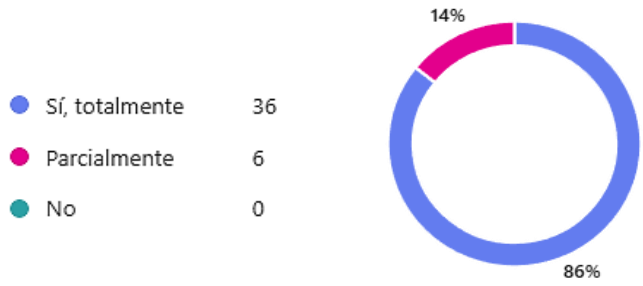


Figura 5.31 Resultados de la undécima pregunta (Encuesta de red). Elaboración propia.

Análisis

Por otra parte, en la Figura 5.31 podemos destacar que la mayoría de los usuarios (86%) manifiesta sentirse totalmente segura al manejar información sensible mediante la red interna, mientras que el 14% indica sentirse solo parcialmente seguro. Ningún usuario considera la red insegura, lo que representa un importante indicador de confianza en la infraestructura.

Interpretación

Estos resultados reflejan que la red implementada cumple con los estándares de seguridad esperados por los usuarios, permitiendo el manejo de datos confidenciales con tranquilidad. Esto es consecuencia directa de la correcta segmentación por VLAN, la instalación de firewalls Fortinet, el uso de switches administrables y otras medidas de seguridad aplicadas desde el site principal. La percepción positiva también indica que los esfuerzos en ciberseguridad, como el control de accesos y la estabilidad del sistema, están siendo efectivos.

Pregunta 12: ¿Ha recibido capacitación sobre el uso seguro de la red y la protección de datos?

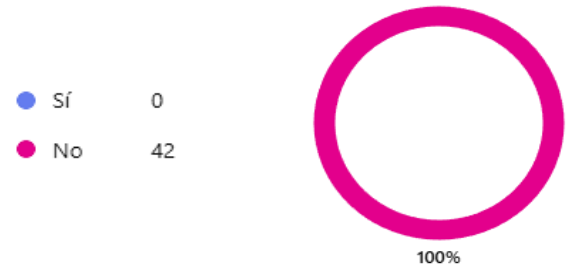


Figura 5.32 Resultados de la duodécima pregunta (Encuesta de red). Elaboración propia.

Análisis

El 100% de los encuestados respondió que no ha recibido capacitación formal sobre el uso seguro de la red ni sobre la protección de datos (véase Figura 5.32). Este resultado evidencia una brecha importante en materia de formación y concientización en ciberseguridad, a pesar de la infraestructura segura implementada.

Interpretación

Aunque los usuarios confían en la red y perciben estabilidad, la ausencia de capacitación formal representa un riesgo potencial. El desconocimiento de buenas prácticas puede derivar en errores humanos que comprometan la seguridad de la información, como el uso indebido de contraseñas, el acceso no autorizado o la apertura de correos sospechosos. Esta situación destaca la necesidad urgente de implementar programas de capacitación continua, enfocados en el uso seguro de la red, la protección de datos sensibles, y la prevención de ataques como phishing o programas malignos.

Pregunta 13: ¿Qué tan satisfecho está con la red y los servicios de telefonía actuales?

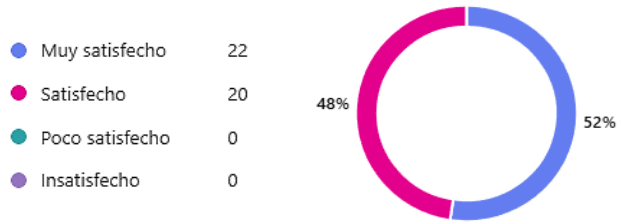


Figura 5.33 Resultados de la decimotercera pregunta (Encuesta de red). Elaboración propia.

Análisis

El 100% de los usuarios expresó satisfacción con la red y los servicios de telefonía IP tras la implementación (véase Figura 5.33). Esta valoración positiva se distribuye casi equitativamente entre quienes se consideran “muy satisfechos” (52%) y “satisfechos” (48%), sin registrar opiniones negativas.

Interpretación

Los resultados reflejan un alto nivel de aceptación y conformidad con el nuevo sistema de comunicaciones implementado, tanto en conectividad de red como en telefonía. La mejora en cobertura, estabilidad, velocidad y calidad de llamadas ha generado un impacto tangible y positivo en la experiencia del usuario. Esto valida la eficacia del proyecto y demuestra que

los objetivos planteados han sido alcanzados desde la percepción de quienes utilizan estos servicios a diario.

Pregunta 14: ¿En qué aspectos recomendaría mejoras adicionales?

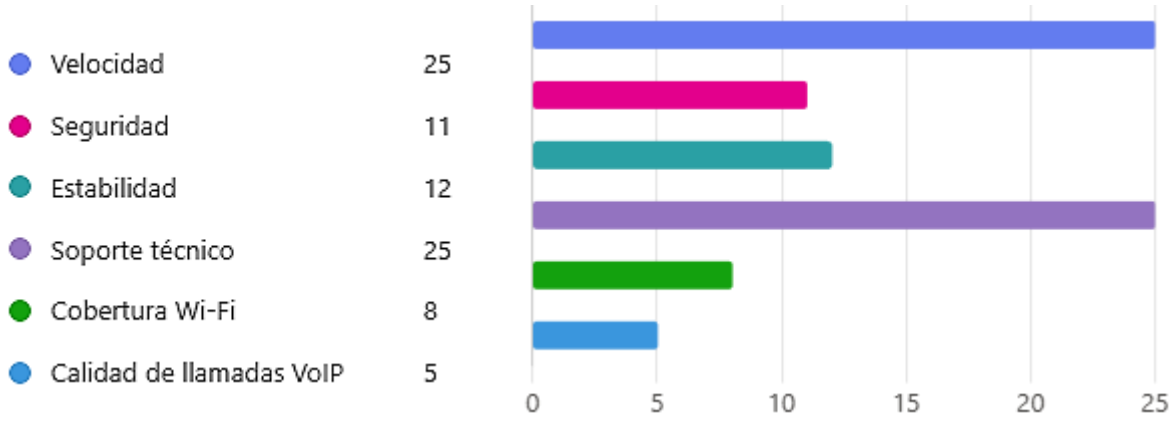


Figura 5.34 Resultados de la decimocuarta pregunta (Encuesta de red). Elaboración propia.

Análisis

Aunque la mayoría de los resultados anteriores muestran un alto grado de satisfacción, esta pregunta permitió detectar áreas con potencial de mejora percibidas por los usuarios. En la Figura 5.34 se destacan las dos categorías con más menciones que fueron velocidad y soporte técnico, con 25 votos cada una, lo cual podría estar relacionado con expectativas más altas tras la mejora de infraestructura o con la necesidad de respuestas aún más ágiles ante incidentes.

La estabilidad y seguridad también obtuvieron una cantidad moderada de respuestas, lo que sugiere que, aunque funcionan correctamente en general, hay margen para reforzarlas, especialmente en entornos críticos o con alto tráfico de datos.

En menor medida, la cobertura Wi-Fi y la calidad de llamadas VoIP fueron mencionadas, lo que podría indicar que algunos espacios específicos aún requieren ajustes finos o monitoreo continuo.

Interpretación

Esta pregunta permite enfocar las futuras acciones de mejora continua. A pesar del desempeño general positivo, la retroalimentación directa de los usuarios sugiere que sería recomendable:

- Ampliar o reforzar la comunicación y capacitación del área de soporte técnico,
- Seguir optimizando parámetros de velocidad en zonas de alta densidad o interferencia,
- Revisar zonas con cobertura irregular de Wi-Fi y posibles cuellos de botella.

Pregunta 15: ¿Qué aspecto considera prioritario mejorar en la red y telefonía IP?

Figura 5.35 Resultados de la decimoquinta pregunta (Encuesta de red). Elaboración propia.

Análisis

Esta pregunta abierta permitió recopilar percepciones directas y sin filtro por parte de los usuarios (véase Figura 5.35). Una parte importante de los encuestados (12%) respondió que no consideran necesaria ninguna mejora, lo que refleja satisfacción con el estado actual del servicio.

Entre las respuestas más frecuentes destacan palabras como “capacitación”, “mejora”, “comentarios”, “mayor velocidad” y “atención”, lo que revela que, si bien el rendimiento técnico es bien valorado, existe una necesidad percibida de mejorar el conocimiento del personal sobre el uso correcto de la red y servicios de telefonía IP. Esto también se relaciona con el 100% de respuestas negativas a la pregunta anterior sobre capacitación recibida.

