El impacto de la automatización electrónica en la transformación de los procesos productivos industriales: una revisión teórica entre los años 2020-2025

Juan Sebastián García Contreras

Asesor

Alexander Flórez Martínez

Universidad Nacional Abierta y a Distancia-UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería-ECBTI

Tecnología en Automatización Electrónica Industrial

2025

Agradecimientos

A Dios, fuente de toda sabiduría y fortaleza, por acompañarme en cada paso de este camino académico, brindándome la claridad para superar los desafíos y la perseverancia para alcanzar mis metas.

A mi familia, por su apoyo incondicional, comprensión y aliento constante. Su amor y confianza fueron el pilar que me sostuvo en los momentos de mayor exigencia.

Al asesor Alexander Flórez Martínez, por su compromiso, guía y valiosos aportes durante el desarrollo de esta monografía. Su orientación profesional y dedicación han sido muy importantes para el cumplimiento de los objetivos propuestos.

A la Universidad Nacional Abierta y a Distancia -UNAD, por brindarme las herramientas académicas, el respaldo institucional y el espacio para desarrollar esta investigación titulada “El impacto de la automatización electrónica en la transformación de los procesos productivos industriales: una revisión teórica entre los años 2020-2025”, que constituye un paso importante en mi formación profesional.

Dedicatoria

Dedico este trabajo, en primer lugar, a Dios, por ser mi guía y darme la oportunidad de crecer personal y profesionalmente.

A mi familia, por su apoyo, paciencia y motivación, que han sido el motor para continuar y culminar este proceso con dedicación y esfuerzo.

Resumen

En los últimos años, la automatización electrónica ha sido muy importante en la transformación de los procesos productivos industriales, especialmente en el contexto de la Industria 4.0. Esta monografía presenta una revisión teórica de estudios realizados entre 2020 y 2025, con el objetivo de analizar cómo esta tecnología ha influido en la forma en que las empresas producen bienes, gestionan sus recursos y enfrentan los desafíos del mercado actual.

A través del uso de sensores, software, controladores y otros dispositivos electrónicos, la automatización ha permitido mejorar la eficiencia, reducir errores, optimizar tiempos de producción y facilitar la toma de decisiones. Sin embargo, también existen barreras que dificultan su implementación, como la falta de conocimiento técnico, la resistencia al cambio y los altos costos de inversión inicial. Por ello, este estudio busca identificar las tecnologías más utilizadas en este período, los beneficios obtenidos, los obstáculos encontrados, y las tendencias que se proyectan hacia el futuro.

Palabras clave: Automatización electrónica, industria 4.0, procesos productivos, innovación tecnológica, transformación industrial, tecnologías digitales, competitividad, eficiencia industrial.

Abstract

In recent years, electronic automation has been very important in the transformation of industrial production processes, especially in the context of Industry 4.0. This monograph presents a theoretical review of studies conducted between 2020 and 2025, with the aim of analyzing how this technology has influenced the way companies produce goods, manage their resources and face the challenges of today's market.

Through the use of sensors, software, controllers and other electronic devices, automation has made it possible to improve efficiency, reduce errors, optimize production times and facilitate decision-making. However, there are also barriers that hinder its implementation, such as lack of technical knowledge, resistance to change and high initial investment costs. Therefore, this study seeks to identify the most used technologies in this period, the benefits obtained, the obstacles encountered, and the trends that are projected for the future.

***Keywords**:* Electronic automation, industry 4.0, production processes, technological innovation, industrial transformation, digital technologies, competitiveness, industrial efficiency.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Introducción

En los últimos años, la industria ha experimentado una gran transformación impulsada por la incorporación de nuevas tecnologías, este fenómeno es conocido como la cuarta revolución industrial o industria 4.0, la cual ha traído consigo una ola de cambios en la forma en que se producen bienes y se gestionan los procesos dentro de las fábricas y una de las principales protagonistas de esta transformación es la automatización electrónica; la cual es una tecnología que combina sistemas electrónicos, sensores, actuadores, controladores y software para realizar tareas que antes dependían completamente de la intervención humana.

La automatización electrónica no es un concepto nuevo, gracias a su aplicación, muchas empresas han logrado optimizar sus procesos productivos, reduciendo tiempos de operación, minimizando errores, mejorando la calidad de los productos y, sobre todo, incrementando su competitividad en un mercado cada vez más exigente y globalizado. Además, esta tecnología ha facilitado la recopilación y análisis de grandes cantidades de datos en tiempo real, lo cual permite tomar decisiones más ágiles y acertadas en cada etapa del proceso industrial.

En este sentido, la automatización electrónica se ha convertido en una herramienta muy importante para afrontar desafíos modernos como la escasez de mano de obra calificada, la necesidad de personalizar productos a gran escala, y reducir el impacto ambiental de las actividades industriales. Tecnologías como la inteligencia artificial, el Internet de las Cosas (IoT), los sistemas de control distribuido (DCS), los controladores lógicos programables (PLC), y la robótica colaborativa, han sido integradas en diferentes sectores industriales para mejorar la eficiencia y la sostenibilidad de los procesos. Sin embargo, este avance tecnológico también ha traído consigo ciertas dificultades y preguntas sobre su impacto social, laboral y ético, por lo tanto, entender cómo ha evolucionado la automatización electrónica en los últimos cinco años,

resulta importante para que las empresas tomen decisiones informadas al momento de transformar sus procesos productivos.

Por ejemplo, en el ámbito laboral, la automatización puede reemplazar ciertas tareas repetitivas o manuales, lo que ha generado preocupación por la pérdida de empleos en algunos sectores. Sin embargo, también ha creado nuevas oportunidades laborales para personas con habilidades técnicas en programación, mantenimiento y análisis de datos y por ende, el reto está en preparar a los trabajadores para adaptarse a estos cambios.

Desde el punto de vista social, la automatización puede mejorar la calidad de vida al permitir una producción más eficiente, segura y limpia. Pero también puede profundizar las brechas entre quienes tienen acceso a la tecnología y quienes no, por eso es importante que el desarrollo tecnológico sea inclusivo y pensado para beneficiar a todos.

En cuanto al impacto ético, surgen preguntas sobre la toma de decisiones automatizadas sin intervención humana, especialmente cuando están en juego derechos fundamentales como la privacidad o el acceso a servicios. En Colombia, por ejemplo, hay leyes que buscan garantizar que estas tecnologías se usen de forma responsable. La Ley 1581 de 2012 y su reglamentación; el Decreto 1377 de 2013, protegen los datos personales. Toda solución automatizada que utilice datos, como el reconocimiento facial o la inteligencia artificial en salud o finanzas, debe cumplir con esta ley, asegurando que las personas tengan control sobre su información.

La Ley 2293 de 2023, conocida como la Ley de Inteligencia Artificial, establece reglas para el uso ético de la inteligencia artificial en el país. Esta ley promueve que la IA se desarrolle respetando los derechos humanos y evitando cualquier tipo de discriminación o uso indebido. Además, el CONPES 3975 de 2019, que es la Política Nacional de Explotación de Datos,

promueve el uso inteligente de los datos (Big Data), con respeto a los principios de ética, seguridad y privacidad.

En lo técnico, también existen normas como la NTC 5801 de ICONTEC, que establece lineamientos para el diseño e implementación de sistemas de control y automatización industrial en Colombia, asegurando que los procesos se desarrollen de forma segura, eficiente y confiable.

Esta monografía tiene como objetivo principal analizar el impacto de la automatización electrónica en la transformación de los procesos productivos industriales, a partir de una revisión teórica de estudios realizados entre los años 2020 y 2025. Al comprender el papel de la automatización electrónica en este proceso de transformación, tanto profesionales como estudiantes del área de tecnología y automatización podrán fortalecer su conocimiento y contribuir a la innovación industrial.

Planteamiento del Problema

En el contexto de la “cuarta revolución industrial”, la automatización electrónica se ha convertido en un componente muy importante para mejorar la productividad, la eficiencia y la calidad de los procesos industriales (Zaga, 2023). Esta tecnología, que integra sensores, sistemas de control, actuadores, software y dispositivos inteligentes, ha demostrado su capacidad para transformar la manera en que se diseñan, ejecutan y supervisan las actividades productivas (Baeza, 2022). Sin embargo, a pesar del evidente potencial que ofrece, su implementación efectiva sigue siendo un desafío considerable para muchas industrias, especialmente en países en desarrollo como Colombia.

Uno de los principales problemas es la falta de conocimiento por parte de los empresarios, técnicos y trabajadores sobre qué implica realmente la automatización electrónica, cuáles son sus beneficios, cuáles son los costos involucrados y cómo se lleva a cabo el proceso de integración dentro de un sistema de producción existente (Martínez A. S., 2023). Esta falta de comprensión puede generar temores, resistencia al cambio y decisiones equivocadas, que terminan limitando la adopción de estas tecnologías y, por ende, reduciendo las oportunidades de modernización y crecimiento.

Además, muchas pequeñas y medianas empresas (pymes) industriales se enfrentan a barreras económicas, técnicas y formativas que dificultan la inversión en soluciones de automatización electrónica (Romero & Pulido, 2024). Algunas no cuentan con personal capacitado en el manejo de estos sistemas, otras carecen de acceso a tecnologías modernas o no tienen planes estratégicos de transformación digital y esto crea una brecha entre aquellas industrias que han logrado avanzar hacia modelos de producción más automatizados y aquellas

que aún dependen de procesos manuales o semiautomatizados, generando desigualdad en términos de productividad y competitividad.

Por otro lado, el rápido ritmo de innovación tecnológica también representa una dificultad. Pues, las soluciones de automatización evolucionan constantemente, por lo que resulta difícil para muchas empresas mantenerse actualizadas y tomar decisiones informadas sobre qué tecnologías adoptar, cómo hacerlo de manera eficiente y sostenible, y cómo asegurar la compatibilidad con los sistemas ya existentes, lo cual puede llevar a implementaciones deficientes, altos costos de mantenimiento, o incluso al abandono de proyectos por falta de resultados esperados.

Bajo esta premisa, se hace necesario realizar una revisión teórica y crítica del impacto que ha tenido la automatización electrónica en la transformación de los procesos productivos industriales en los últimos cinco años (2020-2025). Esta revisión permitirá entender cómo se ha aplicado esta tecnología en diferentes contextos, qué beneficios ha reportado, qué obstáculos han surgido, y qué aprendizajes se pueden extraer para mejorar su implementación futura. Pues, comprender esto es importante para identificar oportunidades de mejora, proponer soluciones prácticas y generar recomendaciones que faciliten la adopción efectiva de la automatización en el sector industrial

Así, el problema central que aborda esta monografía se puede formular de la siguiente manera: ¿Cómo ha impactado la automatización electrónica la transformación de los procesos productivos industriales entre los años 2020 y 2025, y cuáles son los principales factores que limitan su integración efectiva en las industrias? Responder a esta pregunta es necesario para guiar la innovación tecnológica en la industria, fortalecer la formación técnica, y contribuir a la construcción de sistemas productivos más eficientes.

Justificación

En un mundo cada vez más interconectado y competitivo, la necesidad de transformar los procesos industriales se ha vuelto una prioridad para las empresas que buscan mantenerse vigentes y eficientes. En este contexto, la automatización electrónica es una herramienta de gran ayuda, no solo para mejorar la productividad y reducir costos, sino también para responder de manera ágil a las demandas del mercado, aumentar la calidad de los productos y garantizar operaciones más sostenibles desde el punto de vista económico, social y ambiental (Muriel, 2023).

La automatización electrónica permite automatizar tareas repetitivas, supervisar procesos en tiempo real, reducir errores humanos, controlar parámetros críticos de producción y optimizar el uso de recursos como la energía y la materia prima y todo esto contribuye a un modelo de producción más inteligente, adaptable y eficiente (Enderica & Molina, 2024). Sin embargo, no todas las empresas logran aprovechar plenamente estas ventajas ya que muchas organizaciones, especialmente en sectores tradicionales o en regiones con menor desarrollo tecnológico, tienen dificultades relacionadas con el desconocimiento, la falta de capacitación del talento humano, el temor al cambio, y los costos iniciales de inversión (Pacheco et al, 2025), y esto limita la posibilidad de avanzar hacia una industria moderna e interconectada, generando brechas tecnológicas que afectan la competitividad.

En este sentido, comprender el impacto real de la automatización electrónica en los procesos productivos industriales no es solo un ejercicio académico, sino una necesidad práctica y estratégica. Este estudio busca analizar, desde una perspectiva teórica cómo ha influido esta tecnología en la transformación de la industria, qué beneficios se han alcanzado, qué retos persisten, y qué recomendaciones pueden derivarse para una implementación más eficaz y

sostenible, se pretende construir una base de conocimiento que oriente tanto a empresas como a instituciones educativas y organismos públicos.

Desde el punto de vista académico, esta monografía representa un aporte al campo de la automatización electrónica industrial, ya que ofrece una recopilación y análisis de información relevante y reciente que puede ser utilizada como base para futuras investigaciones, proyectos de innovación o desarrollo curricular. Para los estudiantes y profesionales de la Tecnología en Automatización Electrónica Industrial, este trabajo les permitirá comprender mejor las tendencias actuales del sector, identificar buenas prácticas, y fortalecer su perfil técnico para responder a las exigencias del mercado laboral.

Por otra parte, esta monografía tiene un valor social y económico, ya que promueve la reflexión sobre cómo el uso estratégico de la tecnología puede contribuir al desarrollo industrial del país, mejorar las condiciones laborales mediante la automatización de tareas peligrosas o repetitivas, y generar nuevas oportunidades de empleo en áreas como el mantenimiento de sistemas automatizados, la programación de controladores, el diseño de procesos inteligentes, entre otros.

Así, esta monografía no solo busca generar conocimiento, sino también aportar soluciones prácticas y aplicables que faciliten el tránsito hacia una industria más automatizada e innovadora.

Objetivos

Objetivo General

Analizar el impacto de la automatización electrónica en la transformación de los procesos productivos industriales mediante una revisión teórica de estudios realizados entre 2020 y 2025.

Objetivos Específicos

Identificar las principales tecnologías de automatización electrónica implementadas en la industria durante el período 2020-2025.

Evaluar los beneficios y desafíos asociados con la integración de estas tecnologías en los procesos productivos.

Determinar las tendencias emergentes y futuras en la automatización electrónica industrial.

Estado del Arte

Principales Tecnologías de Automatización Electrónica Implementadas en la Industria Durante el Período 2020-2025

Incidencia de la Pandemia Covid-19 en las Tecnologías de Automatización Electrónica

El período entre los años 2020 y 2025, experimentó una transformación en los procesos industriales, impulsada en gran parte por la pandemia de COVID-19. La crisis sanitaria, declarada oficialmente por la Organización Mundial de la Salud en marzo de 2020, exigió una reducción en la presencia física en fábricas y oficinas, incitando una rápida adopción de automatización electrónica (OMS, 2020). Sectores que dependían de mano de obra presencial tuvieron que reinventarse con asistencia tecnológica. De hecho, el Foro Económico Mundial (Russo, 2020), indicó que un 43 % de las empresas planeaba reducir personal mediante la implementación de herramientas como la inteligencia artificial y la robótica. Si bien la adopción tuvo muchas desigualdades, pues, hubo rápidas respuestas en grandes empresas, mientras que las pymes enfrentaron muchos obstáculos (Ripani & Soler, 2021), nadie duda que este fue un punto de inflexión en cómo se entiende la eficiencia, resiliencia y competitividad en la industria moderna.

Uno de los sectores más impactados ha sido el ámbito educativo. Debido a la pandemia por COVID-19, las instituciones educativas se vieron forzadas a migrar a modelos de enseñanza virtual y esta situación llevó a una rápida adopción de plataformas digitales automatizadas, como Google Classroom, Moodle y Microsoft Teams. Estas herramientas integraron funciones automáticas que permiten hacer un seguimiento constante del aprendizaje, evaluar el progreso del estudiante, asignar tareas y generar informes sin necesidad de intervención manual continua (CEPAL, 2020). Esta transformación ha permitido una educación más accesible, organizada y

personalizada, como lo reconoce la UNESCO, al decir que las tecnologías digitales ayudaron a garantizar la continuidad educativa a nivel mundial durante los confinamientos sanitarios (UNESCO, 2024).

En el sector salud, la automatización también tuvo mucha importancia ya que se implementaron soluciones tecnológicas como chatbots para orientar a los pacientes en línea (Torres et al, 2025), ayudando a reducir la carga del personal médico y brindar información inmediata y se emplearon algoritmos para rastrear contactos de personas contagiadas, y se utilizaron robots para desinfectar hospitales y entregar medicamentos, minimizando así el riesgo de contagio. Según la Organización Mundial de la Salud (OMS, 2021), estas tecnologías automatizadas mejoraron notablemente la respuesta sanitaria en varios países, especialmente en aquellos con sistemas de salud colapsados o con poca disponibilidad de personal médico.

Por otro lado, en el comercio electrónico, empresas como Amazon y Alibaba aprovecharon la inteligencia artificial y la robótica para enfrentar la creciente demanda generada por las restricciones de movilidad (Porcelli, 2020). Estas compañías optimizaron sus cadenas de suministro mediante sistemas automáticos que clasifican productos, preparan envíos y gestionan inventarios sin intervención humana directa, esta estrategia permitió mantener la eficiencia logística y cumplir con los tiempos de entrega, incluso en los momentos más críticos de la crisis sanitaria.

Así pues, la pandemia actuó como un acelerador de la automatización a nivel global, pues, empresas y gobiernos que estaban en proceso de digitalización se vieron obligados a acelerar este paso, mientras que otros que no habían iniciado dicho proceso se vieron forzados a adaptarse rápidamente y marcó un punto de inflexión en cómo se concibe el trabajo y la producción en el siglo XXI.

Ahora bien, las siguientes, son las tecnologías que lideraron esta transformación:

IIoT con modelo Edge-to-Cloud: El Internet Industrial de las Cosas (IIoT) ha sido una tecnología muy importante para conectar equipos y sensores mediante internet. El llamado "edge-to-cloud", parte del procesamiento de datos ocurre cerca de los dispositivos (borde o edge), y el resto en la nube. Eso permite un control remoto más eficiente, mejor visibilidad en tiempo real de la producción y toma de decisiones inmediatas. Muchas áreas como manufactura, logística o transporte se beneficiaron al poder monitorear cada paso del proceso (Rozo-García, 2020).Sin embargo, trabajar con tantos datos también aumenta los riesgos de ciberataques y exige una conectividad confiable.

5G y el IoT masivo: La llegada del 5G fue un salto tecnológico muy grande, pues, gracias a su alta velocidad, latencia ultra baja y capacidad de conectar millones de dispositivos, se convirtió en la base para un IoT masivo, el cual es muy importante para fábricas inteligentes, salud digital o transporte automatizado (Campos & Cavada, 2021). Permitió desde cirugías a distancia (Flores, 2020), hasta vehículos autónomos. Pero no todo fue bueno, pues, desplegar 5G requiere una gran inversión, dificultades en la seguridad, genera enormes volúmenes de datos que hay que procesar eficazmente y depende de infraestructura estable.

Ethernet determinista con TSN (Time-Sensitive Networking): La combinación de 5G con Ethernet determinista (TSN) fue otra innovación, ya que TSN ofrece transmisión de datos de forma sincronizada y confiable, muy importante en procesos industriales donde cualquier demora es una dificultad. Por ello, mediante network slicing, se pueden priorizar los datos más urgentes, integrando redes móviles y cableadas de forma eficiente (Sánchez J. C., 2021). Aun así, los estándares aún no están completamente definidos, y su implementación requiere ajustes técnicos, los cuales no solo son complejos, sino que también son costosos.

