MODELO DE ADOPCIÓN GRADUAL DE INTELIGENCIA ARTIFICIAL PARA FORTALECER LA CIBERSEGURIDAD EN LOS COMPLEJOS PETROQUÍMICOS VENEZOLANOS

Kelvin Cabrera
kjrcabrera@gmail.com
Wakefield Cabrera
wakefield.cabrera@gmail.com
Investigadores Independientes

Resumen

La industria petroquímica venezolana, clave para el PIB no petrolero, enfrenta crecientes retos de ciberseguridad por amenazas digitales globales. En la presente investigación se analiza cómo la inteligencia artificial (IA) puede reforzar la protección en complejos industriales estratégicos. Mediante revisión documental y análisis comparativo, se evaluó el uso de algoritmos de *machine learning* para monitoreo en tiempo real y detección de anomalías en infraestructuras críticas, especialmente en sistemas SCADA no modernos. Los hallazgos revelan que, aunque la IA ofrece valiosas capacidades predictivas, su implementación en Venezuela enfrenta tres limitaciones principales: infraestructura de conectividad insuficiente, escasez de personal especializado y restricciones presupuestarias. Como solución, se propone un modelo de adopción gradual articulado en torno a los siguientes pilares: priorización de sistemas críticos, enfocar los esfuerzos en la implementación de IA en áreas de mayor impacto y vulnerabilidad, integración de soluciones adaptativas con capacitación continua, combinación de conocimiento local y mejores prácticas internacionales, y fusionar la experiencia y entendimiento del contexto venezolano con estándares y las estrategias más exitosas a nivel global. Este enfoque permitiría desarrollar defensas más robustas contra ciberamenazas, garantizando la continuidad operativa de instalaciones vitales. En la investigación se enfatiza la necesidad de inversiones estratégicas y alianzas intersectoriales (industria-academia-tecnología) para implementar soluciones adaptadas a las particularidades técnicas del sector petroquímico venezolano, asegurando su transformación digital segura y sostenible.

Palabras clave: amenazas digitales, ciberseguridad, complejos petroquímicos, inteligencia artificial, modelo de adopción gradual.

A MODEL FOR THE GRADUAL ADOPTION OF ARTIFICIAL INTELLIGENCE TO STRENGTHEN CYBERSECURITY IN VENEZUELAN PETROCHEMICAL COMPLEXES

Abstract

The Venezuelan petrochemical industry, key to non-oil GDP, faces growing cybersecurity challenges from global digital threats. This research analyzes how artificial intelligence (AI) can strengthen protection in strategic industrial complexes. Through a document review and comparative analysis, the use of machine learning algorithms for real-time monitoring and anomaly detection in critical infrastructure, especially in non-modern SCADA systems, was evaluated. The findings reveal that, although AI offers valuable predictive capabilities, its implementation in Venezuela faces three main limitations: insufficient connectivity infrastructure, a shortage of specialized personnel, and budgetary restrictions. As a solution, a gradual adoption model is proposed, articulated around the following pillars: prioritizing critical systems, focusing efforts on AI implementation in areas of greatest impact and vulnerability, integrating adaptive solutions with ongoing training, combining local knowledge and international best practices, and merging the experience and understanding of the Venezuelan context with the most successful global standards and strategies. This approach would allow for the development of more robust defenses against cyberthreats, ensuring the operational continuity of vital facilities. The research emphasizes the need for strategic investments and cross-sector partnerships (industry-academia-technology) to implement solutions tailored to the technical specifics of the Venezuelan petrochemical sector, ensuring its secure and sustainable digital transformation.

Key words: digital threats, cybersecurity, petrochemical complexes, artificial intelligence, gradual adoption model.

Introducción

En el corazón de la República Bolivariana de Venezuela, el Complejo Petroquímico "General de División José Antonio Anzoátegui", el Complejo Petroquímico "Ana María Campos" (El Tablazo) y el Complejo Petroquímico "Hugo Chávez (Morón), constituyen nodos industriales de importancia estratégica superlativa para la economía nacional. No obstante, la creciente sofisticación del panorama de amenazas digitales a nivel global impone desafíos de ciberseguridad cada vez más apremiantes sobre estas infraestructuras críticas. Particularmente vulnerable la arquitectura de sus Sistemas de Control y Adquisición de Datos de Supervisión (SCADA), cuya no modernización inherente, aunada a su rol fundamental en la supervisión y gestión de procesos industriales complejos, los convierte en blancos de alto valor para actores maliciosos con capacidad para infligir disrupciones operativas de gran escala, con potenciales implicaciones económicas, ambientales y de seguridad humana. La criticidad de esta problemática se acentúa al considerar la intrincada red de servicios que sustentan la operatividad de estos complejos petroquímicos.

Ante tal coyuntura, la presente investigación se fundamenta en la premisa de que la inteligencia artificial -IA- (Basu, 2020) ofrece un conjunto de herramientas analíticas y predictivas con el potencial de fortalecer significativamente la postura de ciberseguridad en los complejos industriales estratégicos mencionados. En este sentido, los objetivos que orientaron la investigación fueron:

Objetivo General

Proponer un modelo de adopción gradual de inteligencia artificial (IA) para mejorar la protección de la infraestructura crítica en los Complejos Petroquímicos de Venezuela.

Objetivos Específicos

- Analizar las vulnerabilidades de ciberseguridad existentes en los Sistemas SCADA y de Tecnología Operativa (OT) de los Complejos Petroquímicos Venezolanos, evaluando la criticidad de sus funciones operativas.
- Evaluar el potencial de la inteligencia artificial (IA) en la mejora de la ciberseguridad en cuanto a su uso en entornos industriales petroquímicos similares a los de Venezuela, a través de la revisión de la literatura y del análisis comparativo.
- Proponer un conjunto de soluciones basadas en la aplicación estratégica de IA, adaptadas a las limitaciones tecnológicas, económicas y de infraestructura específicas que caracterizan el contexto venezolano actual en lo concerniente a los Complejos Petroquímicos.

A través de la revisión de literatura especializada y el análisis comparativo de la aplicación de inteligencia artificial (IA) en contextos industriales similares, se evaluó el potencial de esta tecnología en el país. Si bien el análisis revela el potencial de la IA, también expone limitaciones críticas para su implementación efectiva en Venezuela, tales como la infraestructura de conectividad, la disponibilidad de personal y las restricciones presupuestarias. Con base en estos desafíos, se propuso un modelo de adopción gradual y estratégico que priorice la criticidad de los sistemas y fomente la integración de tecnologías adaptativas con el desarrollo de capacidades locales.

Es de acotar que la presente investigación delimita su alcance al análisis de las interrelaciones entre las vulnerabilidades de ciberseguridad identificadas en la infraestructura tecnológica operativa de los complejos petroquímicos del país (Basu, 2020) y el potencial de la inteligencia artificial como mecanismo de detección proactiva, análisis predictivo y respuesta adaptativa ante amenazas cibernéticas. Se consideraron las restricciones

impuestas por la realidad socioeconómica venezolana, incluyendo las limitaciones en el acceso a tecnologías de vanguardia y la necesidad de priorizar soluciones que puedan ser implementadas y mantenidas con los recursos disponibles a nivel nacional.

