

INTELIGENCIA ARTIFICIAL Y SOSTENIBILIDAD DIGITAL

Infraestructura, Seguridad y Ciudadanía Inteligente



**Coordinador
Juan Mejía Trejo**



INTELIGENCIA ARTIFICIAL Y SOSTENIBILIDAD DIGITAL

*Infraestructura, Seguridad
y Ciudadanía Inteligente*



INTELIGENCIA ARTIFICIAL Y SOSTENIBILIDAD DIGITAL

*Infraestructura, Seguridad
y Ciudadanía Inteligente*

Juan Mejía Trejo
(Coordinador)



AMIDI
Academia Mexicana
de Investigación y Docencia
en Innovación

Este libro fue sometido a un proceso de dictamen por pares doble ciego, de acuerdo con las normas establecidas por el Comité Editorial de la editorial Academia Mexicana de Investigación y Docencia en Innovación (AMIDI).



Esta obra se encuentra bajo la licencia Atribución-No Comercial-Sin Derivadas 4.0 (CC BY-NC-ND 4.0), de Creative Commons. Usted puede descargar esta obra y distribuir en cualquier medio o formato dando crédito a los autores, pero no se permite su uso comercial ni la generación de obras derivadas.

Primera edición, 2026

© D.R. 2026, Academia Mexicana de Investigación
y Docencia en Innovación (AMIDI)
Av. Paseo de los Virreyes 920, Col. Virreyes Residencial
C.P. 45110, Zapopan, Jalisco, México
direccion@amidi.mx

Maquetación y diseño: Ediciones de La Noche

Distribución digital: Academia Mexicana de Investigación y Docencia en Innovación (AMIDI). Responsable del registro DOI, la gestión de metadatos y la publicación en AMIDI.Biblioteca.



AMIDI
Academia Mexicana
de Investigación y Docencia
en Innovación

ISBN AMIDI: 978-607-26875-9-2

Hecho en México
Made in Mexico

Contenido

Introducción	1
Juan Mejía-Trejo	
Capítulo 1. IA y centros de datos: Crisis energética y sostenibilidad verde	3
Juan Mejía-Trejo	
Juan Mejía-Mancilla	
Capítulo 2. Tecnologías de información, inteligencia artificial y sostenibilidad en ecosistemas hiperconvergentes para el desarrollo futuro	27
Hernán Rivera-Melendrez	
Capítulo 3. Aplicaciones móviles inteligentes para la sostenibilidad: de la conciencia ambiental a la acción ciudadana mediada por IA.	49
Fabricio Francisco Hernández-Gómez	
Capítulo 4. <i>Multicast</i> inteligente adaptativo: un modelo de transmisión seguro impulsado por aprendizaje automático	75
José Isidro Cerda-Silva	
Capítulo 5. Aplicación de herramientas de inteligencia artificial para facilitar el cumplimiento de ISO/IEC 27001	93
Héctor Andrés Alcalá-Gutiérrez	

Introducción

La acelerada e inusitada expansión de la inteligencia artificial está reconfigurando de manera profunda las bases energéticas, tecnológicas y sociales sobre las cuales operan las instituciones contemporáneas. Este proceso de transformación plantea desafíos significativos en términos de sostenibilidad, seguridad y gobernanza, al tiempo que abre oportunidades para el diseño de infraestructuras digitales más eficientes y orientadas al bienestar social. En este contexto, el *eBook IA y sostenibilidad digital: infraestructura, seguridad y ciudadanía inteligente* reúne cinco contribuciones que, desde enfoques complementarios, analizan cómo la transformación digital puede encaminarse hacia un desarrollo tecnológico responsable, seguro y centrado en las personas.

El volumen articula una visión integral en la que la innovación tecnológica dialoga con la responsabilidad social y la sostenibilidad a largo plazo, abordando problemáticas críticas asociadas al crecimiento exponencial de la infraestructura digital. El primer capítulo examina la creciente demanda energética de los centros de datos impulsada por modelos avanzados de inteligencia artificial, y propone un marco analítico para comprender la sostenibilidad operativa de infraestructuras críticas en escenarios de alta complejidad tecnológica.