Interoperabilidad mediante OPC UA: Una cuestión que es mucha importancia en la automatización es cómo hacer que equipos de distintos fabricantes se comuniquen sin problemas. Aquí es donde entró OPC UA, un estándar que permite esta interoperabilidad, incluso en entornos con cortafuegos o firewall, es decir, ese sistema de seguridad que actúa como una barrera de control entre una red interna; por ejemplo, la red de una empresa y el exterior como internet. Su función principal es permitir o bloquear el tráfico de datos según un conjunto de reglas definidas, con el objetivo de proteger los sistemas contra accesos no autorizados, ataques o fugas de información (Bandera & Contreras, 2020)**,** y lo hace con seguridad mediante cifrado y firmas digitales (Jácome et al, 2022). Esto facilita la integración en plantas heterogéneas, aunque adaptar sistemas más antiguos y capacitar al personal requieren de tiempo y recursos.

Gemelos Digitales (Digital Twin): El concepto de Gemelo Digital implica crear una réplica virtual de un proceso o sistema real (Chicaiza et al, 2024). Esto permite simular situaciones, prever fallas, optimizar producción e incluso ahorrar costos antes de realizar cambios físicos. Esta tecnología permitió mantenimiento preventivo más efectivo y toma de decisiones más rápida (Bustamante-Limones et al, 2024). La desventaja más importante que tiene es su alto costo inicial, pues, se necesita infraestructura tecnológica avanzada y personal capacitado para aprovechar todo su potencial.

Robots colaborativos o Cobots: A diferencia de los robots tradicionales, los robots colaborativos, o cobots, están diseñados para trabajar junto a personas, sin necesidad de barreras físicas y con sensores que los detienen al detectar contacto humano (Guamán et al, 2022). Son fáciles de reprogramar, ofrecen flexibilidad y alivian tareas repetitivas o pesadas, lo que mejora la productividad (Gandino & Mamani, 2020).El lado negativo, es que no alcanzan la fuerza ni

velocidad de robots industriales y siguen siendo costosos, lo cual limita el hecho de que puedan implementarse en empresas más pequeñas.

Visión artificial con Deep Learning: La visión artificial apoyada en deep learning se ha consolidado como una herramienta muy importante para el control de calidad (Pico & Marroquín, 2023). Permite detectar defectos superficiales en producción de forma automática, reduciendo errores humanos y pérdidas económicas. Es ampliamente usada en sectores como la automotriz, farmacéutica, o alimenticia y de ingeniería biomédica (Sarmiento-Ramos, 2020). Pero esto depende de contar con infraestructura que sea robusta y grandes volúmenes de datos para entrenar los modelos, lo cual implica una inversión muy grande.

Mantenimiento predictivo con Machine Learning: Otra tecnología importante es el mantenimiento predictivo, el cual utiliza sensores y algoritmos o machine learning, para prever fallas antes de que ocurran. Esto evita paradas imprevistas, es decir, la suspensión o interrupción de la operación de un proceso, sistema o equipo. Es decir, cuando una máquina, una línea de producción o un sistema industrial deja de funcionar, ya sea de forma programada, por ejemplo, para mantenimiento o imprevista, en este caso, por fallas, averías o emergencias (Tapia et al, 2024). También, prolonga la vida útil de los equipos y permite planificar intervenciones en el momento justo, reduciendo costos (Salgado et al, 2024).

En instalaciones eléctricas como transformadores, los algoritmos pueden estimar el tiempo real de vida útil restante (Q et al, 2022). La desventaja, es que requiere una gran inversión en sensores, infraestructura y conocimientos específicos para manipular los datos eficientemente.

Ciberseguridad industrial mediante IA: A medida que la industria se digitaliza, también aumentan los riesgos de ataques cibernéticos. Las soluciones basadas en inteligencia artificial permiten identificar dispositivos conectados, analizar cómo se comunican, detectar patrones

anormales y responder rápido ante amenazas (Cortés-Llanganate & Quevedo-Sacoto, 2024).Por ello, son muy importantes en sectores como la energía, la salud o el transporte. Sin embargo, implementar estas soluciones es costoso, requiere confianza en proveedores externos y personal especializado, y puede generar alertas falsas, es decir, recibir una notificación que indica la presencia de una amenaza o ataque, cuando en realidad no existe tal riesgo. Esto ocurre porque los sistemas basados en inteligencia artificial y algoritmos de detección, al ser muy sensibles, pueden interpretar como sospechoso un comportamiento que en realidad es normal.

Por ejemplo, una planta de energía que utiliza un sistema de ciberseguridad con IA y el sistema detecta que un técnico está accediendo remotamente a un controlador industrial para hacer mantenimiento, como esa acción no es común en los patrones habituales, el sistema la clasifica como un posible intento de intrusión externa y genera una alerta cuando en realidad, no se trata de un ataque, sino de una operación la cual es legítima. Entonces, pueden saturar al personal de seguridad, ya que deben revisar muchos avisos que no representan un peligro real, generan desconfianza en el sistema de protección, pues los trabajadores pueden dejar de tomar en serio las alarmas y consumen tiempo y recursos que deberían enfocarse en amenazas verdaderas.

Así las cosas, entre 2020 y 2025, la industria adoptó con fuerza muchas de estas tecnologías que respondieron a la urgencia de la pandemia, que aceleró cambios previstos para años, como es posible ver en sectores que implementaron chatbots, robótica o plataformas educativas automatizadas (Hernandez & Cruz, 2022) y aunque la adopción tuvo desigualdades, al favorecer grandes empresas y países con más infraestructura, la continuidad de procesos automatizados tras la pandemia demuestra que este impacto fue no solo por ese espacio de tiempo, sino que ha sido un cambio duradero que día a día sigue evolucionando (Cathles et al, 2022). Pues, la automatización electrónica en este período no solo significó mayor eficiencia y

control, sino también superar y abordar desafíos sobre cómo equilibrar aspectos como la inversión, capacitación, seguridad y sostenibilidad en esta nueva etapa industrial.

Tabla 1

Principales Tecnologías de Automatización y Digitalización Industrial (2020-2025): Características, Ventajas, Desventajas, Sectores de Aplicación

Tecnología	Características	Ventajas	Desventajas	Sectores donde más se usa	Artículo
IIoT con Edge-to-Cloud (sensores conectados más cómputo en el borde y en la nube para automatizar monitoreo y control)	Es una conexión de dispositivos físicos a través de internet; recopila, transmite y analiza datos en tiempo real.	Mejora la eficiencia operativa, facilita la trazabilidad y el monitoreo remoto	Riesgos de ciberseguridad y alta dependencia de la conectividad.	Manufactura, transporte, logística, salud.	Revisión de las tecnologías presentes en la industria 4.0 (Rozo-García, 2020).
Redes 5G privadas para automatización (con URLLC para control inalámbrico fiable) 5G	Quinta generación de redes móviles. Ofrece alta velocidad, baja latencia y capacidad de conectar un número muy grande de dispositivos al	Velocidades muy superiores a 4G. Comunicación casi en tiempo real. Soporte para ciudades inteligentes. Base para la transformación	Altos costos de infraestructura. Falta de hoja de ruta clara en algunos países. Necesidad de armonizar espectros de frecuencia.	Telecomunicaciones, transporte inteligente, manufactura avanzada, salud (cirugías remotas), energía, ciudades inteligentes.	Análisis para la implementación de la tecnología 5g basados en el modelo GSMA y su interacción con

Tecnología	Características	Ventajas	Desventajas	Sectores donde más se usa	Artículo
Internet de las Cosas (IoT) con 5G	mismo tiempo. Su arquitectura es flexible y escalable, lo que permite adaptarse a distintos escenarios (eMBB, mMTC y URLLC). Red de objetos y sensores conectados que transmiten datos en tiempo real. Con 5G se apoya en tecnologías NB-IoT y LTE-M, que permiten conectar millones de dispositivos con	digital e Industria 4.0. Mejor cobertura incluso en interiores. Capacidad de gestionar dispositivos masivos. Ahorro energético en sensores. Facilita automatización y control remoto.	Riesgos de seguridad en redes abiertas. Generación de enormes volúmenes de datos que requieren sistemas avanzados de análisis. Dependencia de infraestructura estable. Costos iniciales de implementación.	Agricultura inteligente, logística y transporte, salud digital, ciudades inteligentes, energía, hogares y fábricas conectadas.	el internet de las cosas en Ecuador (Campos & Cavada, 2021).

Tecnología	Características	Ventajas	Desventajas	Sectores donde más se usa	Artículo
	bajo consumo de energía.				
Ethernet determinista: TSN (programación de tráfico, sincronización tiempo real)	Combina redes móviles 5G con redes cableadas TSN. TSN garantiza bajo retardo y alta fiabilidad en la transmisión. 5G aporta movilidad y flexibilidad. Uso de network slicing para dividir la red en segmentos (slices) según necesidades de cada servicio.	Conecta dispositivos industriales con gran rapidez y seguridad. Permite comunicaciones en tiempo real. Soporta múltiples servicios al mismo tiempo gracias al slicing. Mejora la eficiencia en fábricas inteligentes.	Altos costos de implementación. El estándar 3GPP aún no define cómo debe hacerse la integración práctica. Complejidad en la sincronización de recursos entre 5G y TSN. Limitaciones en los simuladores actuales (ej. no priorizan flujos críticos).	Industria 4.0 (automatización, robótica, fábricas inteligentes). Transporte industrial de datos críticos. Energía y sistemas eléctricos. Comunicaciones industriales con alta fiabilidad.	Integración de 5G y TSN en redes privadas industriales (Sánchez J. C., 2021).

Tecnología	Características	Ventajas	Desventajas	Sectores donde más se usa	Artículo
Interoperabilidad con OPC UA (modelado de información)	Permite la comunicación entre diferentes controladores industriales, incluso de distintos fabricantes. Funciona con sistemas abiertos. Integra seguridad mediante cifrado y firma digital. Facilita la conexión con protocolos diversos. Puede trabajar con sistemas SCADA y cortafuegos.	Hace más fácil la interconexión de equipos de distintas marcas. Reduce la complejidad en la configuración. Ofrece seguridad con cifrado y firma digital. Permite validar datos de manera inmediata entre el sistema SCADA y los controladores. Es tolerante a cortafuegos y entornos con restricciones.	Requiere un nivel inicial de adaptación en empresas que usan sistemas tradicionales. Puede demandar mayor capacitación técnica para su implementación. En algunos casos, depende de la infraestructura tecnológica existente.	Automatización industrial. Energía y servicios públicos. Plantas de manufactura. Procesos donde se integran sistemas de diferentes fabricantes. Sistemas de control y supervisión (SCADA).	Variantes de la Tecnología OPC-UA y su utilización en la interconexión de Controladores Industriales con diferentes protocolos de comunicación (Jácome et al, 2022).

Tecnología	Características	Ventajas	Desventajas	Sectores donde más se usa	Artículo
Gemelo Digital (Digital Twin) para supervisión y optimización	Son representaciones virtuales de un proceso, producto o sistema real. Se apoyan en la simulación, el análisis de datos y el uso de tecnologías digitales. Permiten observar y predecir el comportamiento de un sistema antes de aplicarlo en la realidad.	Mejoran la eficiencia operativa. Optimización de procesos de producción. Facilitan el mantenimiento preventivo. Ayudan en la gestión de inventarios. Aumentan la capacidad de adaptación a cambios del mercado. Reducen costos. Apoyan la toma de decisiones más rápidas y acertadas. Impulsan la mejora	Requieren alta inversión inicial en infraestructura tecnológica. Necesitan personal capacitado. Es complejo de implementar. Pueden generar dependencia tecnológica.	Industria de manufactura (optimización de líneas de producción). Gestión de inventarios. Procesos industriales complejos (automatización, eficiencia energética, mantenimiento). Industria 5.0, donde se busca la integración de la tecnología con el trabajo humano.	Evaluación del uso de gemelos digitales en los sistemas de producción (Bustamante-Limones y otros, 2024).

Tecnología	Características	Ventajas	Desventajas	Sectores donde más se usa	Artículo
		continua y la integración de nuevas tecnologías.			
Robots colaborativos (cobots) y HRC	Son brazos robóticos diseñados para trabajar junto a las personas, no para reemplazarlas. Compactos y fáciles de mover en la planta. Incorporan sensores que los hacen seguros: se detienen si detectan un obstáculo o contacto humano. Se pueden reprogramar de	Mayor flexibilidad en la producción. No requieren grandes barreras de seguridad. Aumentan la productividad al trabajar 24/7. Reducen el esfuerzo físico humano en tareas pesadas o repetitivas. Mejoran la calidad del producto. Se adaptan a la producción personalizada.	Alto costo inicial de inversión. Requiere capacitación para su programación y uso. No siempre reemplazan la fuerza o velocidad de un robot industrial tradicional. En algunos países, hay desafíos legales o regulatorios en temas de seguridad laboral.	Líneas de manufactura y ensamble. Fábricas inteligentes (Industria 4.0). Pymes manufactureras que necesitan flexibilidad. Sectores que buscan pasar de producción masiva a producción personalizada. Industrias que integran	Marco de referencia para la incorporación de Cobots en líneas de manufactura (Gandino & Mamani, 2020).

Tecnología	Características	Ventajas	Desventajas	Sectores donde más se usa	Artículo
	forma sencilla para distintas tareas.	Fácil reconfiguración según las necesidades.		digitalización e IoT en sus procesos.	
Visión artificial con Deep Learning para inspección	Usa inteligencia artificial para reconocer defectos o fallas en la superficie de productos durante la producción. Se apoya en técnicas complementarias como Machine Learning y Transfer Learning. Trabaja con visión artificial (cámaras y sensores) y	Alta precisión en la detección de defectos. Reduce costos al evitar que productos defectuosos lleguen al cliente. Automatiza el control de calidad, disminuyendo la dependencia de la inspección humana. Evita errores por cansancio o subjetividad de los trabajadores.	Requiere un alto volumen de datos para entrenar los sistemas. Necesita infraestructura tecnológica costosa (sensores, cámaras, sistemas de procesamiento). Su implementación depende del presupuesto de la empresa. No existe una sola técnica que sea la	Manufactura en general (para detectar fallas en productos). Industria farmacéutica, donde la calidad es crítica y los errores pueden tener consecuencias graves. Minería (ejemplo: análisis con rayos X para control de calidad). Sectores con	Aplicación de Deep Learning para la identificación de defectos superficiales utilizados en control de calidad de manufactura y producción industrial: una revisión de la literatura (Pico & Marroquín, 2023).

Tecnología	Características	Ventajas	Desventajas	Sectores donde más se usa	Artículo
	grandes volúmenes de datos (Big Data). Aprende de diferentes ejemplos y contextos, lo que le permite adaptarse a distintos procesos industriales.	Permite identificar las causas de los defectos (equipos dañados, desgaste, mala operación, etc.). Mejora la eficiencia y la capacidad de reacción en la planta.	mejor en todos los casos, se debe probar y combinar varias	producción masiva y exigencia alta (automotriz, electrónica, alimentos, etc.).	
Mantenimiento predictivo con Machine Learning (PdM-ML)	Utiliza datos de sensores en tiempo real para anticipar fallas en máquinas o equipos. Aplica algoritmos de aprendizaje automático (redes neuronales, máquinas de	Reduce costos al evitar reparaciones imprevistas y paradas largas. Aumenta la confiabilidad de los equipos. Optimiza el tiempo de mantenimiento (se hace cuando	Requiere gran cantidad de datos históricos y en tiempo real, lo cual no siempre está disponible. Necesita inversión en sensores, infraestructura tecnológica y	Energía eólica (turbinas y sistemas eléctricos). Ferrocarriles (mantenimiento de vías y trenes). Manufactura (máquinas de producción). Infraestructuras	Mantenimiento predictivo basado en machine learning: una revisión sistemática de la literatura y perspectivas en la industria 4.0

Tecnología	Características	Ventajas	Desventajas	Sectores donde más se usa	Artículo
	soporte vectorial, métodos de conjuntos). Permite estimar la vida útil restante de un activo y planificar intervenciones antes de que ocurra una avería. Forma parte importante de la Industria 4.0 porque conecta datos, inteligencia artificial y sistemas productivos complejos. Se enfoca en rodamientos, piezas	realmente se necesita, no antes ni después). Prolonga la vida útil de las máquinas. Mejora la sostenibilidad, al usar mejor los recursos y reducir desperdicios. Permite decisiones basadas en datos en lugar de suposiciones. Predice fallas antes de que ocurran, evitando daños mayores. Extiende la vida útil de las máquinas y	especialistas. La implementación puede ser costosa para empresas pequeñas. El desempeño depende de la calidad de los datos (datos incompletos o ruidosos reducen la precisión). Requiere datos de buena calidad obtenidos de sensores especializados. La implementación necesita conocimiento técnico en datos y	(puentes, carreteras, sistemas críticos). Industria automotriz (por los altos costos de paradas inesperadas). Fábricas de bienes de consumo (para reducir pérdidas en producción). Maquinaria rotativa en general (plantas de energía, manufactura, motores eléctricos).	predictive maintenance based on machine learning: a systematic literature review and perspectives in industry 4.0 (Tapia et al, 2024). Preprocesamiento de datos en el pronóstico de fallos de rodamientos para el mantenimiento

Tecnología	Características	Ventajas	Desventajas	Sectores donde más se usa	Artículo
	importantes en motores y máquinas rotativas. Usa sensores de vibración para detectar señales tempranas de desgaste. Aplica un método de preprocesamiento de datos que mejora la calidad de la información antes de usarla en modelos de inteligencia artificial. Emplea algoritmos como redes	rodamientos. Reduce costos de mantenimiento y paradas imprevistas. Aumenta la precisión en la detección de fallas (mejora de hasta 74.4% frente a otros métodos). Usa menos recursos computacionales que otros enfoques, lo que lo hace más eficiente.	ML, lo cual puede ser complejo. Los resultados dependen del correcto preprocesamiento de los datos. No todas las empresas cuentan con los recursos para sensores y sistemas avanzados.		predictivo (Salgado et al, 2024).

Tecnología	Características	Ventajas	Desventajas	Sectores donde más se usa	Artículo
	neuronales, máquinas de soporte vectorial, árboles de decisión, regresión lineal, bosques aleatorios, entre otros. Permite predecir fallos con más antelación y estimar la vida útil restante (RUL).				
Mantenimiento predictivo con Machine Learning aplicado a transformadores de distribución	Se enfoca en rodamientos, piezas importantes en motores y máquinas rotativas. Usa sensores de vibración para detectar señales	Predice fallas antes de que ocurran, evitando daños mayores. Extiende la vida útil de las máquinas y rodamientos. Reduce costos de	Requiere datos de buena calidad obtenidos de sensores especializados. La implementación necesita conocimiento	Industria automotriz (por los altos costos de paradas inesperadas). Fábricas de bienes de consumo (para reducir pérdidas en	Metodología para el mantenimiento predictivo de transformadores de distribución basada en

Tecnología	Características	Ventajas	Desventajas	Sectores donde más se usa	Artículo
	tempranas de desgaste. Aplica un método de preprocesamiento de datos que mejora la calidad de la información antes de usarla en modelos de inteligencia artificial. Emplea algoritmos como redes neuronales, máquinas de soporte vectorial, árboles de decisión, regresión lineal, bosques aleatorios,	mantenimiento y paradas imprevistas. Aumenta la precisión en la detección de fallas (mejora de hasta 74.4% frente a otros métodos). Usa menos recursos computacionales que otros enfoques, lo que lo hace más eficiente.	técnico en datos y ML, lo cual puede ser complejo. Los resultados dependen del correcto preprocesamiento de los datos. No todas las empresas cuentan con los recursos para sensores y sistemas avanzados.	producción). Maquinaria rotativa en general (plantas de energía, manufactura, motores eléctricos).	aprendizaje automático (Q et al, 2022).