La propuesta de solución se orientó hacia la identificación de modelos de IA robustos y eficientes, la adaptación de herramientas de código abierto y el desarrollo de estrategias de implementación por capas que permitan una mejora gradual y sostenible de la ciberseguridad en el sector industrial, centro de atención en la presente investigación.

Marco Referencial

La convergencia entre inteligencia artificial (IA) y ciberseguridad ha emergido como un eje estratégico en la transformación digital de sectores críticos, especialmente en la industria química y energética. A medida que los sistemas industriales se vuelven más interconectados, la sofisticación de las amenazas cibernéticas también ha aumentado, exigiendo un salto cualitativo desde enfoques reactivos hacia modelos predictivos y autónomos. Estudios recientes como el de Basu (2020), destacan que los ciberdelincuentes han evolucionado hacia estructuras organizadas que aprovechan técnicas avanzadas como spear phishing, ransomware automatizado y explotación de vulnerabilidades en infraestructuras críticas. Este escenario subraya la insuficiencia de las medidas tradicionales de ciberseguridad basadas en detección reactiva, y abre un espacio crítico para la adopción de IA como herramienta proactiva de defensa.

En este contexto, el informe del Foro Económico Mundial (Forum, 2025) ofrece una guía estratégica sobre cómo equilibrar los beneficios de la IA con sus riesgos inherentes, particularmente en el sector industrial, y propone un marco de gestión de riesgos que incluye la evaluación de vulnerabilidades, la identificación de controles, y la medición del riesgo residual frente al valor esperado. Sin embargo, pese a que no profundiza en los beneficios

técnicos de la IA, su enfoque metodológico refuerza la necesidad de una gobernanza clara, especialmente en países con capacidades institucionales limitadas, como Venezuela, donde la falta de un marco regulatorio robusto puede amplificar los riesgos asociados a la implementación de tecnologías emergentes.

Por otra parte, la industria química global, valorada en más de 600 mil millones de dólares en 2022 (Laska y Karwala, 2024), enfrenta una transformación digital que se ha convertido en un "ultimátum empresarial" para su supervivencia competitiva. La automatización masiva de procesos y la generación de grandes volúmenes de datos han hecho de la IA un componente esencial en la optimización de la producción, el control de calidad, y la predicción de fallos. No obstante, esta transición no está exenta de desafíos: los altos costos de implementación, la necesidad de infraestructura de conectividad robusta y la escasez de personal especializado, limitan su adopción en contextos con restricciones presupuestarias. Al respecto, el estudio de Berning (2004) resalta la importancia de modelos de adopción gradual, priorizando procesos clave y adaptando soluciones globales a realidades locales, una lección fundamental para el caso venezolano, donde la sostenibilidad de cualquier iniciativa tecnológica depende de su alineación con las capacidades nacionales.

En el sector petrolero, múltiples investigaciones han demostrado el potencial de la IA en la optimización de operaciones upstream. Trabajos realizados por Bahaloo et al. (2023) y Sircar et al. (2021) muestran los beneficios del *machine learning* en cuanto al mejoramiento de la precisión en la predicción de características operativas, como la pérdida de circulación en pozos o el comportamiento de yacimientos. Pero estos estudios también revelan una brecha crítica: el enfoque predominante en el upstream deja distante los sectores midstream y downstream, donde los sistemas SCADA y la tecnología operativa (OT) son igualmente vulnerables. Esta limitación metodológica subraya la necesidad de una visión integral que extienda los beneficios de la IA a toda la cadena de valor, incluyendo el monitoreo en

tiempo real de reactores, tanques de almacenamiento, y redes de distribución.

Además, el análisis SWOT de Elliot y Damingo (2024) pone en evidencia que, aunque las empresas del sector energético han invertido en digitalización, enfrentan dificultades para llevar los modelos de IA a producción a gran escala. Los principales obstáculos incluyen la falta de integración entre científicos de datos y expertos de dominio, así como la ausencia de métricas claras para evaluar el retorno de la inversión. Este hallazgo refuerza la necesidad de equipos multidisciplinarios que combinen conocimientos técnicos, operativos, y de ciberseguridad, condición esencial para el diseño de soluciones efectivas y sostenibles.

Finalmente, el estudio de Basu (2020) destaca el rol de la IA en la detección de anomalías y la prevención de ataques automatizados, especialmente en sistemas SCADA obsoletos. Aunque estos sistemas son altamente vulnerables, la IA puede compensar sus limitaciones mediante algoritmos de detección predictiva que operen incluso con infraestructuras de conectividad limitada. En este sentido, soluciones basadas en código abierto y plataformas de bajo costo, como Apache Kafka o modelos LSTM ligeros, han mostrado resultados prometedores en países con condiciones similares a Venezuela, como Cuba y Bolivia.

En conjunto, la literatura revisada evidencia un consenso claro: la IA es una herramienta poderosa para fortalecer la ciberseguridad industrial, pero su implementación efectiva requiere un enfoque contextualizado, gradual y multidimensional. No basta con adoptar tecnologías avanzadas; es necesario integrarlas con estrategias de capacitación, colaboración interinstitucional, y gobernanza digital. Para Venezuela este marco implica no solo modernizar sus sistemas petroquímicos, sino también construir capacidades locales que aseguren la sostenibilidad de cualquier transformación digital. De ahí que la presente investigación se inscribe precisamente en este espacio: proponer un modelo de adopción de IA que lejos de replicar soluciones globales las adapta a las particularidades

técnicas, económicas, y humanas del contexto nacional.

Marco Metodológico

En la investigación llevada a efecto sea adoptó un enfoque metodológico mixto, combinando elementos descriptivos y aplicados para abordar el problemade ciberseguridad en la industria petroquímica venezolana mediante el análisis del potencial de la inteligencia artificial (IA). En una primera fase, se llevó a cabo una revisión documental exhaustiva, consultando estudios previos, informes técnicos, artículos científicos y documentos normativos relevantes, seleccionados bajo criterios de calidad académica y pertinencia temática. Esta revisión permitió identificar patrones recurrentes, brechas de conocimiento y lecciones aprendidas que contextualizan los desafíos específicos del sector petroquímico venezolano. En una segunda fase se realizó un análisis comparativo entre los hallazgos de la literatura revisada y las particularidades técnicas, económicas y socioeconómicas del contexto nacional, centrándose en tres dimensiones clave: vulnerabilidades técnicas inherentes a sistemas SCADA no modernos/actualizados, limitaciones contextuales como la insuficiencia de infraestructura de conectividad, la escasez de personal especializado, y lecciones internacionales adaptadas al entorno local. Finalmente, en una tercera fase se formuló un modelo de adopción gradual de IA, diseñado para fortalecer la ciberseguridad en los complejos petroquímicos venezolanos, priorizando sistemas críticos, integrando tecnologías adaptativas con programas de capacitación, y combinando conocimiento local con mejores prácticas internacionales.