Interpretación

El enfoque de mejora ya no se centra tanto en infraestructura como en fortalecer el uso, soporte y protocolos de atención, así como en proporcionar capacitaciones formales sobre el uso seguro, eficiente y profesional de los sistemas disponibles.

5.1.4 Encuesta de Evaluación del Sistema de Videovigilancia IP

Pregunta 1: ¿La calidad de imagen de las cámaras es suficiente para sus necesidades?

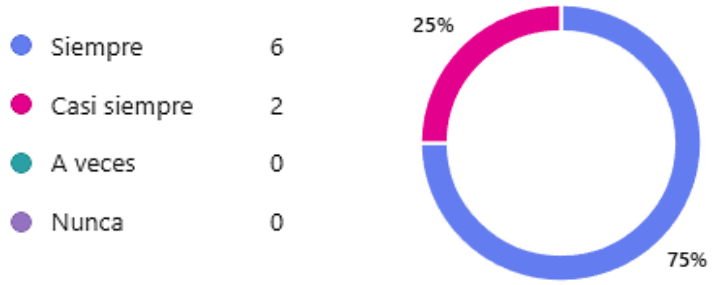


Figura 5.36 Resultados de la primera pregunta (Encuesta de videovigilancia). Elaboración propia.

Análisis e interpretación

En la Figura 5.36, los resultados indican que el 100% de los encuestados considera que la calidad de imagen de las cámaras IP instaladas es suficiente para cubrir sus necesidades operativas, siendo la mayoría (75%) quienes afirman que siempre es suficiente y el resto (25%) quienes indican que casi siempre lo es.

Este resultado refleja una alta satisfacción general con respecto a la calidad de video, lo cual valida tanto la correcta selección del equipamiento como la implementación técnica del sistema. No se reportan casos en los que la calidad haya sido deficiente o insuficiente, lo cual sugiere que la resolución, ángulo de visión y condiciones de iluminación están siendo adecuadamente gestionadas por el sistema de videovigilancia instalado.

Pregunta 2. ¿Con qué frecuencia experimenta problemas de acceso a las cámaras (tiempos de carga, caídas, pantallas en negro)?

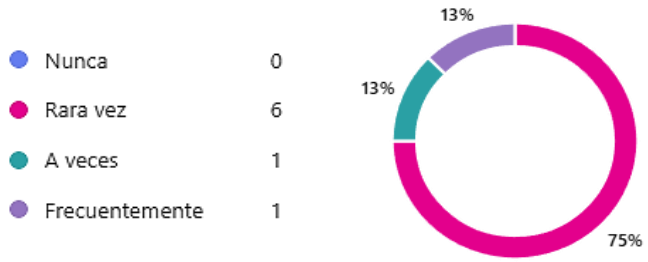


Figura 5.37 Resultados de la segunda pregunta (Encuesta de videovigilancia). Elaboración propia.

Análisis e interpretación

Los resultados muestran que el 75% de los usuarios afirma que rara vez experimenta problemas de acceso a las cámaras, mientras que un 13% lo ha experimentado ocasionalmente y otro 13% lo reporta como frecuente. No hubo respuestas que indiquen que nunca ocurren estos problemas (véase Figura 5.37).

Aunque la mayoría indica que los problemas son esporádicos y no representan una afectación constante, el hecho de que exista un caso con recurrencia frecuente (13%) sugiere que podría haber un punto específico de mejora, posiblemente relacionado con la red local, la capacidad del grabador NVR o el acceso remoto.

Este dato resalta la importancia de continuar con el monitoreo del sistema y considerar una revisión puntual del caso reportado como "frecuente", ya que un sistema de videovigilancia óptimo debe garantizar acceso inmediato y estable en todo momento, especialmente en eventos críticos.

Pregunta 3. ¿El sistema de grabación (NVR) permite acceder fácilmente a eventos pasados?

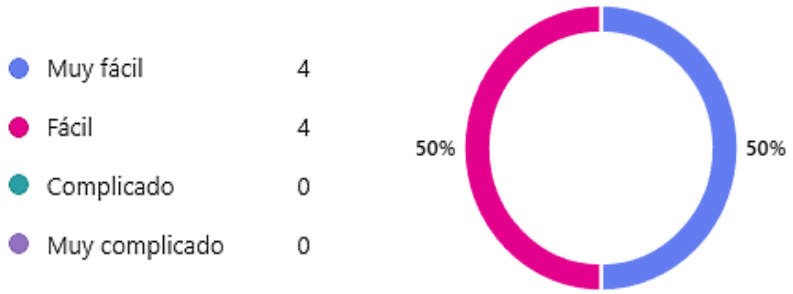


Figura 5.38 Resultados de la tercera pregunta (Encuesta de videovigilancia). Elaboración propia.

Análisis e interpretación

La Figura 5.38 deja clara que la totalidad de los encuestados considera que el acceso a eventos pasados a través del sistema de grabación NVR es sencillo, dividiéndose equitativamente entre quienes lo califican como “muy fácil” (50%) y “fácil” (50%). Este resultado refleja una alta satisfacción del usuario con la interfaz y funcionalidad del NVR implementado, lo cual es fundamental para tareas de supervisión, auditoría o seguimiento de incidentes.

El hecho de que no se hayan registrado respuestas en las opciones "Complicado" o "Muy complicado" confirma que la solución instalada es intuitiva y accesible, cumpliendo con uno

de los objetivos principales del sistema de videovigilancia: la recuperación ágil y eficiente de evidencia audiovisual.

Pregunta 4. ¿Qué tan intuitiva considera la interfaz de acceso a cámaras (desde PC, aplicación móvil o monitor en sitio)?

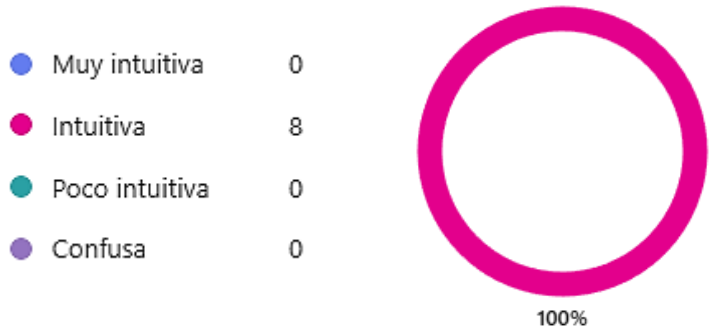


Figura 5.39 Resultados de la cuarta pregunta (Encuesta de videovigilancia). Elaboración propia.

Análisis e interpretación

Se muestra en la Figura 5.39 que 100% de los usuarios calificó la interfaz de acceso a cámaras como “intuitiva”, sin registrar ninguna respuesta en categorías negativas ni en la opción de excelencia (“muy intuitiva”). Esto indica que, aunque los usuarios no consideraron la experiencia de uso como sobresaliente, sí la encuentran comprensible, accesible y funcional para sus necesidades diarias.

Este resultado es positivo y refleja una curva de aprendizaje baja, lo cual es beneficioso para usuarios con diferentes niveles de experiencia tecnológica. La consistencia en la percepción también sugiere que no hay barreras evidentes en el uso del sistema.

Pregunta 5. ¿Ha recibido capacitación sobre el uso del sistema de videovigilancia?

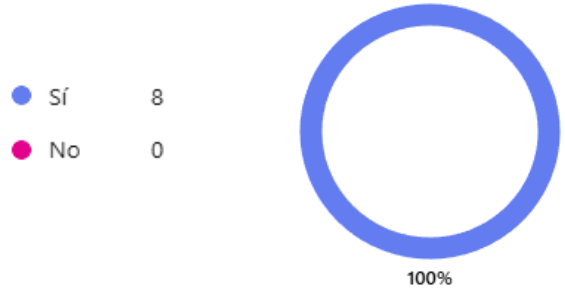


Figura 5.40 Resultados de la quinta pregunta (Encuesta de videovigilancia). Elaboración propia.

Análisis e interpretación

El 100% de los participantes respondió afirmativamente, confirmando que todos los usuarios que interactúan con el sistema de videovigilancia han recibido capacitación adecuada (véase Figura 5.40). Este resultado evidencia una correcta ejecución del plan de implementación, donde no solo se instalaron los equipos, sino que también se aseguró que el personal involucrado contara con las herramientas y conocimientos necesarios para operar el sistema eficientemente.

