UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO
ESCUELA SUPERIOR DE TIZAYUCA

Maestría en Gestión y Desarrollo de Nuevas Tecnologías

TESIS

PROPUESTA DE RED INDUSTRIAL SEGURA Y ESCALABLE PARA EL ENTORNO MANUFACTURERO BASADA EN NORMAS Y ESTÁNDARES INTERNACIONALES EN UNA EMPRESA PRODUCTORA DE NEUMÁTICOS EN MÉXICO

Que para obtener el grado de
Maestra en Gestión y Desarrollo de Nuevas Tecnologías

PRESENTA

Raquel Mejía García

Directora

Dra. Evangelina Lezama León

Comité tutorial

Mtro. Alonso Ernesto Solís Galindo

Dr. Eduardo Alvarado Santos

Tizayuca, Hgo., México, junio 2026

Universidad Autónoma del Estado de Hidalgo
Escuela Superior de Tizayuca
Campus Tizayuca

ESTizayuca/707/2026
Asunto: Autorización de impresión

Mtra. Ojuky del Rocío Islas Maldonado
Directora de Administración Escolar
Presente.

El Comité Tutorial de la **TESIS** del programa educativo de posgrado titulado **"PROPUESTA DE RED INDUSTRIAL SEGURA Y ESCALABLE PARA EL ENTORNO MANUFACTURERO BASADA EN NORMAS Y ESTÁNDARES INTERNACIONALES EN UNA EMPRESA PRODUCTORA DE NEUMÁTICOS EN MÉXICO"**, realizado por la sustentante **RAQUEL MEJÍA GARCÍA** con **número de cuenta 184027** perteneciente al programa de **MAESTRÍA EN GESTIÓN Y DESARROLLO DE NUEVAS TECNOLOGÍAS**, una vez que ha revisado, analizado y evaluado el documento recepcional de acuerdo a lo estipulado en el Artículo 110 del Reglamento de Estudios de Posgrado, tiene a bien extender la presente:

AUTORIZACIÓN DE IMPRESIÓN

Por lo que la sustentante deberá cumplir los requisitos del Reglamento de Estudios de Posgrado y con lo establecido en el proceso de grado vigente.

Atentamente
"Amor, Orden y Progreso"
Tizayuca, Hidalgo a 26 de junio de 2026

El Comité Tutorial

Dra. Evangelina Lezama León
Nombre y firma del director

Mtro. Alonso Ernesto Solís Galindo
Nombre y firma del miembro del comité

Dr. Eduardo Alvarado Santos
Nombre y firma del miembro del comité

Carretera Tizayuca-Pachuca Km. 2.5 s/n, Tizayuca, Hidalgo, México; C.P. 43800
Teléfono: 7717172000 Ext. 50501, 50502
tizayuca@uaeh.edu.mx
uaeh.edu.mx

DEDICATORIA

Dedico la presente tesis a Dios por guiarme en cada etapa de mi vida y permitirme concluir este importante y difícil sueño.

A mi familia, que me apoya con todo cariño y amor, pero principalmente a mi hno. Samuel Mejía, por compartir tantas experiencias, trabajo, logros y batallas juntos que me inspiran a seguir adelante para demostrar que nada en esta vida te encadena y limita más que nuestra propia mente y nada nos controla más que nuestros propios miedos; el éxito lo determina la perseverancia y constancia, no la suerte.

AGRADECIMIENTOS

Agradezco este logro a Dios, por darme la fuerza para perseverar y la sabiduría para emprender este proyecto, del cual cada éxito es un testimonio de que él está presente en mi vida.

Durante el proceso de esta investigación, he contado con la dicha de recibir el apoyo de muchas personas que contribuyeron de diferentes maneras a la finalización de este trabajo.

Expreso mi más profundo agradecimiento a la Universidad Autónoma del Estado de Hidalgo por brindarme la oportunidad y los recursos para llevar a cabo esta investigación.

De la misma manera, deseo manifestar un sincero reconocimiento a mi directora de tesis, la Dra. Evangelina Lezama León, por su guía, dirección, paciencia y orientación durante todo el desarrollo; reconozco su amplia experiencia en el ámbito educativo y profesional, que fue clave para permitirme concluir con la elaboración de mi propuesta de tesis.

A mis hermanos y sobrinos por ser mi pilar e inspiración fundamental, a mi mamá que me brinda su amor y apoyo incondicional en todo momento y principalmente cuando estuve a punto de abandonar mis objetivos.

De manera especial, agradezco a mi esposo Aldo López por su gran y sincero apoyo en este corto tiempo y por ser parte de mis mayores sueños.

Finalmente, me gustaría mostrar mi más grande agradecimiento a mi hijo Aldo Emilio, quien me inspira en cada momento a realizar todo por él.

DESCARGO DE RESPONSABILIDAD

La información contenida en esta tesis es el resultado de una investigación académica y no debe ser interpretada como asesoramiento profesional en el diseño de redes de telecomunicaciones industriales. El autor no se hace responsable de cualquier consecuencia derivada del uso que se haga de esta información. El autor se exime de toda responsabilidad ante cualquier malentendido o acción derivada de la aplicación de las recomendaciones presentadas en el presente trabajo.

Los contenidos aquí presentados se utilizan con fines académicos y de investigación. Se ha procurado la debida citación de las fuentes originales; sin embargo, cualquier infracción involuntaria es ajena a la voluntad del autor. El presente trabajo es una obra académica de carácter personal. La Universidad Autónoma del Estado de Hidalgo no se hace responsable por el contenido aquí presentado, ni por las consecuencias que deriven de su aplicación o uso indebido por parte de terceros.

RESUMEN

En esta tesis se presenta una propuesta de diseño de infraestructura de red para entornos manufactureros, considerando la convergencia entre Tecnologías de Información (IT) y Tecnologías Operativas (OT). A partir de una revisión documental y normativa (ISO/IEC, IEEE, ANSI/TIA, IEC 62443, NIST), se identificaron brechas en la literatura y la ausencia de guías unificadas que integren seguridad, escalabilidad y gobernanza en redes industriales.

El trabajo presenta una arquitectura lógica y física que contempla segmentación IT/OT mediante DMZ (Zona desmilitarizada) industrial, backbone de alta capacidad (≥100 Gb), distribución redundante (25 Gb en OT, 10 Gb en acceso), integración de tecnologías inalámbricas (Wi-Fi 6) y lineamientos de ciberseguridad basados en Zero Trust. La evaluación de la propuesta incluye escenarios de migración tecnológica, análisis comparativo normativo, matrices de riesgo (FMEA) e indicadores de desempeño (KPI), lo que permite validar la coherencia interna y la alineación normativa de la propuesta. Se concluye que el diseño propuesto constituye un marco teórico-propositivo que orienta la transición hacia infraestructuras resilientes, seguras y preparadas para la Industria 4.0, aunque con la limitación de no incluir validación en entornos piloto reales.

Palabras clave: Infraestructura de red, IT/OT, manufactura, seguridad, escalabilidad.

ABSTRACT

This thesis presents a proposed network infrastructure design for manufacturing environments, focusing on the convergence of Information Technology (IT) and Operational Technology (OT). Based on a documentary and normative review (ISO/IEC, IEEE, ANSI/TIA, IEC 62443, NIST), research identified gaps in the literature and the lack of unified guidelines integrating security, scalability, and governance in industrial networks.

The project presents a logical and physical architecture that includes IT/OT segmentation through an industrial DMZ, a high-capacity backbone (≥100 Gb), redundant distribution (25 Gb in OT, 10 Gb at the access layer), integration of wireless technologies (Wi-Fi 6), and cybersecurity strategies aligned with Zero Trust principles. Conceptual evaluation comprises technological migration scenarios, comparative normative analysis, risk assessment (FMEA), and performance indicators (KPIs), ensuring coherence and compliance with international standards. The results highlight that the proposed design provides a theoretical and practical framework for transitioning toward resilient, secure, and Industry 4.0-ready infrastructures, while acknowledging the limitation of lacking validation in real-world pilot implementations.

Keywords: Network infrastructure, IT/OT, manufacturing, security, scalability.

índice

Figuras

Tablas

CAPÍTULO I. INTRODUCCIÓN

1.1 Antecedentes

El ser humano está inmerso en procesos de innovación y evolución constante que transforman a gran velocidad, entre los siglos XVIII, XIX y XX se han desarrollado cuatro revoluciones industriales que marcaron las bases de los sistemas de producción, transformando radicalmente la sociedad, la economía y la aplicación tecnológica en el entorno de TI/OT en los procesos industriales (Cosme Da Costa, et al., 2024).

La primera revolución industrial destacó por transformar a la sociedad agrícola y manual por la mecanización, la segunda revolución industrial evoluciona las técnicas y tecnologías en la industria, introduciendo la producción masiva; la tercera revolución nombrada científico tecnológica, basada en el aprovechamiento de informática y finalmente la industria 4.0 sustentada en varios principios; entre los más relevantes: interoperabilidad, descentralización, analítica en tiempo real, virtualización, orientación a servicio, modularidad y escalabilidad (Cosme Da Costa, et al., 2024)

En esta Industria converge la tecnología en el ámbito de TI/OT, en los sistemas propietarios, haciendo indispensable la utilización de protocolos y estándares genéricos para las soluciones de arquitecturas híbridas, con capacidad de soportar las operaciones de la infraestructura crítica aportando soluciones de seguridad, almacenamiento y procesamiento (Moreno et al., 2024).

La adopción de la industria 4.0 en el entorno manufacturero transforma principalmente a las redes de datos industriales debido a que el enfoque y la evolución está basada en la interconexión de sistemas, la computación en la nube, el Internet de las Cosas (IoT), la Inteligencia Artificial (IA), la robótica y la realidad aumentada (AR) (Mora, 2024). La infraestructura de las redes industriales converge

en Tecnologías de Información (IT), Infraestructura orientada a la gestión de datos empresariales, aplicaciones administrativas y servicios digitales; y Tecnologías Operativas (OT), enfocadas en los sistemas que supervisan y controlan procesos físicos en plantas industriales, como SCADA, DCS y PLCs, desempeñando roles complementarios en la operación y gestión de entornos industriales (Moreno et al., 2024).

Esta convergencia de tecnologías IT/OT en los procesos manufactureros obliga a fortalecer la seguridad de la red, mediante la implementación de firewalls, sistemas de detección de intrusos (IDS), y el uso de VLANs para segmentar el tráfico de red (Panko & Panko, 2018). Además, de establecer políticas de seguridad claras.

Dado a lo anterior y a las transformaciones que ha tenido la industria manufacturera es claro que la innovación actúa como común denominador, lo que implica que es una actividad esencial para todo tipo de industria, con independencia del sector, el ámbito de actuación, el tamaño y el enfoque desde el que se analice dicha competitividad; la innovación es el elemento clave que permite a las empresas conseguir ventajas competitivas (Suárez, et al., 2007).

Las innovaciones o transformaciones conllevan realizar implementaciones tecnológicas que requieren una infraestructura de red robusta, que permita estar preparados para los distintos desarrollos tecnológicos que demandan los servicios en la red con el objetivo de intercambiar información. En la actualidad, muchas empresas no se fijan en la importancia de una buena administración a nivel tecnológico de red, seguridad e infraestructura (Briggeth & Plazarte, 2023).

En el caso de una empresa productora de neumáticos, que en lo sucesivo denominaremos MB por cuestiones de confidencialidad, representa la segunda empresa más importante en México y número uno a nivel mundial, con 120 plantas en 25 países; no se limita a la automatización básica o a la integración IT/OT, también demanda la adopción de tecnologías avanzadas como big data, inteligencia artificial (IA) y robótica industrial, que requieren redes escalables, seguras y de alto desempeño, por lo tanto, la infraestructura de la red constituye un factor decisivo

para que se puedan implementar estas soluciones a escala, garantizando continuidad operativa y resiliencia.

1.2 Formulación del problema

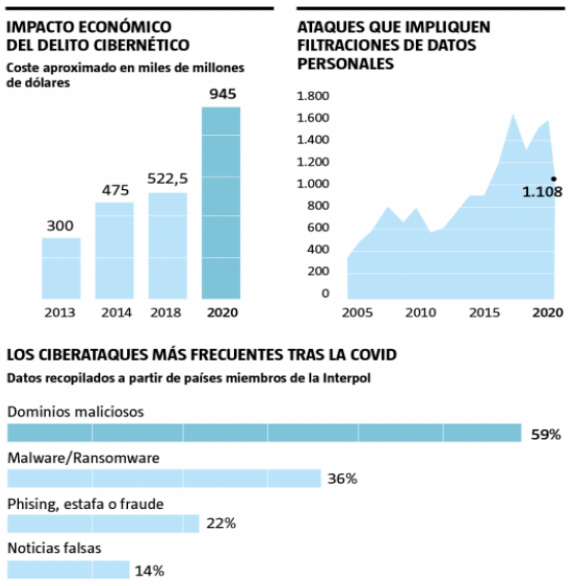
En el sector industrial, es necesario que exista una conexión estable y correcta para el intercambio de información en tiempo real, con las mínimas dificultades, ya que transportan información de diversa índole. La infraestructura de las redes, los centros de datos y las telecomunicaciones, permite el transporte de los datos y la interconexión hacia la red de redes (Internet). Por ello, es de vital importancia crear conciencia sobre las acciones que se deben tomar en lo referente a las inversiones y el otorgamiento de los recursos necesarios para asegurar la continuidad de los servicios, así como la implementación y el mantenimiento de sus proyectos (Díaz & Olmos, 2021).

Para las empresas, la tecnología y comunicación de redes son una herramienta fundamental, ya que este sistema permite que la operación se realice de forma óptima. En múltiples ocasiones se detectan servicios de red inestables que afectan la operación de las compañías (Briggeth & Plazarte, 2023).

La industria manufacturera dedicada a la transformación de materias primas a través de procesos de producción, control de calidad, inventario, logística e ingeniería, desempeña un papel fundamental en la economía global, aportando a la innovación y ayudando con el crecimiento económico, por lo que es esencial que cuente con una infraestructura que le permita optimizar la eficiencia y la calidad de la producción y sus procesos. Un modelo de operación de la infraestructura considera elementos de gestión de la tecnología, el talento humano y la tecnología requerida. Además, otorga las herramientas necesarias para asegurar la continuidad del servicio, enfrentando los riesgos potenciales a los que pueden estar expuestos la infraestructura de redes, los centros de datos y las telecomunicaciones (Díaz & Olmos, 2021).

Se ha analizado que, además de los problemas antes mencionados, se suman pérdidas irreversibles de información vital para la empresa. Toda organización, y principalmente las empresas de manufactura que involucran procesos, debe tener una red bien diseñada para el funcionamiento eficiente. Un claro ejemplo de las afectaciones que sufren los sectores al no contar con infraestructuras robustas ni redes de telecomunicaciones seguras son los impactos económicos ocasionados por los ciberataques. A continuación, se ilustran algunas pérdidas de los años 2013-2020.

Figura 1 Pérdidas de los años 2013-2020 por ataques cibernéticos



Fuente: McAfee, Interpol y Fondo Monetario Internacional (2021)

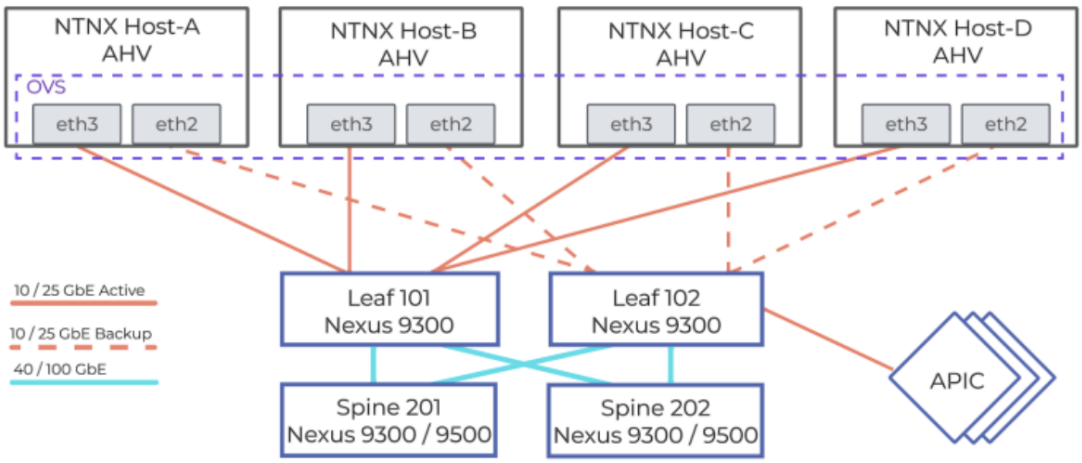
Esta investigación analiza la infraestructura de red LAN de la empresa MB productora de neumáticos en México, para proponer un diseño de red industrial que permita la escalabilidad, seguridad y adopción de nuevas tecnologías, elegida por ser el número uno a nivel mundial y su importante presencia en 25 países con 120 plantas en el mundo, además de la exportación a países como Estados Unidos, Chile, Argentina y Colombia.

La topología de la red LAN de la empresa MB es un diseño jerárquico o de árbol organizado en niveles, nodo de enlace troncal con switches catalyst C9400R con puertos de velocidades a 1/10 Gbps en fibra o cobre desde el que se ramifican los nodos intermedios con switches catalyst C9300 con puertos de velocidades a 1/10 Gbps y los nodos de acceso switches catalyst C2960X y C9200L con puertos de velocidades a 1Gbps. Segmentada en redes de área virtual (VLANs) para separar el tráfico OT de IT. Conectada a una red SDWAN que comunica las regiones de América.

En los últimos años, la empresa MB ha experimentado problemáticas al implementar nuevas tecnologías en la red de datos puesto que no cumple con los requerimientos mínimos de operación para el aprovechamiento del rendimiento adecuado del software o hardware, una de las deficiencias fue al presentarse la necesidad urgente de migrar el ambiente virtual de VMware a raíz de la adquisición por Broadcom en 2023 reestructurando el modelo del negocio aplicando suscripción obligatoria, precios por núcleo, mínimo de licencias, paquetes unificados, eliminación de versiones gratuitas, generando un fuerte aumento en los costos operativos, fuera de los montos asignados.