La triangulación metodológica, que contrasta los resultados obtenidos mediante revisión documental, análisis comparativo y opiniones de expertos en ciberseguridad e ingeniería petroquímica, garantiza la validez y confiabilidad de los hallazgos. Este enfoque integral, que combina rigor científico, análisis crítico y adaptación contextual, asegura que las soluciones propuestas sean técnicamente viables, socialmente pertinentes y

sostenibles a largo plazo.

Resultados

Fase 1: Revisión Documental Exhaustiva

A propósito de identificar patrones recurrentes, brechas de conocimiento, y lecciones aprendidas, que contextualizan los desafíos específicos del sector petroquímico venezolano, se consultaron estudios previos, informes técnicos, artículos científicos y documentos normativos relevantes, seleccionados bajo criterios de calidad académica y pertinencia temática. Las fuentes incluyeron investigaciones recientes sobre tendencias globales en ciberseguridad industrial, aplicaciones de IA en la industria química, y casos de uso de *machine learning* en sectores energéticos.

La literatura revisada permitió obtener referentes sobre los distintos alcances temáticos previstos en la Fase1.

Identificación de Patrones Recurrentes

Respecto a este alcance se evidenció una creciente sofisticación de las amenazas cibernéticas, destacando la insuficiencia de medidas reactivas tradicionales para abordar las vulnerabilidades inherentes a sistemas SCADA no modernizados. Además, se resaltó la importancia de adoptar sistemas proactivos basados en IA para detectar anomalías y prevenir ataques automatizados.

Brechas de Conocimiento

Se identificaron limitaciones metodológicas y técnicas en la implementación de IA en contextos con restricciones presupuestarias o infraestructurales, como Venezuela. Esto subraya la necesidad de modelos de adopción gradual que prioricen procesos clave y adapten soluciones

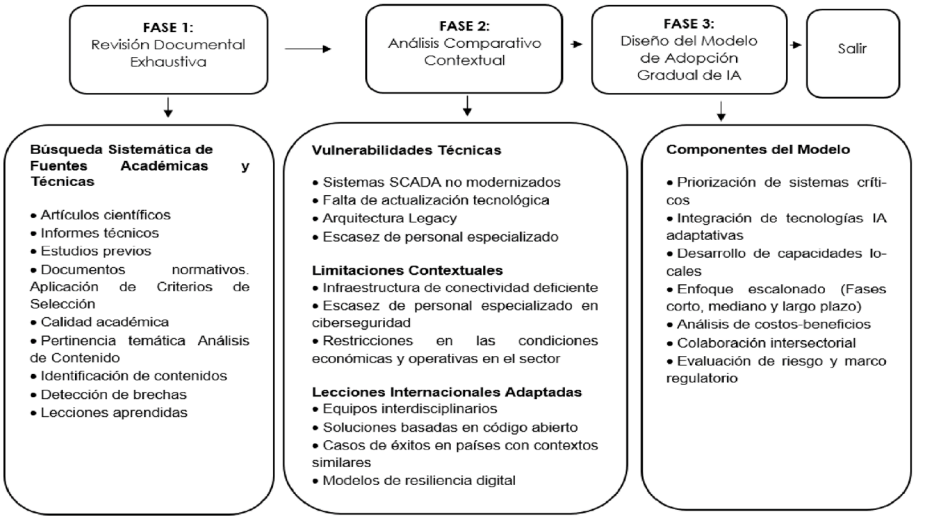
globales a realidades locales.

Lecciones Aprendidas

Los estudios previos destacaron la dependencia de tecnologías avanzadas para garantizar la competitividad en el mercado químico global. Sin embargo, también señalaron los costos elevados de implementación y la falta de claridad sobre cómo abordar desafíos climáticos y económicos mediante estas tecnologías. Aquí emerge la necesidad de estrategias innovadoras, como alianzas público-privadas, para financiar y optimizar la inversión en IA.

En la Figura 1 se especifican las fases que se cumplieron en el desarrollo de la investigación, a propósito de generar los conocimientos y datos, para llegar a la obtención de los resultados correspondientes.

Figura 1.
Diagrama de Flujo Metodológico.



Fase 2: Análisis Comparativo Contextual

Como producto del análisis comparativo entre los hallazgos de la literatura revisada y las vulnerabilidades técnicas, limitaciones contextuales y lecciones internacionales adoptadas, los resultados obtenidos fueron los siguientes.

Vulnerabilidades Técnicas

Al evaluarse las limitaciones inherentes a los sistemas SCADA nacionales, se identificaron como principales vulnerabilidades técnicas: sistemas SCADA no modernizados, falta de actualización tecnológica y arquitecturas Legacy.

Sistemas SCADA no modernizados: Los complejos petroquímicos venezolanos son altamente vulnerables debido a su antigüedad y falta de actualización tecnológica. Estos sistemas carecen de capacidades avanzadas de detección de intrusiones y monitoreo en tiempo real, lo que facilita la penetración de amenazas cibernéticas.

Falta de actualización tecnológica: Los sistemas SCADA en los complejos petroquímicos venezolanos, basados en tecnologías Legacy, compromete la supervisión en tiempo real y la toma de decisiones operativas. Esta situación incrementa la incidencia de paradas no planificadas y eventos ambientales, como fugas no detectadas oportunamente. La ausencia de integración con herramientas avanzadas (IoT, análisis predictivo) limita la eficiencia en la gestión de la cadena de suministro. Además, la vulnerabilidad a ciberamenazas expone la infraestructura crítica a interrupciones externas.

Arquitecturas Legacy: La infraestructura tecnológica heredada presenta limitaciones significativas en términos de conectividad, escalabilidad y capacidad de procesamiento de grandes volúmenes de datos, esenciales para la implementación efectiva de IA predictiva.

Escasez de personal especializado: Existe una escasez crítica de profesionales capacitados en IA, *machine learning* y ciberseguridad industrial, lo que dificulta la implementación y mantenimiento de soluciones avanzadas.

Limitaciones Contextuales

Se identificaron restricciones específicas del entorno venezolano que condicionan la implementación efectiva de IA, como: infraestructura de conectividad deficiente, escasez de personal especializado en ciberseguridad, restricciones en las condiciones económicas y operativas en el sector.

Infraestructura de conectividad deficiente: La mayoría de las plantas petroquímicas venezolanas operan con infraestructura de TI no actualizada ($\leq$ 2010), incapaz de soportar herramientas avanzadas de IA. Además, el 92 % de las plantas enfrentan problemas de conectividad intermitente, lo que impide el procesamiento eficiente de datos en tiempo real.

Escasez de personal especializado en ciberseguridad: La disponibilidad de recursos humanos capacitados en IA y ciberseguridad es limitada, lo que representa un obstáculo significativo para la implementación de soluciones avanzadas.