Tecnología	Características	Ventajas	Desventajas	Sectores donde más se usa	Artículo
	entre otros. Permite predecir fallos con más antelación y estimar la vida útil restante (RUL).				
Ciberseguridad ICS/OT (IDS/NIDS industriales)	Identificación de activos y detecta qué equipos están conectados a la red industrial. Mapeo de comunicaciones y muestra cómo se conectan y hablan entre sí los dispositivos. Análisis de comportamiento, ya que la IA	Detección temprana y precisa de ataques y fallos, incluso aquellos que los antivirus o firewalls tradicionales no ven. Protección de infraestructuras críticas (energía, agua, transporte, salud, etc.) donde una falla puede causar graves daños.	Costo elevado de implementación y mantenimiento. Requiere personal especializado para configurarlo y operar los sistemas de IA. Puede haber falsos positivos (alertas de amenazas que realmente no son peligros). Algunos sistemas heredados (viejos)	Energético (plantas de generación y redes eléctricas). Petróleo y gas (refinerías, oleoductos, plataformas). Agua y saneamiento (sistemas de potabilización y distribución).	Soluciones de monitoreo de ciberseguridad en redes industriales basadas en Inteligencia Artificial. Revisión de literatura (Cortés-Llanganate & Quevedo-Sacoto, 2024).

Tecnología	Características	Ventajas	Desventajas	Sectores donde más se usa	Artículo
	aprende cómo debería comportarse la red y alerta cuando ocurre algo extraño. Gestión de vulnerabilidades pues, identifica puntos débiles en los equipos y redes. Detección de amenazas pues, reconoce patrones de ataque conocidos y también anomalías nuevas.	Automatización inteligente gracias al uso de IA, lo que permite respuestas más rápidas. Visibilidad completa de la red OT/ICS, algo que antes era muy limitado. Compatible con sistemas antiguos que no fueron diseñados con seguridad incorporada.	son difíciles de integrar totalmente. Dependencia tecnológica, pues, las empresas deben confiar en soluciones externas de fabricantes.	Manufactura (fábricas automatizadas). Transporte (ferrocarriles, aeropuertos, logística). Salud (hospitales con equipos médicos conectados).	

Nota. La tabla muestra un comparativo de tecnologías recientes de automatización industrial, destacando sus características, ventajas, desventajas, sectores de uso y referentes académicos.

Marco Teórico

Beneficios y Desafíos Asociados con la Integración de Tecnologías de Automatización Electrónica en los Procesos Productivos.

La Automatización Electrónica

La automatización electrónica se define como el uso de sistemas electrónicos, software y tecnologías digitales para controlar y operar procesos industriales con mínima o nula intervención humana (Martínez et al, 2023), esta tecnología integra componentes como sensores, actuadores, controladores programables y software especializado, permitiendo ejecutar tareas de forma eficiente, precisa y repetitiva. Con el tiempo, la automatización ha evolucionado de simples mecanismos mecánicos a sistemas inteligentes que forman parte de la Industria 4.0, transformando la manera de producir y optimizar procesos en sectores industriales.

Ventajas de la Automatización Electrónica

Mayor Eficiencia en la Producción: Una de las principales ventajas de automatizar es que se puede hacer más en menos tiempo y esto se debe a que las máquinas no necesitan pausas para descansar, comer o dormir. Además, pueden trabajar con una velocidad constante y repetitiva sin perder precisión. Por ejemplo, en una línea de ensamblaje de teléfonos celulares, un brazo robótico puede colocar componentes electrónicos con una exactitud milimétrica en cuestión de segundos, tarea que a una persona le llevaría más tiempo y sería más propensa a errores por cansancio.

Reducción de Errores Humanos: Cuando las tareas dependen exclusivamente de las personas, pueden presentarse equivocaciones debido a múltiples factores como el estrés, el agotamiento o la distracción. En cambio, los sistemas automatizados están programados para ejecutar instrucciones específicas de forma exacta cada vez y esto se traduce en menos productos

defectuosos. Por ejemplo, en una fábrica de medicamentos, donde una máquina dosificadora automatizada puede asegurar que cada cápsula contenga exactamente la misma cantidad de sustancia activa, evitando así posibles fallos que afecten la salud del consumidor.

Reducción de Costos Operativos a Largo Plazo: Aunque al principio pueda parecer costoso implementar tecnología automatizada, con el tiempo esa inversión se recupera porque disminuye la necesidad de contratar mucha mano de obra para tareas básicas, se reducen las pérdidas por errores y se aprovechan mejor los materiales. Por ejemplo, en una planta de embotellado de agua, un sistema automatizado puede llenar, tapar y etiquetar botellas sin intervención humana, lo que evita desperdicio de envases, mejora el tiempo de entrega y reduce la cantidad de operarios requeridos.

Adaptabilidad a los Cambios y Crecimiento del Negocio: Según el libro "***La Industria 4.0 en la sociedad digital*** de Antoni Garrell y Llorenc Guillera (Antoni Garrell, 2019)", otra gran ventaja es que los sistemas automatizados pueden ajustarse a nuevas condiciones de forma más sencilla que los sistemas manuales. Si se necesita producir más unidades por una alta demanda o cambiar el diseño de un producto, solo es necesario reprogramar el sistema (Antoni Garrell, 2019). Por ejemplo, una empresa de calzado que automatiza su proceso puede cambiar el modelo de zapatilla a fabricar solo ajustando su software, sin necesidad de cambiar toda la línea de producción manualmente.

Aumento de la Seguridad en el Trabajo: Según la tesis "***Diseño de un sistema de gestión de salud y seguridad ocupacional basado en el Acuerdo Gubernativo 229-2014 en una empresa de proyectos eléctricos ubicada en la ciudad de Guatemala*** de Josué Antonio Ortíz Mata (Mata, 2022)", muchas industrias realizan procesos que implican riesgo físico para las personas, como manejar sustancias químicas peligrosas, cortar materiales pesados o trabajar con

calor extremo. La automatización permite que esas tareas las realicen máquinas diseñadas para resistir tales condiciones, reduciendo así el riesgo de accidentes laborales (Mata, 2022). Por ejemplo, en la industria metalúrgica, los robots pueden encargarse de fundir y moldear metales sin poner en peligro a ningún trabajador.

Desafíos y Desventajas de la Automatización de Procesos

Aunque automatizar los procesos trae múltiples beneficios, también es importante tener en cuenta algunas desventajas que pueden surgir durante su implementación o funcionamiento.

*Incertidumbre Laboral o Miedo al Reemplazo**:*** Según el artículo *" **automatización y el futuro*** de Mateo Josué Granda Riera, David Alexander Bacuilima Chamba, Eugenia Salomé Songor Tepán (Riera et al, 2023)", uno de los efectos sociales más visibles de la automatización es el temor que sienten muchos trabajadores de ser reemplazados por máquinas o sistemas automáticos y este miedo no es infundado, en sectores donde las tareas repetitivas son comunes, ya que es justamente en esas áreas donde más se aplican estas tecnologías (Riera et al, 2023). Por ejemplo; en una planta empacadora de alimentos, los operarios que antes se encargaban de organizar las cajas pueden ser reemplazados por brazos robóticos que lo hacen más rápido y sin descanso. Esto puede causar preocupación entre los empleados, quienes temen perder su empleo. Sin embargo, también es cierto que la automatización puede abrir nuevas oportunidades, como puestos relacionados con el mantenimiento, programación o supervisión de los sistemas automatizados. De hecho, en empresas que logran aumentar su producción gracias a la automatización, puede generarse crecimiento y expansión, lo cual a largo plazo puede traducirse en la creación de nuevos empleos, aunque con perfiles laborales diferentes.

*Alta Inversión Inicial**:*** Según **"*Coloquio de investigación formativa 2021-2, Resúmenes ejecutivos*** de Omar Antonio Vega (Vega, 2021)**",** automatizar no es simplemente comprar una

máquina y encenderla, sino que requiere una planificación, adquisición de tecnología, capacitación del personal, instalación de sistemas y, en muchos casos, asesoría externa. Todo esto implica un gasto económico importante que puede representar un obstáculo para pequeñas y medianas empresas.

Por ejemplo, una empresa que produce textiles desea automatizar la parte del corte de tela. Para hacerlo, debe invertir en un software especializado, una cortadora láser automática, entrenar a sus trabajadores para operar el nuevo sistema, y contar con soporte técnico en caso de fallos y este proceso puede requerir mucho dinero y tiempo de adaptación. Por eso, muchas empresas deben evaluar si esta inversión traerá beneficios suficientes a mediano o largo plazo, como para justificar el gasto inicial (Vega, 2021).

*Disminución de la Flexibilidad en los Procesos**:*** Según el trabajo de grado ***"Mejora en los procesos del área de compras y presupuesto en constructora Celaque*** de Ligia Cecilia Rodríguez Hernández" (Hernández, 2025), una vez que se automatiza un proceso, hacer cambios o ajustes puede volverse complicado si no se ha planeado adecuadamente desde el principio. Según el trabajo de grado "***Sistema de información basado en un enfoque de procesos, para la optimización de la otorgación de créditos. Caso empresa Comebra*** *de* Roly Rolando Quisé Coarite", los sistemas automatizados suelen seguir una secuencia estricta de tareas, y modificar esa secuencia puede requerir reprogramación, rediseño del software o incluso sustituir algunos equipos (Coarite, 2020).

Por ejemplo, una panadería industrial que automatizó la producción de cierto tipo de pan. Si después desea cambiar la receta, el tamaño del producto o introducir una nueva línea de pan con ingredientes distintos, puede encontrar obstáculos, ya que el sistema automatizado fue diseñado para una receta específica. Esto significa que se necesitaría reconfigurar las máquinas,

ajustar sensores o adquirir nuevos módulos, lo que puede generar costos adicionales y tiempo de inactividad. Para evitar esto se necesita escoger soluciones tecnológicas que sean escalables y que se puedan adaptar fácilmente a los cambios futuros de la empresa.

Transformación de los Procesos Productivos Industriales

La implementación de la automatización electrónica ha transformado los procesos productivos industriales y esta transformación, según el artículo "***El rol de la inteligencia artificial en la automatización y la gestión de la cadena de suministr****o* de Velasco Rigoberto Zambrano Burgos; Jael Dolores Zambrano Mieles y Dolores Mieles Cevallos (Burgos et al, 2025)", se manifiesta en la mejora de la eficiencia operativa, la reducción de errores, la optimización de recursos y la capacidad de adaptación a las demandas del mercado. Por ejemplo, la integración de la analítica de datos y la automatización ha permitido a las empresas anticipar fallos en los equipos, realizar mantenimientos predictivos y ajustar los procesos en tiempo real para maximizar la productividad.

El artículo "***Transformación productiva y nueva actualidad de las políticas industriales en América Latina*** de Mario Castillo y Carlos Ominami (Castillo & Ominami, 2024)", propone que es necesario renovar las políticas industriales teniendo en cuenta cuatro factores que son la adaptación al cambio climático, la incorporación de tecnologías digitales en la industria, como la industria 4.0, la búsqueda de mayor autonomía productiva por ejemplo, fabricando más localmente y la inclusión social. Estos elementos permiten modernizar y transformar los procesos productivos industriales de forma sostenible y justa, con una visión de integración regional y desarrollo a largo plazo.

A pesar de los beneficios evidentes, la adopción de la automatización electrónica enfrenta varios desafíos. Entre ellos se encuentran:

Falta de Conocimiento y Capacitación: Muchas empresas carecen de personal capacitado para operar y mantener sistemas automatizados. Por ejemplo, en el artículo *"**Los desafíos tecnológicos y el rol del contador en la automatización de procesos contables*** de Pilay-Asunción, Dayana Damaris y Marcos-Rodriguez, Kathia Laura" (Pilay-Asunción & Marcos-Rodriguez, 2025), se dice que, para el caso de los contadores, uno de los principales desafíos que enfrenta la contabilidad en la era digital es la necesidad de cerrar la brecha formativa en competencias tecnológicas. Aunque muchos contadores dominan software básico, existen deficiencias importantes en áreas muy importantes como el análisis de datos, la ciberseguridad y la inteligencia artificial y esto limita su capacidad para adaptarse a la automatización y cumplir un rol estratégico en entornos digitales. Además, las pequeñas Y medianas empresas enfrentan obstáculos económicos y de capacitación, lo que dificulta la implementación de herramientas avanzadas y superar estos retos exige capacitación continua, integración de sistemas y políticas robustas de ciberseguridad.

Resistencia al Cambio: Incorporar nuevas tecnologías puede generar incertidumbre y resistencia entre los empleados, afectando la adopción de la automatización. Frente a esto el artículo "Innovación en la gestión empresarial nuevas tecnologías y su rol en la eficiencia organizacional de Stjepan Johany Striseo Martínez (Martínez S. J., 2024)," explica cómo las nuevas tecnologías están cambiando la forma en que se manejan las empresas, ayudándolas a trabajar de manera más eficiente, están haciendo que los procesos sean más rápidos, precisos y seguros. Sin embargo, también señala un desafío importante el cual es la resistencia al cambio, ya que cuando se introducen estas tecnologías, algunos empleados y líderes pueden sentirse inseguros o temerosos, lo que puede dificultar que las empresas aprovechen completamente estas

herramientas. Para que la tecnología funcione bien, se necesita gestionar bien el cambio dentro de la organización, ayudando a las personas a adaptarse y entender los beneficios.

Costos de Inversión: La implementación de sistemas automatizados requiere una inversión inicial significativa y esto representa una barrera para pequeñas y medianas empresas. El artículo "***impacto de la inteligencia artificial en el asesoramiento tributario mediante un estudio de Caso en la Cafetería Casa Café*** de Stalin Alexander Lalon-Pinduisaca y Alfredo Jacob Coello-Panchana (Lalon-Pinduisaca & Coello-Panchana, 2025)", refiere que inteligencia artificial (IA) puede ayudar a las pequeñas empresas, como en este caso a la Cafetería Casa Café, a manejar mejor sus impuestos. Antes, esta cafetería tenía muchos errores al declarar impuestos y pagaba muchas multas. Pero al usar un sistema con IA llamado SIGO CONTIFICO, logró reducir los errores en un 70%, las multas en un 97% y los costos en un 46.7%.

Sin embargo, también se menciona un problema y es que para comenzar a usar este tipo de tecnología hay que hacer una inversión grande al principio. Esto significa que, aunque a largo plazo trae beneficios, para muchas pequeñas y medianas empresas puede ser difícil pagar los costos iniciales del sistema y de capacitar al personal y a pesar de esto, el estudio muestra que vale la pena porque mejora mucho la eficiencia y el cumplimiento con las normas.

Ciberseguridad: La interconexión de sistemas aumenta la vulnerabilidad a ataques cibernéticos, lo que requiere medidas de seguridad robustas para proteger la información y los procesos industriales. Ejemplo de ello es el artículo "***Análisis de la amenaza cibernética en el sector energético argentino: implicancias para la seguridad nacional de*** Héctor Germán Medina Giménez, Sandra Verónica Martínez, Gerardo Daniel Ortiz", el cual menciona que la energía es muy importante para cualquier país, y en el caso de Argentina, también es muy vulnerable a los ciberataques, especialmente porque ahora todo está conectado a internet; las

redes, las empresas y las tecnologías. Esto hace que sea más fácil que alguien desde otro lugar del mundo intente atacar digitalmente nuestras estructuras importantes, como las que producen gas y petróleo.

El estudio se enfoca en “Vaca Muerta”, una zona en el sur del país que tiene grandes reservas de gas y petróleo, y que es muy importante para la economía argentina y justamente por ser tan valiosa, puede convertirse en un objetivo para ataques cibernéticos. Por ello, hay que mirar qué tan protegida está esa infraestructura, cómo se pueden prevenir esos ataques y qué puede hacer el país para mejorar su seguridad digital.

Análisis de Riesgos y Amenazas en Entornos Automatizados

En los entornos automatizados, como fábricas, plantas de energía o sistemas industriales que usan tecnología para controlar procesos, existen riesgos que pueden afectar su funcionamiento. Estos riesgos pueden ser físicos**,** es decir, aquellos que pasan directamente sobre los equipos, cibernéticos como los ataques o problemas en la parte informática o combinados cuando se juntan ambos.

Amenazas Físicas

En el caso de las amenazas físicas hay dos comunes:

*Fallas de equipos**:*** Los sistemas automatizados dependen de máquinas como sensores, actuadores y otros dispositivos electrónicos que ayudan a que los procesos funcionen solos. Si estos equipos son viejos, no se actualizan o no reciben mantenimiento, pueden fallar en cualquier momento y esa falla puede detener la producción, generar errores en los procesos o incluso dañar toda una línea de trabajo (M et al, 2019).

Sabotajes: El sabotaje ocurre cuando una persona causa daños de forma intencional. Puede ser alguien de dentro de la empresa, por ejemplo, un trabajador molesto o inconforme o

alguien externo que logra entrar sin autorización. Estas acciones buscan interrumpir operaciones, dañar máquinas o manipular los procesos. Además de afectar económicamente, pueden poner en riesgo la seguridad de los trabajadores y del lugar (Barranco, 2021).

Amenazas Cibernéticas

Malware y ransomware en entornos OT: Las redes de Tecnología Operativa (OT), que controlan maquinaria en tiempo real, son vulnerables a malware y ransomware orientados a interrumpir procesos físicos o cifrar datos importantes como PLC (Controladores Lógicos Programables) o SCADA (Supervisory Control and Data Acquisition -Supervisión, Control y Adquisición de Datos). Entonces, cuando se dice que un malware o ransomware puede "cifrar datos importantes como PLC o SCADA", significa que el atacante puede bloquear el acceso a esos sistemas (Niño, 2023). Si un PLC es secuestrado, las máquinas dejan de funcionar correctamente; y si un SCADA se ve comprometido, la empresa pierde la capacidad de monitorear y controlar el proceso industrial (Osorio-Sierra y otros, 2020). Esto no solo causa pérdidas económicas, sino también riesgos de seguridad para las personas y el medio ambiente.

Un ejemplo de ello es LogicLocker, un ransomware de prueba de concepto capaz de secuestrar controladores lógicos programables (PLC), bloquear accesos legítimos y alterar salidas físicas, como liberar niveles peligrosos de sustancias químicas).

Intrusiones remotas: En los entornos automatizados, existen conexiones entre las redes de Tecnologías de la Información (TI), las cuales son los sistemas y herramientas que manejan datos, información y comunicaciones en una organización, como los computadores, redes, servidores, correos electrónicos, bases de datos y aplicaciones de gestión. Cuya función principal es almacenar, procesar y proteger la información para apoyar la administración, la toma de

decisiones y la operación empresarial. Por ejemplo; el sistema de nómina de una empresa o una institución de salud (Llanes & García, 2021), el correo corporativo o la red interna de usuarios.