Como consecuencia fue necesario buscar una solución para mitigar los elevados costos, eligiendo realizar una migración hacia Nutanix por ser una plataforma que permite la portabilidad transparente, no obstante, durante la implementación se encontró una nueva problemática en la red por no cumplir con los requerimientos mínimos de implementación del fabricante mostrados en la figura 2.

Figura 2 Requerimientos de NUTANIX



Fuente: https://portal.nutanix.com/

En la figura 2 se observan las mejores prácticas de red del fabricante, en donde requiere equipos de la familia Nexus en el Core interconectados a velocidades de 40/100 Gbps con conexiones de red de 10/25 Gbps hacia los hosts, indicando que los equipos de la familia Catalyst no cumplen con los requisitos de alto rendimiento en los centros de datos, pero son aceptables para bajo rendimiento (NUTANIX, 2026) limitando el alcance que se puede lograr con la nueva plataforma.

Otra deficiencia se presentó al actualizar la arquitectura de SDWAN reemplazando los Firewalls CISCO por Firewalls de Palo alto network, este proceso se realizaría en etapas migrando las reglas de acuerdo a la criticidad de las subredes y VLANs configuradas para no afectar la operación, poniendo en la etapa final las reglas de las subredes que no eran parte de la operación OT ni del ambiente virtual, pero se enfrentó que una vez iniciado el cambio todas las infraestructuras de escritorios virtuales (VDI´s) tenían acceso a internet, además de los clientes delgados (monitores, wyses) y scaner´s, sumando que la correcta comunicación no fue la esperada debido a que la segmentación y los equipos asignados a las diferentes VLANs no estaba planificada o estructurada correctamente, poniendo en riesgo tanto los procesos de operación como la información de la empresa, mostrando una red vulnerable y con oportunidad de reforzar la seguridad con listas de acceso (ACL)

internas, además confirmar la separación de los procesos IT/OT totalmente para evitar que las problemáticas de cada una no se interfieran.

1.3. Justificación

La industria manufacturera tiene un impacto en la economía de cualquier país, en el caso de México, su relevancia se relaciona con la posición de liderazgo que ocupa en el mundo. Las exportaciones de la industria manufacturera de México tienen una amplia variedad de productos, desde equipo de transporte, computación, maquinaria y equipo, productos derivados del petróleo y del carbón, entre otros (Bátiz & Albarrán, 2023). En general, la industria manufacturera en México generó 7.01 billones de pesos al tercer trimestre de 2025, dentro de esta industria se cuenta con 647,333 unidades económicas con una inversión extranjera directa de 19,407 millones de dólares y emplea a 39 mil 800 personas. Lo anterior permite distinguir la importancia de la industria manufacturera (Data México, 2025).

Es relevante mencionar la importancia de esta investigación debido a que la tecnología es un campo de crecimiento e innovación a nivel mundial, ya que se presenta en todos los sectores de nuestra sociedad. A pesar de que la tecnología es importante en nuestro país, muchos en la industria aún no la aceptan como herramienta o ayuda para su propio desarrollo (Moreno et al. 2024).

Según la Organización de las Naciones Unidas para el Desarrollo Industrial (UNIDO, 2020), la manufactura avanzada depende cada vez más de la interconectividad digital y de infraestructuras de red resilientes. Por tanto, se tiene el propósito de exponer las necesidades de las redes y de proporcionar soluciones. Vera (2021) menciona que las nuevas tecnologías han venido impactando al mundo actual especialmente en lo relacionado con el progreso y el desarrollo de la información y de las comunicaciones (TICs). Es por esa razón que las redes, tanto de datos como

de voz, deben estar diseñadas de tal forma que puedan prevenir cualquier inconveniente y a la vez poder brindar eficiencia, escalabilidad y seguridad.

En el mundo altamente competitivo de hoy, las empresas, instituciones y organizaciones deben mejorar su proceso de comunicaciones para poder innovar y mantener su crecimiento tecnológico, debido a que la información que se requiera debe estar disponible de forma rápida y confiable (Jiménez & Lira, 2015).

El impacto económico de las telecomunicaciones incluye su aporte en distintas áreas, tales como la productividad, el emprendimiento e innovación y el empleo lo que se traduce en un mayor crecimiento económico. El efecto más evidente de las telecomunicaciones es en relación con el aumento de productividad, dada la incidencia positiva a nivel de individuos, de organizaciones y de países que genera el avance en las comunicaciones, la conectividad y el acceso eficiente a la información (Jiménez & Lira, 2015).

El sistema de cableado es la inversión en tecnología que durará más y es la base para el funcionamiento de todas las demás tecnologías. El sistema de cableado estructurado está diseñado para promover cambios y expansiones frecuentes, y es la base para construir una red de información moderna (Cevallos, 2022). Con lo anterior se observa la importancia de realizar infraestructuras de red bajo normas y estándares que garanticen el tiempo de utilidad del cableado estructurado, además de superar las limitaciones de conectividad actuales y garantizar la integración futura de tecnologías emergentes sin necesidad de reemplazos reactivos de equipos críticos.

Algunas de las deficiencias que se encontraron al realizar el análisis de la red de la empresa MB, fue la limitación en la escalabilidad, obsolescencia en equipamiento que puede ocasionar interrupción de comunicación con servicios internos y externos, además de identificar que no están separados los procesos IT/OT en su totalidad, lo que pone en riesgo la seguridad de la información y los procesos

operativos. La incorporación de tecnologías exige infraestructuras de red escalables que soportan Ethernet de alta velocidad (25/50/100 Gb), baja latencia y confiabilidad en la transmisión (McKinsey, 2025).

Por lo que se considera viable realizar una propuesta de red industrial bajo normas y estándares que permita asegurar la escalabilidad de nuevas tecnologías, alta disponibilidad de servicios, separación de redes IT/OT que asegure tanto la información como la producción de neumáticos en todo momento para evitar pérdidas económicas a esta industria. De acuerdo con Moreno et. al. (2024), implementar una infraestructura de red cableada e inalámbrica moderna, administrada, ágil y segura ayudará a aumentar la productividad industrial y reducir los costos operativos mejorando la productividad, calidad y resiliencia, así como garantizar la seguridad en las operaciones industriales.

1.4. Objetivos de la investigación

1.4.1. Objetivo general

Diseñar una propuesta de infraestructura de red industrial para la empresa MB, basada en normas y estándares internacionales que permitan la seguridad y escalabilidad tecnológica, así como la adopción de nuevas tecnologías.

1.4.2. Objetivos específicos

- Describir las limitaciones en la infraestructura de red de la empresa MB frente a los requerimientos tecnológicos actuales mediante la investigación y observación para identificar las necesidades mediante indicadores clave de desempeño (KPIs) y un Análisis de Modos y Efectos de Falla de escalabilidad y seguridad (FMEA).

— Identificar normas, estándares y mejores prácticas para el diseño de redes escalables y seguras en la industria manufacturera mediante la búsqueda de información en organismos internacionales y bases de datos de la industria.

— Diseñar una propuesta de infraestructura de red contemplando elementos como medios de transmisión, capacidad, segmentación lógica y seguridad que permita la continuidad de operaciones al adoptar nuevas tecnologías.

1.5. Pregunta de Investigación

¿Qué elementos debe contemplar una infraestructura de red industrial para la empresa MB para procurar la seguridad, escalabilidad y disponibilidad al adoptar nuevas tecnologías?

CAPÍTULO II. MARCO TEÓRICO

2.1 Estado del arte

Para determinar el conocimiento previo del tema se realizó una revisión sistemática de bibliografía con enfoque en el método Prisma, donde en primera instancia debe tenerse definida la pregunta de investigación, desarrollar un protocolo de revisión, seleccionar los estudios, extraer los datos, evaluar la calidad de los estudios y finalmente hacer un análisis y síntesis de los datos.

Se consideraron tanto la pregunta de investigación como las palabras clave. Se diseñó una ecuación de búsqueda donde se contemplan las palabras clave definidas en este trabajo: Infraestructura de red, IT/OT, manufactura, seguridad, escalabilidad. Se realizó la búsqueda en la base de datos Scopus con la siguiente ecuación:

TITLE-ABS-KEY ("network infrastructure" OR "industrial network infrastructure" OR "communication infrastructure" OR "network architecture") AND ("IT/OT" OR "IT-OT" OR "IT/OT convergence" OR "IT/OT integration" OR ("information technology" OR "operational technology")) AND (manufacturing OR "smart manufacturing" OR "industrial automation" OR "Industry 4.0") AND (security OR cybersecurity OR "industrial cybersecurity" OR "network security") OR (scalability OR scalable) AND (standards OR standardization OR "technical standards") AND ("best practices" OR guidelines OR frameworks)

La ecuación muestra que se han considerado palabras relacionadas con cada uno de los términos de la ecuación, así mismo, los operadores lógicos “AND” indican los términos que no deben excluirse. Del resultado de esta búsqueda se consideraron criterios de inclusión y exclusión de artículos, seleccionando los artículos que hayan sido publicados en un rango de no más de 5 años (2021 a 2026) en idioma Inglés, así mismo se seleccionaron los artículos con acceso abierto. Para la extracción de datos se ha categorizado y descrito el tipo de evidencia, con enfoque en la metodología utilizada, el sector, el lugar y la aplicación, esto con el fin de identificar la relación con el presente trabajo.

El resultado fue un conjunto de 152 artículos de los cuales se seleccionaron los más relevantes para este estudio agrupándolos en áreas que abarcan 1. Arquitectura e integración IT/OT, 2. Seguridad de la infraestructura y 3. Comunicaciones industriales.

Dentro de los artículos relacionados con arquitectura e integración se encuentra de Lee, et al. (2021) que propone una arquitectura con dominios de usuario, servicios en la nube, sensado, control y dispositivos, basada en una plataforma OPC UA que combina modelos cliente/servidor y PubSub y la arquitectura de referencia ISO/IEC 30141. El objetivo de dicho estudio es proponer una arquitectura integrada para IIOT (Internet Industrial de las Cosas) para resolver problemas de interconexión, interoperabilidad y comunicación en tiempo real entre sistemas de manufactura y equipos industriales. Este estudio se realizó bajo la metodología de diseño de

arquitectura con validación experimental apoyándose en la arquitectura de referencia ISO/IEC 30141 para facilitar la integración entre dominios IT/OT.

En Sladek y Doucek (2026) se aborda el diseño de una arquitectura IIoT estandarizada y orientada a definir una infraestructura de red para soportar la convergencia IT/OT en entornos manufactureros. La metodología empleada es el diseño de un framework y la validación de casos de uso. El artículo reporta que el Framework diseñado en este artículo que aporta una visión de arquitectura estandarizada, observa una reducción de 20% en el tiempo de diseño arquitectónico, que una red industrial se espera que sea escalable, segura y gobernable.

Okafor et al. (2021) proponen una arquitectura de red biofísica dinámica con el objetivo de mejorar la gestión y distribución de datos en sistemas ciberfísicos con diversas fuentes, ubicaciones y demandas de procesamiento. La metodología de esta propuesta consiste en el diseño de una arquitectura biofísica basada en sensores iFog CPSS. El artículo modela y organiza el flujo de datos a partir de la arquitectura propuesta para servicios basados en la localización de actividades en tiempo real. Este se orienta a demostrar la viabilidad del aprovisionamiento de datos en ecosistemas complejos de forma flexible y escalable. El resultado principal es la propuesta de una arquitectura adecuada para sistemas con una alta complejidad de datos y la necesidad de procesamiento distribuido.

Una propuesta de arquitectura orientada a datos para ecosistemas IIoT avanzados fue publicada por Carrascal et al. (2025) donde los autores estudian cómo una arquitectura definida por software mejora la capacidad de análisis, la escalabilidad y la gestión en aplicaciones industriales avanzadas. La metodología que utilizaron se centra en una arquitectura cloud-edge data driven, en la que se distribuyen funciones de procesamiento, de control y análisis. El resultado obtenido en dicho artículo es la formulación de una arquitectura de edge intelligence para IIoT que mejora la capacidad de procesamiento cercano a la fuente de datos, también ayuda en la escalabilidad y en la reducción de dependencia de la nube central.

Los artículos que se han clasificado con respecto a su relación con seguridad de la infraestructura se analizan a continuación, iniciando con Min et al. (2025) que estudia el problema de la coexistencia de sistemas heredados con nuevos requisitos de conectividad y seguridad, observando la necesidad de una infraestructura que proporciona conectividad, proteja y segmente entornos legacy o heredados (tecnologías antiguas que siguen operando porque cumplen funciones críticas) además de alinearse con el marco de seguridad NIST CSF 2.0 articulando la normatividad y ciberseguridad. El resultado de su investigación es la propuesta de arquitectura de seguridad Zero Trust adaptada al entorno manufacturero para mitigar riesgos de ciberseguridad.

Examinar cómo tecnologías, por ejemplo, 5G, IIoT, CPS, Edge/Fog, Blockchain y analítica pueden aumentar la superficie de ataques a las redes de comunicación industriales, es un objetivo de la investigación de Ahmad et al. (2024). Su artículo es una revisión de literatura utilizando una metodología que consiste en revisar y clasificar la literatura sobre seguridad en comunicaciones industriales, agrupando los problemas y las soluciones de acuerdo con las tecnologías habilitadoras. El resultado fue una síntesis de amenazas, vulnerabilidades y brechas de investigación y soluciones de seguridad., mostrando un panorama actualizado de amenazas y requisitos de seguridad para la conectividad industrial, en específico en entornos con 5G, CPS e IIoT, con ello se observa la importancia de incorporar desde el diseño, criterios de seguridad, segmentación y protección de comunicaciones.

En Kouari et al. (2025) se propone e implementa una estrategia de ciberseguridad robusta para entornos IIoT/Industria 4.0 con base en una arquitectura segmentada y también en la colaboración IT y OT, se incorporaron honeypots en diferentes niveles de la arquitectura industria con el fin de detectar y monitorear además de mejorar la respuesta ante amenazas. La finalidad de dicho estudio fue fortalecer la seguridad de infraestructuras industriales interconectadas, sobre todo ante los riesgos de la convergencia IT/OT concluyendo que la arquitectura propuesta mejora

la visibilidad temprana ante amenazas en entornos IIoT al combinar segmentación, honeypots, IDS, SIEM (Gestión de eventos y e información de seguridad) y CTI.

En el artículo de Melis et al. (2025) se propone un gemelo digital de una red TSN (Time-Sensitive Networking) en el que se replica el comportamiento de infraestructura industrial aplicando pruebas de seguridad donde se utiliza el modelo STRIDE para el análisis de amenazas. La propuesta se orientó en emular el entorno de comunicaciones, realizar escenarios de ataque para observar el efecto de las vulnerabilidades sobre la disponibilidad, integridad y sincronización del tráfico crítico. El resultado fue una plataforma experimental para pruebas de ciberseguridad sobre redes TSN que ayudará a identificar las vulnerabilidades y evaluar medidas de mitigación antes de desplegarlas en entornos reales. Con este artículo se observa que los gemelos digitales pueden apoyar en cuanto a la validación de la seguridad para reducir riesgos al realizar pruebas sobre la planta de producción.

Las comunicaciones móviles, redes inalámbricas y en general la infraestructura sin cables es un elemento que habilita la automatización industrial donde convergen sistemas OT. En Zeydan (2025) analizaron el papel de las comunicaciones móviles, en específico la 5G y tecnologías afines en la automatización industrial, donde identificaron su arquitectura, aplicaciones y desafíos técnicos. La metodología de este artículo de revisión o survey técnico es examinar las arquitecturas de comunicaciones móviles para entornos industriales casos de uso en automatización asociados a latencia, confiabilidad, seguridad, cobertura y coexistencia con redes cableadas y OT tradicionales. El análisis que realizan concluye en que las comunicaciones móviles son un habilitador importante para la automatización industrial, especialmente en entornos que cuenten con robots móviles, sensores inalámbricos, monitoreo remoto y manufactura inteligente. Identifican desafíos críticos como la integración con sistemas OT ya existentes, la necesidad de muy baja latencia, la seguridad de las comunicaciones y la coexistencia con arquitecturas industriales ya instaladas.

Carral S. (2025) realizó una investigación de seguridad en las redes industriales con el objetivo de diseñar, desplegar y analizar un entorno virtualizado IT/OT simulando amenazas para determinar el impacto y aplicar medidas de seguridad efectivas. Para esta investigación se empleó la metodología práctica basada en la virtualización de un entorno industrial en el que convergen elementos IT/OT.

Este proyecto se centra en tres fases:

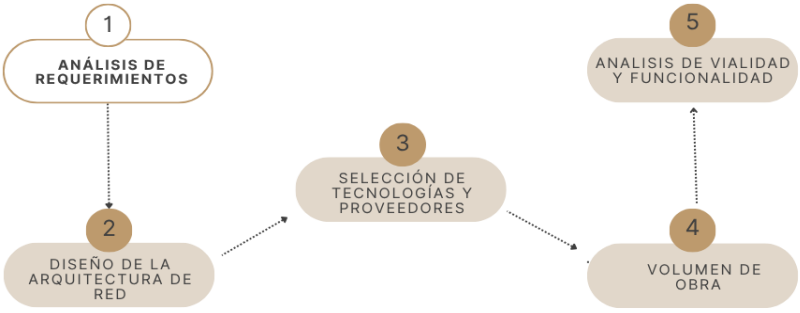
1.- Fase de diseño: Simulación del entorno sobre el que se basará el ataque, usando la herramienta VirtualBox para alojar máquinas simuladas.

2.- Análisis de fases de un ciberataque: Se presenta mediante el uso de diferentes herramientas y técnicas para lograr una explotación completa de una red.

3.- Fase de ataque a la red previamente montada: Para deducir y concluir los peligros a los que se puede ver expuesta la red OT, además de ver hacia dónde puede evolucionar la ciberseguridad en entornos industriales.

Por último, Moreno (2024) expone las cinco fases del proceso para realizar el diseño de la red en la industria de las bebidas carbonatadas que se muestran en la figura 3 y que a continuación se describen.

Figura 3 Proceso para el diseño de una red industrial



Fuente: Elaboración propia basada en Moreno (2024).

Fase 1. Análisis de requerimientos: Se evalúa la infraestructura de comunicaciones, identifica los dispositivos que deben conectarse a la red, los protocolos de comunicación que se utilizarán y la seguridad necesaria para realizar el análisis de las necesidades de la empresa.