El segundo capítulo profundiza en el papel de las arquitecturas hiperconvergentes como elemento clave para la construcción de ecosistemas de tecnologías de la información resilientes, capaces de integrar eficiencia energética, automatización de procesos y reducción de riesgos operativos. A continuación, el tercer capítulo vincula la inteligencia artificial con la acción ciudadana mediante el análisis de aplicaciones móviles orientadas a fomentar la conciencia ambiental, la participación social y la toma de decisiones informada en entornos urbanos.

El cuarto capítulo introduce un modelo de transmisión inteligente basado en MIA (Multicast Inteligente Adaptativo), diseñado para atender de manera simultánea los desafíos de seguridad, eficiencia energética y continuidad operativa en redes distribuidas. Finalmente, el quinto capítulo analiza el potencial de las herramientas de inteligencia artificial para fortalecer la gobernanza y el cumplimiento normativo, particularmente en sistemas de gestión alineados con la norma ISO/IEC 27001, mediante la mejora de la trazabilidad, la reducción de la carga operativa y el apoyo a la toma de decisiones estratégicas.

En conjunto, este libro invita a recorrer un ecosistema en el que la infraestructura digital, la seguridad de la información y la ciudadanía convergen para enfrentar los retos de un mundo profundamente interconectado. Más que una recopilación de estudios independientes, la obra constituye una propuesta colectiva que concibe la sostenibilidad digital como un compromiso ético, técnico y social indispensable para el futuro de la transformación digital.

Capítulo 1

IA y centros de datos: Crisis energética y sostenibilidad verde

Juan Mejía-Trejo¹

Juan Mejía-Mancilla²

Resumen

El estudio se plantea en un contexto donde el crecimiento súbito e inesperado de la inteligencia artificial hace intenso el consumo energético de los centros de datos, lo cual produce incertidumbre sobre su viabilidad futura. Basado en esto, se planteó la pregunta de investigación: ¿Cuál es el modelo teórico de sostenibilidad energética de un centro de datos con demanda de IA? Esta interrogación definió el problema central y orientó el propósito del ensayo: la construcción de un marco analítico capaz de explicar la interacción de la demanda energética de IA, la infraestructura eléctrica, la eficiencia tecnológica y la gestión organizacional como sostenimiento energético de estas

1. Universidad de Guadalajara, Guadalajara, Jalisco, México. email: jmejia@cucea.udg.mx. ORCID: 0000-0003-0558-1943
2. Academia Mexicana de Investigación y Docencia en Innovación, Guadalajara, Jalisco, México. email: jmejia@amidi.mx. ORCID:0009-0006-9451-2745

infraestructuras. En 2025 se realizó una revisión documental sistemática del estado del arte y se diseñó una propuesta metodológica futura basada en PLS-SEM para su validación empírica. El proceso permitió la identificación de patrones, vacíos y factores clave base de la propuesta para el modelo teórico integrador. Se obtuvieron hallazgos teóricos (*Scientia*) que establecen la estructura sistémica del fenómeno energético a través del descubrimiento de variables y su interrelación, mientras que los hallazgos prácticos (*Praxis*) ofrecieron elementos clave para la toma de decisiones de los administradores de los centros de datos. El estudio es original por describir e integrar cuatro variables predictoras en un modelo multidisciplinario y coherente. Se concluyó finalmente que la sostenibilidad energética en un centro de datos con intensa demanda de IA depende de un equilibrio entre tecnología, infraestructura y gobernanza, se reconocen limitaciones asociadas a la falta de validación empírica, y se proponen líneas futuras de investigación.