Por su parte, las Tecnologías de Operación (OT), son los sistemas y dispositivos que controlan y supervisan procesos físicos e industriales, como los sensores, actuadores, controladores lógicos programables (PLC), sistemas SCADA y máquinas automatizadas, cuya función principal es garantizar que las operaciones físicas funcionen de manera segura, continua y eficiente. Por ejemplo; un sistema que controla la apertura de válvulas en una planta de agua, el que regula la temperatura en una fábrica de alimentos o el que maneja robots en una línea de producción.

Entonces, si un atacante logra aprovechar estas conexiones, puede ingresar desde afuera del sistema usando diferentes medios, como un correo electrónico con archivos maliciosos o incluso un dispositivo externo infectado, por ejemplo, una memoria USB. Una vez dentro, el atacante tiene la posibilidad de alterar parámetros de control, acceder a información sensible o manipular a distancia el funcionamiento de las máquinas.

Amenazas combinadas (físico-cibernéticas): Aquí hablamos de ataques que empiezan en el ámbito digital, pero terminan afectando directamente lo físico. Un ejemplo claro es cuando un malware logra modificar la programación de un controlador lógico programable (PLC), que es el dispositivo encargado de dirigir el funcionamiento de una máquina o proceso industrial. En este caso, el ataque no solo daña la información, sino que también puede detener la producción, alterar procesos o incluso causar accidentes. Por eso, este tipo de amenazas son tan peligrosas: porque no se quedan en lo virtual, sino que producen consecuencias reales y materiales.

Factores Estructurales de Vulnerabilidad en Entornos Automatizados

Sistemas obsoletos o heredados: En muchos entornos industriales todavía se utilizan sistemas antiguos para controlar máquinas, procesos o infraestructuras críticas, es decir, son aquellas infraestructuras cibernéticas que son muy importantes porque con su funcionamiento proporcionan un servicio indispensable, como por ejemplo la energía eléctrica o el gas. Estos equipos, llamados sistemas heredados, fueron creados en una época en la que la ciberseguridad no era una prioridad, porque no se pensaba que pudieran ser conectados a redes externas (López et al, 2024).

El problema es que dichos sistemas funcionan con un software y firmware desactualizado, que en muchos casos ya no recibe soporte del fabricante. Esto significa que no se aplican parches de seguridad ni actualizaciones que corrijan fallos detectados con el tiempo y por eso, estos sistemas se convierten en un punto débil dentro de la red industrial, ya que los atacantes pueden aprovechar esas vulnerabilidades conocidas para entrar, manipular datos o interrumpir procesos y a veces no es fácil reemplazarlos porque están integrados en la operación y el costo de modernizarlos es muy alto. Por lo que, el uso de sistemas obsoletos en entornos automatizados expone a la organización a mayores riesgos de ataque, porque son frágiles ante amenazas modernas y difíciles de proteger sin medidas adicionales.

Ambientes heterogéneos y falta de segregación: En muchos entornos industriales, conocidos como OT (Tecnología Operacional), se utilizan al mismo tiempo equipos y sistemas de distintas generaciones. Es común encontrar máquinas muy antiguas, diseñadas hace décadas, que siguen funcionando junto a tecnologías modernas conectadas a internet. A esto se le llama ambiente heterogéneo (Chalacán et al, 2021).

El problema aparece porque, en muchos casos, no existe una segregación adecuada, es decir, una separación entre las redes de la empresa (IT, como correos, servidores o bases de datos) y las redes de operación (OT, como PLC, SCADA o sensores). Cuando estas redes no están bien segmentadas ni tienen controles de acceso sólidos, un atacante que logre entrar por la parte de IT, por ejemplo, a través de un correo con malware, puede moverse con relativa facilidad hacia la red OT. Este "movimiento lateral" le da la posibilidad de afectar directamente los sistemas que controlan procesos físicos, como energía, agua, transporte o producción industrial.

En pocas palabras; hacer uso de tecnologías nuevas y viejas sin una separación ni control adecuados abre la puerta para que una amenaza informática pase de la oficina al área de producción, aumentando el riesgo de fallos o sabotajes.

Brecha entre TI y OT: En una organización industrial se usa la TI (Tecnología de la Información), la cual se ocupa de sistemas informáticos, redes, servidores, aplicaciones, datos y todo lo relacionado con la gestión digital y la OT (Tecnología Operacional), la cual se encarga de los equipos y sistemas que controlan procesos físicos, como máquinas, líneas de producción, plantas de energía, sistemas de agua y demás según sea el caso (Isaza, 2024).

El problema surge porque los equipos humanos de cada área tienen formaciones distintas. Por ejemplo, el personal de OT suele ser experto en mantener la maquinaria funcionando y garantizar la seguridad de los procesos, pero rara vez recibe capacitación en ciberseguridad y el personal de TI, en cambio, sabe mucho sobre seguridad informática, redes y software, pero no domina cómo funcionan los procesos industriales ni las consecuencias de detenerlos o alterarlos.

Esa diferencia de conocimientos genera una brecha de comunicación y coordinación y como resultado, muchas veces se aplican soluciones de seguridad pensadas para entornos de TI

directamente en sistemas OT, pero estas pueden no funcionar bien o incluso causar problemas. Por ejemplo, instalar un parche de seguridad en un sistema de control industrial podría detener la producción si no se prueba adecuadamente, lo que sería muy grave en una planta que no puede interrumpirse.

Por eso, la falta de entendimiento entre los equipos de TI y OT impide crear defensas conjuntas y eso deja a las organizaciones más vulnerables frente a ciberataques.

Casos e Impacto de Incidentes en Sistemas y Redes de Automatización Industrial (2020-2025)

Entre 2020 y 2025, se han documentado incidentes en Colombia y a nivel internacional que evidencian pérdidas económicas y afectación a la continuidad operativa. Por ejemplo, la infraestructura energética en Argentina, como los campos de Vaca Muerta, ha sido blanco de ataques cibernéticos que comprometen la producción de gas y petróleo (Wyczykier & Acacio, 2024).

En Colombia: En los últimos años, Colombia ha sido uno de los países más afectados por los ciberataques en entornos de tecnología operacional (OT), es decir, en aquellos sistemas que controlan procesos industriales como plantas de energía, fábricas o servicios públicos. Según reportes, en 2024 los intentos de ataques en América Latina crecieron un 38 % (Barcenas, 2025), y Colombia recibió alrededor de 36 mil millones de intentos, lo que la ubica como uno de los países más vulnerables (Duitama, 2025). Esto significa que prácticamente todos los días, los sistemas industriales del país están expuestos a intentos de intrusión que, de ser exitosos, podrían detener la producción o dañar equipos.

Otro punto importante está en el Internet de las Cosas (IoT), en 2024, en Colombia, según reporte de la Asociación Colombiana de Informática Sistemas y Tecnologías Afines (ACIS), se registraron más de 280 mil ataques contra dispositivos conectados, como cámaras de vigilancia y grabadores digitales (DVR), con un 31% de aumento respecto al año anterior (ACIS , 2025), es posible ver que, a medida que crece el uso de estos dispositivos, también aumenta la superficie de ataque que los delincuentes aprovechan.

En cuanto a las infraestructuras más importantes o críticas como se les llama también, como la energía, el petróleo o el gas, según la empresa internacional de ciberseguridad

Kaspersky, los datos del primer trimestre de 2025 muestran que el 21% de los computadores de sistemas de control industrial (ICS) en América Latina detectaron y bloquearon malware y, aunque hay mecanismos de defensa, gran parte de los equipos sigue en riesgo (Kaspersky, 2025).

El impacto económico también puede verse, porque en 2025, el costo promedio de recuperación de una empresa colombiana después de un ataque de ransomware fue de 870 mil dólares, es decir, alrededor de $3.525.213.900 y a esto se suma el gasto adicional en tiempo y esfuerzo que deben realizar los equipos de TI y de ciberseguridad para contener el daño, restaurar operaciones y reforzar los sistemas (Martín, 2025).

A nivel internacional: A nivel internacional, también se han presentado casos donde el problema es más grave, un ejemplo es el ransomware experimental LogicLocker, el cual fue diseñado para atacar controladores lógicos programables (PLC), que son los equipos que permiten controlar procesos industriales. Aunque todavía no se ha propagado masivamente, los atacantes ya están desarrollando herramientas para manipular la lógica de las máquinas.

Un caso emblemático, aunque anterior a 2020, es el de Stuxnet. Este fue el primer gusano informático; es decir, un tipo de malware diseñado para propagarse automáticamente a través de redes y dispositivos sin necesidad de intervención directa del usuario, el cual logró modificar directamente los PLC de una planta industrial, en este caso para alterar procesos de centrifugado nuclear. Aunque ocurrió hace más de una década, sigue siendo un referente porque mostró cómo un ataque digital puede tener consecuencias físicas terribles donde el virus tomó el control de más de mil máquinas y les ordenó autodestruirse (BBC News Mundo, 2015).

En cuanto a estadísticas recientes, según la empresa internacional de ciberseguridad Kaspersky, durante el primer trimestre de 2025 se encontró que el 22 % de los sistemas ICS a nivel mundial fueron afectados por malware (Kaspersky, 2025) y los sectores más

comprometidos fueron el de la energía, la manufactura, la automatización de edificios, petróleo y gas, por lo que es posible ver que, la amenaza no distingue fronteras ni niveles de desarrollo tecnológico porque tanto países industrializados como en desarrollo se enfrentan a estos riesgos.

Impacto en Procesos Productivos

Los ataques en estos entornos no solo afectan a las máquinas, sino a toda la cadena de valor de las empresas y los servicios públicos. Sus principales consecuencias son la interrupción operativa, pues, una fábrica puede detener su línea de producción por horas o incluso días, lo que genera pérdidas económicas y retrasos en la entrega de productos. En Colombia, como se mencionó, la recuperación puede costar cientos de miles de dólares y en empresas más grandes o de alcance internacional, la cifra puede multiplicarse.

La pérdida de reputación y confianza también es una consecuencia grave, por ejemplo, si un hospital, una empresa de energía o una aerolínea se ven afectados, los usuarios pueden perder la confianza en su capacidad de garantizar un servicio seguro y finalmente los riesgos acumulados que esto conlleva, pues, muchos sistemas OT siguen utilizando equipos y software antiguos, que no fueron diseñados para resistir ciberataques. Esto significa que un solo ataque puede tener efectos en cascada, afectando varios procesos a la vez (Díaz & Rodríguez, 2025).

Medidas de Seguridad Implementadas en Procesos Productivos Automatizados

Evaluación del Nivel de Adopción de Controles de Seguridad en Entornos Industriales

En sectores industriales como la manufactura y la energía, es muy importante garantizar la seguridad porque cualquier interrupción afecta directamente la producción y la continuidad de los servicios. Con la llegada de la Industria 4.0, la integración de tecnologías digitales ha mejorado la eficiencia, pero también esto ha generado nuevos riesgos de ciberseguridad que deben ser atendidos mediante controles físicos, lógicos y de red.

Seguridad física: La seguridad física sigue siendo la primera línea de defensa en los entornos industriales. Implica controlar el acceso a instalaciones sensibles, como salas de servidores, centros de control, gabinetes eléctricos o dispositivos de automatización. Este control puede lograrse mediante credenciales de identificación, sistemas biométricos o cámaras de vigilancia. La falta de protección física abre la puerta a sabotajes o manipulaciones que afectan directamente la operación de los sistemas.

Controles lógicos y de red: En el ámbito digital, uno de los mecanismos más adoptados es la segmentación de red, el cual consiste en dividir la red en diferentes zonas con funciones específicas; es decir, una red corporativa, una red de control (ICS) y una red de automatización. Esto ayuda a contener amenazas, impidiendo que un ataque en un área se propague a toda la infraestructura.

La Agencia de Ciberseguridad de Estados Unidos (CISA) ha recomendado la segmentación como una de las prácticas más eficaces para proteger los sistemas de Tecnologías de Operación (OT) (CISA, 2024). Además de la segmentación, se utilizan VLANs, firewalls industriales, zonas desmilitarizadas (DMZ) y servidores de salto llamados también jump servers, que limitan los accesos y establecen barreras adicionales de protección.

Otros controles lógicos como el uso de sistemas de detección y prevención de intrusos (IDS/IPS), auditorías periódicas de seguridad y el monitoreo continuo del tráfico en la red OT para identificar actividades sospechosas a tiempo.

A pesar de que las empresas reconocen la importancia de estas medidas, su adopción no es completa debido a la falta de personal capacitado en ciberseguridad industrial (Muñoz-Pinzón y otros, 2024), los altos costos de implementación y la complejidad de integrar los entornos de TI

(Tecnologías de la Información) y OT (Tecnologías de Operación) los cuales, dificultan que estas prácticas se apliquen de forma generalizada.

Herramientas y Tecnologías Clave para Fortalecer la Seguridad

Sistemas SCADA: Los sistemas SCADA (por las siglas en inglés de Supervisory Control And Data Adquisition), son sistemas de supervisión, control y adquisición de datos (Chuquitarco & Tapaicela, 2022). Estos son el núcleo de la supervisión y control en entornos industriales. Para mantenerlos seguros, es necesario fortalecer la autenticación mediante métodos multifactor, implementar contraseñas que sean seguras y robustas, asignar permisos basados en roles y limitar accesos temporales para reducir el riesgo de accesos indebidos y mejorar la trazabilidad.

Segmentación de red: La segmentación, ya mencionada en los sistemas SCADA, no solo divide los activos en grupos, sino que también permite controlar los flujos de información entre cada segmento. Esto se logra mediante el uso de firewalls industriales, VLANs y DMZ, acompañados de monitoreo constante.

Control de acceso biométrico o mediante credenciales: Estos controles refuerzan tanto la seguridad física como la lógica. Solo el personal autorizado puede acceder a equipos críticos, reduciendo las posibilidades de errores humanos o actos de sabotaje.

Cifrado de datos: El cifrado es una medida que protege la información cuando se transmite o se almacena, evitando que pueda ser interceptada o manipulada. Aunque su aplicación en entornos OT no es tan común como en TI, cada vez más protocolos industriales incorporan cifrado al trabajar sobre TCP/IP.

Sistemas de respaldo automatizados: Los respaldos regulares permiten restaurar configuraciones de SCADA, controladores o servidores en caso de incidentes como ataques de

malware, errores humanos o fallas técnicas. Esto asegura la continuidad operativa y minimiza pérdidas (Jiménez, 2023).

Estándar IEC 62443: La norma internacional IEC 62443 establece buenas prácticas y controles técnicos para proteger los sistemas de control industrial (Ingertec, 2025). Su enfoque en zonas y conductos de seguridad, junto con la definición de niveles de protección, facilita una gestión más ordenada de los riesgos.

Monitoreo continuo y defensa en capas: Una estrategia de seguridad con políticas organizacionales, capacitación del personal, actualizaciones periódicas, sistemas antivirus, segmentación de red y monitoreo.

Capacidad de respuesta avanzada (EDR y ZTNA): Los datos se han convertido en uno de los recursos más importantes para cualquier empresa, ya sea grande o pequeña (Loachamín, 2023). Entre ellos están la información personal, los datos confidenciales, ideas protegidas y hasta cifras del mercado. Como toda esa información se guarda y mueve en sistemas tecnológicos, es necesario protegerla para evitar robos o ataques que interrumpan el trabajo normal de las organizaciones. Con la digitalización y los cambios que trajo la pandemia, las empresas usan más tecnología y eso también ha abierto más puertas a los delincuentes informáticos, que aprovechan con métodos modernos como engaños, ataques invisibles o técnicas muy elaboradas para entrar a los sistemas.

Las soluciones modernas son el uso de Endpoint Detection and Response (EDR) y Zero Trust Network Access (ZTNA). Estas tecnologías verifican la seguridad de dispositivos antes de permitir su conexión a la red y permiten detectar amenazas en tiempo real, lo cual permite fortalecer las defensas frente a ataques dirigidos (Ibarra & Escobar, 2025).

Tabla 2

Medidas de Seguridad Implementadas en Procesos Productivos Automatizados

Medida	Objetivo principal
Seguridad física	Evitar accesos no autorizados o sabotajes
Segmentación de red y firewalls	Limitar movimiento lateral de amenazas
SCADA	Proteger sistemas críticos mediante autenticación y control
Cifrado y protocolos seguros	Proteger datos en tránsito
Respaldos automatizados	Garantizar recuperación post-incidente
Normas IEC 62443	Establecer gestión de seguridad estructurada
Monitoreo, EDR y respuesta rápida	Detectar y contener amenazas en tiempo real

Nota. La tabla muestra los principales controles físicos, lógicos y de red adoptados en sectores industriales para proteger sistemas automatizados y reducir riesgos operacionales.

Normativas y Marcos Regulatorios Aplicables en Colombia y de Referencia Internacional

En el contexto colombiano, las empresas que operan sistemas automatizados como planta, manufactura, energía y agua, deben conocer y acatar normas nacionales e internacionales que protegen los datos, regulan las conductas delictivas relacionadas con tecnologías y orientan las buenas prácticas de seguridad.

Ley 1581 de 2012 de Protección de datos personales: Es la norma marco en Colombia sobre tratamiento de datos personales, que establece obligaciones para quienes recolectan, usan o almacenan datos personales, es decir, a los responsables y encargados del tratamiento, y

reconoce derechos de los titulares, como el acceso, la rectificación y la supresión de los mismos (Congreso de Colombia , 2010).

Esto es muy importante porque muchos procesos automatizados generan datos personales como los registros de acceso, videovigilancia, bitácoras de usuarios y datos de proveedores, entonces, la Ley 1581 obliga a proteger esta información y a implementar medidas técnicas y administrativas adecuadas para hacerlo.

En caso de un incidente, por ejemplo, en caso de filtración o pérdida de datos, la organización debe atender derechos de los titulares y puede enfrentar sanciones si no demuestra consentimiento, finalidades legítimas o medidas de protección. Por eso, la seguridad en redes OT/SCADA y los respaldos seguros se vinculan directamente con el cumplimiento de esta ley.

Ley 1266 de 2008 de Habeas data financiero: Esta es una ley que regula el manejo de datos personales en bases de datos, con énfasis en la información financiera, crediticia y comercial (Congreso de la República , 2008). La misma, fue parcialmente reglamentada por el decreto 1081 de 2015 y reconoce el derecho de los titulares a conocer y rectificar información contenida en bases de datos.

Esta ley es importante porque las empresas industriales mantienen historiales financieros, datos de clientes y proveedores, y registros que, si se exponen, pueden afectar la reputación y la operación. Por ello, la ley requiere cuidados especiales al procesar y compartir información financiera, lo que implica controles de acceso lógico, cifrado y auditorías.

Ley 1273 de 2009 de los Delitos informáticos: Esta**,** introduce en el Código Penal colombiano tipos penales relacionados con la protección de la información y los sistemas informáticos, como el acceso no autorizado, daño informático, interceptación, uso indebido de

información, entre otros. Esta ley tipifica conductas que, en el entorno OT, pueden equivaler a sabotaje digital (Congreso de Colombia , 2009).

Cuando un atacante accede a un PLC, modifica parámetros de control o instala malware, esas acciones pueden constituir delitos tipificados por la Ley 1273. Esto no solo obliga a las empresas a denunciar incidentes, sino también a fortalecer medidas preventivas para evitar que sus sistemas sean utilizados como herramientas criminales.