Fase 2. Diseño de la arquitectura de red: Se realizará el diseño de la planimetría de la planta para identificar de manera precisa la distribución espacial de las instalaciones; se continuará realizando el diseño de la red; para ello se elige la topología más adecuada y los protocolos de seguridad que mejor se acoplen.

Fase 3. Selección de tecnologías y proveedores: Posteriormente se seleccionarán los equipos y dispositivos que se utilizarán para el desarrollo de la red de telecomunicación industrial 4.0. Estos deben ser de alta calidad, confiables y capaces de manejar grandes volúmenes de datos, así como operar en entornos industriales exigentes, además de la compatibilidad con el equipo ya existente.

Fase 4. Volumen de obra: Para realizar esta fase, se evalúa la rentabilidad y el impacto financiero del proyecto del diseño de la red de telecomunicaciones. Se identifica el costo de la inversión inicial para diseñar y construir la red de telecomunicaciones.

Fase 5. Análisis de viabilidad y funcionalidad: En la última fase Moreno (2024) evalúa el diseño de la red de telecomunicaciones, si es o no viable y funcional, por medio de una simulación de acuerdo con los objetivos y necesidades de la planta de producción, incluyendo la capacidad de la red, estabilidad, seguridad y análisis de riesgos asociados con el diseño de la red de telecomunicaciones, incluyendo posibles fallas técnicas, problemas de seguridad.

Para evaluar la viabilidad y funcionalidad de una infraestructura de red en entornos industriales, resulta indispensable apoyarse en metodologías consolidadas que permitan estructurar el proceso de diseño, implementación y gestión. Estas

metodologías ofrecen marcos de referencia que integran tanto la perspectiva técnica como la de gestión del ciclo de vida de la red, asegurando que la propuesta se alinee con estándares internacionales y con las necesidades específicas de la planta de producción. Como señalan Hernández et al. (2018), el rigor metodológico en proyectos de ingeniería aplicada permite traducir requerimientos complejos en soluciones prácticas y evaluables.

En este sentido, la tabla 1 presenta una síntesis de metodologías relevantes, entre las que destacan el ciclo PPDIOO de Cisco, los lineamientos de cableado estructurado bajo estándares EIA/TIA y el enfoque top–down, las cuales brindan pautas prácticas para garantizar que el diseño de red sea confiable, escalable y seguro.

Tabla 1 Metodologías relevantes para el proceso de diseño de una red industrial.

Metodología	Descripción	Autor
PPDIOO	Cisco ha presentado el ciclo de un proyecto en 6 fases, las cuales son: preparación, planificación, diseño, implementación, operar y optimizar.	Quirumbay, D. (2023)
Metodología bajo estándares EIA/TIA de cableado estructurado	Sigue los siguientes estándares: 568A - Permite hacer una planeación y proyectar el diseño de una forma modular. 569 - Rutas óptimas y espacios en donde se instalan los cables. 606 - Administración de los servicios, ocupación de las rutas, utilización de los pares, etc. 607 - Especifica cómo se deberán proteger los equipos e instalaciones de telecomunicaciones contra descargas eléctricas.	López, V. (2005)
Top - down	Es un enfoque estructurado que se centra inicialmente en las aplicaciones y los requisitos de los usuarios antes de seleccionar dispositivos, cables y otras tecnologías para implementar la red. Este método asegura que la red diseñada sea confiable, segura y escalable, alineándose con los objetivos comerciales y técnicos del cliente. Las fases de esta metodología son: - Identificación y objetivos del cliente - Diseño de una red lógica	Saavedra.(2017)

- Diseño de la red física
- Testeo, optimización y documentación de la red.

Fuente: Elaboración propia

De manera general, se observa que la investigación aquí expuesta se dirige hacia la convergencia IT/OT, procurando la interoperabilidad, la seguridad de las comunicaciones industriales, encontrando propuestas de arquitecturas que contemplan los retos importantes. Aún se observa que se requiere de propuestas integrales que se centren en el diseño de infraestructura de red para entornos manufactureros, donde se desarrolle una arquitectura de que incluya topología, segmentación, interoperabilidad, escalabilidad, medios de transmisión y ciberseguridad sustentado con normas como ISO/IEC, ANSI/TIA, IEC 6243 y NIST. Esta propuesta busca reducir ese vacío mediante una propuesta de infraestructura de red orientada a la convergencia IT/OT en manufactura.

2.2. Bases teóricas

2.2.1 Redes de datos

Santillán, et al. (2018) indican que una red de telecomunicaciones está formada por los sistemas de transmisión, los equipos de comunicaciones y demás recursos que permitan la transmisión de señales entre puntos de terminación definidos mediante cable, medios ópticos u otra índole. Construidas con el objetivo de prestar servicios de comunicaciones con la calidad de servicio deseada, con base en incorporar en la misma una combinación de tecnologías que hacen posible disponer de un gran ancho de banda y una alta capacidad de comunicación.

Pensadas para intercambiar datos empleando protocolos de comunicación, compuestos de un grupo de nodos que procesan la información, enlaces que conectan estos nodos y permiten el envío-recepción de la información, así como

protocolos de comunicación que son la serie de reglas y acuerdos establecidos para esta comunicación (Barbancho et al. 2020).

2.2.1.2. Tipos de redes de datos

Existen múltiples tipos de redes de comunicación (LAN, WAN, MAN, WLAN, PAN, CAN, entre otras), cada una con características particulares en cuanto a alcance, capacidad y propósito. Sin embargo, en el ámbito de la industria manufacturera resultan más relevantes las redes LAN, MAN y WAN debido a que permiten soportar la interconexión de equipos en plantas de producción, la integración de sistemas entre diferentes edificios o campus industriales y la conexión con sedes remotas o proveedores externos. Estas tres tipologías constituyen la base de las infraestructuras de red sobre las que se articulan las tecnologías habilitadoras de la Industria 4.0, ya que responden a requerimientos de escalabilidad, confiabilidad y cobertura en entornos corporativos y productivos (Stallings, 2021).

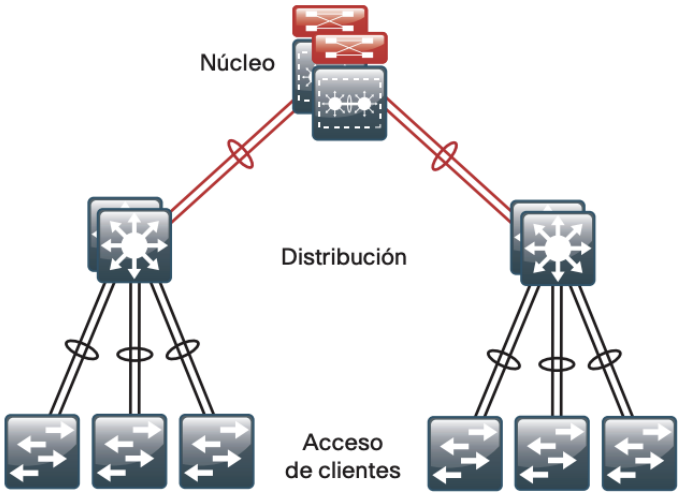
2.2.1.3 Red LAN

Barbancho et al. (2020) describen las redes LAN, redes de área local, como redes de comunicaciones que interconectan nodos localizados dentro de un mismo edificio. Además de ser recursos tecnológicos eficientes que permiten el intercambio de información entre equipos de cómputo interconectados entre sí (Ley, 2021).

Modelo de diseño jerárquico

El diseño jerárquico de una red LAN permite restringir los cambios operativos a un subgrupo de la red, facilitando la administración, mejora la recuperabilidad y aísla las fallas. Se divide en tres capas: capa de acceso, capa de distribución y capa central (figura 4) Monterrubio (2023).

Figura 4 Figura 4.- Diseño jerárquico de una red LAN



Fuente:https://www.cisco.com/

Cisco (2014) Refiere que cada capa ofrece una funcionalidad diferente para la red y las describe de la siguiente manera:

Capa de acceso: ofrece a los terminales y usuarios acceso directo a la red tanto inalámbrica como por cable, incluye características y servicios para garantizar seguridad y accesibilidad.

Capa de distribución: une las capas de acceso enviando el tráfico de una red local a otra y ofrece conectividad a los servicios.

Capa central o núcleo: ofrece conectividad entre las capas de distribución para entornos de LAN grandes.

2.2.1.4 Red MAN

Las redes metropolitanas (MAN) se forman por la interconexión de varias redes LAN que se encuentran a mayores distancias, incluidas en su edificio o campo, pero que no sobrepasan el ámbito urbano Monterrubio (2023).

Es una red cuyo diámetro no va más allá de 50 km y responde claramente a la necesidad de un sistema de comunicaciones de tamaño intermedio con beneficios que superan a los que pueden ofrecer las redes LAN o WAN. Se trata de una red de alta velocidad que se extiende más allá de la cobertura de una LAN sin las restricciones a los métodos normales de las WAN (Zuñiga, 2023).

2.2.1.5 Red WAN

Las redes WAN (redes de área amplia), de acuerdo con Barbancho et al. (2020), se definen como redes de comunicación que cubren un área geográfica extensa.

Utilizan los servicios de operadoras, como empresas proveedoras de servicios de telefonía, empresas proveedoras de servicios de cable, sistemas satelitales y proveedores de servicios de red.

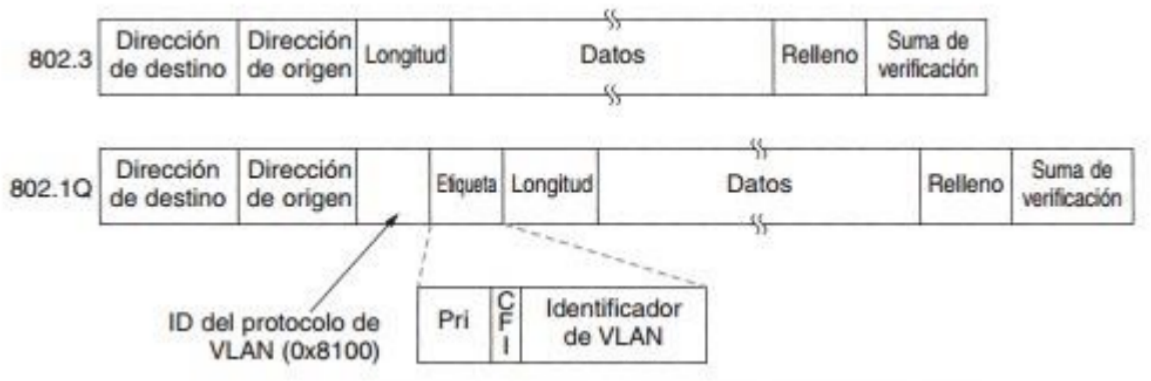
Las redes WAN interconectan redes enteras, empleando protocolos de transmisión y conceptos de dirección. Una WAN funciona en la capa física, la capa de enlace y la capa de red. Los sistemas intermedios o nodos de red, como conmutadores, puentes y enrutadores garantizan que los paquetes de datos enviados se reenvían a la dirección correcta. Mediante el hardware, los paquetes de datos se envían de una subred a la otra y se entregan al participante de red correcto, la tecnología básica de esto es la pila de protocolos TCP/IP. (Rodríguez et al. 2022)

2.2.2 Redes Virtuales Locales (VLAN)

Las redes virtuales locales (VLAN) segmentan una red física en redes lógicas, creando aislamiento y mejor control del tráfico de red. Esta tecnología permite aumentar la seguridad, el rendimiento y el aprovechamiento de los recursos disponibles, ya que hace posible implementar políticas de acceso específicas para diferentes grupos de usuarios y aplicaciones además de facilitar la administración de la red (Ramos & Martínez, 2023).

A partir del proyecto del grupo de trabajo 802 (conjunto de normas que regularizan y estandarizan las redes LAN y WAN) la IEEE desarrolló 802.1Q, mecanismo que permite segmentar una red física en varias redes lógicas, sin problemas de interferencia entre ellas. 802.1Q no encapsula la trama original, más bien añade 4 bytes al encabezado Ethernet original mismo que se muestra en la figura 5 (Yungán & Narváez, 2022).

Figura 5 Figura 5.- Formato de trama Ethernet y 802.1Q



Fuente: Yungán & Narváez (2022).

La figura 5 presenta la adición de dos nuevos campos de 2 bytes cada uno. El primer campo corresponde al identificador del protocolo de VLAN con un valor 0x8100. El segundo campo de 2 bytes contiene tres subcampos

1. Prioridad distingue el tráfico en tiempo real.

2. CFI- Identificador de formato canónico, indica el orden de los bits en las direcciones.

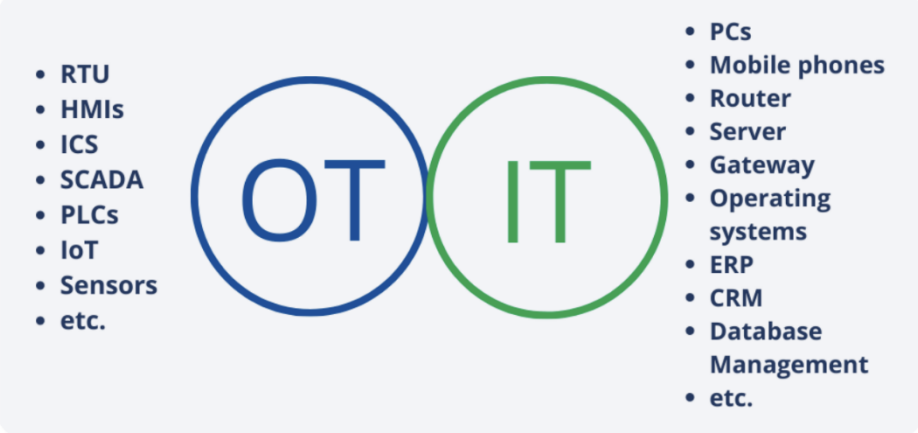
3. El identificador de VLAN representa al identificador de VLAN a la que pertenece la trama.

2.2.3 Convergencia IT/OT

En el contexto industrial moderno es fundamental diferenciar las Tecnologías de la Información (IT) y Tecnologías Operativas (OT) figura 6, la primera se refiere a todos los sistemas y herramientas relacionadas con el procesamiento, almacenamiento y transmisión de datos digitales además de gestionar la información, incluye servidores, bases de datos, sistemas de almacenamiento y redes corporativas (Carral, 2025).

Por otro lado, el entorno OT, abarca los sistemas y dispositivos diseñados para supervisar, controlar y automatizar los procesos físicos de producción o servicios. Se incluyen PLCs (controlador lógico programable), controla dispositivos eléctricos o mecánicos como motores, sensores y válvulas de forma automática y programable, sistemas SCADA (Sistema para controlar sistemas remotos en un entorno industrial), redes industriales y buses de campo (Moreno et al. 2024).

Figura 6 Elementos IT/OT



Fuente: (Carral, 2025).

En la figura 6 se muestra la diferencia de componentes pertenecientes a cada una de las redes OT/ IT.

La convergencia IT/OT cita la integración progresiva de los sistemas informáticos tradicionales (IT) con los sistemas de control industrial (OT), con la intención de

crear un ámbito conectado, eficiente y automatizado debido a que permite que la información fluya desde la planta de producción hasta los niveles directivos en tiempo real (Carral, 2025).

2.2.4 Redes industriales y Sistemas de seguridad

Una red industrial es una infraestructura de comunicación diseñada concretamente para conectar dispositivos y sistemas que monitorean, supervisan y controlan procesos físicos en plantas industriales (PLC, RTU, DCS, HMI, SCADA, sensores, actuadores, etc). Su objetivo no es el intercambio general de información empresarial, sino de asegurar el control fiable, con requisitos de disponibilidad, determinismo y seguridad que mantienen procesos productivos constantes y críticos (Vargas, 2026).

Sistemas de Control Industrial

Los Sistemas de Control Industrial (ICS de sus siglas en inglés) son redes de telemando y telecontrol de procesos compuestos por autómatas industriales llamados PLC (Programmable Logic Controller) interconectados entre sí y cada uno de ellos con sensores digitales o analógicos. Diseñados para supervisar y actuar en los procesos industriales (Kamlofsky et al., 2017).

Desde su desarrollo han evolucionado de ser entornos aislados, con hardware, software y protocolos de comunicación propietarios, a utilizar tecnologías estándares que han facilitado su interconexión con las redes tradicionales de tecnologías de información (TI) con el objetivo de una mejor integración y reducción de costes. En cambio, las tecnologías que utilizan las redes industriales no fueron diseñadas para estar interconectadas y por ello, generalmente carecen de mecanismos de seguridad presentes en redes TI, como el cifrado de las comunicaciones, cortafuegos o sistemas de detección de intrusiones (SDI). (Iturbide et al., 2016).

Supervisión, Control y Adquisición de Datos

Los SCADA (Supervisory Control and Data Acquisition) es un software que muestra gráficamente el estado de cada componente de la planta, con la posibilidad de actuar sobre ellos. Se diseñaron para controlar sistemas industriales, conectando PCs con las redes autómatas industriales; conformando la interfaz hombre-máquina. Originalmente se instalaban en salas aisladas, con acceso restringido. Con el tiempo surgió la necesidad de vincularlos a la red corporativa e incluso a internet. (Iturbide et al. 2016).