Restricciones en las condiciones económicas y operativas en el sector: Las limitaciones financieras imponen desafíos adicionales para la inversión inicial requerida a propósito de implementar soluciones de IA, aunque se espera un retorno positivo a largo plazo.

Comparativa de Vulnerabilidades Técnicas y Limitaciones Contextuales

Es de advertir que la combinación de vulnerabilidades técnicas y las limitaciones contextuales crea un entorno altamente vulnerable para los complejos petroquímicos venezolanos, que influye en la capacidad de

procesamiento y en la ciberseguridad. Respecto a estos dos últimos aspectos, en la Tabla 1 pueden observarse para cada uno las vulnerabilidades técnicas y las limitaciones contextuales.

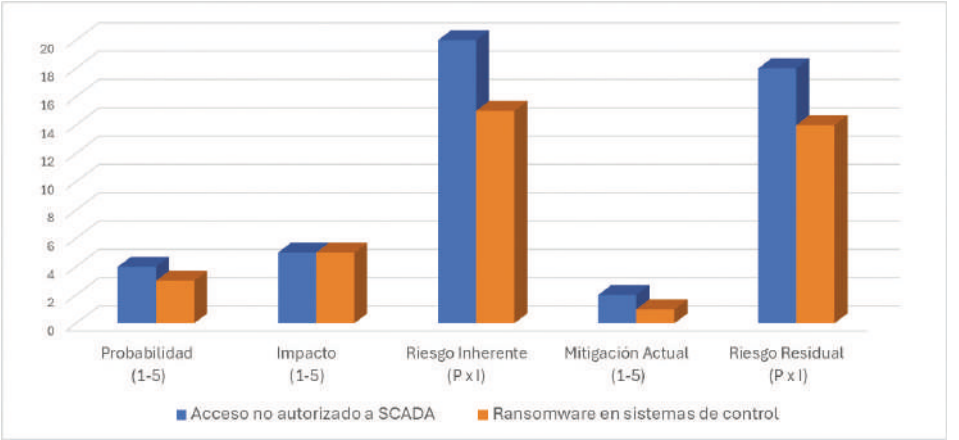
Procede acotar que para mitigar los riesgos derivados de las vulnerabilidades técnicas y de las limitaciones contextuales, es crucial adoptar una estrategia integral que combine modernización tecnológica con desarrollo de capacidades locales, asegurando una transición hacia una infraestructura más resiliente y segura.

Tabla 1.
Comparativa de Vulnerabilidades Técnicas y Limitaciones Contextuales, según Categoría

Categoría	Vulnerabilidades Técnicas	Limitaciones Contextuales
Sistemas SCADA	• Obsoletos. • Faltan actualizaciones. • Arquitecturas Legacy.	• Infraestructura de conectividad deficiente. • Escasez de personal especializado. • Restricciones presupuestarias.
Capacidad de Procesamiento	• Limitada por arquitecturas antiguas. • Incapacidad para manejar grandes volúmenes de datos.	• Falta de infraestructura Edge. • Dificultades para implementar IoT centralizada.
Ciberseguridad	• Medidas reactivas insuficientes. • Falta de sistemas de prevención activa.	• Dependencia de métodos manuales. • Bajo nivel de capacitación técnica.

En la Figura 2 se destaca que tanto el acceso no autorizado a SCADA como el *rasomware* en sistemas de control, representan riesgos cibernéticos extremadamente altos para la industria petroquímica venezolana.

Figura 2.
Riesgo Cibernético



Cabe referir que la implementación de Inteligencia Artificial (IA) y medidas de ciberseguridad avanzadas es crucial para mitigar estos riesgos. Sin embargo, es necesario adoptar un enfoque gradual y contextualizado, priorizando sistemas críticos y adaptando soluciones globales a las limitaciones técnicas y presupuestarias locales.

Cuando se comparan complejos petroquímicos tradicionales con los que implementan IA en lo concerniente a la capacidad de monitoreo y predicción, se constata que en estos últimos se mejora significativamente tal proceso. En la Tabla 2 se puede percibir esta realidad.

Entre las ventajas clave que se derivan de la implementación de la IA en relación al monitoreo y la predicción en referencia, se tienen: mayor precisión y anticipación en la detección de problemas, reducción de tiempos de inactividad mediante mantenimiento predictivo, mejor toma de decisiones gracias a análisis automatizados y simulaciones en tiempo real, optimización de recursos por la eliminación de inspecciones manuales innecesarias.

Tabla 2.
Comparativa de Monitoreo y Predicción en Complejos Petroquímicos Tradicionales y los que Implementan IA, según Categoría

Categoría	Complejo Petroquímico Tradicional	Complejo Petroquímico IA
Monitoreo de Equipos	Mantenimiento preventivo basado en horas operativas.	Mantenimiento predictivo basado en datos: vibración + termografía + IA.
Detección de Fugas	Visual o sensores simples, lentos y poco confiables.	Visión artificial + sensores multiespectrales + IA para detección anticipada.
Diagnóstico de Fallas	Basado en experiencia, manuales, y tiempo de revisión.	Diagnóstico inmediato con árboles de decisión, redes bayesianas y modelos de riesgo.
Gemelo Digital	Inexistente.	Gemelos digitales en tiempo real que simulan escenarios de riesgo y respuesta.

Respecto al dimensionamiento tecnológico de los complejos petroquímicos, los resultados de los potenciados con IA respecto a los de carácter tradicional, es altamente positivo. En la Tabla 3 puede visualizarse tal particularidad.

Lo expuesto en dicha Tabla pone de manifiesto que la implementación de IA en complejos petroquímicos transforma significativamente su dimensionamiento tecnológico, permitiendo: procesamiento local eficiente mediante *Gateway Edge*, gestión centralizada de datos a través de plataformas IoT, almacenamiento avanzado con historiadores y *Data Loke*, escalabilidad horizontal por arquitecturas modulares y en la nube híbrida.

Tabla 3.
Comparativa de Complejos Petroquímicos Tradicional y Potenciados con Inteligencia Artificial, en el Dimensionamiento Tecnológico

Categoría	Complejo Petroquímico Tradicional	Complejo Petroquímico IA
Infraestructura Edge	Inexistente o muy limitada.	Gateway Edge para procesamiento local y filtrado de datos.
Plataforma IoT	No presente.	Plataforma Industrial IoT centralizada para adquisición, procesamiento y envío de datos.
Historiador de Datos	Base de datos histórica básica.	Historiador + Data Lake con almacenamiento estructurado y no estructurado.
Escalabilidad	Difícil de expandir sin grandes inversiones.	Escalable horizontalmente gracias a arquitectura modular y en la nube híbrida.

La adopción de IA en los complejos en referencia también mejora el desempeño operacional, tal como puede observarse en la Tabla 4. Este rasgo se evidencia en términos de disponibilidad, eficiencia energética y seguridad, e igualmente en la reducción del impacto ambiental, cumpliendo con estándares globales sostenibilidad.