Esto contribuye directamente a la eficacia del sistema, ya que reduce errores humanos, mejora los tiempos de respuesta ante incidentes, y aumenta el nivel de confianza del usuario en el uso de la tecnología. Además, refleja un enfoque preventivo de la organización al evitar que el sistema se subutilice por falta de formación.

Pregunta 6. ¿Considera suficiente la cobertura de cámaras en las áreas que requiere monitorear?

Figura 5.41 Resultados de la sexta pregunta (Encuesta de videovigilancia). Elaboración propia.

Análisis e interpretación

En la Figura 5.41 se muestra la totalidad de los encuestados afirmando que la cobertura de cámaras es completamente suficiente en las áreas que requieren monitoreo. Este resultado confirma la correcta planeación, ubicación y cantidad de dispositivos instalados, lo cual garantiza que todos los puntos críticos o estratégicos están siendo vigilados de forma efectiva.

Este nivel de cobertura no solo facilita una mayor seguridad operativa, sino que también permite una respuesta oportuna ante cualquier evento relevante, lo que mejora los controles internos, la supervisión remota y la trazabilidad en caso de incidentes.

Además, la ausencia de respuestas negativas o parciales indica que no existen zonas ciegas ni carencias evidentes en el sistema, lo cual valida el diseño previo de los mapas de calor y los criterios de instalación definidos durante la fase de diagnóstico e implementación.

Pregunta 7. ¿Con qué frecuencia se presentan fallos en cámaras (desenfoque, pérdida de señal, mala iluminación)?

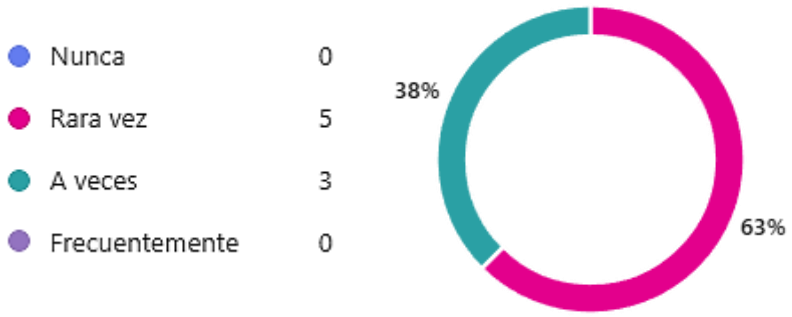


Figura 5.42 Resultados de la séptima pregunta (Encuesta de videovigilancia). Elaboración propia.

Análisis e interpretación

En la Figura 5.42 los resultados indican que, aunque la mayoría de los usuarios no experimenta fallos recurrentes, sí se han presentado incidentes esporádicos relacionados con calidad de imagen o funcionamiento de las cámaras. El 63% de los encuestados reporta que estos problemas ocurren rara vez, mientras que el 38% los ha percibido ocasionalmente.

La ausencia de respuestas en las categorías de "nunca" y "frecuentemente" sugiere un nivel aceptable pero no perfecto de confiabilidad, en el cual la mayoría de los fallos no afectan de forma crítica la operación, pero son perceptibles en ciertos momentos.

Este resultado no representa una deficiencia estructural del sistema, pero refuerza la necesidad de establecer rutinas de mantenimiento preventivo, especialmente en cámaras con mayor exposición a condiciones ambientales (polvo, vibración, iluminación cambiante, etc.).

También puede considerarse implementar un sistema de monitoreo proactivo de salud de cámaras (heartbeat, alertas por señal perdida) para anticipar y atender estos casos antes de que generen un impacto mayor.

8. Cuando se reporta un problema en videovigilancia, ¿qué tan rápido se soluciona?

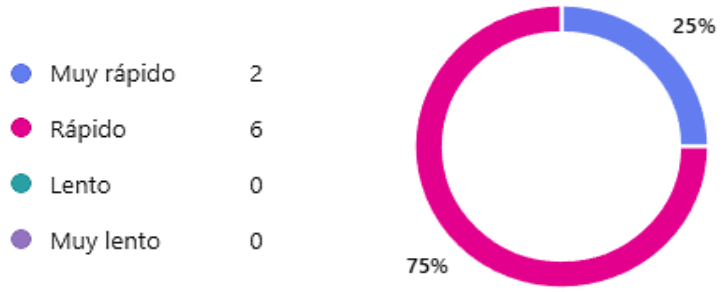


Figura 5.43 Resultados de la octava pregunta (Encuesta de videovigilancia). Elaboración propia.

Análisis e interpretación

Los resultados de esta pregunta reflejan una alta eficiencia en los tiempos de respuesta del equipo encargado de atender incidencias en el sistema de videovigilancia (véase Figura 5.43). El 100% de los usuarios percibe una atención oportuna, ya que ninguna respuesta fue clasificada como lenta o muy lenta.

El 75% de los encuestados indicó que la solución llega en un tiempo "rápido", mientras que un 25% la califica como "muy rápida", lo que evidencia una percepción positiva generalizada respecto al soporte técnico. Estos datos sugieren que el personal de TI o vigilancia cuenta con protocolos de atención efectivos y con la disponibilidad técnica adecuada para resolver incidentes de forma ágil, lo cual refuerza la confiabilidad operativa del sistema.

Pregunta 9. ¿Qué tan útil considera el sistema de cámaras para la seguridad, monitoreo de procesos y prevención de incidentes?

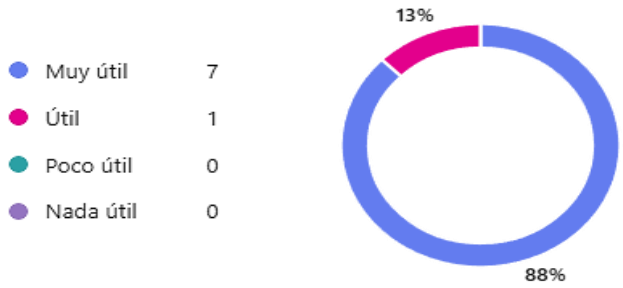


Figura 5.44 Resultados de la novena pregunta (Encuesta de videovigilancia). Elaboración propia.

Análisis e interpretación

En la Figura 5.44 los resultados indican que el sistema de videovigilancia instalado es altamente valorado por los usuarios en términos de funcionalidad y utilidad práctica. El 100% de los encuestados lo considera útil en algún grado, siendo destacable que el 88% lo percibe como “muy útil” para la seguridad, el monitoreo de procesos y la prevención de incidentes.

Este nivel de satisfacción sugiere que el sistema no solo cumple su función disuasiva y de vigilancia, sino que además está bien integrado en los procesos de operación, seguridad y control. La respuesta positiva refuerza la idea de que la videovigilancia se ha convertido en una herramienta clave para mantener entornos seguros y supervisados, tanto en áreas críticas como en operaciones rutinarias.

La baja percepción de inutilidad (0%) evidencia también una adopción exitosa y una percepción favorable por parte de los usuarios, lo que valida tanto el diseño como la implementación del sistema.

Pregunta 10. ¿Qué nivel de satisfacción tiene con el sistema actual de videovigilancia IP?

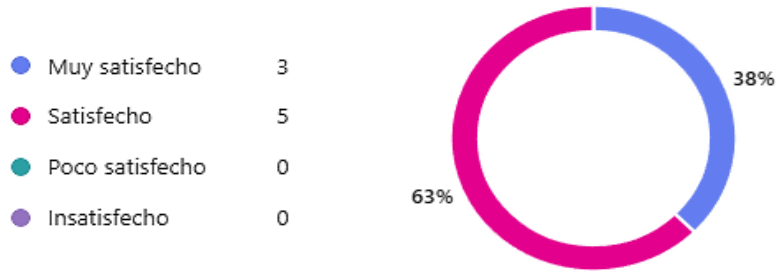


Figura 5.45 Resultados de la décima pregunta (Encuesta de videovigilancia). Elaboración propia.

Análisis e interpretación

Los resultados reflejan un alto nivel de satisfacción general con el sistema de videovigilancia IP implementado (véase Figura 5.45). El 100% de los usuarios se declara satisfecho o muy satisfecho, lo cual es un fuerte indicador de que el sistema está cumpliendo con las expectativas en cuanto a funcionalidad, utilidad, accesibilidad y calidad de imagen.

Aunque la mayoría de los encuestados se ubica en el nivel de “satisfecho” (63%), y un menor porcentaje en “muy satisfecho” (38%), la ausencia total de respuestas negativas (como “poco satisfecho” o “insatisfecho”) reafirma que la implementación ha sido positiva y que el sistema ha sido bien recibido por los usuarios.