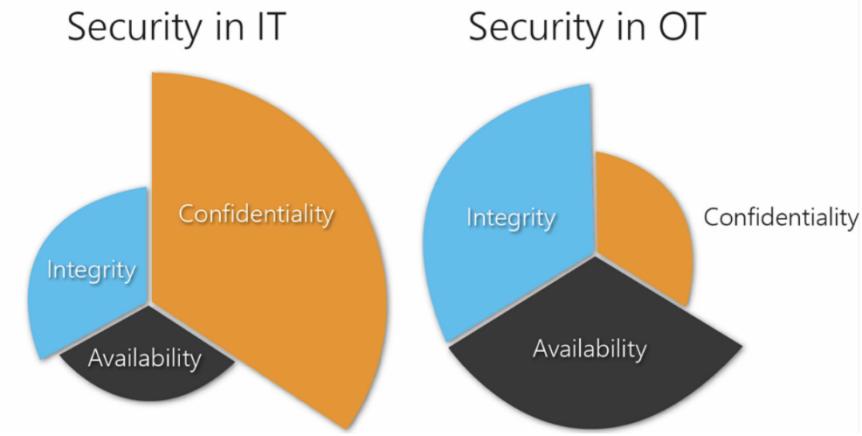
Seguridad industrial

La tecnología corporativa y la industrial dejaron la seguridad entre ambas. Hasta hace pocos años, era impensable que un ICS se pudiera infectar con un virus informático. En el año 2010 el sistema SCADA de las plantas de enriquecimiento de uranio de Irán fue atacado por un virus llamado Stuxnet. Esto desconcertó a analistas estratégicos de todo el mundo. La comunidad internacional mostró gran preocupación por la seguridad de las infraestructuras basadas en estas tecnologías. (Kamlofsky et al., 2017)

Las recomendaciones de las normas ISO27000 y NIST SP800-30 revisión 1 y los múltiples desarrollos realizados, ayudan a proteger la seguridad de los activos informáticos. (Kamlofsky et al., 2017)

Dada la tradicional vulnerabilidad de este tipo de redes y su importante papel en el correcto funcionamiento de sociedades modernas, es necesario desarrollar mecanismos de seguridad destinados a redes industriales. Sin embargo, a la hora de diseñar este tipo de soluciones, se debe tener en cuenta que las redes TI e industriales tienen objetivos y necesidades de seguridad diferentes mostrados en la figura 7. Mientras que las redes industriales tienen como objetivo el control de equipamiento físico, en las redes TI el objetivo es el transporte de datos. (Iturbide et al., 2016).

Figura 7 Prioridades de seguridad IT/OT



Fuente: Carral (2025).

2.2.4.2 Segmentación y zona desmilitarizada (DMZ)

Una de las prácticas esencial en la convergencia IT/OT es la segmentación de red, que radica en dividir la red en zonas aisladas con reglas de comunicación estrictas entre ellas. Para evitar que un ataque iniciado en IT pueda propagarse fácilmente al entorno OT. Otra configuración habitual es el uso de una DMZ (Zona Desmilitarizada) industrial entre los entornos IT y OT. Esta zona intermedia alberga servicios que requieren comunicación cruzada (como servidores de actualización, proxies o servidores SCADA) y actúa como una barrera de contención (Carral, 2025).

La zona desmilitarizada, es clave para la propia división entre la red ICS y la empresarial, es decir, entre la operación OT e IT. Además de actuar como zona de alojamiento de los servidores principales de OT, también actúa como amortiguador para la red industrial debido a su separación mediante Firewalls, sistemas de prevención de intrusiones (IPS) u otros (Martínez, 2025).

2.2.4.3 Firewalls industriales

Los firewalls protegen las redes industriales de amenazas externas, controlan el tráfico entre las redes IT y OT y brindan una capa adicional de seguridad esencial para proteger las redes y sistemas de control en los medios industriales. Al establecer reglas de acceso y filtrar el tráfico de red, ayudan a evitar intrusiones no autorizadas, ataques cibernéticos y el acceso restringido a los dispositivos críticos de la infraestructura (Mora, 2024).

Además, de otorgar seguimiento y dominio sobre el tráfico de red, los firewalls industriales brindan una supervisión constante y la capacidad de tomar medidas proactivas para mitigar las amenazas de seguridad, es decir su implementación fortalece la ciberseguridad y la fiabilidad de las operaciones industriales, colaborando a la protección de activos, la continuidad del negocio y la seguridad del personal (Mora, 2024)

2.2.4.4 NMS/SIEM

Rodríguez, 2020 describe el sistema de gestión de red (NMS), como una aplicación o conjunto de aplicaciones que permiten monitorizar y gestionar componentes de software y hardware de la red de una manera sencilla y eficaz, un NMS es útil para descubrimiento de los dispositivos de red, supervisión de los dispositivos de red, análisis de rendimiento de la red, gestión de dispositivos de la red y notificaciones inteligentes o alertas personalizables.

Los SIEM (gestión de información y eventos de seguridad) emplean diversas tecnologías para recopilar, analizar y correlacionar datos de seguridad, que integra la recopilación de registros (logs) de dispositivos y sistemas, análisis de comportamiento de usuarios, detección de amenazas en tiempo real, gestión de incidentes de seguridad, inteligencia de amenazas, y capacidades de cumplimiento normativo (Carral, 2025).

En entornos industriales, aplicar SIEM es esencial para monitorear y gestionar la seguridad de la red. Porque permiten recopilar, analizar y correlacionar datos de diferentes fuentes dentro del entorno industrial, como sistemas de control, dispositivos de red y aplicaciones. Esto proyecta la postura de seguridad y contribuye a detectar amenazas de manera proactiva (Carral, 2025).

2.2.5 Protocolos industriales Ethernet

El avance de la comunicación industrial ha ido del serial a soluciones basadas en Ethernet e IoT, adaptándose a las demandas de velocidad, flexibilidad y seguridad. La comunicación industrial es indispensable porque se enfoca en los sistemas y tecnologías que hacen posible el flujo de información entre equipos y sistemas dentro de entornos industriales. El traspaso de datos es necesario para mantener el control y la supervisión de los procesos (Moro & Puco, 2025).

A continuación, se presentan los principales protocolos de comunicación mediante lógica cableada.

Protocolo Modbus

Protocolo que transmite información entre los equipos electrónicos que estén conectados al mismo bus, es un protocolo de comunicación maestro, esclavo. Una gran cantidad de dispositivos de campo lo utilizan para lograr comunicarse con SCADA’s y PLC’s. La comunicación en Modbus lo determina el propio protocolo. Siempre existe un maestro que consulta datos a uno o múltiples esclavos al mismo tiempo (Moro & Puco, 2025).

Pese a su amplia adopción es relevante observar las desventajas tales como que no cuenta con características de seguridad, sin tiempo reales garantizados ni sincronizados, omite mecanismos nativos de autenticación, se emplea principalmente en la instrumentación de procesos continuos. Su implementación en

sistemas SCADA ha permitido consolidar arquitecturas de supervisión robustas y de bajo costo. Pero requiere medidas compensatorias de seguridad a nivel de arquitectura (Vargas, 2026).

Protocolo Profinet

Tecnología de comunicación industrial fundamentada en Ethernet, se emplea en sistemas de automatización y control de procesos donde es necesario facilitar la transmisión de datos tanto en tiempo real como en aplicaciones que no requieren esta condición, ofrece una comunicación eficiente confiable y con comportamiento determinístico dentro de las redes industriales lo cual conduce una interacción rápida y precisa entre diferentes equipos. Esta tecnología sobresale por su compatibilidad con la infraestructura Ethernet existente lo que posibilita aprovechar redes ya implementadas agregando que alcanza velocidades de transmisión elevadas que resultan indispensables en entornos donde la velocidad y la precisión son factores críticos asimismo su capacidad para operar de forma determinística asegura tiempos de respuesta predecibles y controlables lo cual resulta fundamental en aquellos procesos que requieren sincronización precisa y ejecución en tiempo real para garantizar el funcionamiento coordinado de las operaciones industriales (Moro & Puco, 2025).

Protocolo OPC UA

Su propósito es la orientación a servicios, interoperabilidad y escalabilidad, integra dispositivos de diferentes fabricantes y soporta conexión con la nube y sistemas IIoT. Permite la interoperabilidad entre sistemas de distintos fabricantes y agiliza la integración con el IIoT y la nube. Este protocolo es fundamental en estrategias de mantenimiento predictivo y digitalización industrial, debido a que permite transmitir no solo valores de proceso, sino también metadatos asociados, calidad del dato y estructuras de modelado de activos.

Sin embargo, no está diseñado para reemplazar protocolos deterministas de control de movimiento, sino para operar en niveles superiores de integración y análisis, es un protocolo complejo y pesado; implementarlo exige recursos computacionales, su adopción requiere de inversiones en actualización de equipos y capacitación (Vargas, 2026).

2.3. Normas, estándares y mejores prácticas de redes en industria manufacturera

Vallina (2013) define los protocolos y estándares de comunicaciones de la siguiente manera: Las comunicaciones entre sistemas informáticos se transmiten en forma de ceros y unos denominados bits, pero no basta con solo el envío de paquetes de bits para comunicarse; es necesario un conjunto de reglas denominado protocolo de comunicaciones, que son los que definen cómo y cuándo se comunican mediante la sintaxis (estructura o formato de los datos), semántica (significado de cada conjunto de bits) y temporización (cuándo y a qué velocidad deben transmitirse los datos).

Otro aspecto primordial son los estándares, debido a que garantizan el funcionamiento de un producto independientemente de su fabricante, al ser el conjunto de normas, acuerdos y recomendaciones técnicas que regulan la tecnología y los protocolos de los sistemas de comunicación. Los estándares de mayor importancia en las telecomunicaciones son: la Organización Internacional de Estándares (ISO), Instituto Americano Nacional de Estándares (ANSI), Asociación de las Industrias Electrónicas (EIA), Unión Internacional de Telecomunicaciones (ITU) e Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) (Vallina, 2013).

El conjunto de estándares ISA99/IEC62443 permite a las redes industriales alcanzar los objetivos operativos conectando la red empresarial a la red industrial de manera segura. Proporcionan un diseño adecuado de la red para operaciones efectivas e implementan las mejores prácticas de ciberseguridad industrial, para una mejora continua. La adopción de estándares es fundamental para la seguridad y eficiencia

del diseño de la red de telecomunicaciones propuesta. Estos estándares brindan una base sólida para la colaboración, garantizando operaciones más seguras y una evolución constante en la planta industrial. (Moreno & Martínez, 2024)

El diseño de infraestructuras de red modernas en la industria manufacturera requiere una alineación rigurosa con normas internacionales**,** estándares técnicos y buenas prácticas de ingeniería, con el fin de garantizar escalabilidad, seguridad, confiabilidad y compatibilidad con tecnologías emergentes. Estas guías constituyen la base para lograr redes que soporten la convergencia IT/OT, la automatización industrial, la analítica avanzada y la ciberseguridad.

2.3.1 Normas y estándares clave

El diseño de infraestructuras de red en la industria manufacturera no puede entenderse sin el marco normativo y estandarizado que regula aspectos de conectividad, seguridad y gestión de los entornos productivos, para garantizar que mantengan continuidad operacional frente a amenazas cibernéticas y a la creciente complejidad de los ecosistemas IT/OT. Asimismo, el World Economic Forum (2023) destaca que la convergencia digital en manufactura requiere tanto de estándares técnicos (Ethernet, Wi-Fi, cableado estructurado) como de marcos de seguridad y gobernanza que permitan unificar criterios en la gestión de riesgos.

En este sentido, se destacan normas y estándares aplicables directamente al sector manufacturero: ANSI/TIA-568 e ISO/IEC 11801 para cableado estructurado; IEEE 802.3 para Ethernet e IEEE 802.11 para Wi-Fi; IEC 62443 y NIST SP 800-82 en ciberseguridad industrial; y ISO/IEC 27001 en gestión integral de la seguridad de la información. Cada uno de ellos constituye un pilar para la propuesta de diseño de red que esta investigación plantea, pues asegura que la infraestructura propuesta sea confiable, escalable y alineada con las mejores prácticas globales. En la tabla 2 se describen las normas que se toman en cuenta para el desarrollo de la propuesta del diseño de red.

Tabla 2 Normas y estándares claves.

Tecnología	Norma	Aplicación
Seguridad TI	Modelo ISO/IEC 2700	Gestión de la seguridad de la información
	Serie ISO/IEC 27032	Directrices para la ciberseguridad
	Serie ISO/IEC 27033	Seguridad de las redes
	Serie ISO/IEC 27034	Seguridad de las aplicaciones
Ciberseguridad en redes industriales convergencia	IET TS 62443-1-1:2009	Redes de comunicaciones industriales. Seguridad de la red y del sistema. Parte 1-1: Terminología, conceptos y modelos.
	IET 62443-2-1:2010	Redes de comunicaciones industriales. Parte 2-1: Establecimiento de un programa de seguridad de control y automatización
	IET TR 62443-2-3:2015	Seguridad para los sistemas de automatización y control industrial. Parte 2-3: Gestión de parches en el entorno IACS
	IEC TR 62443-3-1:2009	Seguridad de la red y del sistema. Parte 3-1: Tecnologías de seguridad para los sistemas de automatización y control industrial.
Conectividad de las redes industriales	IEC 61158	Redes de comunicaciones industriales
Infraestructura de redes industriales	ANSI/TIA-568 ISO/IEC 11801	Cableado estructurado: Definición de la infraestructura física de las telecomunicaciones en edificios industriales y comerciales, incluye categorías, distancias y parámetros de desempeño.
Medio de transmisión	IEEE 802.3 Ethernet	Regula tecnologías de transmisión por ethernet

IEEE 802.11 WI-FI	Define protocolos de redes inalámbricas WI-FI, incluyendo WI.FI 6, WI-FI 7

Fuente: Elaboración propia basada en Moreno & Martínez (2024)

2.3.2 Mejores prácticas

Además de la adopción de normas internacionales, la literatura y la práctica industrial coinciden en que la sostenibilidad y resiliencia de las redes en manufactura dependen de la aplicación de mejores prácticas que respondan a la realidad operativa de cada planta. Estas prácticas complementan los marcos normativos, traduciéndose en estrategias técnicas de implementación que aseguran la continuidad operativa, la escalabilidad tecnológica y la protección frente a riesgos cibernéticos. Según la IEC (2021), el diseño de redes industriales debe articularse en torno a principios de seguridad por diseño y redundancia, mientras que la NIST (2023) subraya la importancia de visibilidad y monitoreo continuo para enfrentar amenazas crecientes en entornos de control industrial. Asimismo, Cisco (2023) y Rockwell Automation (2023) resaltan que las mejores prácticas constituyen una guía operativa para que las redes no solo cumplan con los estándares, sino que también se mantengan alineadas con los objetivos de productividad y confiabilidad de la industria manufacturera, en la tabla 3 se muestran recomendaciones y detalles fundamentales para lograr un diseño de red adecuado.

Tabla 3 Mejores prácticas

Recomendación	Detalle
Segmentación IT/OT	Segmentación de redes corporativas y redes de control mediante VLANs, mejora la eficiencia, seguridad, aísla los problemas, reduce y administra el tráfico.
Redundancia en enlaces y equipos críticos	Aplicar arquitecturas resilientes (por ejemplo, anillos de redundancia o protocolos como HSR/PRP) incrementa la disponibilidad operacional.

Uso de cableado certificado	Se recomienda mínimo CAT6A para soportar 10 Gb/s en tramos de hasta 100 m y reduce la diafonía, garantizando longevidad de la inversión.
Monitoreo con sistemas NMS/SIEM	Herramientas de gestión de red (NMS) y de eventos de seguridad (SIEM) centralizan la visibilidad y facilitan la respuesta temprana ante fallas o incidentes.
Diseñar la red para escalabilidad a 5–10 años.	El diseño debe contemplar capacidad para nuevas generaciones de Ethernet (25/50/100 Gb) y tecnologías emergentes con una proyección de 5-10 años mínimo.

Fuente: Elaboración propia basada en Ramos & Martínez, 2023

La adopción de estos estándares y buenas prácticas no sólo estandariza y regula la interoperabilidad y confiabilidad de la red industrial, sino que también fortalece su resiliencia frente a ciber amenazas y garantiza la preparación tecnológica para las próximas décadas. En síntesis, una red industrial moderna (basada en estándares abiertos (IEEE 802.3), segmentación y controles de seguridad (NIST/OT, IEC-inspirado), se constituye en un activo estratégico para sostener la competitividad manufacturera en contextos de automatización intensiva, convergencia IT/OT y explotación de datos avanzados. (Ramos & Martínez, 2023).

2.4. Gobernanza tecnológica

La gobernanza tecnológica se entiende como el conjunto de políticas, normas, procesos y estructuras organizativas que garantizan el uso adecuado, seguro y eficiente de las tecnologías de la información y la comunicación (TIC) en una organización (Weill et al., 2004). En el caso de la industria manufacturera, la gobernanza tecnológica cumple un papel estratégico porque asegura que las decisiones relacionadas con la infraestructura de red se encuentren alineadas con los objetivos del negocio, los marcos normativos internacionales y las prácticas de ciberseguridad industrial (Mora, 2024).

De acuerdo con Unido (2020), la transformación digital en manufactura requiere de marcos de gobernanza que promuevan la integración de la tecnología con los procesos productivos, evitando implementaciones aisladas y favoreciendo la escalabilidad y sostenibilidad de las soluciones. En este sentido, la gobernanza tecnológica implica adoptar estándares como IEC 62443, ISO/IEC 27001 o IEEE 802.3, también establecer mecanismos de control, supervisión y mejora continua que permitan la resiliencia de la red frente a fallos técnicos y amenazas de seguridad (ISO, 2022).

La gobernanza tecnológica permite garantizar la trazabilidad normativa del diseño teórico, ya que cada decisión de arquitectura (segmentación IT/OT, cableado estructurado, protocolos de comunicación, políticas de seguridad) responde a un marco regulatorio y a un objetivo organizacional específico. Esto contribuye a que el modelo propuesto en esta tesis no sea únicamente viable desde el punto de vista técnico, sino también replicable, auditable y sustentado en principios de gestión tecnológica responsable (Kerlinger et al. 2002).

CAPÍTULO III. DISEÑO METODOLÓGICO

3.1. Alcance de la investigación

La presente investigación parte de la necesidad de comprender los patrones de obsolescencia y las limitaciones técnicas de la red industrial de la empresa manufacturera de neumáticos MB, a partir de la recopilación de información y análisis de la red actual, evidencias que serán evaluadas por el comité tutorial de forma confidencial, para posteriormente diseñar una propuesta de infraestructura de red industrial IT/OT basada en normas y estándares internacionales como IEC 62443, ISO/IEC 27001 e IEEE 802.3. que satisfacen la creciente demanda de servicios digitales y regulan la capacidad de manejar eficientemente tanto el

volumen de tráfico de datos como las necesidades de comunicación interna y externa.