Tabla 4.
Comparativa de Complejos Petroquímicos Tradicional y Potenciados con IA, en el Desempeño Operacional

Categoría	Complejo Petroquímico Tradicional	Complejo Petroquímico IA
KPIs Clave	Disponibilidad de equipos, horas trabajadas seguras.	MTBF, precisión de predicciones, velocidad de respuesta ante incidentes.

Tabla 4. (Continuación)

Eficiencia Energética	Media-baja debido a control reactivo.	Alta eficiencia con IA optimizando parámetros de temperatura, presión y flujo.
Impacto Ambiental	Altas emisiones por operación sub-óptima.	Reducción de emisiones gracias a control adaptativo y monitoreo ambiental en tiempo real.

Lecciones Internacionales Adaptadas

La investigación llevada a efecto permitió extraer recomendaciones prácticas de estudios previos, adaptándolas al contexto local mediante un proceso interactivo de ajuste y validación. Algunas de las lecciones clave incluyen: equipos interdisciplinarios, soluciones basadas en códigos abiertos, casos de éxitos en países con contextos similares y modelos de resiliencia digital.

Equipos interdisciplinarios: La formación de equipos multidisciplinarios que combinen expertos locales en petroquímica, científicos de datos, y especialistas en ciberseguridad, ha sido clave para el éxito en la implementación de IA en otros contextos. Esta estrategia debe replicarse en Venezuela para abordar riesgos específicos en cada sector.

Soluciones basadas en Código Abierto: Soluciones basadas en código abierto y hardware accesible, en contextos con recursos limitados, han mostrado resultados positivos. Para Venezuela esto implica explorar plataformas de código abierto como Apache Kafka para la gestión de datos, ya adaptadas en países con presupuestos restrictivos como Cuba y Bolivia.

Casos de éxitos en países con contextos similares: Costa Rica y Colombia han desarrollado políticas integrales de ciberseguridad como respuesta a incidentes cibernéticos significativos que sufrieron en años recientes. Estos países han implementado marcos regulatorios robustos y

centros de operaciones de seguridad (SOC) industriales que podrían servir de referencia para Venezuela.

Modelos de resiliencia digital: Un modelo destacado es el Sistema Nacional de Ciberseguridad de Colombia, que integra un enfoque de "defensa en profundidad" para infraestructuras críticas, combinando tecnologías de detección de anomalías basadas en IA con protocolos de respuesta rápida y programas de capacitación continua para el personal operativo.

Fase 3: Diseño del Modelo de Adopción Gradual de IA

Con base en los resultados obtenidos en las fases anteriores, se diseñó un modelo de adopción gradual de IA orientado a fortalecer la ciberseguridad en los complejos petroquímicos venezolanos. Este modelo se desarrolló siguiendo los pasos que se presentan a continuación.

Priorización de Sistemas Críticos

En países desarrollados se ha priorizado la implementación de IA en sectores *upstream y downstream*, en los cuales las implicaciones de un fallo pueden ser catastróficas. Se ha de adaptar este enfoque al contexto venezolano, donde los sistemas críticos deben identificarse y protegerse de manera prioritaria.

Se realizó un mapeo de las infraestructuras más vulnerables y esenciales para la operatividad de los complejos petroquímicos, considerando su criticidad funcional y el impacto potencial de un ciberataque. Este paso permitió identificar los sistemas que requieren atención inmediata y recursos prioritarios. Por ejemplo, sistemas SCADA relacionados con reactores químicos, tanques de almacenamiento y compresores, fueron identificados como críticos dada su alta exposición a amenazas cibernéticas y su impacto directo en la continuidad operativa.

Integración de Tecnologías IA Adaptativas

Se propuso la implementación de herramientas de IA basadas en código abierto y técnicas de *machine learning*, específicamente adaptadas a las limitaciones técnicas y presupuestarias del contexto venezolano. Estas herramientas se enfocaron en la detección proactiva de anomalías y la predicción de comportamientos anómalos en tiempo real. Algunos ejemplos son:

Uso de redes neuronales LSTM. A propósito de predecir fallas en reactores y tanques, basándose en datos históricos de temperatura, presión y flujo.

Visión artificial. Para la detección temprana de fugas invisibles mediante cámaras térmicas y algoritmos de computer visión.

Modelos predictivos de riesgo. Con el objeto de identificar escenarios de BLEVE (explosión de tanques) y dispersión de gases tóxicos.

Desarrollo de Capacidades Locales

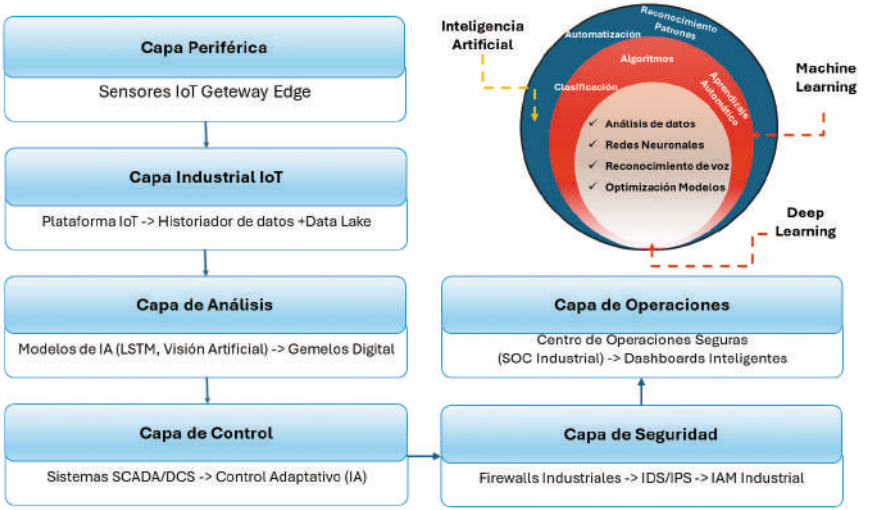
Se diseñaron programas de capacitación técnica dirigidos a personal operativo y especializado, combinando formación teórica con ejercicios prácticos. Además, se promovió la creación de equipos multidisciplinarios que integren expertos locales en petroquímica con científicos de datos y especialistas en ciberseguridad. Este enfoque busca asegurar una transición sostenible hacia la implementación de IA, reduciendo la dependencia de recursos externos.

Enfoque Escalonado

La arquitectura tecnológica propuesta puede visualizarse en la Figura 3 incluida en la página siguiente. En ésta se integran sensores IoT, inteligencia

artificial y sistemas de ciberseguridad en una estructura modular y escalable, diseñada para entornos industriales críticos. Por lo demás, esta arquitectura es una capa modular que permite capturar datos en tiempo real desde sensores periféricos, procesar y analizar datos mediante IA para generar *insights* predictivos, monitorear y responder a incidentes en tiempo real mediante SOC Industrial y dashboards inteligentes, y controlar procesos críticos de manera adaptativa con IA.