Decreto 1078 de 2015 de la Reglamentación del sector TIC: Es el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones en Colombia; compila normas y competencias del Ministerio TIC y regula aspectos administrativos y técnicos del sector (Colombia, 2015).

El Decreto 1078 establece responsabilidades institucionales y procedimientos relacionados con las TIC en Colombia, a las organizaciones que usan infraestructuras de telecomunicaciones o servicios gestionados por terceros les interesa porque define obligaciones regulatorias y requisitos para la prestación de servicios digitales que impactan la disponibilidad y continuidad de sistemas OT.

ISO/IEC 27001de la Gestión de seguridad de la información: Es la norma internacional para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Define requisitos para identificar riesgos, aplicar controles y asegurar la mejora continua (ICONTEC, 2013).

ISO/IEC 27001 ofrece un marco organizado para gestionar riesgos de información que incluyen datos de TI y, cuando se adapta, aspectos de OT. Adoptar un SGSI ayuda a demostrar cumplimiento con requisitos legales, por ejemplo, la protección de datos y a estructurar controles técnicos y administrativos para prevenir, detectar y responder a incidentes.

IEC 62443 de Seguridad en sistemas de control industrial (IACS / OT): Es una serie de normas internacionales específicas para la ciberseguridad de los sistemas de automatización y control industrial (Industrial Automation and Control Systems, IACS), la cual cubre requisitos para fabricantes, integradores y operadores, y recomienda arquitecturas como zonas y conductos, procesos de ciclo de vida y controles técnicos (Ingertec, 2025).

La IEC International Electrotechnical Commission, es decir, la Comisión Electrotécnica Internacional, es la guía más especializada para proteger PLC, SCADA, RTU y otros componentes OT. Sus recomendaciones en cuanto a la segmentación por zonas, gestión de cambios, pruebas de seguridad en fábricas y en campo son directamente aplicables a la seguridad operacional y son complementarias a ISO/IEC 27001. Por lo cual, adoptarla ayuda a reducir riesgos técnicos específicos del control industrial.

NIST Cybersecurity Framework (CSF)- Referencia internacional para gestión de riesgos: Es el marco desarrollado por el NIST (EE. UU.) National Institute of Standards and Technology, es decir, el Instituto Nacional de Estándares y Tecnología de EE. UU, que organiza buenas prácticas en funciones como identificar, proteger, detectar, responder y recuperar, el cual es ampliamente usado como referencia para diseñar programas de gestión de riesgos cibernéticos y que, actualmente se encuentra en evolución a versiones 2.0, incorporando nuevas materias como gestión de riesgos emergentes (NIST, 2024).

El NIST CSF ayuda a que las organizaciones colombianas estructuren programas de ciberseguridad siguiendo funciones claras y métricas y se integra bien con ISO 27001 e IEC 62443, en la medida que la ISO aporta el sistema de gestión, IEC las medidas técnicas OT y la NIST ofrece un lenguaje operacional para gobernanza y respuesta ante incidentes.

Por todo lo anterior, es posible ver que, la Ley 1581 y la Ley 1266 obligan a proteger los datos personales y financieros; por lo tanto, las empresas deben aplicar controles como cifrado, control de acceso, políticas de retención y procedimientos para atender solicitudes de titulares. Estas obligaciones son verificables por autoridades y, ante incidentes, la ausencia de medidas puede implicar sanciones administrativas.

Por su parte, la Ley 1273 tipifica conductas delictivas informáticas y ante ataques que impliquen accesos no autorizados o sabotaje digital, la empresa debe coordinar con autoridades competentes y disponer de evidencias técnicas ya sea a través de los llamados logs como conjunto de datos o copias forenses para apoyar la investigación.

En cuanto al marco técnico y operativo, la IEC 62443 ofrece controles técnicos específicos para sistemas OT en zonas y conductos, gestión de parches, pruebas de seguridad en PLC/SCADA, y la norma ISO/IEC 27001 obliga a un sistema de gestión que gestione riesgos y permita demostrar debida diligencia y la NIST CSF permite planear detección, respuesta y recuperación para ofrecer una defensa integral en la protección de datos, la seguridad informática y la operación de sistemas de control industrial.

Los marcos recomiendan planes de continuidad, respaldo y pruebas de recuperación, pues, estos planes son muy importantes para restablecer producción luego de incidentes y para mitigar impactos económicos y de seguridad. La ISO 27001 y la NIST CSF explicitan la necesidad de ejercicios, pruebas y revisión continua. Por lo cual, implementar estas normas obliga a que la empresa articule equipos técnicos, responsabilidades y gobernanza. Por ejemplo, la creación de un Comité de Seguridad que incluya responsables OT y TI, políticas unificadas de acceso, gestión de cambios y evaluación continua del riesgo. Y la IEC 62443 en cuanto a procesos y responsabilidades específicas para entornos OT.

De esta manera, cumplir estas normas reduce la probabilidad de incidentes, facilita la respuesta cuando ocurren y demuestra diligencia debida frente a clientes, reguladores y aseguradoras y puede mitigar sanciones administrativas y reputacionales en caso de incidentes.

Para las organizaciones industriales en Colombia, la protección frente a incidentes exige cumplir la normativa nacional en cuanto a las leyes 1581, 1266, 1273 y el Decreto 1078 y adoptar marcos internacionales como la ISO/IEC 27001, IEC 62443 y NIST CSF que, permiten gestionar riesgos, proteger datos personales y financieros, prevenir delitos informáticos y asegurar la continuidad operativa, establecer controles técnicos de segmentación, cifrado, parches, backups, políticas y responsabilidades y procesos de detección y respuesta equivalentes al riesgo de operar sistemas automatizados.

Tabla 3

Normativas y Estándares para Seguridad y Cumplimiento en Plantas Industriales Automatizadas en Colombia

Norma/Marco regulatorio	Alcance	Medidas obligatorias	Acciones recomendadas en OT
Ley 1581 de 2012	Protección datos personales	Consentimiento, derechos de titulares, confidencialidad	Control de acceso, cifrado, políticas de privacidad
Ley 1266 de 2008	Datos financieros	Exactitud, rectificación, restricciones de uso	Auditorías de acceso, cifrado de registros sensibles

Norma/Marco regulatorio	Alcance	Medidas obligatorias	Acciones recomendadas en OT
Ley 1273 de 2009	Delitos informáticos	Tipificación penal de accesos ilícitos y sabotaje	Registro de incidentes, evidencia digital segura
Decreto 1078 de 2015	Regulación TIC	Requisitos para proveedores y servicios digitales	Evaluación de proveedores, continuidad operativa
ISO/IEC 27001	SGSI – Seguridad de la información	Evaluación de riesgos, controles, mejora continua	Implementar SGSI, monitoreo, entrenamiento
IEC 62443	Seguridad en entornos OT	Zonas y conductos, niveles de seguridad, diseño seguro	Segmentar red, hardening, gestión de parches
NIST CSF	Gestión de riesgos cibernéticos	Funciones: Identificar, Proteger, Detectar, Responder, Recuperar	Mapear funciones, indicadores, mejora continua

Nota. La tabla resume las principales normas vigentes y marcos de referencia en ciberseguridad y protección de datos aplicables a entornos industriales en Colombia.

Mejores Prácticas y Tecnologías Emergentes para la Protección de la Automatización Electrónica

Tendencias Emergentes en Automatización Industrial

Mantenimiento Predictivo: Según la tesis "***Sistema de monitoreo de vibraciones por medio de modelos de mantenimiento predictivo 4.0 PHM y sistemas inerciales con el propósito de diagnosticar el estado y salud de activos*** de Jose Dumar Sierra Riaño y Miguel Ángel Otalora León (Riaño & León, 2023)," el mantenimiento predictivo es una de las tendencias más destacadas en la industria porque esta técnica consiste en utilizar sensores y sistemas de análisis de datos para predecir cuándo una máquina puede fallar, lo que permite realizar reparaciones antes de que ocurra un daño mayor. A diferencia del mantenimiento correctivo que se hace después de que algo se daña, o el preventivo que se hace en intervalos programados, el mantenimiento predictivo ayuda a ahorrar tiempo y costos, y a mantener los equipos funcionando de manera continua.

Según el artículo "***Importancia de la implementación de mantenimiento preventivo en las plantas de producción para optimizar procesos*** de Cristian Sebastián Arroyo Vaca y Romel Fabian Obando Quito (Vaca & Quito, 2022)", el mantenimiento predictivo no solo reduce los tiempos de parada en la producción, sino que también mejora la seguridad del personal y extiende la vida útil de los equipos industriales. Además, permite tomar decisiones más informadas basadas en el estado real de las máquinas, gracias al uso de tecnologías como el Internet de las cosas (IoT) y la inteligencia artificial.

Robótica Colaborativa: Otra tendencia importante es el uso de robots colaborativos, conocidos como "cobots".Según el artículo "***Marco de referencia para la incorporación de Cobots en líneas de manufactura*** de Sergio Salimbeni y Daniel Mamani, (Salimbeni & Mamani,

2020)"a diferencia de los robots tradicionales, que trabajan aislados por seguridad, los cobots están diseñados para trabajar junto a las personas de forma segura por lo que estos robots pueden realizar tareas repetitivas o peligrosas, mientras que los operarios se enfocan en actividades que requieren juicio o creatividad.

De acuerdo con la Federación Internacional de Robótica (Pelegrí, 2019), el uso de cobots ha aumentado considerablemente en industrias como la automotriz, electrónica y alimentaria, debido a su capacidad de mejorar la productividad sin reemplazar por completo al trabajador humano. Según la ***tesis "Robótica aplicada, un paso ya presente en el futuro. Análisis de mercado consecuencias de implantación e introducción en las PYMES*** de Jorge Deiro Ferre (Ferre, 2021),", su flexibilidad, facilidad de programación y bajo costo hacen que sean una opción accesible incluso para pequeñas y medianas empresas.

Gemelos Digitales: Los gemelos digitales son réplicas virtuales de procesos, máquinas o sistemas reales, que permiten simular su funcionamiento sin afectar la producción física. Estos modelos digitales pueden usarse para probar cambios, predecir comportamientos y optimizar operaciones de forma segura y económica. Los gemelos digitales permiten a las empresas tomar mejores decisiones estratégicas, ya que proporcionan una visión clara y en tiempo real del desempeño de sus activos y facilitan el desarrollo de nuevos productos, la mejora de procesos y la capacitación del personal (Bustamante-Limones et al, 2024).

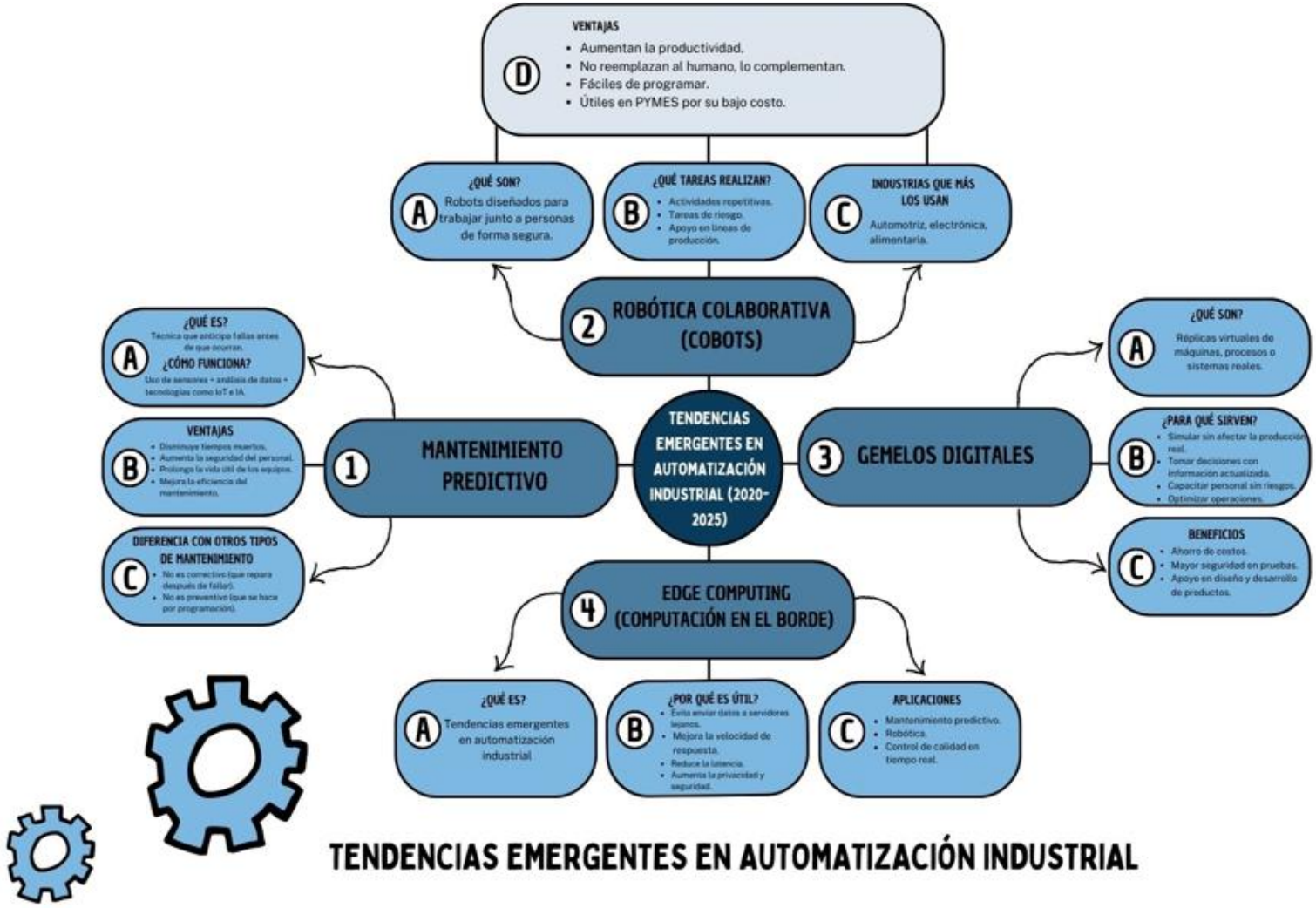
Edge Computing: Según el trabajo de grado "***Estudio de una plataforma para Edge Computing e IoT*** de Mikel Sanabria Sánchez (Sánchez M. S., 2020)", el edge computing, o "computación en el borde", consiste en procesar los datos en el mismo lugar donde se generan, en lugar de enviarlos a un servidor central o a la nube. Esta tecnología es especialmente útil en

entornos industriales donde se necesita tomar decisiones en tiempo real y con baja latencia, es decir, sin demoras.

El edge computing permite una mayor velocidad de respuesta en procesos automatizados, ya que la información no tiene que viajar largas distancias. También mejora la privacidad y la seguridad de los datos, porque se procesan localmente y no se exponen tanto a internet, esta tendencia es muy buena para aplicaciones como la robótica, el mantenimiento predictivo y el control de calidad en tiempo real.

Figura 1

Mapa Mental, Tendencias Emergentes en Automatización Industrial



Prácticas Emergentes de Protección en Automatización Electrónica

Arquitectura de Confianza Cero (Zero Trust Architecture, ZTA): En entornos industriales no se puede confiar en lo que está dentro de la planta, tal como se ha hecho referencia en líneas anteriores, por ello, la Confianza Cero propone verificar explícitamente cada acceso, ya sea de un usuario, equipo o servicio y otorgar permisos mínimos, segmentando recursos críticos, es decir, los más importantes y monitoreando de forma continua. NIST define Zero Trust como un conjunto de principios que elimina la confianza implícita basada en la ubicación de red, y requiere autenticación y autorización continuas antes de conectar con un recurso (Rose et al, 2020).

Para operaciones industriales, las guías de CISA recomiendan adaptar estos principios al contexto OT lo cual consiste en segmentar en zonas y conductos, controlar el acceso a nivel de activo, aplicar listas de control de acceso estrictas, y visibilizar tráfico este-oeste entre celdas de la planta para detectar movimientos laterales (CISA, 2024). Adoptar ZTA en OT reduce la superficie de ataque, dificulta escalamiento de privilegios y sostiene la continuidad operacional al contener incidentes sin detener líneas completas de producción.

Detección de anomalías con inteligencia artificial: Los procesos automatizados generan grandes volúmenes de datos por ejemplo señales, telemetría y logs, los cuales pueden aprovecharse para detectar desviaciones sutiles antes de que se conviertan en fallas o intrusiones. La literatura reciente muestra que enfoques de aprendizaje no supervisado, por ejemplo, autoencoders, isolation forest y modelos híbridos combinando técnicas estadísticas y redes neuronales, logran identificar anomalías en redes industriales y procesos de control, incluso cuando no se dispone de amplios conjuntos (Pereiro, 2022).

En la práctica, esto se traduce en soluciones que aprenden el "comportamiento normal" de celdas de manufactura, PLCs o redes de sensores, y alertan tempranamente sobre patrones de comunicación atípicos, variaciones de vibración o temperatura o secuencias de comandos inusuales. Integrado con tu estrategia de mantenimiento predictivo, este enfoque acorta el tiempo de detección, disminuye paradas no planificadas y eleva la seguridad del personal y de los activos.

Redes privadas industriales 5G/LTE NPN o campus networks: Para aislar y proteger mejor los sistemas de automatización, muchas plantas están desplegando redes móviles privadas como Non-Public Networks y NPN, que ofrecen baja latencia, alta confiabilidad y control local del plano de seguridad. Las alianzas y organismos del sector describen arquitecturas NPN desde modos que ellos denominan totalmente "*stand-alone"* (Handzel, 2020), es decir, sin recursos compartidos con la red pública, hasta integraciones con el operador, con mecanismos de autenticación mutua, cifrado e integridad de extremo a extremo.

En manufactura, estas redes permiten segmentar celdas y robots, priorizar tráfico de control, y mantener los datos de producción dentro del sitio (data sovereignty), lo cual permite reducir la exposición a Internet y fortalece la continuidad durante incidentes en redes corporativas.

Monitoreo continuo y en tiempo real: Consiste en hacer inventario de activos, registro y monitoreo continuo de eventos, supervisión de integridad, y análisis de tráfico industrial, todo ello ajustado a los requisitos de seguridad y seguridad funcional propios del proceso (NIST, 2024). Las guías internacionales para OT recomiendan los paneles en tiempo real, sensores pasivos en SPAN/TAP para no interferir con el control, correlación de alertas con contexto del proceso, y pruebas de respuesta que no comprometan la seguridad operacional. Un monitoreo

bien diseñado acorta el MTTD/MTTR, es decir; cuánto tarda una organización en descubrir que hay un problema o incidente y cuánto se demora en solucionarlo o volver todo a la normalidad, lo cual, apoya decisiones informadas del personal de planta y evita paros extendidos al detectar y contener incidentes en fases tempranas.

Estas prácticas sostienen la continuidad y reducen riesgos en la medida que ayudan a la prevención y contención; por ejemplo, Zero Trust limita el movimiento lateral y mantiene incidentes acotados a una celda o zona, evitando la propagación a líneas completas, permiten la detección temprana, puesto que la IA para anomalías identifica desviaciones incipientes en variables de proceso y patrones de red antes de que escalen a fallas o ataques disruptivos. Permiten también el aislamiento y la calidad de servicio; por ello, las redes privadas industriales ofrecen aislamiento lógico y físico, priorización de tráfico crítico y políticas de seguridad locales que sostienen la producción incluso ante problemas en la red TI corporativa y finalmente el monitoreo continuo, con registros y telemetría contextualizados, habilita manuales de respuesta más precisos y restablecimiento seguro de operaciones, cumpliendo los principios rectores de la seguridad de la información de confidencialidad, integridad y disponibilidad (Balladares & Chichande, 2020).