El alcance de la investigación es descriptivo, se documentan las características actuales de las redes industriales y se detallan los elementos que debe contener una infraestructura de red moderna. De acuerdo con Guevara et al. (2020), los estudios descriptivos permiten especificar propiedades importantes de objetos o procesos, lo que en este caso se refleja en la caracterización de arquitecturas IT/OT. Se caracteriza el estado actual de las redes industriales y se documentan sus principales limitaciones.

El estudio es una propuesta, por lo que no se implementa físicamente en la planta. Se incluyen escenarios que permiten analizar la pertinencia y factibilidad del modelo mediante indicadores (capacidad, latencia, seguridad, disponibilidad).

3.2. Diseño de investigación

En cuanto al diseño de investigación, este es no experimental, transversal y documental. Es no experimental debido a que no se manipulan variables en entornos controlados, sino que se observan, analizan y contrastan las condiciones existentes (Kerlinger & Lee, 2002). Es transversal porque se analiza el fenómeno en un periodo único de tiempo, considerando las condiciones actuales y las proyecciones de evolución tecnológica. Finalmente, es documental porque se sustenta en el análisis sistemático de normas, estándares y reportes de organismos internacionales y lineamientos técnicos publicados por entes como IEEE, NIST e ISO (Cardona & Castaño, 2019).

La justificación del uso de análisis comparativos radica en que permiten construir un marco de referencia sólido y extrapolable a diferentes contextos manufactureros, evitando enfoques empíricos aislados. La propuesta está fundamentada en cuerpos normativos universales, garantizando escalabilidad y replicabilidad (Nohlen, 2020).

3.3. Población, contexto y unidad de estudio

El contexto de estudio corresponde a la industria manufacturera de neumáticos MB de gran escala en México, caracterizada por procesos productivos que requieren de alta disponibilidad, integración de tecnologías de automatización y creciente incorporación de soluciones IIoT.
La unidad de estudio corresponde a la infraestructura de red convergente IT/OT en la empresa de neumáticos MB. Incluye el procesamiento, almacenamiento y transmisión de información de los sistemas de gestión empresarial, así como los sistemas de control industrial (SCADA, PLCs, robótica) y puntos de acceso inalámbrico en planta.

Específicamente se realiza la observación, el levantamiento y análisis de requerimientos mediante una lista de chequeo de comparativa con protocolos y estándares que debe cumplir una red industrial vs lo que se tiene implementado en una de las plantas de la segunda empresa productora de neumáticos más importante de México del sector manufacturero productor de llantas a nivel transnacional que cuenta con 2 plantas en México y 120 plantas en todo el mundo.

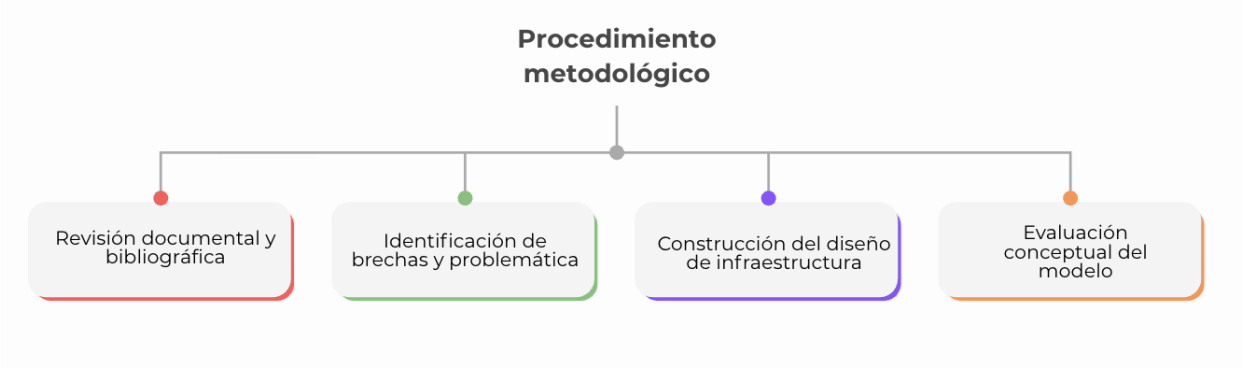
La delimitación del estudio establece que se analizará una de las plantas con procesos de automatización industrial estandarizados, en las cuales la infraestructura de red debe permitir escalabilidad para IIoT, resiliencia ante ciber amenazas y compatibilidad con arquitecturas modernas de seguridad (IEC 62443). No se contempla la validación en campo físico ni la evaluación económica detallada de la implementación, dado que el alcance es estrictamente documental.

3.4. Procedimiento metodológico

El procedimiento metodológico seguido en esta investigación se estructuró en cuatro fases principales, con el propósito de garantizar coherencia entre los objetivos planteados y el desarrollo de resultados. Estas fases comprenden la revisión documental y bibliográfica**,** la identificación de brechas y problemática tal

como se muestra en la figura 8**.** El enfoque adoptado responde a la necesidad de establecer una secuencia sistemática, sustentada en normas, estándares, y metodologías reconocidas, lo que permite asegurar la validez del diseño de red propuesto (Hernández-Sampieri y Mendoza, 2018; Kerlinger y Lee, 2002).

Figura 8 Síntesis del procedimiento metodológico.



Fuente: Elaboración propia.

A continuación, se describe cada una de las fases del procedimiento metodológico de esta investigación:

Fase 1.- Revisión documental y bibliográfica: La primera fase consistió en la identificación de las normas y estándares internacionales relevantes para infraestructura de red en entornos industriales, como ISO/IEC 11801, IEEE 802.3 y 802.11, ANSI/TIA-568, IEC 62443, NIST SP 800-82 e ISO/IEC 27001. Estos documentos constituyeron la base normativa para sustentar las decisiones de diseño (Cardona & Castaño, 2019). Este análisis permitió identificar hitos evolutivos y tendencias que inciden directamente en los requisitos de red manufacturera (UNIDO, 2020). El principal entregable de esta fase fue la tabla de clasificación de normas y estándares relevantes para la construcción del diseño de la red propuesta.

Fase 2.- Identificación de brechas y problemática: La segunda fase correspondió a la identificación de brechas entre la infraestructura de red tradicional y los requerimientos de la industria 4.0. Se utilizó un diagrama de Ishikawa para

representar las causas principales de obsolescencia: cableado antiguo, topología plana, falta de seguridad, baja capacidad y ausencia de monitoreo. Cada una de estas causas fue vinculada con impactos como limitaciones tecnológicas, segmentación inadecuada y aumento de la superficie de ataque OT (Moreno & Martínez, 2024).

Fase 3.- Construcción del diseño de infraestructura: En la tercera fase se desarrolló la propuesta de infraestructura de red, la cual integra principios de arquitectura, segmentación, cableado, tecnologías inalámbricas, seguridad y monitoreo.

- Arquitectura lógica y física: se definió un esquema core–distribución–acceso, con separación IT/OT y la inclusión de una DMZ industrial para comunicaciones seguras entre dominios.
- Segmentación: se estableció un diseño de VLANs y VRFs para dominios de IT, OT, IIoT, invitados y gestión, aplicando rutas y ACL en puntos de control reforzados con NGFW e IPS (Mora 2024).
- Capacidad y cableado: se recomendó CAT6A mínimo para 10GBASE-T**,** fibra OM4/OS2 en backbone y enlaces redundantes,
- Red inalámbrica: se incorporó la adopción de Wi-Fi 6/6E/7, con criterios de densidad, latencia, diseño RF y seguridad mediante 802.1X**.**
- Seguridad y gobernanza: el modelo aplicó la lógica de zonas y conductos de IEC 62443, junto con controles de NIST SP 800-82 e ISO/IEC 27001, extendidos hacia un enfoque de Zero Trust para accesos remotos.
- Observabilidad: se incluyeron prácticas de telemetría, monitoreo y visibilidad mediante NMS, NetFlow/IPFIX, syslog, SNMPv3 y tableros de indicadores de servicio**.**

Fase 4.- Evaluación documental del modelo: Finalmente, la cuarta fase consistió en la evaluación documental, que se realizó mediante la construcción de escenarios de migración y comparación de indicadores antes y después.

- Escenarios de migración: se analizaron casos como la transición de 10 → 25 Gb en agregación OT, la migración de CAT6 a CAT6A/CAT7, la actualización de Wi-Fi 5 a Wi-Fi 6
- Indicadores clave (KPIs): capacidad de transmisión, latencia, disponibilidad, seguridad, tiempo medio de detección (MTTD) y de recuperación (MTTR).
- Análisis de riesgos: se utilizó la metodología Failure Mode and Effects Analysis (FMEA) para valorar riesgos derivados de los cambios en red, cableado y seguridad (Kerlinger y Lee, 2002).
- Criterios de aceptación: se establecieron umbrales teóricos, como ≥50% de reducción de oversubscription partiendo de la regla general recomendada por CISCO (2008), para la sobreasignación que es de 20:1 para los puertos de acceso en el enlace ascendente de acceso a distribución, para los enlaces de distribución a núcleo, la recomendación es de 4:1 y en el centro de datos, puede ser necesaria una relación de 1:1. Y ≥30% de mejora en tiempos de detección de incidentes para estar dentro de la métrica establecida por el SOC (Centro de Operaciones de Seguridad) que se utiliza para evaluar la eficiencia de las capacidades de detección y respuesta ante amenazas tiempo medio para detectar una amenaza < 24 horas.

En conjunto, este procedimiento permitió construir, sustentar y evaluar un modelo de infraestructura de red aplicable a la empresa productora de neumáticos MB, demostrando tanto su viabilidad conceptual como su alineación a estándares internacionales.

3.5 Técnicas e instrumentos de recolección de información

La recolección de información en esta investigación se basó en un enfoque documental y sistemático presentado de forma confidencial al comité tutorial para su evaluación, acorde con el carácter documental–propositivo del modelo. Como lo señala Cardona & Castaño (2019), la investigación documental permite organizar y extraer conocimiento a partir de fuentes normativas, técnicas y académicas, favoreciendo el desarrollo de propuestas fundamentadas.

En este sentido, se aplicaron las siguientes técnicas:

- Búsqueda sistemática de literatura en bases de datos especializadas y repositorios de organismos internacionales, tales como IEEE Xplore, Scopus, NIST, ISO e IHS Standards, siguiendo criterios de actualidad (2000–2025), pertinencia temática y aplicabilidad al contexto manufacturero.
- Selección de fuentes considerando la relevancia, el alcance (IT, OT, seguridad, cableado), el año de publicación y la aplicabilidad directa al diseño de infraestructura.
- Construcción de matrices de extracción de información, que permitieron organizar los requisitos normativos, los parámetros tecnológicos y las mejores prácticas, estableciendo una trazabilidad clara hacia el modelo propuesto.

Estas técnicas garantizaron información robusta y pertinente, alineada con lo que Hernández-Sampieri & Mendoza (2018) definen como un insumo esencial para estudios de diseño conceptual.

3.6. Técnicas de análisis de información

El análisis de la información recopilada se estructuró en varios niveles:

Análisis comparativo normativo: En el que se relacionaron exigencias de normas y estándares internacionales (ISO/IEC, IEEE, ANSI/TIA, IEC 62443, NIST SP 800-82) con sus implicaciones directas en el diseño de red. Esta técnica permitió derivar criterios objetivos de arquitectura y seguridad.

Análisis de escenarios teóricos (antes/después): donde se compararon indicadores de rendimiento, seguridad y escalabilidad en configuraciones tradicionales frente a las propuestas.

Evaluación conceptual mediante indicadores clave de desempeño (KPI):

Capacidad de transmisión tomando como base las recomendaciones del estándar 802.3 en velocidades de redes empresariales de 40 Gb/s, 100 Gb/s, 200 Gb/s y hasta 400 Gb/s.

Latencia de acuerdo con los parámetros de la UIT-T (2003) que establece como límite 400 ms para no generar desfases mientras que los rangos recomendados son:

- Excelente: < 20 ms.
- Bueno: entre 20 ms y 50 ms.
- Aceptable: Hasta 100 ms.

Disponibilidad basada en la norma ANSI/TIA-942-B en 4 niveles:

- Tier 1: 99.67% de disponibilidad (hasta 28.8 horas de caída al año)
- Tier 2: 99.74% de disponibilidad (hasta 22.6 horas de caída al año).
- Tier 3: 99.982% de disponibilidad (hasta 1.5 horas de caída al año).
- Tier 4: 99.995% de disponibilidad (hasta 5 minutos de caída al año).

Tiempo medio de detección (MTTD) bajo los valores aceptados y recomendados por Inflo (2026):

- Menos de 24 horas (< 24h): nivel aceptable
- Menos de 4 horas (< 4h): estado muy bueno

- Menos de 1 hora (< 1h): nivel de élite recomendado

Tiempo medio de reparación (MTTR) tiempo de referencia a partir del 2026 < 4 horas. (Inflo, 2026).

Matrices de riesgo tipo FMEA: que permitieron identificar modos de fallo, efectos y acciones de mitigación en escenarios de migración tecnológica.

Con el método FMEA se identificaron y previeron sistemática y prospectivamente los riesgos asociados con un proceso. Se efectúa una catalogación de los riesgos por cada actividad realizada, tabla 4, se detallan las causas y las posibles consecuencias que se pueden generar si el riesgo se hace efectivo, por medio de tablas de valores califican la severidad (tabla 5), la ocurrencia (tabla 6) y detección (tabla 7) (Lurita & Lurita, 2024).

Tabla 4 Tabla de catalogación de riesgos.

Clasificación	Descripción
Riesgo menor	No se toma acción o tratamiento alguno
Riesgo moderado	Se toma alguna acción o tratamiento
Riesgo Alto	Se realizan una evaluación selectiva e implementa mejoras específicas
Riesgo crítico	Se dejan registros de modificación en la prestación del servicio y mejora de cada una de las actividades

Fuente: Hurtado et al., 2019.

Tabla 5 Tabla de severidad

Clasificación	Descripcion	Puntaje
Catastrofico	La consecencia puede generar daños y afectar la inegridad (evento centinela)	5
Mayor	La consecuencia puede cancelar todo el proceso o servicio generando insatifaccion	4
Moderado	La consecuencia puede interrupir el proceso y generar inconformidad	3
Menor	La consecuencia puede ser percibida	2
Insignificante	Ningun efecto	1

Fuente: Hurtado et al., 2019.

Tabla 6 Tabla de ocurrencia

Clasificación	Descripcion	Puntaje
Casi seguro	Se espera que el evento ocurra En la mayoria de las circunstancias	5
Probable	El evento probablemente ocurrira en la mayoria de las circunstancias	4
Posible	El evento podria ocurrir en algun momento	3
Improbable	El evento puede ocurrir en algun momento	2
Raro	El evento puede ocurrir solo en circunstacias exepcionales	1

Fuente: Hurtado et al., 2019.

Tabla 7 Tabla de detección

Clasificación	Descripcion	Puntaje
Casi imposible	La situacion se detecta < 85%	5
Menor	La situacion se detecta en un 85%	4
Moderao	LA situacion se detecta en un 90%	3
Alto	La situacion se detecta en un 95%	2
Casi seguro	La sictuacion se detecta en un 99%	1

Fuente: Hurtado et al., 2019.

Se presenta la calificación de cada riesgo en donde lo más trascendental es la severidad o gravedad y la probabilidad de ocurrencia; se realiza el cálculo del NPR = Severidad (S) x Ocurrencia (O) x Detección (D). Cada FM de acuerdo con la escala de calificación FMEA la fórmula es RPN=O x S x D (Hurtado et al., 2019) que se emplea para evaluar el impacto del riesgo al que se le aplica un plan de acción o tratamiento. La prioridad del problema para el caso lo obtienen por medio del NPR, una vez determinado este valor se comienza la evaluación sobre la base de definición de riesgo (Hurtado et al., 2019).

Estas herramientas son congruentes con la recomendación de Kerlinger & Lee (2002), quienes destacan la importancia de utilizar métodos analíticos para transformar evidencia documental en modelos con valor aplicado.

3.7. Criterios de validación del modelo

La validez del modelo se garantiza a partir de tres ejes:

1. Alineación normativa comprobada: Garantizando que cada componente de diseño respondiera a requisitos explícitos de estándares internacionales (ISO/IEC, NIST, IEC).

2. Coherencia interna del diseño: Mediante la trazabilidad establecida en matrices norma-decisión de diseño - KPI. Esta relación permitió avalar consistencia y congruencia conceptual.

3. Evaluación conceptual positiva: Determinada por el cumplimiento de criterios de aceptación definidos en los escenarios de migración (p. ej., reducción de oversubscription ≥50%, latencia ≤1 ms en celdas críticas).

La consistencia con el objetivo general confirma que la infraestructura planteada cumple con el propósito de escalar, asegurar comparabilidad y habilitar la adopción de nuevas tecnologías en la empresa manufacturera de neumáticos MB. Estos criterios reflejan lo señalado por Bunge (2000), quien establece que la validez de un modelo documental radica tanto en su coherencia lógica como en su capacidad para resolver el problema planteado.

3.8. Limitaciones metodológicas

La metodología seleccionada permitió desarrollar un modelo sólido, se reconocen limitaciones, como a) carácter teórico del modelo, dado que no se implementó en un entorno físico real, lo cual restringe la validación empírica directa; b) dependencia de literatura y normas disponibles, lo que puede sesgar la propuesta hacia fuentes mayormente occidentales y con énfasis en grandes fabricantes; c) falta de validación en piloto real, pues el modelo se evaluó conceptualmente mediante escenarios y no a través de pruebas en campo.

A pesar de estas limitaciones, la investigación aporta un marco documental replicable, en línea con lo planteado por la Organización de las Naciones Unidas para el Desarrollo Industrial (UNIDO, 2020), respecto a la necesidad de dotar a la industria de marcos de referencia normativos y tecnológicos para enfrentar los retos de la digitalización.

CAPÍTULO IV. PROPUESTA TÉCNICA

4.1 Revisión documental y bibliográfica

El propósito de esta revisión fue fundamentar la propuesta del diseño de infraestructura de red con base en evidencia científica, normativa internacional y guías de referencia de la industria manufacturera para asegurar que el diseño de la red esté alineado con los objetivos y requisitos de la industria de manera eficaz y efectiva.

Se aplicaron fuentes primarias (normas y estándares internacionales), para proponer un diseño de red sólido que se amolde a las necesidades de la empresa manufacturera MB, con normativas reconocidas, como NIST, IEC 62443, ISA-95 y la serie ISO 27000, literatura científica de bases como IEEE Xplore y ScienceDirect.