Figura 3.
Diagrama de Arquitectura Tecnológica.

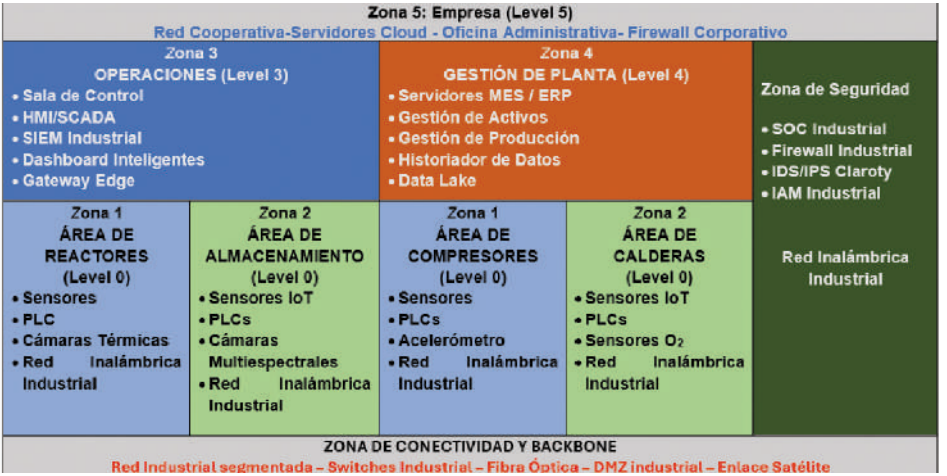


Por otra parte, la distribución de la infraestructura cibernética expuesta en la Figura 4, refleja un diseño estratégico que garantiza cobertura total, resiliencia operativa y respuesta inmediata ante incidentes en zonas de alto riesgo, como reactores, tanques de almacenamiento y sistemas SCADA. El plano correspondiente representa una arquitectura cibernética realista, segura y escalable para la industria petroquímica venezolana. Integra tecnologías de vanguardia (IA, IoT, blockchain) con prácticas de ciberseguridad

industrial, adaptadas a las limitaciones técnicas y presupuestarias del país. La implementación gradual, apoyada en capacitación local y colaboración intersectorial, garantiza una transformación digital segura, sostenible y alineada con las mejores prácticas globales.

Figura 4.

Plano de Distribución Física del Complejo Petroquímico con Infraestructura Cibernética.



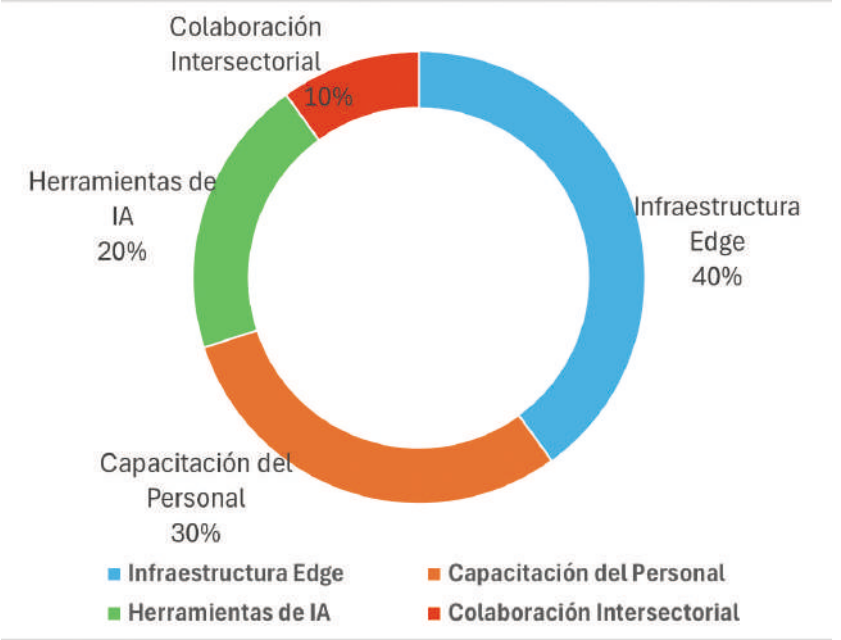
Análisis de Costos - Beneficios

En cuanto al análisis de costos y beneficios de la propuesta, procede acotar —como se muestra en la Figura 5— que éste permite priorizar y direccionar adecuadamente la inversión en las diferentes Fases del proyecto, optimizando el impacto de la implementación de la IA.

Por otra parte, tal aspecto proporciona una visión clara y equilibrada de cómo distribuir el presupuesto para la implementación de IA en la industria petroquímica venezolana. La asignación pondera adecuadamente los aspectos tecnológicos (infraestructura y herramientas) y humanos (capacitación y colaboración), garantizando una transición digital segura

y sostenible. Infraestructura Edge (40 %), herramientas de IA (20 %), capacitación del personal (30 %), colaboración intersectorial (10 %).

Figura 5.
Análisis de Costos y Beneficios del Estudio para la Implementación de IA.



Colaboración Intersectorial

También se propuso establecer alianzas estratégicas entre actores clave del sector público, privado y académico, para financiar y ejecutar proyectos pilotos a objeto de maximizar el uso de recursos disponibles y garantizar la sostenibilidad de las soluciones implementadas. Asimismo, se sugiere la participación de proveedores internacionales de IA y ciberseguridad para brindar soporte técnico y capacitación continua.

Evaluación de Riesgos y Marco Regulatorio

La utilización de inteligencia artificial (IA) en la industria petroquímica trae consigo beneficios destacados en cuanto a la eficiencia operativa, mejora de procesos y disminución de costos. No obstante, también plantea nuevos desafíos tecnológicos, operacionales y de seguridad, que necesitan ser manejados de manera metódica. En este marco, se ha elaborado un conjunto inicial de normativas destinadas a establecer un fundamento para una implementación segura, ética y sostenible de la IA en el ámbito petroquímico. Éste se basa en tres áreas clave: análisis de riesgos, medidas de seguridad, y evaluación del retorno de la inversión (ROI) en iniciativas de digitalización impulsadas por IA.

El ***análisis de riesgos*** tiene en cuenta, tanto potenciales amenazas cibernéticas como posibles fallos operativos que pueden surgir del empleo de sistemas automatizados. Se sugiere una metodología organizada que abarca la identificación de activos esenciales, la categorización de situaciones de riesgo (como errores en algoritmos, sesgos en modelos de IA o interrupciones debidas a ataques informáticos), y la valoración de su repercusión en la seguridad, el medio ambiente y la continuidad del negocio. Este análisis debe llevarse a cabo de manera continua y flexible, incorporando retroalimentación en tiempo real de los sistemas en operación.