Palabras clave: inteligencia artificial, centros de datos, eficiencia energética, sostenibilidad verde, crisis energética

1. Introducción

En 2024, el consumo energético de centros de datos en EE. UU. superó el 4% de la demanda eléctrica nacional (Shehabi *et al.*, 2024), lo que evidencia una presión sin precedentes por el crecimiento acelerado de la inteligencia artificial. Es así que los centros de datos se han convertido en una infraestructura crítica destinada a sostener las aplicaciones más avanzadas de la IA. Sin embargo, su veloz crecimiento ha intensificado el consumo de energía eléctrica, lo cual ha generado serias preocupaciones respecto a la estabilidad y la sostenibilidad del suministro. Varios estudios recientes han demostrado que estas infraestructuras han alcanzado demandas de consumo equiparables con las de países completos, lo que demuestra la urgencia de realizar análisis para proponer correcciones al impacto energético de manera planeada (Aslan *et al.*, 2024; Masanet *et al.*, 2020). El estado del arte también reveló que los centros de datos han evolucionado hacia arquitecturas más especializadas y densas, e impulsado a los modelos de IA más sofisticados, que han aumentado de forma exponencial los requeri-

mientos computacionales. Aunque han avanzado las tecnologías de eficiencia, tales como la refrigeración líquida o los sistemas eléctricos optimizados, aún persisten límites a escala estructural que restringen su efecto mitigador (Khosravi *et al.*, 2024; Mondal *et al.*, 2023). Además, la revisión de literatura más reciente, ha mostrado el vacío de modelos conceptuales o teóricos que sean capaces de articular al mismo tiempo la demanda energética, la vulnerabilidad eléctrica, la eficiencia operativa y la gobernanza sostenible, lo que obstaculiza anticipar los impactos para diseñar estrategias coherentes (Murino *et al.*, 2023; Wang *et al.*, 2024). Por otro lado, los diagnósticos energéticos han revelado la creciente vulnerabilidad en los sistemas eléctricos nacionales. En México, por ejemplo, el PRODESEN 2024–2038 documentó rezagos muy significativos en la infraestructura, así como una demanda en constante ascenso que amenaza la estabilidad del suministro eléctrico (IMCO, 2024; SENER, 2023). En los Estados Unidos, los informes federales han registrado incrementos súbitos relacionados con megacentros de datos de IA (Shehabi *et al.*, 2024; DOE, 2024). A escala global se tienen proyecciones de un crecimiento sostenido del consumo energético asociado a IA para la próxima década (McKinsey, 2024).

Ante este panorama, el presente ensayo examina críticamente la interdependencia entre la IA, los centros de datos y la sostenibilidad energética, y propone un modelo teórico orientado a responder la pregunta: *¿cuál es el modelo teórico de sostenibilidad energética de un centro de datos con demanda de IA?* La propuesta aporta una visión estratégica y multidisciplinaria que implica aspectos ambientales y sociales.

2. Desarrollo

En este apartado se presenta la sección 2.1, que contextualiza el panorama de tecnología y energía como consecuencia del crecimiento acelerado de la inteligencia artificial y la infraestructura digital que la sostiene. También se problematiza sobre cómo dicha expansión ha intensificado la demanda y, por lo tanto, la presión sobre los sistemas eléctricos, lo cual genera cuestionamientos muy críticos respecto de la operación sostenible de los centros de datos. Esta reflexión inicial permite dimensionar inicialmente la magnitud del desafío y justifica la

revisión de antecedentes en tres planos, mundial, internacional y nacional, la cual se desarrolla en la sección 2.2, así como un análisis del estado del arte expuesto en la sección 2.3, donde se examinan diversos modelos, hallazgos científicos y enfoques metodológicos que explican la compleja interdependencia entre IA, consumo energético y sostenibilidad.

2.1. Contexto y problematización

La segunda década del siglo XXI es testigo de una expansión altamente demandante de la infraestructura digital, junto a un crecimiento exponencial de la inteligencia artificial, lo cual ha transformado de manera profunda el panorama energético mundial. Los centros de datos, en otro tiempo considerados solo soportes tecnológicos, se convirtieron en nodos críticos donde la demanda eléctrica tiene un impacto directo en la estabilidad de los sistemas energéticos nacionales y la agenda global de sostenibilidad. En la última década se tienen múltiples informes técnicos que muestran que el consumo energético aumentó a ritmos superiores a los previstos, lo cual ha obligado a recalibrar estimaciones y a replantear la comprensión del fenómeno desde perspectivas multidisciplinarias. La complejidad del problema no radica únicamente en el consumo eléctrico absoluto, sino también en su interacción con factores como emisiones de carbono, capacidad de las redes, disponibilidad de energías renovables, avances tecnológicos y gobernanza digital (US Department of Energy. DOE. 2024).