4.1.1 Mapa de fuentes consultadas

En la industria existen diversos estándares por lo cual los organismos encargados de la normalización a nivel internacional IEC e ISO han preparado una referencia de los estándares y técnicas en la industria 4.0 con el objetivo de hacer posible una convergencia con respecto a las tecnologías al momento de la implementación (Moreno & Martínez, 2024).

La tabla 8 lista el cuerpo documental utilizado, clasificado según tipo de fuente, alcance, año de publicación y su relevancia para el modelo.

Tabla 8 Fuentes documentales relevantes para el modelo de red

Fuente	Tipo	Alcance	Año	Relevancia
ISO/IEC 11801	Norma	Cableado estructurado	2017	Define categorías y desempeño de cableado en edificios industriales.
ANSI/TIA-568.2-D	Norma	Cableado estructurado	2018	Estándar de referencia en instalaciones de cobre y fibra.
IEEE 802.3	Estándar	Ethernet (10–400 Gb)	2022	Base de las velocidades actuales y futuras en backbone industrial.
IEEE 802.11ax/ay/be	Estándar	Redes inalámbricas Wi-Fi 6/7	2021–2024	Soporte para movilidad y alta densidad en entornos industriales.
IEC 62443	Norma	Ciberseguridad industrial	2021	Define niveles de seguridad para sistemas de control industrial.
NIST SP 800-82r3	Guía	Seguridad en ICS/SCADA	2022	Mejores prácticas de seguridad en OT.
ISO/IEC 27001	Norma	Gestión de seguridad de la información	2022	Marco SGSI aplicado a IT/OT.
Cisco (2023), *Industrial Networking Trends*	Whitepaper	IoT/IIoT y SDN	2023	Perspectiva de fabricantes sobre tendencias IT/OT.
Siemens (2022), *Whitepaper Industrial Edge*	Whitepaper	Integración IT/OT	2022	Casos de referencia en manufactura.
Xu et al. (2021)	Artículo	Redes 5G e IoT industrial	2021	Aplicaciones emergentes en fábricas inteligentes.
Farooq & ul Haq (2022)	Artículo	Zero Trust en entornos OT	2022	Estrategias de seguridad basadas en identidades.
Zhang et al. (2023)	Artículo	SDN aplicado a manufactura	2023	Evaluación de escalabilidad y control.

Fuente: Elaboración propia con base en la revisión bibliográfica consultada entre 2018 y 2023.

4.1.2 Síntesis normativa y su impacto en el diseño

La infraestructura de red industrial debe alinearse con un marco normativo robusto. La tabla 9 presenta un cuadro comparativo de los principales estándares, sus exigencias y su implicación directa en el diseño de redes.

Tabla 9 Matriz norma–requisito–implicación de diseño

Norma/Estándar	Enfoque	Implicación en el diseño
ISO/IEC 11801	Categorías de cableado, fibra multimodo/monomodo	Selección de cableado CAT6A+ y OM4/OS2 para garantizar 10–40 Gb.
ANSI/TIA-568.2-D	Desempeño de cableado estructurado en cobre	Instalaciones certificadas mín. CAT6A para asegurar migración a 10GBASE-T.
IEEE 802.3	Definición de velocidades Ethernet hasta 400 Gb	Planificación de core y agregación con soporte a 25/40/100 Gb.
IEEE 802.11 (ax, be)	Estandarización Wi-Fi 6/7	Implementación de celdas de alta densidad en entornos de planta.
IEC 62443	Seguridad en sistemas de control	Diseño en zonas y conductos, firewalls industriales, DMZ.
NIST SP 800-82	Seguridad en ICS	Controles en SCADA/PLC, segmentación IT/OT.
ISO/IEC 27001	Gestión de seguridad de la información	Adopción de un SGSI para integridad, disponibilidad y confidencialidad.

Fuente. Elaboración propia.

La aplicación de normas y estándares es esencial para proteger los activos críticos involucrados en estos procesos, como sistemas de control. Esto reduce el riesgo de interrupciones operativas o daños a la infraestructura, además, garantiza la integridad de los datos que se transfieren entre los mencionados sistemas (Mora, 2024).

4.1.3 Tendencias en tecnología para redes industriales

Las tendencias tecnológicas en redes industriales apuntan a mayores capacidades, seguridad reforzada y convergencia IT/OT. Dado que la convergencia IT/OT hace referencia a la integración progresiva de los sistemas informáticos tradicionales (IT) con los sistemas de control industrial (OT), a fin de crear un entorno más conectado, eficiente y automatizado. Esta unión es uno de los pilares fundamentales de la Industria 4.0. (Carral, 2025). A continuación, se mencionan las principales tendencias y sus características:

- Ethernet 25/40/100 Gb
  Escalabilidad para transmisión de datos de IA, robótica y visión artificial (IEEE, 2022).

- Wi-Fi 6
  Alta densidad y baja latencia, útil para AGVs y sensores móviles (IEEE, 2021).

- SDN (Software Defined Networking)
  Mayor flexibilidad y control centralizado en redes industriales (Rodriguez et al. 2020).

- SASE/Zero Trust
  Arquitecturas de seguridad basadas en identidad y acceso mínimo necesario (Kumar, 2021).

La industria 4.0. Exige que las redes industriales no solo sean robustas y seguras, sino también escalables y eficientes para soportar el crecimiento del negocio. En este contexto, el diseño y la configuración de una red adecuada se convierten en un factor crucial para el éxito empresarial (Carral, 2025).

4.2 Diagnóstico

El propósito de este apartado es caracterizar las problemáticas comunes en la infraestructura de red en la segunda empresa productora de neumáticos más importante de México y traducirlas en requisitos técnicos que sirvan de base para el modelo propuesto. El diagnóstico se fundamenta en literatura científica, normativa internacional (ISO/IEC, ANSI/TIA, IEEE, IEC 62443, NIST).

4.2.1 Patrones de obsolescencia en redes industriales

A partir del análisis documental y de casos de referencia, se identifican patrones recurrentes de obsolescencia en las redes de manufactura, que son los siguientes:

- **Topologías segmentadas incorrectamente**
  Ausencia de VLANs, firewalls internos y DMZ que expone los sistemas de control industrial (OT) a riesgos de intrusión (NIST, 2022).

- **Capacidad limitada**
  Enlaces de 1–10 Gb, insuficientes para actualización o migración de tecnologías (IEEE, 2022).

- **Infraestructura física obsoleta**
  Uso predominante de cableado CAT5e/CAT6, sin soporte garantizado para más de 1–10 Gb (ISO/IEC 11801, 2017).

- **Equipos de switching/core desactualizados**
  Incapaces de soportar 25/40/100 Gb o funciones modernas de telemetría y SDN.

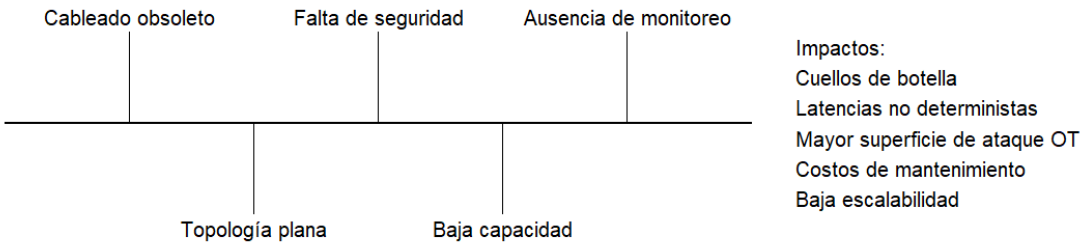
- Falta de monitoreo centralizado (NMS/SIEM)

Lo que dificulta la detección temprana de anomalías y fallas (Cisco, 2023).

4.2.2 Análisis causa-efecto

La figura 9 presenta un diagrama causa-efecto (Ishikawa) que vincula las limitaciones actuales en la empresa manufacturera de neumáticos MB con sus impactos en competitividad y seguridad.

Figura 9 Diagrama de Ishikawa: causas de obsolescencia en redes industriales.



Fuente. Elaboración propia.

La figura ilustra cómo factores como el cableado obsoleto, topologías planas, ausencia de seguridad, baja capacidad y falta de monitoreo se traducen en impactos negativos: cuellos de botella, latencias no deterministas, incremento de la superficie de ataque, costos de mantenimiento y baja escalabilidad.

4.2.3 Síntesis del diagnóstico

El diagnóstico revela que las redes industriales tradicionales no cumplen con los requerimientos modernos de capacidad, seguridad y escalabilidad. Las principales brechas detectadas son de dependencia de cableado y equipos obsoletos (CAT5e/6, switches de 1–10 Gb), ausencia de segmentación formal IT/OT,

aumentando riesgos de ciberataques, limitada capacidad de monitoreo (sin SIEM ni telemetría avanzada) y proyecciones de crecimiento de endpoints sin planeación estructural. Este análisis se convierte en la base para la propuesta de diseño de esta investigación de tesis.

4.3. Diseño de la propuesta

El diseño de la propuesta tiene como objetivo plantear una infraestructura de red actualizada y alineada con normas internacionales (ISO/IEC, ANSI/TIA, IEEE, IEC, NIST), que permita a la empresa manufacturera de neumáticos MB, prepararse para migraciones tecnológicas futuras y soportar procesos críticos de IT y OT.

4.3.1 Requisitos cuantitativos de red

En el caso de la infraestructura de red de la empresa manufacturera MB, además de estar bajo normas y estándares, debe cumplir con parámetros indicadores y procesos estandarizados de las plantas. La tabla 10 sintetiza los KPIs mínimos propuestos para el diseño de red estructurado.

Tabla 10 KPIs de red industrial base

Métrica	Objetivo base	Notas
Capacidad (Core/Distribución)	25–40 Gb	Escalable a 100 Gb en 5 años.
Capacidad (Acceso)	≥10 Gb	Usuarios/VDI e IoT intensivo.
Oversubscription	3:1 (máx.)	Balance entre costo y desempeño.
Disponibilidad (IT)	≥99.9%	Aceptable para oficinas administrativas.
Disponibilidad (OT/ICS)	≥99.99%	Requiere redundancia activa.
MTTR (Mean Time to Repair)	≤4 h	SLA recomendado.

Métrica	Objetivo base	Notas
Cobertura Wi-Fi	≥95% de planta	Wi-Fi 6/7 con roaming optimizado.
Seguridad mínima	ACL, NGFW, IDS/IPS, SIEM	Segmentación IT/OT y DMZ.
Proyección de endpoints	+15–20% anual	Escalabilidad en 5–10 años.

Fuente. Elaboración propia.

4.3.2 Arquitectura lógica

El modelo propuesto se estructura bajo una topología jerárquica en tres capas (core, distribución, acceso) con dominios IT y OT con los dispositivos mostrados en la tabla 11, claramente separados mediante una DMZ industrial**.** Se recomiendan enlaces troncales redundantes en backbone y distribución para permitir resiliencia (Cisco, 2022).

Tabla 11 Dispositivos y equipos existentes en la red.

Tecnología	Dispositivo	Cantidad
OT	PLC	>250
	HMI	>250
	SCADA	0-20
	CCTV	100 - 250
	AGV	20 - 100
	Scanners	>250
	Prensas	20-50
	K1s	20-50
	ASRS	0-20
	Steelastic	0-20
	Banburys	0-20

	Tubuladuras y calandrias	20-100
IT	AP	100 - 250
	switches	50 - 150
	Routers	0 - 20
	Firewalls	0 - 20
	Servidores	0 - 20
	Usuarios conectados a la red	> 250
	Telefonía móvil	>250
	Impresoras	100 - 250
	VDI	>250

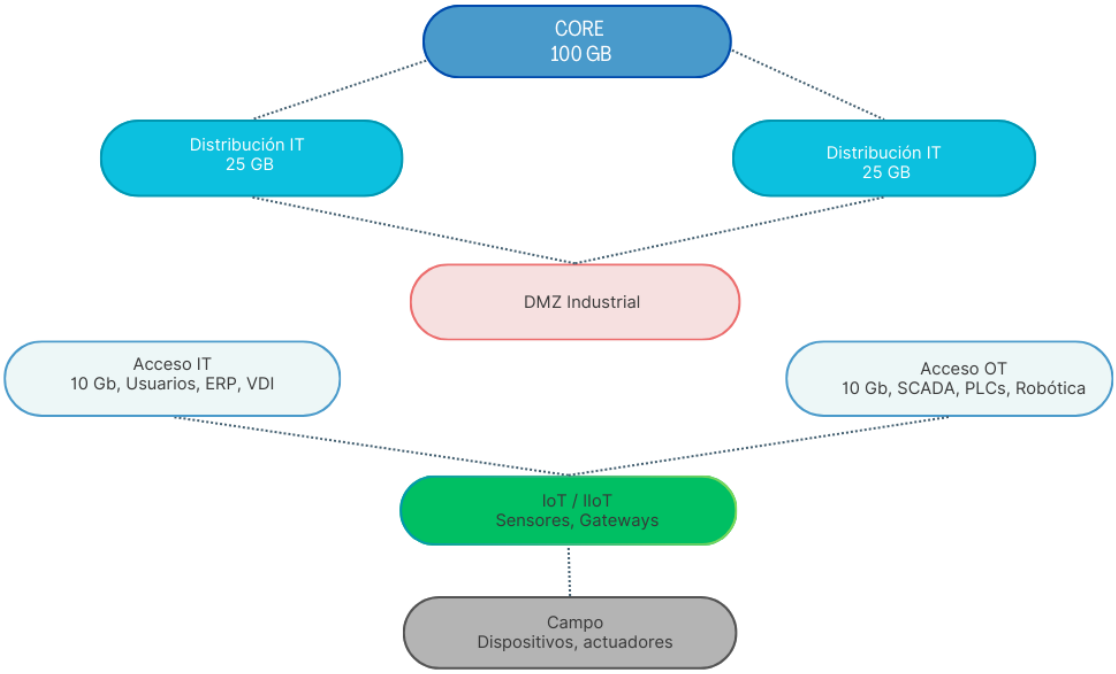
Fuente: Elaboración propia

En la tabla 11 se presentan los equipos conectados en cada una de las tecnologías IT/OT en donde se consideran la cantidad de uso de la siguiente manera:

Bajo	0-20
Medio	20-100
Alto	100-250
Muy alto	>250

A continuación, la figura 10 presenta la topología lógica y física propuesta para el caso de estudio.

Figura 10 Topología lógica y física propuesta



Fuente. Elaboración propia.

A continuación, se describen las capas del diseño jerárquico del modelo propuesto:

Core 100 Gbps: De acuerdo con el estándar de red 802.3 y la aplicación de redes de alta velocidad en el entorno industrial se propone el core a 100 Gbps, este agrega el tráfico que proviene de la capa de distribución, lleva a cabo el enrutamiento entre las diferentes subredes que forman una red, procesa los paquetes aplicando mecanismos de control y filtrado, y proporciona salida a Internet. (Sánchez, 2015).

Distribución 25 Gbps: une la capa core y la capa de acceso para ofrecer conectividad a los servicios. Permite escalabilidad al servir como un punto de agregación para múltiples switches de la capa de acceso. (Cisco, 2014).

Acceso IT/OT: Los dispositivos accesibles al usuario y dispositivos terminales se conectan a la red, que ofrece conectividad inalámbrica y cableada. Contiene características de seguridad y recuperabilidad de la red. (Cisco, 2014).

DMZ Industrial: red añadida entre una red protegida y una red externa para ofrecer un nivel de seguridad adicional. Es un paso hacia la defensa en profundidad, dado que adiciona un nivel extra de seguridad por detrás de un simple perímetro. Funciona para la segmentación de redes de TI/OT con características de seguridad integradas (Alvarez, 2021).

4.3.3 Segmentación de red

La segmentación de red es parte fundamental de la propuesta, donde se define a través de VLANs, estructuradas en dominios: IT, OT (celdas de producción, SCADA/PLCs), invitados y gestión. Con base en las normativas IEC 62443 y en el estándar IEEE 802.1Q, se propone una segmentación de VLANs adecuada para la infraestructura de red en cinco áreas principales:

1. Administrativa (IT), contempla aplicaciones como ERP, colaboración, VDI, con requisitos como throughput alto (1–10 Gb por usuario en VDI), QoS para aplicaciones críticas, seguridad perimetral (NGFW, IDS/IPS).

2. Planta de producción (OT) considera los aplicativos de SCADA, PLCs, robótica, visión artificial y con requisitos como baja latencia (<10 ms), determinismo con TSN, disponibilidad ≥99.99%, redundancia de enlaces y switches.

3. Sistemas de control industrial (ICS), con una estructura de segmentación en zonas y conductos conforme a IEC 62443, con DMZ como capa intermedia. Y con requisitos de seguridad perimetral, flujos “northbound” (hacía IT) y “southbound” (hacia campo).

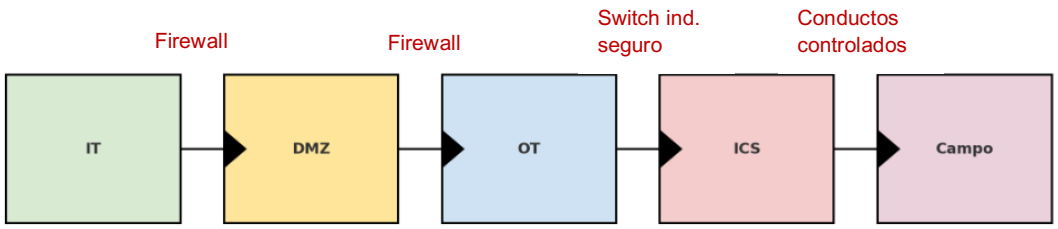
4. IoT/IIoT, con aplicaciones como sensores, actuadores, gateways y con los requisitos de onboarding seguro (certificados), soporte para protocolos industriales (MQTT, OPC UA), alta densidad de endpoints.

5. Visitantes/Contratistas, con acceso temporal a red Wi-Fi y requisitos de aislamiento en VLAN específica, portal cautivo, expiración de credenciales, ancho de banda limitado.

Cada segmento se protege con ACLs (listas de control de acceso), NGFW (firewall de nueva generación) e IPS (sistema de prevención de intrusión) y se integra en la DMZ según las guías de IEC 62443 y NIST SP 800-82.