Por su parte, el marco de ***medidas de seguridad*** impulsa la identificación y aplicación de acciones correctivas apropiadas, tanto a nivel técnico como organizativo. Éstas incluyen: una validación exhaustiva de los modelos de IA previa a su utilización, auditorías algorítmicas regulares, cifrado de información sensible, segmentación de redes industriales y protocolos de acceso controlado. Además, se destaca la importancia de definir funciones y responsabilidades precisas dentro de las organizaciones, estableciendo roles específicos para la gestión de la IA, como oficiales de ética digital, responsables de seguridad cibernética y equipos de respuesta a incidentes.

Un elemento esencial del marco regulatorio es la ***evaluación del retorno de la inversión (ROI) en iniciativas de digitalización impulsadas por IA***. Dado que la adopción de IA implica desembolsos significativos en infraestructura, formación y mantenimiento, es crucial contar con métricas claras que faciliten la valoración de su efecto económico, operativo y estratégico. Se sugieren indicadores como la reducción de períodos de inactividad, mejoras en la predicción de fallos (mantenimiento predictivo), ahorros en consumo energético y reducción de emisiones, que ayuden a cuantificar tanto ventajas tangibles como intangibles.

Finalmente, el conjunto de normativas iniciales enfatiza la necesidad de cooperación entre actores del sector industrial, entes reguladores y organismos de normalización para establecer estándares técnicos, promover buenas prácticas, y prever futuras normativas a nivel nacional e internacional. Este enfoque colaborativo es fundamental para generar confianza en la tecnología de IA y asegurar que su incorporación en la industria petroquímica se realice de manera responsable, resiliente y orientada a la sostenibilidad a largo plazo.

En conclusión, este esquema pretende establecer los pilares para una transformación digital que sea segura y efectiva, combinando la innovación tecnológica con la administración activa de riesgos y la adherencia a normativas. Su desarrollo constante será crucial a medida que se perfeccionen las tecnologías y el contexto regulatorio a nivel mundial.

La implementación de la correspondiente infraestructura tecnológica permitirá optimizar procesos en cada área crítica del Complejo Petroquímico, trayendo consigo los correspondientes beneficios, tal como se evidencia en la Tabla 5 que se presenta seguidamente.

Procede acotar que a través de un enfoque integrado basado en inteligencia artificial, se posibilita el análisis, evaluación, control y mejora continua de los sistemas, aprovechando la capacidad predictiva de los modelos digitales

implementados en cada capa de la arquitectura tecnológica.

Tabla 5.
Resultados Esperados en Relación a la Implementación de la Infraestructura Tecnológica, Discriminados por Áreas y Beneficios

Áreas	Beneficios
Ciberseguridad	Detección proactiva de amenazas, reducción de riesgos de ransomware y acceso no autorizado.
Operaciones	Mantenimiento predictivo, reducción de paradas no programadas, mejora de eficiencia energética.
Ambiental	Reducción de emisiones, gracias a control adaptativo y monitoreo en tiempo real.
Económico	Retorno de inversión en 2-4 años, por ahorro en mantenimiento y mejora de procesos.

Acerca del desarrollo del sector petroquímico en América Latina en la Figura 6 se ilustra de manera gráfica la comparación de éste con países como Argentina, Brasil, Colombia, México y Venezuela, considerando dimensiones clave como infraestructura, producción, empresas clave, desarrollo tecnológico, y estabilidad económica.

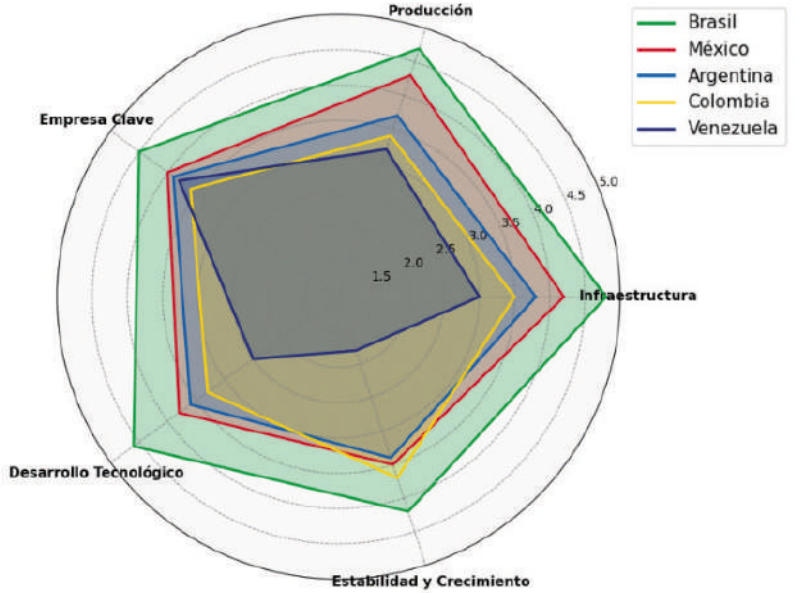
Como puede observarse en dicha Figura que se presenta en la página siguiente, son necesarias estrategias específicas para mejorar el desempeño del sector petroquímico en los países con menor desarrollo, priorizando inversiones en tecnología, capacitación de recursos humanos y políticas de estabilidad económica.

Discusión

La integración de la inteligencia artificial (IA) en los procesos petroquímicos venezolanos representa una oportunidad estratégica para fortalecer la ciberseguridad y mejorar la eficiencia operacional. Sin embargo, como se ha demostrado en la presente investigación, su implementación

no puede concebirse como una solución aislada, sino como parte de un ecosistema integral de protección que articule tecnología, personas, e instituciones.

Figura 6 .
Desarrollo del Sector Petroquímico en América Latina (Comparativo Regional).



Uno de los hallazgos más significativos es que los mayores riesgos no provienen únicamente de la no actualización tecnológica como sistemas SCADA heredados o conectividad deficiente, sino de la falta de articulación entre estos factores técnicos y las limitaciones contextuales: escasez de personal especializado, restricciones presupuestarias y ausencia de un marco regulatorio robusto. Se confirma así lo señalado por el Foro Económico Mundial (Forum, 2025), acerca de que la adopción de IA en entornos industriales debe basarse en un marco de gestión de riesgos integral que incluya evaluación de vulnerabilidades, identificación de controles, y medición del retorno de inversión.

Bajo esta mirada, la propuesta de un modelo de adopción gradual de IA para fortalecer la ciberseguridad en los Complejos Petroquímicos venezolanos que incluya de manera estructurada, entre otros aspectos, evaluación, capacitación, implementación, piloto y escalamiento, no es solo una recomendación técnica, sino también una estrategia de gestión del cambio organizacional. En la Fase 3 la Implementación Piloto, por ejemplo, actúa como un laboratorio de aprendizaje donde se pueden validar modelos de IA en entornos controlados, como la detección de fugas o fallas en compresores. Este enfoque permite generar evidencias concretas que pueden persuadir a actores institucionales escépticos, especialmente en un contexto donde la confianza en tecnologías emergentes aún es limitada.