Estos resultados sugieren que si bien hay áreas que podrían seguir optimizándose para elevar aún más la experiencia del usuario (por ejemplo, facilidad de acceso, mejoras en interfaz, cobertura específica), en términos generales el sistema ya ofrece una solución robusta y confiable para la videovigilancia en el entorno empresarial.

Pregunta 11. ¿Qué mejoras recomendaría para el sistema de videovigilancia (ej. mayor cobertura, mejor calidad de imagen, más al almacenamiento, acceso remoto, etc.)?

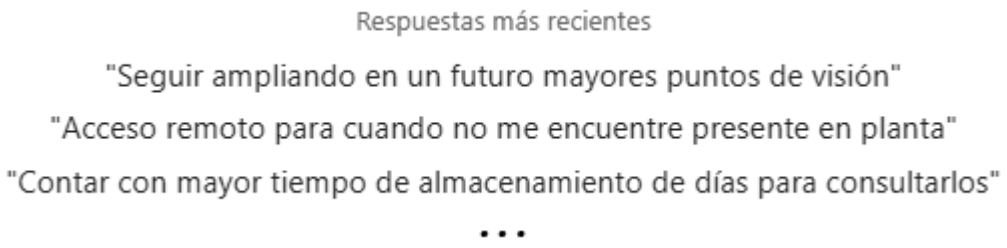


Figura 5.46 Resultados de la undécima pregunta (Encuesta de videovigilancia). Elaboración propia.

Análisis e interpretación

En el resumen de la Figura 5.46, las sugerencias de mejora por parte de los usuarios, aunque limitadas en cantidad, son altamente valiosas y orientadas a reforzar la funcionalidad del sistema en el mediano y largo plazo.

Ampliación de cobertura: La recomendación de instalar más cámaras o puntos de visión refleja una intención de alcanzar una vigilancia más completa, posiblemente en áreas que aún no cuentan con cobertura visual total o que requieren nuevos ángulos.

Acceso remoto: Este punto señala la necesidad de habilitar o mejorar el acceso a las cámaras desde fuera de planta. La solicitud apunta a una mayor flexibilidad operativa y control en tiempo real, lo cual es especialmente útil para supervisión ejecutiva o fuera de horarios laborales.

Mayor almacenamiento: Los comentarios sobre extender el período de retención de grabaciones sugieren que el tiempo actual podría resultar limitado en caso de análisis posterior de incidentes. Se recomienda evaluar discos adicionales, escalabilidad del NVR o soluciones en la nube si se requiere una retención mayor.

En conjunto, estas observaciones indican que, aunque el sistema es funcional y cumple con las necesidades actuales, existe una visión de mejora progresiva por parte de los usuarios, lo cual es positivo para futuros ciclos de inversión tecnológica.

5.1. Síntesis

El presente capítulo expuso de forma detallada los resultados obtenidos tras la implementación del proyecto de modernización tecnológica de la red industrial, telefonía IP y sistema de videovigilancia en la empresa. A partir de un enfoque comparativo entre la situación inicial y la condición posterior a la intervención, se evidenció una mejora significativa en los principales indicadores de conectividad, tales como velocidades de descarga y subida, latencia de red y estabilidad del servicio Wi-Fi, tanto en áreas administrativas como en zonas de producción. Asimismo, se documentó con evidencia fotográfica la instalación de equipamiento clave como switches, puntos de acceso, cámaras IP y teléfonos VoIP, además de la organización del site principal mediante racks, organizadores y etiquetado estructurado.

Las mediciones realizadas en distintos puntos y distancias demostraron el cumplimiento de los objetivos de cobertura y desempeño establecidos en la propuesta técnica, mientras que las encuestas de validación dirigidas al personal permitieron recoger la percepción general de los usuarios respecto a la calidad del servicio. En ellas, se obtuvo una alta satisfacción en cuanto a velocidad, estabilidad, confiabilidad y soporte técnico, tanto en la red inalámbrica como en la telefonía IP y videovigilancia. Finalmente, se identificaron áreas de mejora futura, tales como la capacitación en seguridad digital y la expansión del sistema de videovigilancia, lo cual servirá como base para nuevas fases del proyecto.

CAPÍTULO VI. Conclusiones

El presente proyecto de modernización de la infraestructura tecnológica permitió cumplir el objetivo general, al reestructurar la red en un entorno industrial mediante la implementación de telefonía VoIP segura, optimizando la conectividad y fortaleciendo la comunicación interna. La intervención integral (diagnóstico, rediseño de la arquitectura, actualización de equipos y reorganización del site) dio como resultado una red más estable, segura y alineada a las necesidades operativas de la planta. Como consecuencia directa, se logró incrementar la eficiencia en los procesos de comunicación, reducir incidencias relacionadas con la conectividad y establecer una plataforma tecnológica confiable, capaz de soportar servicios críticos como telefonía IP y videovigilancia sin afectar la operación diaria.

Las mediciones técnicas realizadas antes y después de la implementación evidenciaron mejoras significativas en el desempeño de la red, destacando el aumento en las velocidades de descarga y subida, la reducción del ping promedio y una menor tasa de fallos de conectividad, incluso en zonas críticas como producción y oficinas administrativas alejadas. Adicionalmente, los resultados de las encuestas de validación indican que más del 95 % del personal considera adecuada la velocidad, estabilidad y calidad del servicio VoIP, lo que confirma de manera objetiva que la infraestructura renovada cumple con los requerimientos técnicos y operativos del entorno industrial.

Como trabajo a futuro se recomienda fortalecer la seguridad informática mediante programas de capacitación dirigidos al personal, dado que una parte de los usuarios manifestó no haber recibido formación específica sobre el uso seguro de la red y los servicios asociados. Además, se propone ampliar la cobertura del sistema de videovigilancia a nuevas áreas operativas, incrementar la capacidad y tiempo de almacenamiento del NVR, e implementar un protocolo de mantenimiento preventivo y actualización tecnológica periódica, con el fin de garantizar la sostenibilidad y evolución de los beneficios alcanzados.

Referencias

Alcarraz Díaz, P. D., & Escobar Díaz, D. A. (2021). *Estudio de un sistema de video vigilancia mediante tecnología PoE para el barrio Calluma Bajo de la Parroquia de Pifo.* Trabajo previo a la obtención del título de Tecnólogo en Electrónica y Telecomunicaciones, Escuela Politécnica Nacional, Quito, Ecuador. Obtenido de https://bibdigital.epn.edu.ec/bitstream/15000/21430/1/CD%2010921.pdf

Altamirano Hernández, E. (2013). *Diseño de una red aplicando PBX e IP.* Tesis de licenciatura, Instituto Politécnico Nacional - Escuela Superior de Ingeniería Mecánica y Eléctrica, Unidad Culhuacán, México, D.F. Obtenido de https://tesis.ipn.mx/jspui/bitstream/123456789/15081/1/I.C.E.%2038-13.pdf

Barceló et al. (2004). *Software libre: Redes de computadores.* Barcelona: Fundació per a la Universitat Oberta de Catalunya.

Barros Losada, T. (2017). *La Industria 4.0: Aplicaciones e Implicaciones.* Universidad de Sevilla, Organización Industrial y Gestión de Empresas II. Sevilla: Universidad de Sevilla. Obtenido de https://biblus.us.es/bibing/proyectos/abreproy/91146/fichero/La+Industria+4.0+Aplicaciones+e+Implicaciones.pdf

Becerra Aldeán, R. F. (2024). *Simulación de un sistema de comunicaciones utilizando la tecnología IEEE 802.11BE.* Trabajo de integración curricular para la obtención del título de Ingeniero en Telecomunicaciones, Escuela Politécnica Nacional, Quito (DMQ). Obtenido de https://bibdigital.epn.edu.ec/bitstream/15000/26198/1/CD%2014418.pdf

Benites Cruz, C. R. (2023). *Red de datos de fibra óptica redundante para la comunicación de los servicios del sistema de gestión industrial de la fábrica Impaecsa-Essity, sede Babahoyo.* Proyecto de investigación, Universidad Técnica de Babahoyo, Babahoyo. Obtenido de http://dspace.utb.edu.ec/handle/49000/14789

Calani, G. (2010). CCTV Analógico vs. IP: Análisis comparativo de tecnologías y sistemas. *Negocios de Seguridad*(54), 214. Obtenido de http://www.rnds.com.ar/revistas/054/RNDS_054.pdf

Caldera Palma, J. C., & Suazo Sequeira, W. E. (2011). *Planeación de un curso especializado en telefonía para profesionales de la industria de telecomunicaciones: Módulo III Telefonía IP.* Tesis de pregrado, Universidad Nacional de Ingeniería, Managua. Obtenido de https://ribuni.uni.edu.ni/1261/1/25717-MIIITIP.pdf

Casierra et al. (2018). Virtualización de Redes y Servidores Emulando Infraestructuras Tecnológicas. *Revista Científica Hallazgos21, 3*, 11. Obtenido de http://revistas.pucese.edu.ec/hallazgos21

Castellón Arenas, A. (2014). *Cableado estructurado: norma EIA TIA 568.* Material educativo, Fundación Tecnológica Antonio de Arévalo - TECNAR, Cartagena de Indias.