Tabla 4

Prácticas Emergentes de Protección en Automatización Electrónica y sus Beneficios Operativos

Práctica-Tecnología	Beneficio operativo
Arquitectura Zero Trust (ZTA)	Limita el acceso no autorizado, segmenta procesos críticos y contiene incidentes, evitando que se propaguen a toda la planta.
Detección de anomalías con IA	Identifica desviaciones tempranas en procesos y redes, reduciendo fallas inesperadas y acortando tiempos de respuesta.
Redes privadas industriales (5G/LTE NPN)	Garantizan baja latencia y alta confiabilidad, con aislamiento lógico/físico que protege datos sensibles y asegura continuidad de la producción.
Monitoreo continuo en tiempo real	Proporciona visibilidad constante de activos y tráfico, lo que facilita la detección y respuesta inmediata ante amenazas o fallas.

Nota. La tabla muestra la relación directa entre cada práctica emergente de ciberseguridad y el beneficio operativo que aporta a la continuidad de procesos automatizados.

Propuestas de Mejora para el Contexto Colombiano

En este apartado se proponen soluciones, las cuales son concretas, viables y graduadas para poder fortalecer la protección de los sistemas de automatización industrial en Colombia. Las recomendaciones deben ir de la mano con las medidas técnicas, la gestión organizativa y el fortalecimiento de las capacidades humanas, es decir, de capacitar al personal de la empresa en estas competencias, procurando un equilibrio entre eficacia y costo para que sean aplicables tanto en grandes plantas como en pequeñas y medianas empresas del país.

*Principio general y enfoque por fases**:*** Esta propuesta parte de hacer una mejora por fases que permita avanzar sin interrumpir la producción ni requerir de grandes inversiones inmediatas. Las cuales, consisten en primera medida en hacer un diagnóstico rápido de máximo 3 meses, y un inventario mínimo viable de activos críticos, esto implica los equipos, las redes y los puntos de control, esto para poder hacer la identificación de procesos que afectan directamente continuidad productiva y valoración de riesgos. Esta etapa debe ser de bajo costo y se puede ejecutar por el personal interno.

Pueden en segunda fase, tomar medidas de mediano costo, como la segmentación lógica de redes, la creación de cuentas con accesos mínimos, copias de seguridad regulares, parches críticos a sistemas no críticos, y establecer procedimientos de respuesta a incidentes a nivel operativo. Esto puede tomar un tiempo de 6 a 9 meses.

Posteriormente, en la tercera fase, se debe hacer la capacitación y gobernanza la cual tiene una duración de 6 a 18 meses, consistente en la formación continua del personal operativo y de gestión, establecer políticas locales alineadas con la Política de Seguridad Digital y planificar ejercicios de respuesta.

En la cuarta fase, se deben hacer las mejoras tecnológicas, lo cual puede tomar de 12 a 36 meses, adoptar gradualmente soluciones como el monitoreo continuo, la detección por comportamiento (IA), y, donde sea rentable, redes privadas industriales o edge computing. Estas inversiones deben priorizarse por su retorno en reducción de paradas no planificadas y ahorro en mantenimiento.

Hacerlo de forma escalonada permite obtener beneficios rápidos y repartir inversión, capacitando a la organización antes de incorporar tecnología más sofisticada.

Relación entre Costo-Beneficio y Aplicabilidad de las Medidas Técnicas y de Gestión

Tabla 5

Medidas Técnicas y de Gestión: Costo-Beneficio y Aplicabilidad

Medida	¿Qué hacer?	Costo	Beneficio	Aplicabilidad Local
Inventario y clasificación de activos	Registrar PLCs, HMI, sensores, redes y protocolos; clasificar según impacto.	Bajo (horas de personal y plantilla estándar).	Focaliza recursos y evita gastos innecesarios.	Guías de MinTIC facilitan adaptación en entidades públicas y privadas.
Segmentación de red y control de accesos mínimos	Separar redes de control y administrativas; listas de control;	Moderado (configuración básica).	Muy alto: reduce propagación de ataques y protege subsistemas.	En empresas con pocos recursos iniciales.

Medida	¿Qué hacer?	Costo	Beneficio	Aplicabilidad Local
	autenticación en equipos críticos.			
Copias de seguridad y planes de recuperación	Respaldos regulares, verificación de integridad, plan de restauración de controladores.	Bajo a moderado (depende del volumen).	Rápida recuperación tras incidentes; reduce pérdidas por paros.	Prioritario en cualquier planta.
Monitoreo pasivo y correlación de eventos	Sensores pasivos (SPAN/TAP), herramientas de análisis.	Moderado (hardware básico y software).	Detección temprana de anomalías, apoya decisiones; reduce MTTD.	Recomendado; respaldado por CISA.
Detección basada en comportamiento (IA)	Pilotos en líneas críticas para entrenar modelos.	Moderado-alto (según despliegue).	Buen retorno: menos fallos y falsos positivos.	Vía experimental costo-efectiva para PYMES.
Compra segura por diseño	Exigir productos con prácticas seguras, soporte	Ligeramente mayor al inicio.	Ahorro a mediano plazo; menos	Respaldado por guías internacionales (CISA).

Medida	¿Qué hacer?	Costo	Beneficio	Aplicabilidad Local
	y actualizaciones.		vulnerabilidades integradas.	
Proveedores gestionados (MSSP/OT services)	Contratar servicios de monitoreo, parches y respuesta.	Recurrente (suscripción).	Práctico y asequible; acelera madurez sin expertos propios.	Muy útil en PYMES.

Nota. La tabla resume medidas técnicas con su costo, beneficio y aplicabilidad local, priorizando acciones de bajo costo y alto impacto para fortalecer la seguridad.

Marco Conceptual

Automatización Electrónica

La automatización electrónica hace referencia al uso de dispositivos y sistemas electrónicos como sensores, actuadores, controladores lógicos programables (PLC), microcontroladores, y software especializado para operar procesos sin intervención humana directa (Holguin & Romero, 2024). Esta tecnología permite controlar, supervisar y optimizar las operaciones industriales de forma precisa y continua.

La automatización industrial es “el uso de tecnologías electrónicas y computacionales junto con sistemas mecánicos para realizar tareas con mínima o nula intervención del ser humano (Nieto, 2006)”. Esto implica la integración de sistemas de control automático que permiten realizar actividades repetitivas o complejas de manera eficiente y con menor margen de error.

Una de las principales funciones de la automatización electrónica es reducir la variabilidad en los procesos y aumentar la confiabilidad del sistema productivo, al tiempo que mejora la seguridad del personal al evitar su exposición a tareas peligrosas (Obregon, 2025).

Procesos Productivos Industriales

Los procesos productivos industriales se definen como el conjunto organizado de actividades y operaciones necesarias para transformar materias primas en productos terminados (Eras-Agila & Meleán-Romero, 2021).Estos procesos incluyen etapas como el diseño, la planificación, la fabricación, el control de calidad y la distribución de los bienes.

Desde el enfoque de la ingeniería de producción, un proceso productivo se clasifica en diferentes tipos: por lotes, continuo, en línea, etc. Dependiendo de la naturaleza del producto y del volumen de producción. Así, los procesos industriales son “sistemas interrelacionados que

utilizan recursos materiales, humanos y tecnológicos para alcanzar una finalidad productiva concreta (Hernández et al, 2021)".

La incorporación de tecnologías de automatización electrónica en estos procesos permite mejorar indicadores como la eficiencia operativa, la calidad del producto y la trazabilidad de la producción, generando entornos de trabajo más organizados, limpios y seguros (Palomero, 2024).

Industria 4.0

El concepto de Industria 4.0, también llamada la cuarta revolución industrial, fue introducido en Alemania en 2011 y hace referencia a la digitalización total de los procesos de producción mediante la integración de tecnologías como el Internet de las cosas (IoT), la inteligencia artificial (IA), el big data, la robótica colaborativa, y los sistemas ciber físicos (CPS) (Aguilar, 2021). Industria 4.0 implica "la organización de las cadenas de valor industrial basada en sistemas ciber físicos (González-González et al, 2023), que permiten la comunicación autónoma entre máquinas, productos, sistemas y personas".

En este contexto, la automatización electrónica forma parte esencial de la Industria 4.0, al actuar como el puente entre el hardware, es decir, los sensores, actuadores, controladores y el software inteligente que es el análisis de datos, algoritmos, aprendizaje automático (Peña et al, 2022). Gracias a esta integración, las industrias pueden lograr mayor flexibilidad, eficiencia energética, personalización masiva de productos y adaptabilidad en tiempo real a las condiciones del mercado (Castrillo, 2023).

Transformación Digital Industrial

La transformación digital en la industria se refiere al proceso de incorporación progresiva de tecnologías digitales en todos los niveles de la empresa, desde la producción hasta la gestión y

la comercialización (Do et al, 2023). Este proceso incluye la automatización de procesos, el uso de datos para la toma de decisiones, la conectividad entre dispositivos y el rediseño de procesos productivos para que sean más ágiles, eficientes y sostenibles (Rodríguez et al, 2024).

Por eso**,** la transformación digital no solo se trata de tecnología, sino de cambiar la mentalidad empresarial hacia una cultura de innovación continua, basada en el análisis de datos, la flexibilidad operativa y la mejora permanente (Rodríguez & Camacho, 2023).

Los Sistemas Sociotécnicos

Es una teoría que plantea que para que la automatización sea exitosa, no basta con integrar tecnología; también debe considerarse el impacto en los trabajadores, las dinámicas organizacionales y el entorno y diseñar procesos equilibrando lo técnico con lo humano (Iglesias & Fasce, 2024).

Modelo TAM (Technology Acceptance Model)

Propuesto por Davis (1989), este modelo explica cómo la percepción de utilidad y facilidad de uso de una tecnología influye en su aceptación (Marín, 2023). Es útil para analizar la resistencia o aceptación de los trabajadores ante la automatización electrónica.

Metodología

Tipo de Investigación

El tipo de investigación seleccionado para esta monografía es descriptivo, ya que su propósito es analizar y explicar de manera detallada las tecnologías de automatización electrónica utilizadas en la industria entre 2020 y 2025, así como los beneficios, desafíos y tendencias emergentes asociadas a ellas. Según (Alban et al, 2020), la investigación descriptiva se enfoca en detallar con precisión fenómenos, situaciones, personas o contextos, sin buscar establecer relaciones causales o intervenir en las variables observadas.

Este tipo de estudio es apropiado cuando se quiere "conocer cómo son y cómo se manifiestan ciertos fenómenos, y cuáles son sus características más importantes (Sampieri y otros, 2013)". En este caso, se pretende caracterizar tecnologías como el mantenimiento predictivo, la robótica colaborativa, los gemelos digitales y el edge computing dentro del contexto de la industria 4.0.

Enfoque

El enfoque adoptado es mixto, ya que se integran tanto elementos cuantitativos como cualitativos. Esta combinación permite obtener una visión más amplia, objetiva y comprensiva del fenómeno estudiado.

El enfoque cuantitativo permite medir, comparar y analizar datos numéricos relacionados con la implementación de las tecnologías, como, por ejemplo, reducción de tiempos, costos o mejoras en eficiencia (Cutanda-López, 2021). Por su parte, el enfoque cualitativo permite comprender las experiencias, percepciones y desafíos humanos asociados a la adopción de la automatización, para analizar su impacto en el entorno laboral e industrial.

Según Creswell (2013), los enfoques mixtos son útiles cuando se quiere comprender un fenómeno tanto desde su dimensión estadística como desde sus implicaciones sociales y culturales, ya que "integran datos cuantitativos y cualitativos en un mismo estudio para proporcionar una perspectiva más completa del problema de investigación (Luza et al, 2023)"

Este enfoque permite medir el nivel de adopción y uso de tecnologías en los últimos cinco años, es decir, desde un análisis cuantitativo y comprender las razones, barreras y opiniones frente a dicha adopción, es decir, desde el punto de vista cualitativo. Además de relacionar los datos objetivos con las percepciones humanas para una visión equilibrada del fenómeno, por lo que favorece la triangulación de información, es decir, la verificación cruzada de los hallazgos a través de diferentes fuentes, técnicas y perspectivas, lo cual fortalece la validez del estudio.

Método de Recolección de Datos

Para llevar a cabo esta investigación se emplearán dos métodos de recolección de datos:

Revisión Documental y Bibliográfica como Fuente Secundaria

Consistirá en la búsqueda, análisis y organización de documentos académicos, tesis, artículos científicos, informes técnicos y libros relacionados con automatización electrónica industrial, publicados entre los años 2020 y 2025.

Esta información se utilizará para construir tablas comparativas de tecnologías, analizar ventajas y desventajas, identificar tendencias emergentes y proyecciones futuras y extraer datos relevantes para mapas mentales y líneas de tiempo.

Instrumentos de Apoyo Interpretativo

Aunque no se realizará una recolección de datos de campo, se emplearán herramientas visuales para el análisis cualitativo e interpretativo de la información secundaria, tales como mapas mentales para organizar beneficios y desafíos y tablas comparativas para evidenciar características, aplicaciones, ventajas y limitaciones como se relacionó en el primer método de recolección de datos.

Justificación del Diseño Metodológico

La elección de un diseño metodológico descriptivo con enfoque mixto se justifica por la necesidad de abordar un fenómeno técnico (automatización) desde una perspectiva integral, considerando tanto su funcionamiento objetivo como su impacto subjetivo en el contexto industrial.

El enfoque descriptivo permite mostrar con claridad el estado actual de las tecnologías de automatización electrónica y facilita la comprensión de sus aplicaciones y beneficios reales, el uso combinado de datos cuantitativos y cualitativos enriquece el análisis, al no quedarse únicamente en cifras, sino ir más allá e incluir aspectos humanos, sociales y éticos y la revisión documental proporciona un respaldo académico confiable, necesario para fundamentar teóricamente la investigación y construir un análisis serio y bien estructurado.

Esta metodología, además, permite al lector entender no solo qué tecnologías se están usando, sino cómo están transformando los procesos productivos y qué desafíos deben afrontar las industrias para adaptarse a los cambios de la cuarta revolución industrial.

Tabla 6

Tabla de Coherencia Metodológica

Objetivo específico	Método	Instrumento	Resultado esperado
Identificar las principales tecnologías de automatización electrónica implementadas en la industria durante el período 2020-2025.	Revisión documental y bibliográfica.	Tablas comparativas.	Listado organizado de tecnologías (mantenimiento predictivo, robótica colaborativa, gemelos digitales, edge computing).
Evaluar los beneficios y desafíos asociados con la integración de estas tecnologías en los procesos productivos.	Análisis cualitativo de fuentes secundarias.	Mapas mentales y tablas comparativas.	Panorama de ventajas (eficiencia, reducción de costos) y desafíos (inversión, capacitación).
Determinar las tendencias emergentes y futuras en la automatización electrónica industrial.	Revisión documental y análisis de proyecciones en informes y artículos	Tablas comparativas.	Identificación de tendencias (IA, analítica avanzada, IoT industrial, seguridad digital) y

Objetivo específico	Método	Instrumento	Resultado esperado
			proyecciones hacia el futuro.

Nota. La tabla muestra la coherencia entre los objetivos, los métodos aplicados y los instrumentos usados, asegurando que cada objetivo tenga un resultado claro y alcanzable.

Discusión Teórica

El análisis teórico permitió comprender cómo la automatización electrónica ha evolucionado en la Industria 4.0, con la integración de tecnologías digitales que optimizan la eficiencia, la calidad y la seguridad en los procesos productivos. Los autores revisados mencionan que esta transformación tecnológica no busca sustituir tareas humanas, sino potenciar la colaboración entre personas y máquinas, para lograr una producción más inteligente, sostenible y segura (Romero & Pulido, 2024).

Desde los fundamentos de los sistemas sociotécnicos, la automatización no puede analizarse solo desde la perspectiva técnica, sino también humana y organizacional. Esto implica diseñar sistemas que equilibren el bienestar del trabajador con la eficiencia de las operaciones (Iglesias & Fasce, 2024). En ese sentido, el Modelo TAM explica que la aceptación de nuevas tecnologías en los entornos industriales depende de la percepción de utilidad y facilidad de uso, por lo que las empresas deben acompañar los cambios tecnológicos con procesos de capacitación y adaptación cultural.

La revisión documental muestra las tendencias emergentes como el mantenimiento predictivo, la robótica colaborativa, los gemelos digitales y el edge computing los cuales son nuevos avances para la industria moderna. Cada una de estas tecnologías contribuye a la mejora de la productividad, la seguridad y la continuidad operativa. Por ejemplo, el mantenimiento predictivo, basado en el análisis de datos y sensores IoT, permite anticipar fallas y reducir paradas no planificadas (Riaño & León, 2023), y por su parte, los cobots facilitan la colaboración entre las personas y las máquinas manteniendo la seguridad (Salimbeni & Mamani, 2020).

De igual forma, las prácticas emergentes de protección, como la Arquitectura Zero Trust (ZTA), la detección de anomalías mediante inteligencia artificial, las redes privadas industriales

(5G/LTE NPN) y el monitoreo continuo en tiempo real, se han convertido en pilares de la ciberseguridad industrial. Estas estrategias permiten a las plantas reducir los riesgos de intrusión, proteger los datos sensibles y garantizar la disponibilidad de los sistemas críticos, reforzando los principios básicos de la seguridad de la información: confidencialidad, integridad y disponibilidad (Balladares & Chichande, 2020).

De la discusión teórica también es posible ver que, aunque estas tecnologías ofrecen grandes beneficios, aún en el contexto colombiano hay muchos desafíos por superar, especialmente en las pequeñas y medianas empresas (PYMES), en las cuales factores como los costos iniciales, la falta de personal especializado y la resistencia al cambio pueden limitar la implementación de las mismas. No obstante, el enfoque gradual propuesto en esta investigación, iniciando con el diagnóstico, las medidas básicas de seguridad, la capacitación y la adopción tecnológica progresiva, permite avanzar hacia una industria digitalizada.

Hallazgos

Como hallazgos, es posible decir que; en Colombia, la incorporación de tecnologías como la robótica, el IoT y la inteligencia artificial aún se encuentra en una etapa intermedia. Sin embargo, hay un crecimiento impulsado por la necesidad de aumentar la eficiencia operativa y reducir costos de mantenimiento.

Aunque las empresas reconocen la importancia de la protección de datos y sistemas, muchas aún no se aplican estrategias integrales de seguridad en entornos OT (tecnología operativa). La mayoría se centra en medidas reactivas, sin políticas estructuradas de prevención o respuesta a posibles incidentes cibernéticos.

La aplicación de Zero Trust, el monitoreo continuo y la detección de anomalías con IA tiene sus beneficios directos en la reducción de tiempos de inactividad y la contención de incidentes. Estas tecnologías no solo protegen los activos industriales, sino que también mejoran la continuidad operativa.

El modelo por fases como el diagnóstico, las medidas básicas, la capacitación y la mejora tecnológica, permite que las pequeñas y medianas empresas puedan fortalecer su seguridad de forma sostenible.