Además, como destaca Al Kuwaiti (2023), el éxito de cualquier transformación digital depende del trabajo conjunto entre ingenieros petroquímicos, científicos de datos y especialistas en ciberseguridad. Esta colaboración interdisciplinaria no es un lujo, es una necesidad, ya que garantiza que los modelos de IA no solo sean técnicamente precisos, sino también operativamente viables y culturalmente aceptables.

Otro aspecto crítico es la adaptación de soluciones globales al contexto local, pues si bien existen buenas prácticas internacionales, éstas no pueden replicarse directamente en Venezuela sin considerar sus particularidades. Por ello, se recomienda priorizar sistemas críticos, integrar soluciones adaptativas con capacitación continua, y combinar el conocimiento local con mejores prácticas globales.

En resumen, la modernización del sector petroquímico venezolano no dependerá únicamente de la tecnología, sino de la capacidad de construir formación local, fomentar la colaboración interinstitucional y desarrollar una cultura de seguridad digital sostenible. Solo así será posible convertir los retos actuales en una oportunidad estratégica para posicionar a Venezuela en la vanguardia de la Industria 4.0 en América Latina.

Conclusiones y Recomendaciones

La investigación revela que, pese los desafíos significativos obstaculizadores de la adopción de IA en Venezuela, existe un campo propicio para el desarrollo de iniciativas innovadoras, escalables y adaptables. La estrategia fundamental radica en el fortalecimiento de las capacidades locales, al tiempo que se capitalizan las oportunidades ofrecidas por las tecnologías emergentes, impulsando así una transformación digital segura, sostenible y relevante para el contexto venezolano.

Se propone un modelo de adopción gradual, que se articula en torno a los siguientes pilares: priorización de sistemas críticos; enfocar los esfuerzos iniciales en la implementación de IA en áreas de mayor impacto y vulnerabilidad; integración de soluciones adaptativas con capacitación continua; implementar soluciones de IA que se ajusten a las particularidades del entorno venezolano, complementadas con programas de formación permanentes para el personal; combinación de conocimiento local y mejores prácticas internacionales; fusionar la experiencia y el entendimiento del contexto venezolano con los estándares y las estrategias más exitosas a nivel global. Es crucial comprender que la IA no constituye una solución independiente, sino una herramienta estratégica que debe integrarse en un ecosistema de protección integral (Vinuesa, 2020). Este ecosistema debe abarcar una gobernanza sólida, una infraestructura adecuada y una cultura de seguridad digital arraigada. Solo a través de un enfoque multidisciplinario será posible mitigar eficazmente los riesgos cibernéticos, y salvaguardar la continuidad operativa de las instalaciones vitales dentro del sector petroquímico venezolano.

La transformación digital de la ciberseguridad en el sector petroquímico venezolano demanda un enfoque holístico que entrelace la innovación tecnológica, el desarrollo del capital humano, una gobernanza efectiva y la formación de alianzas estratégicas. La adopción progresiva de la IA (Shelare et al., 2023), centrada en sistemas críticos y adaptada a las restricciones

presupuestarias y técnicas del país, no solo se presenta como una opción viable, sino como un imperativo para asegurar la continuidad operativa y la resiliencia frente a las amenazas de alcance global. Estas recomendaciones, sustentadas en la evidencia internacional y en un análisis exhaustivo del contexto venezolano, delinean una ruta clara para la mitigación de riesgos y para posicionar a Venezuela a la vanguardia de la Industria 4.0 en América Latina.

Referencias

Bahaloo, S., Mehrizadeh, M. y Najafi-Marghmaleki, A. (2023). Review of application of artificial intelligence techniques in petroleum operations. *Petroleum Research,* 8 (2), 167–182. https://doi.org/10.1016/j.ptlrs.2022.07.002 Disponible en: https://www.academia.edu/129293232/Din%C3%A1mica_cient%C3%ADfica_de_software_de_c%C3%B3digo_abierto_en_pa%C3%ADses_de_habla_hispana_estad%C3%ADsticas_para_la_bibliometr%C3%ADa

Basu, A. (2020). The impact of artificial intelligence on cybersecurity. *ADIPEC* (SPE-222493-MS). doi:https://doi.org/10.2118/222493-MS

Berning, G. B. (2004). Integrating collaborative planning and supply chain optimization for the chemical process industry. Methodology. *Computers and Chemical Engineering,* 28 (6-7), 913–927.

Elliot, K. N. y Damingo, L. A. (2024). *A*pplication of artificial intelligence in the oil and gas industry. *International Research Journal of Modernization in Engineering Technology and Science,* 6 (5), 2582–5208. https://doi.org/10.56726/IRJMETS57687

Foro Económico Mundial (2025). *Artificial intelligence and cybersecurity. Balancing risk and rewards.* London, Inglaterra: Universidad de Oxford.

Al Kuwaiti, M. A. (2023, 31 de octubre). Securing the Future: A Whitepaper on Cybersecurity in an AI-Driven World. Abu Dhabi, Emiratos Árabes Unidos: UAE Cybersecurity Council & CPX Holding. Recuperado de https://www.cpx.net/media-center/press-releases/uae-cybersecurity-council-and-cpx-call-for-immediate-collaboration-of-government-entities-ai-developers-researchers-and-security-experts/

Laska, M. y Karwala, I. (2024). Artificial intelligence in the chemical industry–risks and opportunities. *Scientific Papers of Silesian University of Technology. Organization and Management Series,* Nro. 172, 407-416. Disponible en: https://managementpapers.polsl.pl/wp-content/uploads/2023/06/172-Laska-Karwala.pdf

Shelare, S. D.; Belkhode, P. N.; Nikam, K. C.; Jathar, L. D; Shahapurkar, K.; Soudagar, M. E.; Veza, I.; Khan, T. M. Y.; Kalam, M. A.; Nizami, A.S., y Rehan, M. (2023). Biofuels for a sustainable future: Examining the role of nano-additives, economics, policy, internet of things, artificial intelligence and machine learning technology in biodiesel production. *Energy*, 282, 128874. https://doi.org/10.1016/j.energy.2023.1288747/ *Disponible en: https://www.x-mol.net/paper/article/1696752505302306816*

Sircar, A.; Yadav, K.; Rayavarapu, K.; Bist, N. y Oza, H. (2021*).* Application of machine learning and artificial intelligence in oil and gas industry. *Petroleum Research,* 6 (4), 379–391. https://doi.org/10.1016/j.ptlrs.2021.05.009 Disponible en: https://www.sciencedirect.com/science/article/pii/S2096249521000429

Vinuesa, R.; Azizpour, H.; Leite, I.; Balaam, M.; Dignum, V.; Domisch, S.; Felländer, A.; Langhans, S. D.; Tegmark, M. y Fuso Nerini, F. (2020). The role of artificial intelligence in achieving the sustainable development goals. *Nature Communications,* 11, 233. https://doi.org/10.1038/s41467-019-14108-y Disponible en: https://www.nature.com/articles/s41467-019-14108-y.pdf