Cisco Systems. (2025). *Wi-Fi 7 and the Growing Future of Wireless.* Cisco Systems. Obtenido de https://www.cisco.com/c/en/us/products/collateral/networking/wireless/wifi7-future-of-wireless-dg.html

Cortes Altamiranda, R. J., & Castellar Jiménez, J. E. (2024). *Diseño de una Infraestructura de Red Segura y Eficiente para la Transformación Organizacional de InnovaNet Technologies.* Trabajo de grado Seminario de Profundización para optar el título de Ingeniero de Sistemas, Universidad Cooperativa de Colombia, Montería, Colombia.

García Mata, F. J. (2011). *Videovigilancia: CCTV usando vídeos IP.* España, España: ELEARNING.

George et al. (August de 2023). Wi-Fi 7: The Next Frontier in Wireless Connectivity. *Partners Universal International Innovation Journal (PUIIJ), 1*(4). doi:10.5281/zenodo.8266217

Jaimes et al. (2011). Gestión tecnológica: conceptos y casos de aplicación. *Gerenc. Tecnol. Inform., 10*(26), 43-54. Obtenido de https://revistas.uis.edu.co/index.php/revistagti/article/view/2289

Jinez Granja, R. D., & Pantoja Prado, C. H. (2020). *Diseño de un sistema de videovigilancia para el barrio Los Pinos de la Parroquia Pifo.* Trabajo previo a la obtención del título de Tecnólogo en Electrónica y Telecomunicaciones, Escuela Politécnica Nacional, Quito. Obtenido de https://bibdigital.epn.edu.ec/handle/15000/21340

John et al. . (2024). Industry 4.0 and Beyond: The Role of 5G, WiFi 7, and Time-Sensitive Networking (TSN) in Enabling Smart Manufacturing. *Future Internet, 16*(345), 19. doi:https://doi.org/10.3390/fi16090345

Joskowicz, J. (2006). *Cableado estructurado.* Versión 5, Universidad de la República, Instituto de Ingeniería Eléctrica, Montevideo. Obtenido de https://www.researchgate.net/publication/27557682_Cableado_estructurado

Kurose, J., & Ross, K. (2017). *Redes de computadoras: Un enfoque descendente* (7.a ed. ed.). Madrid, España: Pearson.

López Rodríguez, J. C. (2007). *Estructura, funcionamiento y aplicación de las Cámaras IP.* Tesis de licenciatura, Universidad Autónoma del Estado de Hidalgo, Pachuca de Soto. Obtenido de http://dgsa.uaeh.edu.mx:8080/handle/231104/1747

López, M. (7 de agosto de 2023). *Cableado estructurado*. Obtenido de Alejandría - Repositorio de conocimiento: https://alejandria.edu.uy/archivos/865

Martínez Tello, A. F. (2025). *Diseño de red inalámbrica para dispositivos IoT, en un ambiente industrial.* Proyecto fin de carrera para optar al título de Ingeniero Electrónico, Universidad

de los Andes. Obtenido de https://repositorio.uniandes.edu.co/server/api/core/bitstreams/58ba500b-d7b4-4ac8-8170-7f50c02f3337/content

Murad et al. (2024). Introduction to Wi-Fi 7: A Review of History, Applications, Challenges, Economical Impact and Research Development. *Mesopotamian Journal of Computer Science*, 128-139. doi:https://doi.org/10.58496/MJCSC/2024/009

Odremán R., J. G. (2014). Gestión tecnológica: estrategias de innovación y transferencia de tecnología en la industria. *Universidad, Ciencia y Tecnología, 18*(73), 181-191. Obtenido de https://ve.scielo.org/pdf/uct/v18n73/art04.pdf

Pangol Lascano, A. M. (2022). Industria 4.0, implicaciones, certezas y dudas en el mundo laboral. *Revista Universidad y Sociedad, 14*(4), 453-465. Obtenido de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202022000400453&lng=es&tlng=

Redacción AvisoVoz. (28 de marzo de 2018). *Avisovoz*. Obtenido de https://www.avisovoz.com/call-center/voip-y-sip.html

Salimbeni, S., & Bianchi, S. (Julio de 2019). Estado actual y evolución de la industria nacional hacia la industria 4.0. *INNOVA UNTREF: Revista Argentina de Ciencia y Tecnología*(3). Obtenido de https://revistas.untref.edu.ar/index.php/innova/article/view/986

Soler Palacín, E. (2009). *Diseño e implementación de una solución de VoIP.* Proyecto Final de Carrera, Universitat Politècnica de Catalunya - Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona, Barcelona, España. Obtenido de https://upcommons.upc.edu/server/api/core/bitstreams/9fa5b573-6698-464d-ae67-8ed58f130e5a/content

Tanenbaum, A. S., & Wetherall, D. J. (2012). *Redes de computadoras* (5ª edición ed.). México: Pearson Educación.

Trefilados Inoxidables de México. (2024). *Trefilados Inoxidables de México.* Obtenido de Trefilados Inoxidables de México: https://www.trefilados.com.mx/

Unión Internacional de Telecomunicaciones (UIT). (2003). *Informe esencial sobre telefonía por el protocolo Internet (IP).* Unidad de Ciberestrategias de la UIT / Grupo de Expertos sobre Telefonía IP del UIT-D. Ginebra, Suiza: UIT (Unión Internacional de Telecomunicaciones). Obtenido de www.itu.int/ITU-D/e-strategies

Veloz Pérez, R. (2019). *Manual para el curso redes y enlaces de fibra óptica: Guía de estudios técnicos* (1.a ed. ed.). Chile: Brainamics.

Yandar Lobón, M., & Moreno Ospina, J. M. (2019). *La industria 4.0: desde la perspectiva organizacional.* Santa Ana de Coro, Venezuela: Fondo Editorial Universitario Servando Garcés de la Universidad Politécnica Territorial de Falcón Alonso Gamero.

Zúñiga Vázquez, H. (Noviembre de 2022). *Infraestructura física de red Ethernet para la industria 4.0.* Tesis de maestría, Tecnológico Nacional de México Campus Querétaro, Querétaro. Obtenido de https://rinacional.tecnm.mx/jspui/bitstream/TecNM/8052/1/TESIS%20HERIBERTO%20Z%C3%9A%C3%91IGA%20V%C3%81ZQUEZ.pdf