Uno de los hallazgos más importantes es que la tecnología por sí sola no garantiza seguridad ni eficiencia. Es necesario que haya primero una formación constante del personal de la empresa, para que las herramientas sean utilizadas correctamente y se genere una cultura organizacional basada en la prevención y la innovación digital.

La transformación digital no debe entenderse como una forma de modernización tecnológica, sino como una reconfiguración de la estructura productiva y cultural de la

organización, donde la toma de decisiones basada en datos se convierte en la parte principal de la gestión industrial.

Conclusiones

La automatización electrónica es el pilar de la Industria 4.0, integra sistemas de hardware, software e inteligencia artificial que optimizan los procesos productivos, reducen la intervención humana y aumentan la precisión operativa. Por ello, su implementación no solo mejora la eficiencia y la calidad, sino que también impulsa la transformación de los entornos industriales hacia una producción más flexible y segura. Este cambio representa una evolución muy importante en la forma en que las organizaciones gestionan sus recursos, priorizando la confiabilidad, la trazabilidad y la seguridad en cada etapa del proceso productivo.

Las tendencias emergentes, como el mantenimiento predictivo, la robótica colaborativa, los gemelos digitales y el edge computing, están redefiniendo el panorama industrial contemporáneo. Estas tecnologías permiten anticipar fallas, optimizar la colaboración entre las personas y las máquinas, simular escenarios productivos y procesar información en tiempo real. Gracias a su aplicación, las industrias logran una gestión más sostenible y eficiente, al mismo tiempo que fortalecen su competitividad y capacidad de adaptación ante los desafíos tecnológicos y económicos de la era digital.

En materia de ciberseguridad industrial, prácticas emergentes como la Arquitectura Zero Trust, la detección de anomalías mediante inteligencia artificial y las redes privadas 5G/LTE son estrategias muy importantes para garantizar la protección de los sistemas automatizados. Estas soluciones permiten reducir vulnerabilidades, segmentar procesos críticos y mantener la continuidad operativa frente a ciberataques o fallos inesperados. En este sentido, la seguridad digital deja de ser un aspecto complementario para convertirse en un componente estructural del ecosistema industrial moderno.

Para el contexto colombiano, la adopción de estas tecnologías debe hacerse de forma gradual, considerando las limitaciones económicas y técnicas de las empresas, especialmente de las pequeñas y medianas industrias. La aplicación de medidas de bajo costo y alto impacto como el inventario de activos, la segmentación de redes, la implementación de copias de seguridad y la capacitación continua del personal, permiten la protección y eficiencia de los procesos automatizados, facilitando la sostenibilidad tecnológica sin comprometer la estabilidad productiva.

Finalmente, la transformación digital industrial no depende únicamente de la incorporación de nuevas tecnologías, sino también del fortalecimiento de las competencias humanas, la gobernanza tecnológica y la consolidación de una cultura de innovación permanente. Por lo tanto, la automatización electrónica redefine la manera de producir, trabajar y proteger los entornos industriales equilibrando el aspecto tecnológico y humano.

Recomendaciones

Fortalecer la formación del personal operativo y técnico en competencias digitales, ciberseguridad industrial y mantenimiento predictivo, para que puedan usar correctamente las nuevas tecnologías y mantener los sistemas seguros.

Adoptar un enfoque por fases, priorizando acciones de bajo costo y alto impacto como el inventario de activos, la segmentación de redes, las copias de seguridad y la creación de políticas básicas de seguridad antes de invertir en tecnologías más avanzadas.

Fomentar alianzas públicas y privadas entre el Estado, universidades y empresas para crear programas de acompañamiento técnico y capacitación, especialmente dirigidos a PYMES industriales del país.

Al adquirir equipos o sistemas, se debe exigir a los proveedores que los productos cuenten con certificaciones de seguridad, soporte técnico y actualizaciones continuas, o implementar las llamadas políticas de copra segura por diseño, para reducir las vulnerabilidades desde el origen.

instalar sistemas que revisen y analicen en tiempo real el funcionamiento de las máquinas para detectar rápidamente fallas o ciberataques, asegurando la disponibilidad de los procesos productivos.

Promover una cultura organizacional de seguridad digital, en la cual todos los niveles de la empresa comprendan su rol en la protección de los sistemas automatizados. Se deben promover hábitos seguros y una actitud preventiva frente al uso de la tecnología.

Actualizar los marcos regulatorios nacionales para incluir de manera más explícita las normas y buenas prácticas internacionales en ciberseguridad industrial, de acuerdo con las exigencias de la Industria 4.0 global.

Referencias

ACIS . (13 de junio de 2025). *Asociación Colombiana de Informática Sistemas y Tecnologías Afines*. Colombia reporta fuerte alza en ciberataques a dispositivos conectados: +31 % en 2024: https://www.acis.org.co/blog/noticias-2/colombia-reporta-fuerte-alza-en-ciberataques-a-dispositivos-conectados-31-en-2024-1095

Aguilar, L. J. (2021). *Internet de las cosas: Un futuro hiperconectado: 5G, Inteligencia Artificial, Big Data, Cloud, Blockhain y ciberseguridad* . Marcombo. https://doi.org/https://books.google.es/books?hl=es&lr=&id=t816EAAAQBAJ&oi=fnd&pg=PR7&dq=El+concepto+de+Industria+4.0,+tambi%C3%A9n+llamada+la+cuarta+revoluci%C3%B3n+industrial,+fue+introducido+en+Alemania+en+2011+y+hace+referencia+a+la+digitalizaci%C3%B3n+total+de+los+p

Alban et al. (2020). Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción). *RECIMUNDO, 4*(3), 163–173. https://doi.org/https://doi.org/10.26820/recimundo/4.(3).julio.2020.163-173

Antoni Garrell, L. G. (2019). *La Industria 4.0 en la sociedad digital.* Marge Books . https://doi.org/https://books.google.com.pe/books?id=YnSIDwAAQBAJ&printsec=frontcover&hl=es#v=onepage&q&f=false

Baeza, V. M. (2022). Prototipo para mejorar la automatización de procesos en las infraestructuras en el sector del agua. *Universitat Oberta de Catalunya*. https://doi.org/http://hdl.handle.net/10609/137869

Balladares, I. A., & Chichande, A. P. (2020). Seguridad informática aplicada a la defensa y seguridad basada en principios jurídicos. *Alternativas, 21*(2), 53-58. https://doi.org/https://dialnet.unirioja.es/servlet/articulo?codigo=9453020

Bandera, E. F., & Contreras, S. L. (2020). Importancia de la implementación de firewall en redes empresariales como mecanismo para la protección de información. *: Ciencia e Ingeniería: Revista de investigación interdisciplinar en biodiversidad y desarrollo sostenible, ciencia, tecnología e innovación y procesos productivos industriales, 7*(1). https://doi.org/https://dialnet.unirioja.es/servlet/articulo?codigo=8742508

Barcenas, A. (19 de mayo de 2025). Ciberataques en aumento: industrias colombianas enfrentan una amenaza silenciosa que ya impacta su operación. *Rockwell Automation; comunicado de prensa* . https://www.rockwellautomation.com/es-pr/company/news/press-releases/ciberataques-en-aumento-en-industria-colombiana.html.

Barranco, M. C. (2021). Sabotaje informático a infraestructuras críticas. Análisis de la realidad criminal recogida en los artículos 264 y 264 bis del Código penal. Especial referencia a su comisión con finalidad terrorista. *Revista de Derecho Penal y Criminología*(25), 77-124. https://doi.org/https://dialnet.unirioja.es/servlet/articulo?codigo=8046490

BBC News Mundo. (11 de octubre de 2015). *El virus que tomó control de mil máquinas y les ordenó autodestruirse: El ataque del gusano Stuxnet destruyó 1000 máquinas en la central nuclear de Natanz, Irán*. BBC News Mundo: https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet

Burgos et al. (2025). El rol de la inteligencia artificial en la automatización y la gestión de la cadena de suministro. *Gestión administrativa, Deporte y Educación, 5*(1), 390-414. https://doi.org/https://doi.org/10.63549/rg.v5i1.607

Bustamante-Limones et al. (2024). Evaluación del uso de gemelos digitales en los sistemas de producción. *AiBi Revista de Investigación, Administración e Ingeniería, 12*(3), 195–204. https://doi.org/10.15649/2346030X.4382

Bustamante-Limones, A., Rodriguez-Borges, C., & Pérez-Rodriguez, J. A. (2024). Evaluación del uso de gemelos digitales en los sistemas de producción. *AiBi Revista de Investigación, Administración e Ingeniería, 12*(3), 195–204. https://doi.org/10.15649/2346030X.4382

Campos, N. O., & Cavada, J. C. (2021). Análisis para la implementación de la tecnología 5g basados en el modelo GSMA y su interacción con el internet de las cosas en Ecuador. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*(43). https://doi.org/10.17013/risti.40.38-54

Castillo, M., & Ominami, C. (2024). Transformación productiva y nueva actualidad de las políticas industriales en América Latina. *Estudios internacionales (Santiago), 56*(207). https://doi.org/http://dx.doi.org/10.5354/0719-3769.2024.73995

Castrillo, V. J. (2023). Transformación e Impacto de la Industria 4.0 en la Logística Internacional y una Cadena. *Trabajo de grado presentado como requisito para optar al título de:Profesional en Comercio Internacional* . Santa Marta, Universidad Antonio Nariño,Facultad de Ciencias Económicas y Administrativas,Programa de Comercio Internacional, Colombia.

Cathles et al. (2022). *¿Cómo aprovechar la inercia para digitalizar a las pymes de la región? Convivir con el coronavirus.* Banco Interamericano de Desarrollo: https://interactive-publications.iadb.org/convivir-con-el-coronavirus/como-aprovechar-la-inercia-para-digitalizar-a-las-pymes

CEPAL. (2020). *La educación en tiempos de la pandemia de COVID-19. Informe Especial de la CEPAL.* CEPAL; UNESCO.

Chalacán et al. (2021). Software educativo heterogéneo y la educación virtual, en tiempos de Covid-19. *Revista Conrado, 17*(S2), 142–148. https://doi.org/https://conrado.ucf.edu.cu/index.php/conrado/article/view/2002

Chicaiza et al. (2024). El Gemelo Digital y su aplicación en la Automática. *Revista Iberoamericana de Automática e Informática Industrial, 21*(2), 91–115. https://doi.org/10.4995/riai.2024.20175

Chuquitarco, A. C., & Tapaicela, M. T. (2022). Diseño de un sistema SCADA para el control de procesos virtuales. *Tesis* . Latacunga, Ecuador , Repositorio Universidad Técnica de Cotopaxi : http://repositorio.utc.edu.ec/handle/27000/9238.

CISA. (7 de febrero de 2024). *Agencia de Ciberseguridad y Seguridad de Infraestructura.* Aviso sobre ciberseguridad : https://www.cisa.gov/sites/default/files/2024-10/aa24-038a_csa_prc_state_sponsored_actors_compromise_us_critical_infrastructure_3_ES.pdf

Coarite, R. R. (2020). Sistema de información basado en un enfoque de procesos, para la optimización de la otorgación de créditos. Caso empresa Comebra. *Trabajo de grado para optar al título de Licenciatura en Ingeniería de Sistemas*. Repositorio Institucional de la Universidad Pública de El Alto, Bolivia: http://repositorio.upea.bo/jspui/handle/123456789/185.

Colombia, P. d. (26 de mayo de 2015). Decreto 1078 de 2015 Sector de Tecnologías de la Información y las Comunicaciones. *Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones*. Colombia : https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=77888.

Congreso de Colombia . (5 de enero de 2009). Ley 1273 de 2009. *Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"*. Colombia : https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492.

Congreso de Colombia . (17 de octubre de 2010). Ley 1581 de 2012. *Por la cual se dictan disposiciones generales para la protección de datos personales.* Colombia : https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981. https://doi.org/https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Congreso de la República . (31 de diciembre de 2008). Ley 1266 de 2008. *Parcialmente Reglamentada por el Decreto 1081 de 2015. Ley estudiada por la Corte Constitucional mediante Sentencia C-1011 de 2008*. Colombia : https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488.

Cortés-Llanganate, L. H., & Quevedo-Sacoto, A. S. (2024). Soluciones de monitoreo de ciberseguridad en redes industriales basadas en Inteligencia Artificial. Revisión de literatura. *593 Digital Publisher CEIT, 9*(6), 5-17 . https://doi.org/10.33386/593dp.2024.6.2629

Cutanda-López, M. T. (2021). Método mixto de investigación: pertinencia y dificultades en el estudio programas de reenganche. *Revista Caribeña de Ciencias Sociales*, 31-48. https://doi.org/https://doi.org/10.51896/caribe/MGUI5478

Díaz, M. E., & Rodríguez, G. A. (2025). *Ciberseguridad en la Frontera Digital: desafíos y oportunidades en los nuevos ecosistemas tecnológicos empresariales.* Sello Editorial ESDEG . https://doi.org/10.25062/9786287818002

Do et al. (2023). Desafíos de la Transformación Digital en las PYMES. *Informe Científico Técnico UNPA, 15*(1), 200-229. https://doi.org/https://doi.org/10.22305/ict-unpa.v15.n1.941

Duitama, K. P. (12 de julio de 2025). *Colombia fue el cuarto país con más ciberataques en la región, 36.000 millones en 2024*. La República : https://www.larepublica.co/internet-economy/colombia-tuvo-36-000-millones-de-ciberataques-4178202

Enderica, C. A., & Molina, C. D. (27 de agosto de 2024). Diseño y simulación de un sistema automatizado para el proceso de mezclado en plantas de producción de bebidas carbonatadas. La Libertad: Universidad Estatal Península de Santa Elena, 2024: https://repositorio.upse.edu.ec/handle/46000/12073.

Eras-Agila, R. d., & Meleán-Romero, R. (2021). Ecosistemas de producción camaroneros . *INNOVA Research Journal, 6*(3). https://doi.org/https://dialnet.unirioja.es/servlet/articulo?codigo=8226345

Ferre, J. D. (2021). Robótica aplicada, un paso ya presente en el futuro. Análisis de mercado consecuencias de implantación e introducción en las PYMES. *Tesis máster*. E.T.S.I. Industriales (UPM): https://oa.upm.es/68769/.

Ferreira, J. G. (2023). El impacto de la inteligencia artificial en los trabajadores despedidos por automatización de servicios. *Revista CES Derecho, 14*(3), 62–81. https://doi.org/https://doi.org/10.21615/cesder.7416

Flores, J. (12 de mayo de 2020). *Practicada la primera operación teleasistida con 5G*. National Geographic; España : https://www.nationalgeographic.com.es/ciencia/actualidad/practicada-primera-operacion-teleasistida-5g_13948

Gandino, S. S., & Mamani, D. (2020). Marco de referencia para la incorporación de Cobots en líneas de manufactura. *PODIUM*(38), 159–180. https://doi.org/10.31095/podium.2020.38.10

González-González et al. (2023). El impacto de las últimas tecnologías en la transformación de la industria. *Economía industrial*(428), 51-57. https://doi.org/https://dialnet.unirioja.es/servlet/articulo?codigo=9364302

Guamán et al. (2022). Automatizar procesos de producción repetitivos en las PYMES con robots colaborativos. *Revista Universidad y Sociedad, 14*(2). https://doi.org/http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202022000200220

Handzel, A. M. (septiembre de 2020). Implementación del Núcleo de Red LTE/5G Virtualizado . *Trabajo Fin de Grado presentado en la Escuela Técnica Superior de Ingeniería de Telecomunicación a, para la obtención del Título de Graduado en Ingeniería de Tecnologías y Servicios de Telecomunicación*. Valencia , Universidad Politécnica de Valencia, España : https://core.ac.uk/download/pdf/335619246.pdf.

Hernández et al. (2021). Propuesta de cadena de valor en la fabricación de paneles fotovoltaicos. *Escritos Contables y de Adminstración, 12*(2), 68-98. https://doi.org/https://dialnet.unirioja.es/servlet/articulo?codigo=8284733

Hernández, L. C. (11 de 02 de 2025). Mejora en los procesos del área de compras y presupuesto en constructora Celaque. *Tesis de grado*. Universidad Tecnológica Centroamericana UNITEC: https://repositorio.unitec.edu/items/1fc2cef3-ccb2-4308-b0bc-015ab994c415.

Hernandez, P. R., & Cruz, D. V. (2022). Los Asistentes virtuales basados en Inteligencia Artificial. *ReCIBE. Revista electrónica de Computación, Informática, Biomédica y*

Electrónica, 11(2), 1-11. https://doi.org/https://www.redalyc.org/journal/5122/512275401001/html/

Holguin, K. J., & Romero, M. D. (2024). Diseño e implementación de un módulo didáctico de instrumentación con integración a un servidor web node-red mediante mini plc logo, para el laboratorio de electrónica y digitales de la Facultad de Ciencias de la Vida y Tecnologías. *Tesis de pregrado*. Repositorio Universidad Laica Eloy Alfaro de Manabí - Uleam, Manta, Ecuador: https://repositorio.uleam.edu.ec/handle/123456789/6969.

Ibarra, A. Y., & Escobar, A. M. (marzo de 2025). Implementación de una arquitectura de acceso a la red de Confianza Cero para mejorar la seguridad perimetral de una empresa retail. *Tesis para optar el Título Profesional de Ingeniero de Redes y Comunicaciones*. Lima, Repositorio Universidad Tecnológica del Perú, Perú: https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/12628/A.Sanchez_A.Reyes_Tesis_Titulo_Profesional_2025.pdf?sequence=1&isAllowed=y.

ICONTEC. (2013). NORMA TÉCNICA NTC-ISO-IEC COLOMBIANA 27001 . *Seguridad de la información, ciberseguridad y protección de la privacidad -Sistemas de gestión de la seguridad de la información -Requisitos*. Colombia , Editada por el Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC) : https://www.iso.org/standard/27001.

Iglesias, L., & Fasce, I. P. (10 de 12 de 2024). Análisis del cambio organizacional y su impacto en el capital humano ante la implementación de tecnologías 4.0. *Trabajo Final de la Carrera Ingeniería Industrial*. Universidad Nacional de Mar del Plata, Facultad de Ingeniería.Departamento de Ingeniería Industrial: http://rinfi.fi.mdp.edu.ar/handle/123456789/988.

Ingertec. (25 de marzo de 2025). *Norma IEC 62443. Ciberseguridad Industrial*. Ingertec: https://ingertec.com/norma-iec-62443/

Isaza, J. L. (2024). Tesis de Maestría en Seguridad Informática sobre Ciberseguridad en la convergencia entre redes IT y OT. *Transformación digital: Convergencia segura entre redes IT y OT*. Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería , Biblioteca digital de la Universidad de Buenos Aires , Argentina : http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1367_MoraIsazaJL.pdf.

Jácome et al. (2022). Variantes de la Tecnología OPC-UA y su utilización en la interconexión de Controladores Industriales con diferentes protocolos de comunicación. *Conectividad, 3*(2), 56-74. https://doi.org/https://dialnet.unirioja.es/servlet/articulo?codigo=9066537

Jiménez, T. P. (2023). Análisis de los protocolos y sistemas de respaldo implementados en los servidores del ISP AVCAMTECH.NET. *Trabajo de grado previo a la obtención del título de Ingeniera en Sistemas de Información* . Ecuador , Universidad Técnica de Babahoyo : http://dspace.utb.edu.ec/handle/49000/14998.