La figura 11 ilustra un esquema de segmentación de red basado en IEC 62443, en donde se observa que las tecnologías de la Información y las tecnologías operativas se encuentran separadas mediante una subred física (DMZ) actuando como zona de seguridad entre ellas, además de contar con un sistema de control industrial (ICS) priorizando la disponibilidad y seguridad operativa antes de permitir conectividades con sistemas finales.

Figura 11 Esquema de zonas y conductos en infraestructura manufacturera.



Fuente. Elaboración propia.

4.3.4 Capacidad de transmisión

Los perfiles de referencia propuestos para el modelo se muestran en la tabla 12.

Tabla 12 Capacidades de transmisión objetivo por capa de red.

Capa/área	Capacidad recomendada	Justificación técnica
Core	≥100 Gb	Tráfico East-West, escalabilidad IA/Big Data
Distribución OT	≥25 Gb	Soporte a visión artificial y respaldos
Acceso cableado	10 Gb	Estaciones de trabajo modernas y CAD/PLM
IoT/IIoT	1–10 Gb	Alta densidad de sensores y gateways
Wi-Fi industrial	Wi-Fi 6	Movilidad de AGVs y equipos portátiles

Fuente. Elaboración propia.

4.3.5 Red de transporte y seguridad

En cuanto a la red de transporte se contempla un cableado estructurado con las siguientes características: medio de cobre se recomienda CAT6A como estándar mínimo para acceso, fibra OM4/OS2 en backbone**,** y rutas físicas redundantes A/B. Para alimentar IoT y videovigilancia, así como incluir PoE+ (IEEE 802.3bt)**.** ISO/IEC 11801

En la red inalámbrica industrial, el modelo incluye Wi-Fi 6/6E para entornos de planta, con roaming optimizado y seguridad en WPA3-Enterprise y 802.1X/EAP-TLS**.**

Respecto a la seguridad, se rige por un enfoque de defensa en profundidad sustentado en normas internacionales. La tabla 13 resume la relación entre estándares y decisiones de diseño.

Tabla 13 Matriz entre estándares y decisiones de diseño

Norma / estándar	Requisito clave	Decisión de diseño	Evidencia / referencia
IEC 62443	Zonas y conductos	Segmentación IT/OT con DMZ	IEC (2018)
NIST SP 800-82	Controles ICS	NGFW + IPS en interconexiones	NIST (2021)
ISO/IEC 27001	SGSI / políticas de seguridad	Gestión centralizada + SIEM	ISO (2018)
ANSI/TIA-568.3-D	Cableado estructurado (fibra)	OM4/OS2 en backbone	TIA (2016)
IEEE 802.3/802.11	Ethernet y Wi-Fi de alta velocidad	Core 100 Gb, Wi-Fi 6	IEEE (2021)

Fuente. Elaboración propia.

4.3.6 Checklist de diseño

El modelo se valida contra los requisitos normativos mediante un checklist, el cual se muestra a continuación.

Validación de propuesta frente a normas internacionales

- ☑ Segmentación por zonas y conductos (IEC 62443).
- ☑ SGSI y políticas (ISO/IEC 27001).
- ☑ Cableado estructurado OM4/OS2 (ANSI/TIA-568).
- ☑ Core ≥100 Gb y distribución ≥25 Gb (IEEE 802.3).
- ☑ Seguridad ICS con NGFW e IDS/IPS (NIST SP 800-82).

Se agregan los patrones reutilizables para facilitar la adopción del modelo, que se muestran en la tabla 14.

Tabla 14 Catálogo de patrones

Patrón	Descripción	Premisas	Limitaciones
Celda OT	Edge L2/L3 con TSN opcional y uplinks redundantes	Baja latencia, disponibilidad	Mayor costo de implementación
DMZ industrial	Jump servers, brokers OPC UA/MQTT, firewalls duales	IT/OT segregadas	Complejidad de gestión
Acceso IoT seguro	NAC con 802.1X/MAB y perfiles diferenciados	Alta densidad de dispositivos	Requiere orquestación avanzada

Fuente. Elaboración propia.

Para este diseño se consideraron aspectos de obsolescencia en equipos, mostrados en el documental de la empresa de forma confidencial al comité tutorial para su validación, se consideró la capa Core a 100 Gbps y distribución a 25 Gbps bajo la referencia del estándar 802.3 y la aplicación en redes industriales, reforzando la seguridad se consideraron los firewalls conectados en la zona perimetral o zona desmilitarizada (DMZ), en donde se encuentran conectados los servicios de ISP y servicios de red que necesitan ser accesibles desde redes externas.

De acuerdo con la IEC 62443 se definieron las zonas y conductos conforme a atributos de seguridad, activos físicos y lógicos, tecnologías autorizadas, evaluación de amenazas y vulnerabilidades, requerimientos de acceso y control y procedimientos de control y mejora continua.

Se propone una redundancia física entre cada uno de los enlaces que conectan cada una de las capas de la red, para la parte Wireless se propone introducir WI-FI 6 en escenarios controlados por el tema de compatibilidades y el riesgo de facilitar conexiones con dispositivos inteligentes con sistemas de seguridad básicos hacen vulnerable a la red frente a los ciberataques. Es importante mencionar que el acceso para el mantenimiento y soporte solo es mediante VPN´s controladas con reglas en los firewalls.

CAPÍTULO V. RESULTADOS

5.1. Evaluación

El propósito de esta sección es demostrar que, al analizar y seleccionar las normas y estándares para diseñar una red industrial, mediante escenarios de migración tecnológica, el modelo de infraestructura de red propuesto resuelve las brechas identificadas en los apartados previos y ofrece escalabilidad hacia el futuro.

La selección y el análisis de información de la evaluación documental procuran una interpretación en base a ciertos criterios y permiten la generación de nueva información (Sánchez et al., 2020).

5.1.1 Escenarios de migración

A continuación, se muestra el análisis de cuatro escenarios representativos de actualización en redes industriales:

Primer escenario:

Migración de 10 Gb a 25 Gb en agregación OT
El aumento de capacidad en la capa de distribución OT reduce la sobresuscripción y permite absorber cargas intensivas de tecnologías demandantes y respaldos de gran volumen.

Tabla 15 Comparación antes/después de la migración a 25 Gb en distribución OT

Métrica	Antes (10 Gb)	Después (25 Gb)	Mejora
Throughput agregado	80 Gbps	200 Gbps	+150%
Oversubscription core:distribución	4:1	1.6:1	-60%
Tiempo de backup 2 TB	32 min	13 min	-59%

Fuente. Elaboración propia.

Segundo escenario:

Migración de CAT6 a CAT6A

El cableado estructurado con CAT6A permite conectividades 10 GBASE-T de hasta 100 m y ayuda al comportamiento frente a diafonía (ANEXT).

Para velocidades igual o superiores de 25 GbE es recomendable evaluar medio de fibra óptica.

Tabla 16 Impacto de la actualización de cableado

Criterio	CAT6	CAT6A
Distancia 10GBASE-T	55 m	100 m
ANEXT (dB)	45	65
Soporte PoE	30 W	90 W
Riesgo de sobrecalentamiento	Alto	Medio

Fuente. Elaboración propia.

Tercer escenario:

Migración de Wi-Fi 5 a Wi-Fi 6

La densidad de dispositivos IIoT y los vehículos de Guiado Automático (AGVs) en planta requiere espectros más eficientes y latencias inferiores a 10 ms.

Tabla 17 Comparación entre Wi-Fi 5 y Wi-Fi 6

Métrica	Wi-Fi 5	Wi-Fi 6
Eficiencia espectral	1x	2x
Latencia promedio (ms)	20	8–10
Nº de dispositivos soportados por AP	200	400
Idoneidad para AGVs/HMI	Aceptable	Óptima

Fuente. Elaboración propia.

5.2 Metodología de contraste

Para evaluar los escenarios se utilizó una comparación Antes/Después con indicadores clave de red (KPIs): capacidad, latencia, disponibilidad, superficie de ataque y tiempos de detección/recuperación (MTTD/MTTR), se realiza una matriz FMEA (análisis de modo y efectos de falla) tabla 14, que permitirá priorizar las correcciones de acuerdo con el valor NPR.

Tabla 18 Matriz de análisis FMEA aplicado a la migración de 10 → 25 Gb

Riesgo	Causa	Efecto	Severidad (1–5)	Ocurrencia	Detección	NPR
Congestión persistente	Demanda superior a 10 Gb	Cuellos de botella	4	3	2	24

Riesgo	Causa	Efecto	Severidad (1–5)	Ocurrencia	Detección	NPR
Fallo en migración	Configuración incorrecta	Downtime OT	4	2	1	8
Desfase equipos legacy	Switches no compatibles	Interrupciones	5	3	2	30

Fuente. Elaboración propia.

Esta evaluación se basa en tres variables calificadas en una escala del 1 al 5:

- Severidad (S): Mide el impacto o la gravedad de la consecuencia si el fallo llega a ocurrir.
- Ocurrencia (O): Mide la probabilidad o frecuencia con la que se espera que suceda la causa raíz del fallo.
- Detección (D): Mide la capacidad de los controles actuales para detectar el fallo antes de que llegue al usuario final o al siguiente proceso.

A partir de estos tres parámetros se calcula el Número de Prioridad de Riesgo (NPR o RPN), mediante la siguiente fórmula matemática:

$$NPR = SxOxD$$

Conforme a la metodología, se establecieron como criterios de aceptación la reducción ≥50% en oversubscription, mejora ≥30% en MTTD.

5.3 Identificación de beneficios, limitaciones y condiciones

El modelo presenta beneficios claros como:

- Rendimiento: mayor throughput, reducción de latencia.
- Resiliencia: redundancia de enlaces, topologías jerárquicas.
- Seguridad**:** segmentación IEC 62443, Zero Trust en accesos remotos.
- Preparación tecnológica: soporte para IIoT, IA y analítica avanzada.

Limitaciones:

- Incremento de CAPEX y OPEX en fases iniciales.
- Dependencia de habilidades técnicas avanzadas en seguridad OT/IT.
- Necesidad de coexistencia temporal con infraestructura legacy.

Condiciones de aplicabilidad:

- Plantas de mediano y gran tamaño con criticidad OT alta.
- Regulaciones industriales alineadas con IEC 62443/ISO 27001.

5.4 Plan de transición teórico

Finalmente, se propone una guía de transición en etapas, sin implementación física, para reducir riesgos, que se muestra en la siguiente tabla 19.

Tabla 19 Etapas de transición de red industrial

Etapa	Acción	Enfoque	Beneficio esperado
1	Segmentación IT/OT + DMZ	Virtualización y VLANs	Aislamiento y seguridad básica
2	Migración cableada CAT6 → CAT6A	Cableado parcial	Soporte para 10/25 Gb
3	Actualización core/distribución a 25–100 Gb	Nuevos switches	Rendimiento y escalabilidad
4	Despliegue Wi-Fi 6/7 en planta	Roaming y AGVs	Baja latencia y densidad

Fuente. Elaboración propia.

Al alinear un diseño de red industrial bajo estándares y normas internacionales, el modelo propuesto responde a los problemas típicos de obsolescencia, además de adaptarse a una ruta de migración escalable hacia la Industria 4.0. Migrar a 25 Gbps permitirá reducir la sobresuscripción al aumentar el ancho de banda se amplía la

capacidad de los enlaces Uplink, para este caso se propone CAT 6a para velocidades de 10 Gbps en distancias máximas de 100 m y ancho de banda de 500 MHz, velocidades mayores es recomendable revisar medio por fibra óptica.

Es preciso mencionar que siempre existirán riesgos aún después de la propuesta, por mencionar algunos: la ingeniería de los ciberataques cada vez es más elaborada que cruzan las barreras de seguridad, especificaciones en los requerimientos de las tecnologías convergentes, las condiciones en las que se instalarán los equipos activos como AP para propagación de WI-FI, switches y cableado estructurado no cambian (temperatura, humedad, distancias, corriente regulada) mismas que pueden continuar afectando.

Por último, añado que existen desventajas de realizar una evaluación documental frente a una implementación real como la detección de fallas, resultados, validación del entorno físico, condiciones operativas que no podrán ser reflejados ni medidos.

La propuesta de red está alineada bajo las recomendaciones de las normas y estándares IEC 62443, NIST SP 800-82, IEEE 802.3 y ANSI/TIA para conseguir los resultados esperados.

CONCLUSIONES

La presente investigación tuvo como propósito principal proponer un diseño de infraestructura de red actualizada, fundamentada en normas y estándares internacionales, orientada a la industria manufacturera de neumáticos en México, delimitada en el sector de producción de llantas. Esta propuesta busca responder a tres desafíos fundamentales identificados desde el planteamiento del problema: (i) la superación de las limitaciones de conectividad presentes en las plantas industriales, (ii) la necesidad de asegurar escalabilidad y comparabilidad en el diseño, y (iii) la preparación de las infraestructuras para la adopción de tecnologías emergentes como IIoT, inteligencia artificial, analítica avanzada y conectividad determinista. Bajo este contexto, se diseña en el capítulo 4 un modelo que integra los elementos centrales de diseño en capas (core, distribución y acceso), segmentación de redes IT/OT mediante DMZ industrial, adopción de cableado estructurado de última generación (CAT6A/OM4/OS2), despliegue de tecnología inalámbrica industrial de vanguardia (Wi-Fi 6/), y alineación a los marcos normativos internacionales más relevantes: IEC 62443, ISO/IEC 27001, NIST SP 800-82 y los estándares IEEE/ANSI-TIA de cableado y comunicación. El cumplimiento del objetivo se evidencia en tres entregables claves que consolidan la propuesta, entre las que se encuentra la arquitectura de la estructura de red, la construcción de matrices de contraste entre normas y decisiones de diseño, que demuestran la trazabilidad normativa del modelo y los escenarios de evaluación conceptual. En el caso de la migración de 10 a 25 Gb en la capa de distribución OT, evidenciaron una reducción del 60% en la sobresuscripción, lo cual valida la escalabilidad del modelo. Asimismo, la transición de cableado CAT6 a CAT6A permite soporte para 10 Gb bajo condiciones marcadas, y compatibilidad con PoE de alta potencia, proyectando la necesidad de recableados reactivos en horizontes de 5 a 10 años. En cuanto a las tecnologías inalámbricas, la migración de Wi-Fi 5 a Wi-Fi 6 se esperan mejoras

sustantivas en eficiencia espectral, habilitando casos de uso críticos como AGVs y HMIs móviles. La solución planteada en esta tesis responde a una problemática frecuente en plantas manufactureras de neumáticos: la fragmentación tecnológica entre redes IT y OT, la obsolescencia del cableado y equipos de acceso, y la falta de lineamientos normativos unificados para entornos híbridos IT/OT. La investigación reafirma que las redes industriales no pueden seguir evolucionando de manera reactiva, respondiendo únicamente a fallas o requerimientos inmediatos. La transformación digital de la manufactura exige que la infraestructura de conectividad se diseñe bajo principios de resiliencia, escalabilidad y cumplimiento normativo. Si bien el modelo propuesto para resolver la problemática observada en la planta de la empresa productora de neumáticos MB, su validación conceptual y su alineación normativa son una propuesta robusta al considerar los estándares y normas internacionales, por lo que puede orientar proyectos de implementación real en la industria teniendo en cuenta que existen limitaciones como la detección de fallas, resultados, validación del entorno físico, condiciones operativas que no podrán ser reflejados ni medidos debido a que es una evaluación documental y no una implementación real.

TRABAJO FUTURO

Este trabajo se limita a realizar una propuesta teórica en base a la experiencia en el ámbito empresarial y manufacturero, tomando en cuenta las mejores prácticas y normativas que permiten respaldar cada uno de los lineamientos.

Como siguiente paso se puede implementar la infraestructura en un ambiente real para comprobar que se logra garantizar la aplicación de tecnologías actuales, correcta comunicación interna, externa y procesos que implican líneas de producción mediante redes de datos adecuadas, además de validar y evaluar el costo-beneficio de contar con infraestructuras de red robustas y bajo normativas actuales.

Futuras líneas de trabajo incluyen el desarrollo de pilotos en entornos controlados, la simulación de escenarios de migración y la evaluación del costo total de propiedad (TCO) para fortalecer la adopción práctica de esta propuesta.

REFERENCIAS

Alvarez, F. (2021). Diseño de redes empresariales modernas. https://www.researchgate.net/profile/Felix-Alvarez-Paliza/publication/346607424_DISENO_DE_REDES_EMPRESARIALES_MODERNAS-2020/links/5fc920a445851568d13a5fb0/DISENO-DE-REDES-EMPRESARIALES-MODERNAS-2020.pdf

Ahmad, I., Rodriguez, F., Kumar, T., Suomalainen, J., Jagatheesaperumal, S. K., Walter, S., Asghar, M. Z., Li, G., Papakonstantinou, N., Ylianttila, M., Huusko, J., Sauter, T., & Harjula, E. (2024). Communications Security in Industry X: A Survey. IEEE Open Journal of the Communications Society, 5, 982–1025. https://doi.org/10.1109/OJCOMS.2024.3356076

Bátiz, J. & Albarrán, D. (2023). Industria manufacturera de México y el Estado de México: producción y empresas grandes, 2023. https://www.researchgate.net/profile/JoseBatizLopez/publication/393374570_Industria_manufacturera_de_Mexico_y_el_Estado_de_Mexico_produccion_y_empresas_grandes_2023_En_la_Revista_de_Analisis_de_Coyuntura_Economica_Economia_Actual_de_la_Universidad_Autonoma_del_Estado_de_Mex/links/6867234607b3253fd1cc1b62/Industria-manufacturera-de-Mexico-y-el-Estado-de-Mexico-produccion-y-empresas-grandes-2023-En-la-Revista-de-Analisis-de-Coyuntura-Economica-Economia-Actual-de-la-Universidad-Autonoma-del-Estado-de-Me.pdf

Barbancho, J., Benjumea, J., Rivera, O., Ropero, J. & Sivianes, F. (2020). Redes Locales. Paraninfo.