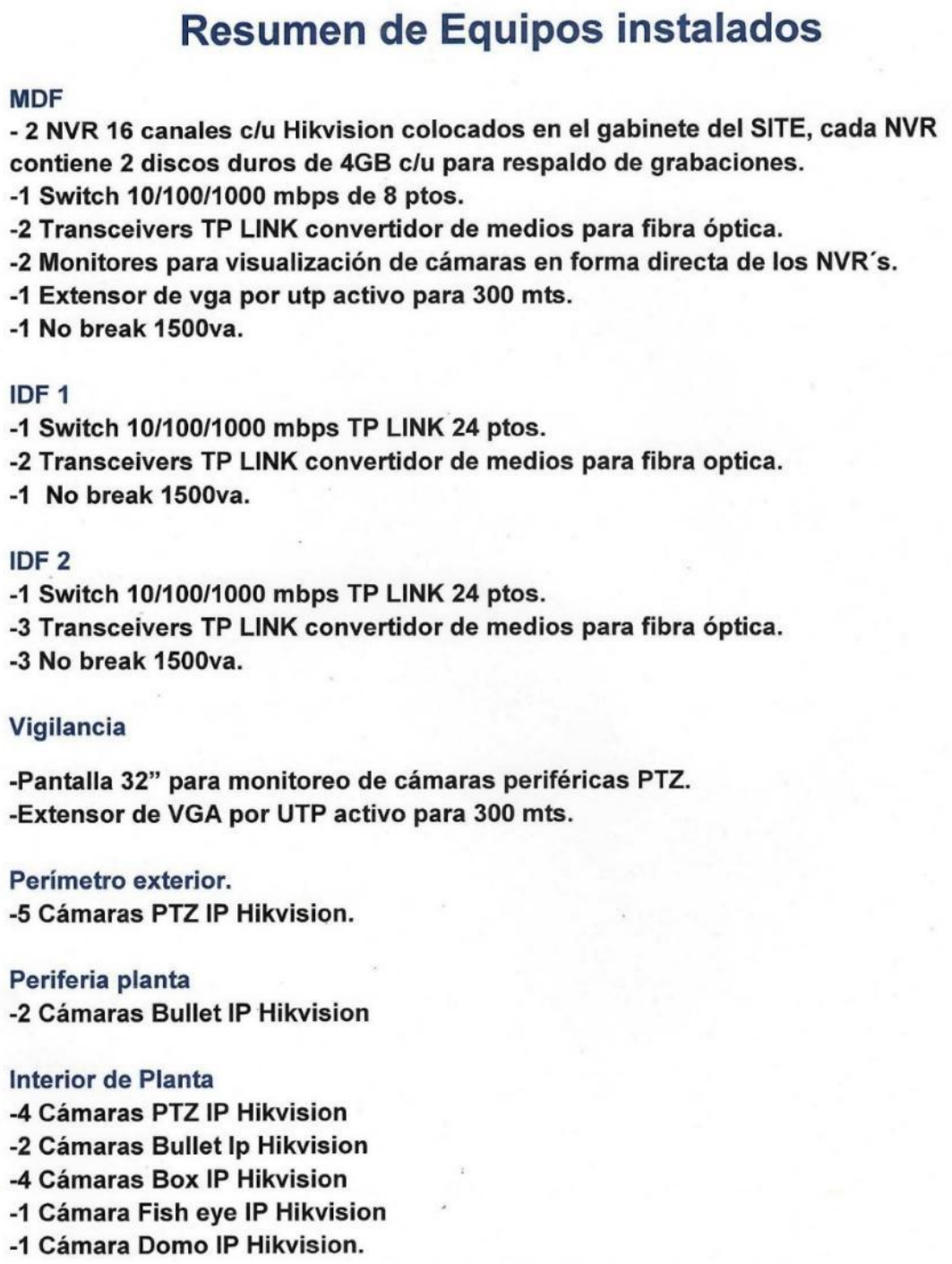
Glosario

- **AP (Access Point):** Dispositivo de red que permite la conexión inalámbrica de equipos finales a una red cableada.
- **Backbone:** Conjunto de enlaces principales que interconectan los distintos segmentos de una red y soportan el mayor volumen de tráfico.
- **Cableado estructurado:** Sistema estandarizado de cables, conectores y dispositivos que permite organizar y administrar la infraestructura de red de forma ordenada y escalable.
- **Cámara bullet:** Tipo de cámara de videovigilancia con diseño cilíndrico, comúnmente utilizada en exteriores o áreas de largo alcance.
- **Cámara domo:** Cámara de videovigilancia con carcasa semiesférica, utilizada principalmente en interiores por su diseño discreto.
- **CCTV (Closed Circuit Television):** Sistema de videovigilancia que utiliza cámaras para la supervisión y control de áreas específicas.
- **Conversor de medios:** Dispositivo que permite la conversión entre señales eléctricas y ópticas, facilitando la interconexión entre enlaces de cobre y fibra óptica.
- **Fibra óptica monomodo:** Tipo de fibra óptica diseñada para transmitir una sola trayectoria de luz, utilizada en enlaces de larga distancia debido a su baja atenuación.
- **Fibra óptica multimodo:** Tipo de fibra óptica que permite múltiples trayectorias de luz, empleada principalmente en enlaces de corta distancia dentro de instalaciones.
- **IDF (Intermediate Distribution Frame):** Gabinete intermedio que distribuye la conectividad de red hacia áreas específicas dentro de una instalación.
- **IP (Internet Protocol):** Protocolo de comunicación que permite el direccionamiento y enrutamiento de paquetes de datos en redes digitales.
- **LAN (Local Area Network):** Red de área local que interconecta dispositivos dentro de un espacio geográfico limitado.
- **Latencia:** Tiempo que tarda un paquete de datos en viajar desde su origen hasta su destino dentro de una red.

- **MDF (Main Distribution Frame):** Gabinete principal donde se concentran los equipos centrales de red y las conexiones troncales.
- **Mini-GBIC / SFP (Small Form-factor Pluggable):** Módulo transceptor intercambiable que permite la conversión de señales eléctricas a ópticas en equipos de red.
- **NVR (Network Video Recorder):** Dispositivo encargado de almacenar, gestionar y reproducir grabaciones provenientes de cámaras IP.
- **Patch cord:** Cable de interconexión utilizado para enlazar equipos de red o paneles de parcheo dentro de una infraestructura de cableado estructurado.
- **Pigtail de fibra óptica:** Cable corto de fibra óptica con conector en un extremo, utilizado para la terminación y empalme de enlaces dentro de gabinetes o distribuidores ópticos.
- **PoE (Power over Ethernet):** Tecnología que permite suministrar energía eléctrica a dispositivos de red a través del cable de datos Ethernet.
- **PTZ (Pan-Tilt-Zoom):** Tipo de cámara de videovigilancia con capacidad de movimiento horizontal, vertical y zoom controlado de forma remota.
- **QoS (Quality of Service):** Conjunto de mecanismos que permiten priorizar el tráfico de red para garantizar el desempeño de aplicaciones críticas.
- **Red troncal:** Infraestructura principal de interconexión que enlaza los distintos segmentos de una red.
- **Segmentación de red:** Práctica que consiste en dividir una red en secciones lógicas para mejorar seguridad, desempeño y administración.
- **Switch:** Dispositivo de red que interconecta múltiples equipos dentro de una red local y gestiona el tráfico de datos entre ellos.
- **Throughput:** Cantidad de datos que una red puede transmitir de manera efectiva en un periodo determinado.
- **Uplink:** Enlace que conecta un dispositivo de acceso con un equipo de mayor jerarquía dentro de la red.
- **VLAN (Virtual Local Area Network):** Segmentación lógica de una red que permite aislar tráfico y mejorar la seguridad y eficiencia.
- **VoIP (Voice over Internet Protocol):** Tecnología que permite la transmisión de voz mediante redes basadas en el Protocolo de Internet.
- **Wi-Fi (Wireless Fidelity):** Tecnología de comunicación inalámbrica que permite la conexión de dispositivos a redes locales sin cableado físico.

Anexos

Anexo A. Resumen de equipos instalados en la red de videovigilancia



Resumen de Equipos instalados

MDF

- 2 NVR 16 canales c/u Hikvision colocados en el gabinete del SITE, cada NVR contiene 2 discos duros de 4GB c/u para respaldo de grabaciones.
-1 Switch 10/100/1000 mbps de 8 ptos.
-2 Transceivers TP LINK convertidor de medios para fibra óptica.
-2 Monitores para visualización de cámaras en forma directa de los NVR´s.
-1 Extensor de vga por utp activo para 300 mts.
-1 No break 1500va.

IDF 1

-1 Switch 10/100/1000 mbps TP LINK 24 ptos.
-2 Transceivers TP LINK convertidor de medios para fibra optica.
-1 No break 1500va.

IDF 2

-1 Switch 10/100/1000 mbps TP LINK 24 ptos.
-3 Transceivers TP LINK convertidor de medios para fibra óptica.
-3 No break 1500va.

Vigilancia

-Pantalla 32" para monitoreo de cámaras periféricas PTZ.
-Extensor de VGA por UTP activo para 300 mts.

Perímetro exterior.

-5 Cámaras PTZ IP Hikvision.

Periferia planta

-2 Cámaras Bullet IP Hikvision

Interior de Planta

-4 Cámaras PTZ IP Hikvision
-2 Cámaras Bullet Ip Hikvision
-4 Cámaras Box IP Hikvision
-1 Cámara Fish eye IP Hikvision
-1 Cámara Domo IP Hikvision.

Figura A 1 Resumen de equipos instalados en la red de videovigilancia IP, incluyendo MDF, IDF, equipos de monitoreo y tipos de cámaras por área.

Fuente: Documentación técnica interna de la empresa..