Kaspersky. (10 de junio de 2025). *Uno de cada cinco sistemas industriales en América Latina fue blanco de malware en 2025: Kaspersky*. Kaspersky: https://latam.kaspersky.com/about/press-releases/uno-de-cada-cinco-sistemas-industriales-en-america-latina-fue-blanco-de-malware-en-2025-kaspersky?srsltid=AfmBOoqzTBsuo9rP2rWGeafiyFJ3-ERBHrPaJPPsyAXbh5Z-FDM-0FXq

Lalon-Pinduisaca, S. A., & Coello-Panchana, A. J. (2025). Impacto de la inteligencia artificial en el asesoramiento tributario mediante un estudio de Caso en la Cafetería Casa Café.

Revista Científica Zambos, Revolución Científica a Través de la Colaboración Multidisciplinaria, 4(1), 310-327. https://doi.org/https://doi.org/10.69484/rcz/v4/n1/92

Llanes, R. P., & García, A. O. (2021). Sistemas para la detección de intrusiones en redes de datos de instituciones de salud. *Revista Cubana de Informática Médica, 13*(2). https://doi.org/https://revinformatica.sld.cu/index.php/rcim/article/view/440/pdf_1

Loachamín, P. F. (2023). Análisis Comparativo de Plataformas de Siem y las Soluciones de Detección y Respuesta Extendida. *Tesis de maestría en Seguridad Informática* . Quito , Repositorio Universidad Israel , Ecuador: http://repositorio.uisrael.edu.ec/bitstream/47000/3558/1/UISRAEL-EC-MASTER-SEG-INF%20-378.242-2023-006.pdf.

López et al. (2024). Modelo de Reingeniería de Software para Sistemas Legados de una Institución de Educación Superior en México. *Revista Científica Multidisciplinar, 8*(2), 1164-1179. https://doi.org/10.37811/cl_rcm.v8i2.10559

Luza et al. (2023). *Métodos mixtos de investigación.* Instituto Universitario de Innovación Ciencia y Tecnología Inudi Perú S.A.C. https://doi.org/https://doi.org/10.35622/inudi.b.106

M et al. (2019). Una revisión a la realidad de la automatización de las pruebas del software. *Computación y Sistemas, 23*(1). https://doi.org/10.13053/cys-23-1-2782

Marín, A. Á. (2023). Aceptación Tecnológica de la Realidad Aumentada en la Formación de Ingenieros en Educación Superior. *Tesis de doctorado* . Programa de Doctorado en Tecnologías de la Información y las Comunicaciones , Universidad Rey Juan Carlos: https://hdl.handle.net/10115/28232.

Martín, S. (28 de agosto de 2025). *Estado de la ciberseguridad, junio 2025*. Ubillibet: https://www.ubilibet.com/es/resultados-ciberseguridad-junio-2025/

Martínez et al. (2023). Beneficios de implementar la automatización en la industrialización de procesos. *Innovación y desarrollo tecnológico, revista digital, 15*(3). https://doi.org/https://iydt.wordpress.com/wp-content/uploads/2023/07/3_24_beneficios-de-implementar-la-automatizacion1.pdf

Martínez, A. S. (julio de 2023). Estudio y análisis de los sistemas de información empresarial e implantación de un CRM en una PYME. Repositorio Universidad de Cantabria : https://hdl.handle.net/10902/29626.

Martínez, S. J. (2024). Innovación en la gestión empresarial nuevas tecnologías y su rol en la eficiencia organizacional. *Edición regular: Investigaciones Interdisciplinarias. SAPIENS International Multidisciplinary Journal,, 1*(1), 148-165. https://doi.org/https://doi.org/10.71068/jeejby43

Mata, J. A. (18 de noviembre de 2022). Diseño de un sistema de gestión de salud y seguridad ocupacional basado en el Acuerdo Gubernativo 229-2014 en una empresa de proyectos eléctricos ubicada en la ciudad de Guatemala. *Tesis de licenciatura* . Licenciatura thesis, Universidad de San Carlos de Guatemala.: http://www.repositorio.usac.edu.gt/17991/.

Mundial, G. B. (5 de marzo de 2024). *Acelerado por la COVID y la inteligencia artificial, el panorama digital en el mundo sigue siendo dispar*. Grupo Banco Mundial : https://www.bancomundial.org/es/news/press-release/2024/03/05/accelerated-by-covid-and-ai-global-digital-landscape-remains-uneven

Muñoz-Pinzón, D. S., Valencia-Rivero, K. T., Caviativa-Castro, Y. P., & Castillo-Bustos, J. S. (2024). Estado actual de la adopción de la industria 4.0 en pymes colombianas: desafíos y

oportunidades. *Revista Politécnica, 20*(39), 99–118. https://doi.org/10.33571/rpolitec.v20n39a7

Muriel, J. T. (junio de 2023). Análisis del nuevo paradigma de la industria 5.0 y su efecto en la estrategia de una empresa tecnológica. Murcia , Repositorio Universidad Católica de Murcia Ta, Espain : http://hdl.handle.net/10952/7678.

Nieto, E. C. (2006). Manufactura y automatización. *Ingeniería e Investigación, 26*(3), 120-128. https://doi.org/https://www.redalyc.org/pdf/643/64326315.pdf

Niño, F. Y. (2023). Ransomware, una amenaza latente en Latinoamérica. *InterSedes, Revista electrónica de las sedes regionales de la Universidad de Costa Rica, XXIV*(49), 92-119. https://doi.org/10.15517/isucr.v24i49

NIST. (26 de febrero de 2024). *El Marco de Seguridad Cibernética (CSF) 2.0 del NIST.* National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología): 10.6028/NIST.CSWP.29.spa

Obregon, J. W. (2025). Informe de análisis de mejora continua para optimizar el mantenimiento de componentes de palas P&H en una empresa minera de la región de Áncash, 2024. *Trabajo de Suficiencia Profesional Para optar el Título Profesional de Ingeniero Industrial*. Perú, Lima: https://repositorio.continental.edu.pe/bitstream/20.500.12394/17300/11/IV_FIN_108_TSP_Soria_Obregon_2025.pdf. https://doi.org/https://hdl.handle.net/20.500.12394/17300

OMS. (11 de marzo de 2020). *La OMS caracteriza a COVID-19 como una pandemia*. Organización Mundial de la Salud : https://www.paho.org/es/noticias/11-3-2020-oms-caracteriza-covid-19-como-pandemia

OMS. (2021). *Estrategia mundial sobre salud digital 2020–2025.* Organización Mundial de la Salud 2021: https://iris.who.int/bitstream/handle/10665/344251/9789240027572-spa.pdf?sequence=1

Osorio-Sierra, A. F., M. J.-H., & Vargas-Montoya, H. F. (2020). Proceso para la identificación, clasificación y control del comportamiento de familias Ransomware. *Revista UIS Ingenierías, 19*(3), 131-142. https://doi.org/10.18273/revuin.v19n3-2020013

Pacheco et al. (2025). Transformación de la ingeniería Industrial a través de tecnologías emergentes para la mejora de procesos. *Innovación y convergencia: impacto multidisciplinar, 6*(1). https://doi.org/https://doi.org/10.60100/rcmg.v6i1.644

Palomero, A. F. (20 de 01 de 2024). Optimización de los procesos de producción con Masterbatches. *Tesis de grado*. Escuela Técnica Superior de Ingeniería de Barcelona , Barcelona , España: http://hdl.handle.net/2117/428582.

Pelegrí, J. (06 de febrero de 2019). *La cuarta revolución industrial: Cobots y automatización*. Universal Robots : https://www.universal-robots.com/es/blog/la-cuarta-revolucion-industrial-cobots-y-automatizacion/

Peña et al. (2022). Estado del arte de la educación en automática. *Revista Iberoamericana de Automática e Informática Industrial*(19), 117-131. https://doi.org/https://doi.org/10.4995/riai.2022.16989

Pereiro, I. P. (2022). Procesamiento escalable de datos de red para sistemas de detección de anomalías. *Trabajo de fin de grado en Ingeniería Informática mención en Tecnologías de la Información*. España , Universidad de Coruña , Facultade de Informática: http://hdl.handle.net/2183/31241.

Pico, L. E., & Marroquín, O. J. (2023). Aplicación de Deep Learning para la identificación de defectos superficiales utilizados en control de calidad de manufactura y producción industrial: una revisión de la literatura. *Ingeniería, 28*(1). https://doi.org/10.14483/23448393.18934

Pilay-Asunción, D. D., & Marcos-Rodriguez, K. L. (2025). Los desafíos tecnológicos y el rol del contador en la automatización de procesos contables. *Innovaciones Interdisciplinarias en Economía y Ciencias Sociales, 5*(1). https://doi.org/ https://doi.org/10.55813/gaea/jessr/v5/n1/178

Porcelli, A. M. (2020). La inteligencia artificial y la robótica: sus dilemas sociales, éticos y jurídicos. *Derecho global. Estudios sobre derecho y justicia, 6*(16). https://doi.org/https://doi.org/10.32870/dgedj.v6i16.286

Q et al. (2022). Metodología para el mantenimiento predictivo de transformadores de distribución basada en aprendizaje automático. *Ingeniería, 27*(3). https://doi.org/10.14483/23448393.17742

Riaño, J. D., & León, M. Á. (2023). Sistema de monitoreo de vibraciones por medio de modelos de mantenimiento predictivo 4.0 PHM y sistemas inerciales con el propósito de diagnosticar el estado y salud de activos. *Tesis o trabajo de investigación presentada(o) como requisito parcial para optar al título de Ingeniero en Control y Automatización*. Bogotá, Colombia, Respositorio Universidad Distrital Francisco José de Caldas: http://hdl.handle.net/11349/38474.

Riera et al. (19 de mayo de 2023). Automatización y el futuro. *Revista juventud y ciencia solidaria: En el camino de la investigación*(13). https://doi.org/http://dspace.ups.edu.ec/handle/123456789/24918

Ripani, L., & Soler, N. (18 de febrero de 2021). *El impacto de la automatización, más allá de las fronteras*. Inter-American Development Bank: https://blogs.iadb.org/trabajo/es/el-impacto-de-la-automatizacion-mas-alla-de-las-fronteras/

Rodríguez et al. (2024). Implicaciones del modelo industria 4.0 en la agroindustria: revisión sistemática. *KANYÚ: Revista científica de ciencias agrícolas y de la salud, 2*(1), 65- 82. https://doi.org/https://doi.org/10.61210/kany.v2iI.75

Rodríguez, J. A., & Camacho, J. E. (septiembre de 2023). Publicación: Como aplicar transformación digital en el sector logístico. *Tesis de maestría*. Bogotá, Universidad Cooperativa de Colombia, Facultad de Ingenierías, Maestría en Tecnologías de la Información y la Comunicación, Colombia: https://hdl.handle.net/20.500.12494/53225.

Romero, M. J., & Pulido, N. G. (2024). La automatización de procesos en Pymes del municipio de Santa María como impulso a su productividad. Escuela de Ciencias Administrativas, Contables, Económicas y de Negocios -ECACEN; Contaduría Pública, Colombia, Universidad Nacional Abierta y a Distancia – UNAD: https://repository.unad.edu.co/jspui/bitstream/10596/64191/1/ngonzalezpupdf.pdf.

Rose et al. (agosto de 2020). *NIST Special Publication 800-207.* Zero Trust Architecture: 10.6028/NIST.SP.800-207

Rozo-García, F. (2020). Revisión de las tecnologías presentes en la industria 4.0. *Revista UIS Ingenierías, 19*(2), 177-191. https://doi.org/10.18273/revuin.v19n2-2020019

Russo, A. (2020). *La recesión y la automatización cambian nuestro futuro laboral, pero hay trabajos que se avecinan, afirma un informe*. World Economic Forum: https://es.weforum.org/press/2020/10/la-recesion-y-la-automatizacion-cambian-nuestro-futuro-laboral-pero-hay-trabajos-que-se-avecinan-afirma-un-informe/

Salgado et al. (2024). Preprocesamiento de datos en el pronóstico de fallos de rodamientos para el mantenimiento predictivo. *Computación y Sistemas, 28*(4). https://doi.org/10.13053/cys-28-4-4913

Salimbeni, S., & Mamani, D. (2020). Marco de referencia para la incorporación de Cobots en líneas de manufactura. *Podium*(38). https://doi.org/https://doi.org/10.31095/podium.2020.38.10

Sampieri, R. H., Collado, C. F., & Lucio, M. d. (2013). 92 Capítulo 5 Definición del alcance de la investigación que se realizará: exploratorio, descriptivo, correlacional o explicativo. En R. H. Sampieri, *Metodología de la investigación* (pág. 92). https://www.esup.edu.pe/wp-content/uploads/2020/12/2.%20Hernandez,%20Fernandez%20y%20Baptista-metodolog%C3%ADa%20Investigacion%20Cientifica%206ta%20ed.pdf.

Sánchez, J. C. (6 de septiembre de 2021). Integración de 5G y TSN en redes privadas industriales. *Tesis de grado* . Granada , Repositorio Escuela Técnica Superior de Ingenierías, Informáticas y de Telecomunicación : https://digibug.ugr.es/bitstream/handle/10481/91900/TFG_JCS.pdf?sequence=1&isAllowed=y.

Sánchez, M. S. (2020). Estudio de una plataforma para Edge Computing e IoT. *Trabajo Fin de Grado / Proyecto Fin de Carrera*. Madrid, España, E.T.S. de Ingenieros Informáticos (UPM), Archivo digital UPM, Universidad Poliécnica de Madrid : https://oa.upm.es/63374/.

Sarmiento-Ramos, J. L. (2020). Aplicaciones de las redes neuronales y el deep learning a la ingeniería biomédica. *Revista UIS Ingenierías, 19*(4), 1-18. https://doi.org/10.18273/revuin.v19n4-2020001

Tapia et al. (2024). Mantenimiento predictivo basado en machine learning: una revisión sistemática de la literatura y perspectivas en la industria 4.0 predictive maintenance based on machine learning: a systematic literature review and perspectives in industry 4.0. *Avances en Ciencias e Ingeniería, 15*(4), 63-93. https://doi.org/https://www.researchgate.net/publication/394384131_MANTENIMIENTO_PREDICTIVO_BASADO_EN_MACHINE_LEARNING_UNA_REVISION_SISTEMATICA_DE_LA_LITERATURA_Y_PERSPECTIVAS_EN_LA_INDUSTRIA_40_PREDICTIVE_MAINTENANCE_BASED_ON_MACHINE_LEARNING_A_SYSTEMATIC_LITERATURE

Torres et al. (2025). El Chatbot aplicado a salud. una revisión bibliométrica. *Revista de Comunicación y Salud: RCyS, 15*(1), 1–18. https://doi.org/https://doi.org/10.35669/rcys.2025.15.e355

UNESCO. (6 de febrero de 2024). *Qué necesita saber acerca del aprendizaje digital y la transformación de la educación*. UNESCO: https://www.unesco.org/es/digital-education/need-know

Vaca, C. S., & Quito, R. F. (2022). Importancia de la implementación de mantenimiento preventivo en las plantas de producción para optimizar procesos. *E-IDEA Journal of Engineering Science, 4*(10), 59-69. https://doi.org/https://doi.org/10.53734/esci.vol4.id240

Vega, O. A. (2021). *Coloquio de investigación formativa 2021-2. Resúmenes ejecutivos.* Repositorio Universidad de Manizales . https://doi.org/https://ridum.umanizales.edu.co/handle/20.500.12746/5817

Wyczykier, G., & Acacio, J. A. (2024). El gas natural como combustible puente: Vaca Muerta en un escenario de transición energética. *Cuadernos de Geografía: Revista Colombiana de Geografía , 33*(1), 214-229. https://doi.org/10.15446/rcdg.v33n1.102046

Zaga, F. A. (2023). Implicancias transformadoras de la Cuarta Revolución Industrial en el mercado laboral. *Newman Business Review, 2*(9), 40–71. https://doi.org/https://doi.org/10.22451/3002.nbr2023.vol9.2.10087

Apéndices

Apéndice A

Cronograma

<table>
<tr><td colspan="3">Cronograma de actividades</td></tr>
<tr><td>Mes</td><td>Actividades</td><td>Producto</td></tr>
<tr><td>Mes 1</td><td rowspan="2">- Revisión de lineamientos institucionales para la monografía.
- Revisión de bases teóricas preliminares sobre automatización electrónica.
- Delimitación del problema, objetivos y justificación.
- Diseño preliminar del esquema del trabajo.
-Capítulos
Capítulo 1: Fundamentos de la automatización electrónica
1.1. Definición y evolución de la automatización electrónica)
1.2. Componentes de los sistemas automatizados
1.3. Importancia estratégica en el contexto de la Industria 4.0
Capítulo 2: Ventajas y desventajas de la automatización electrónica
2.1. Ventajas principales
2.2. Desventajas y limitaciones
Capítulo 3: Transformación de los procesos productivos industriales con automatización electrónica (2020-2025)
3.1. Cambios operativos y productivos
3.2. Modernización industrial en América Latina</td><td rowspan="2">- Esquema preliminar aprobado.
- Definición de bases bibliográficas iniciales.</td></tr>
<tr><td>Planeación inicial y delimitación del tema</td></tr>
</table>

	Capítulo 4: Desafíos actuales en la implementación de la automatización electrónica 4.1. Falta de capacitación especializada 4.2. Resistencia organizacional al cambio 4.3. Costos de inversión inicial elevados 4.4. Riesgos de ciberseguridad Capítulo 5: Tendencias emergentes de automatización electrónica (2020-2025) 5.1. Mantenimiento predictivo 5.2. Robótica colaborativa (Cobots) 5.3. Gemelos digitales 5.4. Edge computing	
Mes 2 Recolección de información bibliográfica y documental	- Búsqueda sistemática de artículos, libros, revistas científicas, informes técnicos (2020-2025). - Revisión de bases de datos académicas (Scopus, ScienceDirect, Google Scholar, Redalyc, Scielo, etc.). - Organización de la información por categorías (tecnologías, beneficios, desafíos, tendencias).	- Base de datos bibliográfica consolidada. - Fichas de lectura o resúmenes analíticos.
Mes 3 Análisis crítico de la información recopilada	- Lectura, profundización y análisis crítico de los estudios encontrados. - Identificación de hallazgos relevantes. - Organización de la información según los objetivos específicos (tecnologías, beneficios, desafíos y tendencias).	- Matriz de análisis temático. - Construcción del marco teórico inicial.
Mes 4	- Redacción del marco teórico basado en la literatura revisada. - Desarrollo del análisis de impacto de la	- Primer borrador de capítulos 1 (Introducción), 2

	automatización (beneficios y retos).	(Marco Teórico) y 3 (Análisis)
Redacción del marco teórico y desarrollo del análisis	- Inclusión de tablas, cuadros comparativos o gráficos de apoyo.	
Mes 5	- Redacción de los resultados del análisis. - Discusión de hallazgos, discusión investigativa. - Formulación de recomendaciones. - Redacción de las conclusiones. - Revisión preliminar del documento completo.	- Borrador completo de la monografía.
Elaboración de resultados, discusión y conclusiones		
Mes 6	- Revisión de redacción, normas de citación, formato APA 7 edición. - Ajustes de fondo y forma según recomendaciones del tutor.	- Monografía finalizada. - Entrega oficial.
Revisión y entrega final	- Verificación con programa antiplagio, derechos de autor. - Preparación de anexos, resumen y presentación final.	
Duración total: 6 meses		