Briggeth, J. & Plazarte,K. (2023). Propuesta de rediseño de la topología en la infraestructura de la red de comunicaciones de la fundación tainate en la ciudad de cayambe. https://dspace.ups.edu.ec/bitstream/123456789/24414/1/TTS1188.pdf

Caballero, B. (2022). Diseño de una mejora a la infraestructura tic basado en las redes, seguridad y monitoreo, para la prevención de vulnerabilidades en la gestión de la infraestructura de la empresa Crusardi S.A.S. https://repository.ucc.edu.co/server/api/core/bitstreams/a6457d6b-a53b-4d2f-8430-1dac70ea6c01/content.

Cardona, J., & Castaño, J. (2019). Investigación documental: una estrategia para el desarrollo de habilidades cognitivas. *Revista Virtual Universidad Católica del Norte, (58),* 5–20. https://doi.org/10.35575/rvucn.n58a3

Carrascal, D., Díaz-Fuentes, J., Manso, N., Lopez-Pajares, D., Rojas, E., Savi, M., & Arco, J. M. (2025). Softwarized Edge Intelligence for Advanced IIoT Ecosystems: A Data-Driven Architecture Across the Cloud/Edge Continuum. Applied Sciences, 15(19), 10829

Cevallos, B. (2022). Desarrollo de un prototipo de comunicación inalámbrica en tiempo real basada en OFDM, que contenga diferentes tipos de mapeo, reformado de pulso y corrección de errores, empleando equipos SDR. https://bibdigital.epn.edu.ec/handle/15000/22728

Cisco. (2008). Campus Network for High Availability Design Guide https://www.cisco.com/c/dam/en/us/td/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampus-dg.pdf#wp1108620

Cisco. (2014). Campus resumen de diseño. https://www.cisco.com/c/dam/r/es/la/internet-of-everything-ioe/assets/pdfs/en-05_campus-wireless_wp_cte_es-xl_42333.pdf

Cisco. (2022). Cisco Annual Internet Report (2018–2023). Cisco Systems. https://www.cisco.com

Cisco. (2023). Industrial Security 3.0 – Design Guide. https://www.cisco.com/c/dam/en/us/td/docs/Technology/Industrial_Security_3-0_DG.pdf

Cisco. (2023). Industrial networking trends 2023. Cisco Systems. https://www.cisco.com

Cisco. (2024). Implementing segmentation in industrial networks (BRKIOT 2882). Cisco Live 2024 session notes. https://www.ciscolive.com/c/dam/r/ciscolive/global-event/docs/2024/pdf/BRKIOT-2882.pdf

Cisco. (2025). Implementing segmentation in industrial networks (BRKIOT 2882). Cisco Live EMEA 2025 update. https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2025/pdf/BRKIOT-2882.pdf

Cosme Da Costa, C., Zarzuelo, D., Balán, A., Goicochea, A., Beltrán, S. (2025). Industria 4.0: Impacto de la Digitalización y la Automatización en la Transformación Social e Industrial. https://revistainclusiones.org/index.php/inclu/article/view/3592/3840

Data México (2025). Industrias manufactureras.

https://www.economia.gob.mx/datamexico/es/profile/industry/manufacturing?redirect=true

Díaz, C., Olmos, J. (2021). Importancia de la Seguridad Física en la Infraestructura de Redes, Centros de Datos y Telecomunicaciones de las Instituciones de Educación Superior. https://www.ties.unam.mx/num03/pdf/Importancia_seguridad_fisica.pdf

Ethernet Alliance. (2024). *2024 Ethernet Roadmap (Digital Version, March 2024)*. https://ethernetalliance.org/wp-content/uploads/2024/03/2024-Ethernet-Roadmap-Digital-Version-March-2024.pdf

Guevara, P., Verdesoto, E., Castro, E. (2020), Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción). https://recimundo.com/index.php/es/article/view/860/1363

Hernández-Sampieri, R., & Mendoza, C. (2018). Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta. McGraw-Hill.

Huidobro, J. (2006). Redes y servicios de telecomunicaciones. Thomson Ediciones Spain Parainifo, S.A.

Hurtado, M., Estacio, J., Fandiño, P. (2019). Análisis de riesgos según la metodología FMEA, basado en el sistema de gestión de calidad. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://d1wqtxts1xzle7.cloudfront.net/82739586/ANALISIS_DE_RIESGOS_SEGUN_LA_METODOLOGIA_-libre.pdf?1648369013=&response-content-disposition=inline%3B+filename%3DANALISIS_DE_RIESGOS_SEGUN_LA_METODOLOGIA.pdf&Expires=1782233482&Signature=U27KDBGFsi3Lgc

usgZdOKmOA9Qw88YaHn8Db9Ym57DveUB0NLlu-kl82GRG~TfMOPxKKEK39gMI3QFKU7zLuLUCNVzpjA6H22rRsD43W6vU0~zN-HWZGwXDQ69I8sXncY-ELxJpamOK~LRqtMpp4mnoyjteeFthH36YfDwuBgJosNr5cg4YYT6KRa7lsAJX1PiaUeIhgThs6-jdRfgz4swUZgNS9LZmjcQytCzONe~N30FCbHNxsi0AuZI~l7gSvYa4ylDD27mndexOhA0i6fJJCTGudKD0QwtryKP1iaFgaSdx7C~2W-jXM0f7siXgjCRBXVVUNC043Nn6bMdROaw__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

IEEE. (2021). IEEE 802.11ax/be standard for wireless LAN. IEEE Standards Association.

IEEE. (2022). IEEE standard for Ethernet (802.3). IEEE Standards Association. https://standards.ieee.org

IEEE 802.3 NEA Ad Hoc. (2025, enero). Proposal – “802.3 Ethernet Interconnect for AI” Assessment. https://www.ieee802.org/3/ad_hoc/ngrates/public/25_01/dambrosia_nea_01_2501.pdf

International Electrotechnical Commission (IEC). (2018). IEC 62443: Industrial communication networks – IT security for networks and systems. IEC.

International Electrotechnical Commission (IEC). (2021). IEC 62443: Security for industrial automation and control systems. IEC.

International Organization for Standardization (ISO). (2017). ISO/IEC 11801: Information technology – Generic cabling for customer premises. ISO.

International Organization for Standardization (ISO). (2018). ISO/IEC 27001: Information security management systems. ISO.

International Organization for Standardization (ISO). (2022). ISO/IEC 27001: Information security, cybersecurity and privacy protection – Information security management systems. ISO.

ISO/IEC. (2017). ISO/IEC 11801: Information technology – Generic cabling for customer premises. International Organization for Standardization.

ISO/IEC. (2022). ISO/IEC 27001: Information security, cybersecurity and privacy protection – Information security management systems. International Organization for Standardization.

Iturbide, M., Iñaki G., Arenaza, I., Zurutuza, U., Uribeetxeberria, R. (2016). Diseño de un banco de pruebas híbrido para la investigación de seguridad y resiliencia en redes industriales. https://www.garitano.info/publications/iturbe2016diseno.pdf

Inflo, (2026). SOC Metrics - MTTD, MTTR and Security KPIs [2026 Guide] https://nflo.tech/knowledge-base/soc-metrics-mttd-mttr-kpi-security/#what-are-soc-metrics

Jiménez, S. & Lira, J. (2015). Desarrollo de las telecomunicaciones: una fuente para el progreso. https://lyd.org/wp-content/uploads/2015/04/SIE-247-Desarrollo-de-las-telecomunicaciones-SJimenez-y-JLira-Marzo2015.pdf

Kamlofsky, J., Abdel, S., Colombo, H., Veiga, D., Costa, E., Milio, C., Semería, M., Hecht, P. (2017). Seguridad en Redes Industriales: Clave para la

Ciberdefensa de las Infraestructuras Críticas. https://sedici.unlp.edu.ar/handle/10915/62725

Kerlinger, F. N., & Lee, H. B. (2002). Foundations of behavioral research (4th ed.). Wadsworth.

Kouari, O., Lazaar, S., & Achoughi, T. (2025). Fortifying industrial cybersecurity: a novel industrial internet of things architecture enhanced by honeypot integration. International Journal of Electrical and Computer Engineering (IJECE), 15(1), 1089–1098. https://doi.org/10.11591/ijece.v15i1.pp1089-1098

Kumar, M. (2021). Modern Approaches to Enterprise Cloud and Network Engineering. https://www.researchgate.net/profile/John-Mathew-26/publication/40086892_Modern_Approaches_to_Enterprise_Cloud_and_Network_Engineering/links/699475ce12f837212a1b84a3/Modern-Approaches-to-Enterprise-Cloud-and-Network-Engineering.pdf

Lee, C., Kim, N., & Hong, S. (2021). Toward Industrial IoT: Integrated Architecture of an OPC UA Synergy Platform. IEEE Access. https://doi.org/10.1109/ACCESS.2021.3135432

Ley, N. (2021). Despliegue de redes de telecomunicaciones: Particularidades y limitaciones. Universidad Externado de Colombia.

López, V. (2005). Metodología para diseños físicos de LAN. https://www.redalyc.org/pdf/730/73000302.pdf

Lurita, L., Lurita, M. (2024). Aplicación de metodología DMAIC y FMEA para la mejora de la eficiencia en el servicio de galvanizado, en el rubro

metalmecánico. https://repositorioacademico.upc.edu.pe/entities/publication/5ff7d7d8-033f-5694-9647-cc593d093b0f

Martínez, Á. (2025). Diseño de una infraestructura de red OT industrial con requisitos de ciberseguridad. https://repositorio.upct.es/server/api/core/bitstreams/65f45fe2-4120-42ca-bde-66a62591827e/content?__goaway_challenge=meta-refresh&__goaway_id=3ef3a1e4244f61dcf66ae1f1a8bba472&__goaway_referer=https%3A%2F%2Frepositorio.upct.es%2Fbitstreams%2F65f45fe2-4120-42ca-bbde-66a62591827e%2Fdownload

Mavare, A. (2023) El surgimiento de las redes industriales. https://dialnet.unirioja.es/servlet/articulo?codigo=8951769

McKinsey & Company. (2025). The top trends in tech: Advanced connectivity. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top-trends-in-tech

Melis, A., Giovine, A., & Rinieri, L. (2025). Time-Sensitive Networking Digital Twin for STRIDE-based security testing. EURASIP Journal on Information Security, 2025(1), 26

Min, C.-H., Kim, D.-H., Yang, H., & Kwak, J. (2025). Towards Secure Legacy Manufacturing: A Policy-Driven Zero Trust Architecture Aligned with NIST CSF 2.0. Electronics, 14(20), 4109. https://doi.org/10.3390/electronics14204109

Miserez, J., Colle, D., Pickavet, M., & Tavernier, W. (2024). Exploiting queue information for scalable delay-constrained routing in deterministic networks. IEEE Transactions on Network and Service Management, 21(5), 5260-5272

Monterrubio, E. (2023). Impacto del uso de la tecnología de la información en la educación para el desarrollo de habilidades tecnológicas en el nivel medio superior. https://repository.uaeh.edu.mx/revistas/index.php/ixtlahuaco/article/view/10393/9939

Moreno, E. (2024). Diseño de una infraestructura de red de telecomunicaciones para la transformación hacia la Industria 4.0 en una planta de producción de bebidas carbonatadas y no carbonatadas. https://repositorio.upse.edu.ec/bitstreams/d3c23c8e-81d2-40eb-9eac-9297c5718647/

Moro, P., Puco, T. (2025). Diseño de una red industrial utilizando protocolo profinet, wireless hart para monitoreo y control de variables de posición, velocidad y aceleración de un servomotor. https://repositorio.utc.edu.ec/server/api/core/bitstreams/106165bb-d93f-4754-97c9-f5831bc3a576/content

National Institute of Standards and Technology (NIST). (2022). Guide to Industrial Control Systems (ICS) Security (SP 800-82 Rev. 3). U.S. Department of Commerce.

National Institute of Standards and Technology (NIST). (2023). Guide to Operational Technology (OT) Security (SP 800-82 Rev. 3). https://csrc.nist.gov/pubs/sp/800/82/r3/final

Nohlen, D. (2020). El método comparativo. https://archivos.juridicas.unam.mx/www/bjv/libros/13/6180/5.pdf

Nutanix, 2026. https://portal.nutanix.com/page/documents/solutions/details?targetId=BP-2050-Physical-Networking:top-of-rack-switching.html

Okafor, K. C., Ndinechi, M. C., & Misra, S. (2021). Cyber-Physical Network Architecture for Data Stream Provisioning in Complex Ecosystems. Transactions on Emerging Telecommunications Technologies, 32(11). https://doi.org/10.1002/ett.4407

Organización de las Naciones Unidas para el Desarrollo Industrial (UNIDO). (2020). Industrial Development Report 2020: Industrializing in the digital age. UNIDO.

Organización de las Naciones Unidas para el Desarrollo Industrial (UNIDO). (2020). Industrial Development Report 2020: Industrializing in the digital age. https://www.unido.org/sites/default/files/files/2020-07/IDR2020_Brief%203_final.pdf

.

Ramos, A., Martínez, L. (2023). Diseño integral de infraestructura de red y segmentación para potenciar la eficiencia en los procesos de la empresa Importh. https://repository.ucc.edu.co/server/api/core/bitstreams/50c4ccfa-5d42-462f-86a7-37410b5f07c0/content

Rodríguez, P. (2020). Gestor Documental para un sistema de gestión de redes. https://repositorio.unican.es/xmlui/bitstream/handle/10902/20806/Rodriguez%20Herranz%20Pablo.pdf?sequence=1&isAllowed=y

Rockwell Automation. (2023). What is a PLC? https://www.rockwellautomation.com/en-us/capabilities/programmable-logic-controller/overview.html

Rockwell Automation & Cisco. (2023). Physical infrastructure for the Converged Plantwide Ethernet (CPwE) architecture (TD). Cisco. https://www.cisco.com/c/dam/en/us/td/docs/solutions/Verticals/CPwE/5-1/Phy_Arch/CPwE-Physical-Infrastructure_Feb2023.pdf

Rodríguez, B., Pincay, E., Maldonado, K., (2022). Las redes WAN y su importancia para los ordenadores. https://revistas.unesum.edu.ec/index.php/unesumciencias/article/view/510/497

Rodríguez, D., Talay, C., González, C. (2021) Explorando las redes definidas por software (SDN). https://sedici.unlp.edu.ar/handle/10915/103546

Saavedra, J. (2017). Metodología Top-Down para el Diseño de Redes. https://juancarlossaavedra.net/2017/06/infografia-metodologia-top-down-para-el-diseno-de-redes/

Sánchez, A., Revilla, D., Alayza, M., Sime, L., Mendívil, L., Tafur, R. (2020). Los Métodos de investigación para la elaboración de las tesis de maestría en educación. https://www.researchgate.net/profile/Diana-Revilla-Figueroa/publication/343426365_LIBRO_LOS_METODOS_DE_INVESTIGACION_-_MAESTRIA_2020/links/5f29733da6fdcccc43a8e56a/LIBRO-LOS-METODOS-DE-INVESTIGACION-MAESTRIA-2020.pdf#page=7

Santillán, C., Molina, T., Vásconez, F., & Luna, G. (2018). Requerimientos y diseño de infraestructura de redes para campus universitarios. CIDEPRO.

Siemens. (2022). Industrial Edge whitepaper. Siemens AG. https://www.siemens.com

Silva, M. (2020). Telecomunicaciones digitales. Universidad del Cuaca

Sladek, P., Maryska, M., & Doucek, P. (2026). An Architectural Framework Design for a Standardised Industrial Internet of Things Solution. Array, 100856.

Stallings, W. (2021). Foundations of modern networking: SDN, NFV, QoE, IoT, and cloud. Pearson.

Suárez, J., Albisu, L., Sotolongo, N. & Blanco, F. (2007). Factores de éxito y fracaso en el comportamiento innovador de las empresas ganaderas cubanas. http://scielo.sld.cu/pdf/pyf/v30n3/pyf08307.pdf

Telecommunications Industry Association (TIA). (2016). ANSI/TIA-568.3-D: Optical Fiber Cabling and Components Standard. TIA.

Unión Internacional de Telecomunicaciones. (2003). Recomendación UIT-T G.114: Tiempo de transmisión de ida para aplicaciones con requisitos de tiempo real (Serie G: Sistemas y medios de transmisión, sistemas y redes digitales). https://www.itu.int/itut/recommendations/rec.aspx?rec=6254&lang=es

Vallina, M. (2013). Infraestructura de redes de datos y sistemas de telefonía. Paraninfo.

Vera J. (2021). Implementación de un sistema eléctrico para la conectividad tecnológica en el laboratorio de telecomunicaciones de la carrera ingeniería en computación y redes. https://repositorio.unesum.edu.ec/bitstream/53000/2685/1/PILAY%20VERA%20JEFFERSON%20EDUARDO.pdf

Vargas, A. (2026). Análisis de las características de las redes de comunicación para la implementación de sistemas industriales robustos en el marco de la industria 4.0.
https://repository.unad.edu.co/bitstream/handle/10596/80153/avargasve.pdf?sequence=3&isAllowed=y

Weill, P., & Ross, J. W. (2004). IT governance: How top performers manage IT decision rights for superior results. Harvard Business School Press.

World Economic Forum. (2023). Advanced Manufacturing: A New Narrative. https://www3.weforum.org/docs/WEF_Advanced_Manufacturing_A_New_Narrative_2023.pdf

World Economic Forum. (2023). State of the Connected World 2023 Edition. https://www3.weforum.org/docs/WEF_State_of_the_Connected_World_2023_Edition.pdf

Xu, L. D., Xu, E. L., & Li, L. (2021). Industry 4.0: Internet of Things, big data, and cybersecurity in manufacturing. Journal of Industrial Information Integration, 23, 100217. https://doi.org/10.1016/j.jii.2021.100217

Yungán, J. Narváez, C. (2022). Evaluación del Protocolo 802.1Q en la Implementación de VLANS en Entornos Wireless Mediante la Aplicación de Software Libre.
DOI: http://dx.doi.org/10.23857/dc.v8i3

Zeydan, E., Arslan, S. S., Turk, Y., Hewa, T., & Liyanage, M. (2025). The role of mobile communications for industrial automation: architecture, applications and challenges. IEEE Open Journal of the Communications Society.

Zuñiga, F. (2023). El big data y su implicación en el marketing.

https://www.seeci.net/revista/index.php/seeci/article/view/832/2275