Anexo B. Planos originales de arquitectura de la red LAN de videovigilancia

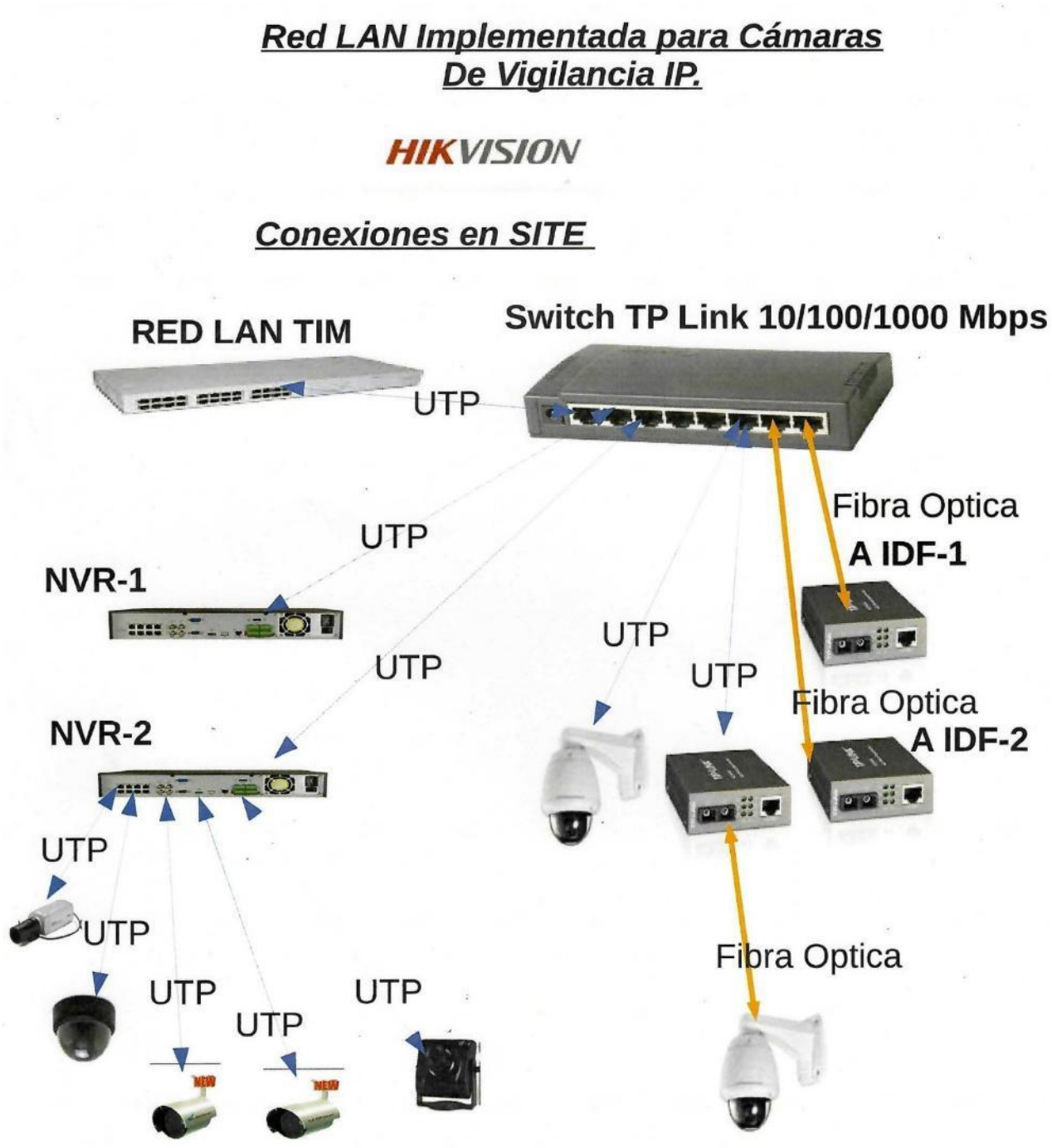


Figura A 2 Diagrama original de la red LAN implementada para cámaras de vigilancia IP en el SITE, mostrando la interconexión entre NVR, switches y enlaces de fibra óptica hacia los IDF.

Fuente: Documentación técnica interna de la empresa.

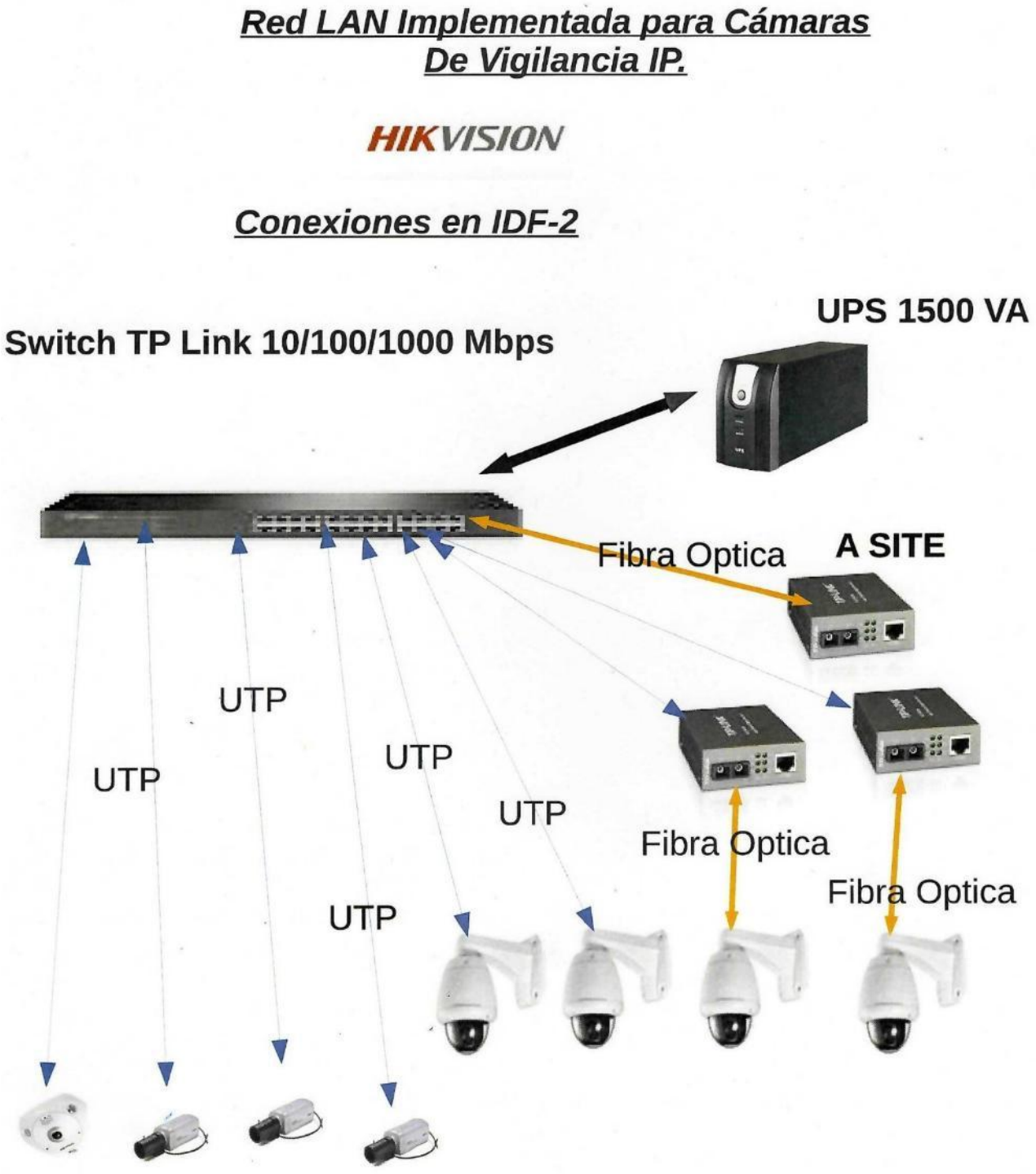


Figura A 3 Diagrama original de conexiones de la red LAN de videovigilancia IP en el IDF-2, incluyendo switch, UPS, enlaces de fibra óptica y cámaras conectadas por UTP.

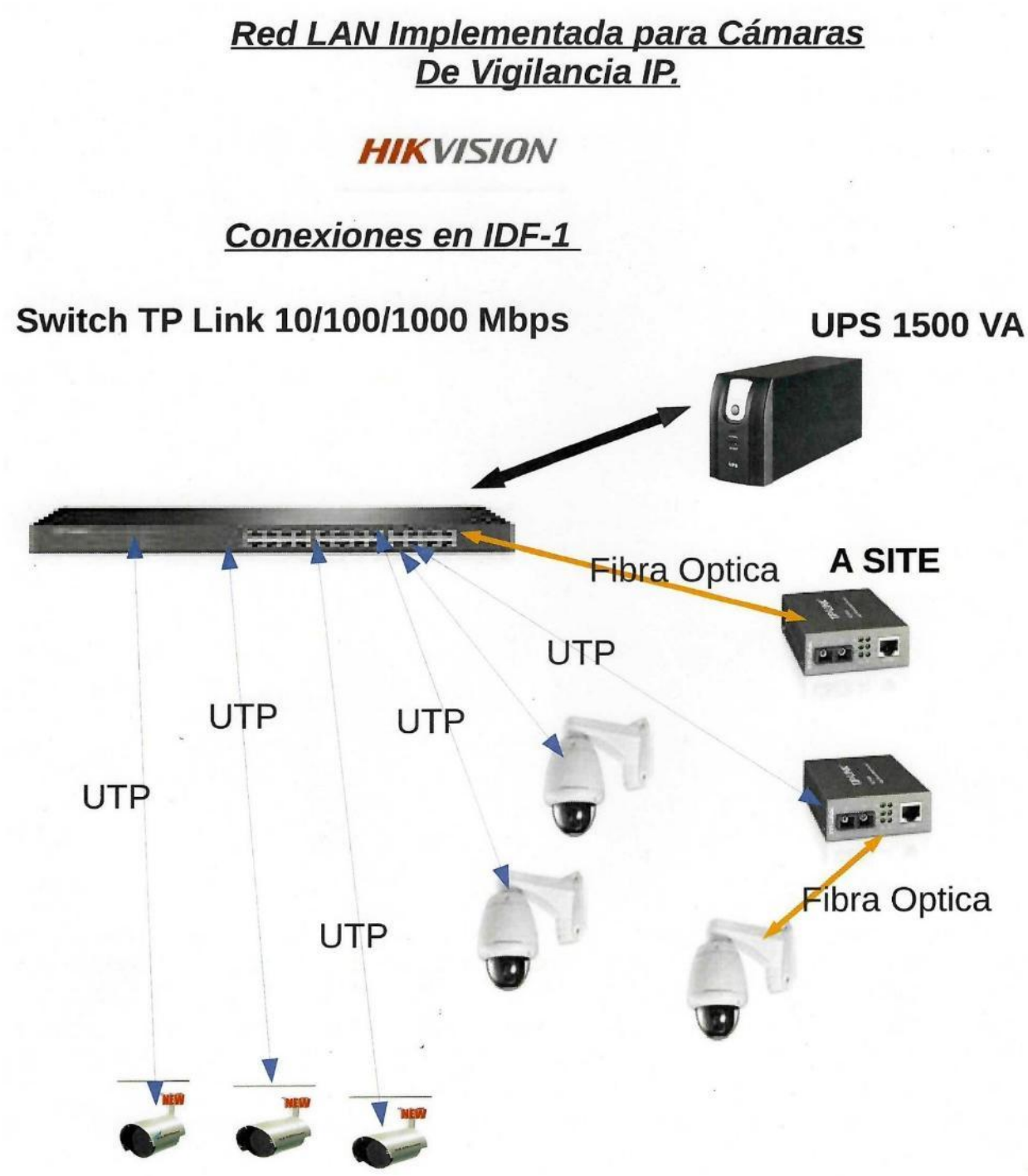
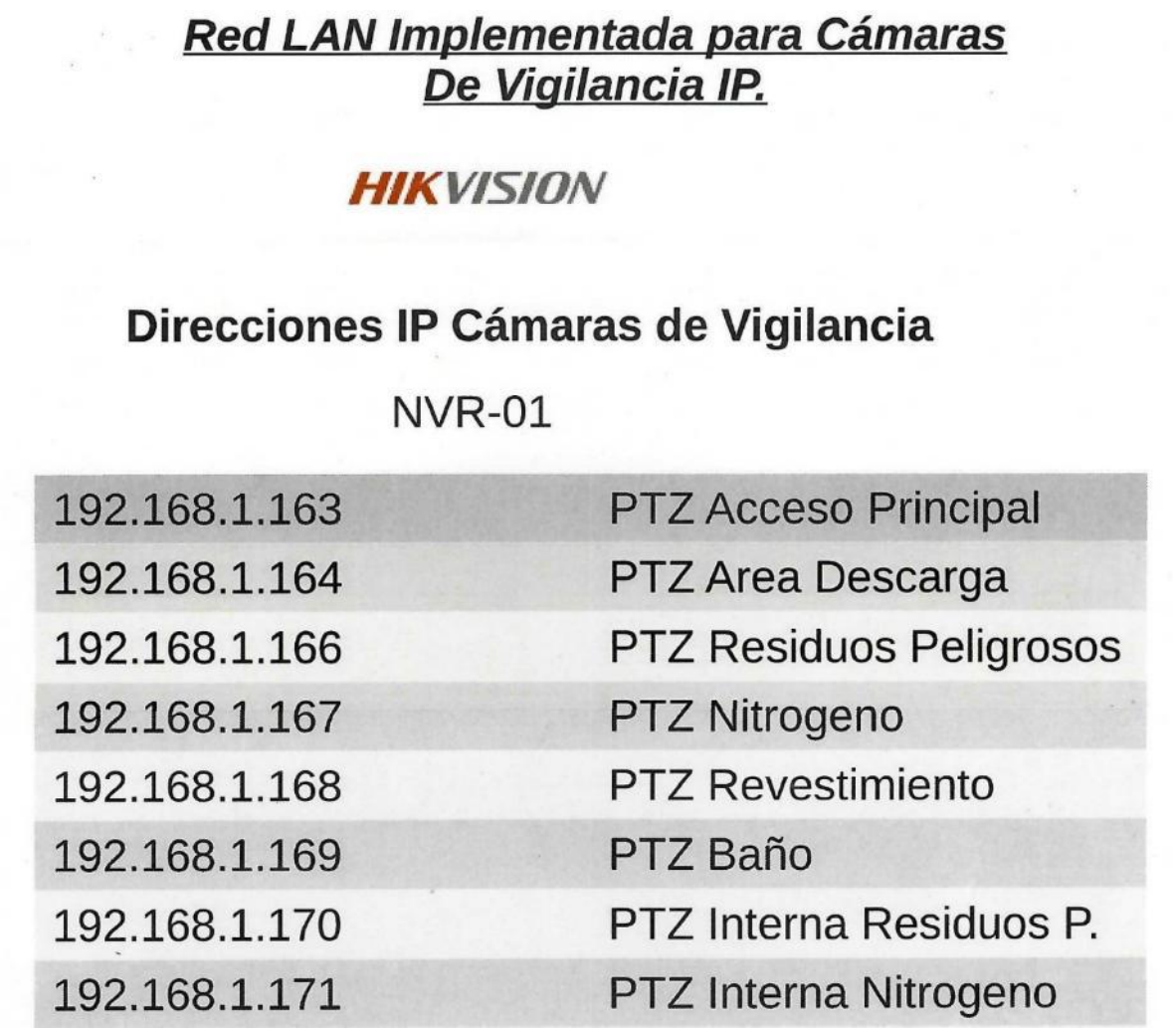


Figura A 4 Diagrama original de conexiones de la red LAN de videovigilancia IP en el IDF-1, con enlaces de fibra óptica al SITE y distribución de cámaras IP por cableado UTP.

Fuente: Documentación técnica interna de la empresa.

Anexo C. Registros históricos de direccionamiento IP del sistema CCTV



Red LAN Implementada para Cámaras De Vigilancia IP.

HIKVISION

Direcciones IP Cámaras de Vigilancia

NVR-01

192.168.1.163	PTZ Acceso Principal
192.168.1.164	PTZ Area Descarga
192.168.1.166	PTZ Residuos Peligrosos
192.168.1.167	PTZ Nitrogeno
192.168.1.168	PTZ Revestimiento
192.168.1.169	PTZ Baño
192.168.1.170	PTZ Interna Residuos P.
192.168.1.171	PTZ Interna Nitrogeno

Figura A 5 Listado histórico de direcciones IP asignadas a cámaras de vigilancia IP del NVR-01 en el segmento 192.168.1.x.

Fuente: Documentación técnica interna de la empresa.