Este escenario genera una tensión estructural que abre un cuestionamiento clave sobre cómo sostener energéticamente el crecimiento de la IA cuando los sistemas eléctricos muestran límites físicos, tecnológicos y ambientales. La literatura internacional ha señalado riesgos crecientes de saturación de redes, desigualdades en infraestructura, modelos de eficiencia insuficientes y vulnerabilidades derivadas de la hiperconcentración de cargas asociadas a IA. En países como México, estas son más agudas por los rezagos históricos en brechas digitales y en la inversión eléctrica. Por lo anterior es necesario construir un marco de referencia que integre antecedentes mundiales, internacionales y nacionales, así como el estado del arte en sostenibilidad, eficiencia, emisiones y arquitectura energética. Esta problematización fundamenta la necesidad de un *modelo teórico de sostenibilidad energética para centros*

de datos con demanda de IA, capaz de articular los hallazgos dispersos y responder a un desafío tecnológico de escala creciente, dada la inviabilidad de sostener el crecimiento exponencial de la IA bajo sistemas eléctricos diseñados para demandas lineales del siglo xx.

2.2. Antecedentes del estado de la cuestión

Esta sección se orienta a verificar los antecedentes que contextualizan la evolución energética y tecnológica de los centros de datos a escala mundial, internacional y en México. La sección 2.3 expone el estado del arte y reúne los modelos, investigaciones y enfoques teóricos más importantes sobre IA, el consumo energético y la sostenibilidad, lo que proporciona el fundamento científico para el análisis base del modelo propuesto.

2.2.1. MUNDIAL

A escala mundial, infraestructura digital y su acelerado crecimiento muestran un significativo incremento de la demanda energética, lo cual es notable en los centros de datos que sostienen servicios en la nube, procesamiento masivo de información y, más que todo, aplicaciones de inteligencia artificial. Los informes internacionales revelaron que estas infraestructuras consumen volúmenes de electricidad comparables a los de industrias, e incluso países completos, lo que ha generado preocupación en consultoras estratégicas y organismos multilaterales. Por ejemplo, La Agencia Internacional de Energía (IEA, 2024) advirtió que el crecimiento de la IA podría duplicar la demanda eléctrica de centros de datos hacia 2030. Masanet *et al.* (2020) han recalibrado las estimaciones globales del uso energético, y muestran que la eficiencia operativa, los avances tecnológicos y la distribución de cargas modificaron sustancialmente las proyecciones iniciales, lo cual revela un fenómeno complejo con la necesidad de proponer el diseño de modelos de evaluación más robustos.

Estudios como el de Aslan *et al.* (2024), en años posteriores, han documentado que los centros de datos aumentaron sus emisiones de gases con efecto invernadero, aun cuando implementaron tecnologías de mitigación avanzadas. Por lo tanto, esto reforzó la discusión sobre la

urgencia de lograr la neutralidad climática a partir de estrategias integradas de optimización térmica, rediseño arquitectónico y transición hacia energías renovables. Al mismo tiempo, las investigaciones globales han presentado marcos conceptuales a fin de guiar el desarrollo sostenible de dichas infraestructuras. Murino *et al.* (2023), por ejemplo, han propuesto un enfoque holístico que articula la responsabilidad ambiental, la circularidad y la eficiencia energética, en el diseño y la operación de los centros de datos.

La literatura también ha demostrado un creciente interés en analizar la relación entre IA y consumo energético. McKinsey (2024) ha advertido que la demanda originada por cargas de IA ha crecido a un ritmo que supera la capacidad de expansión de diversos sistemas eléctricos, lo cual genera riesgos de vulnerabilidad por saturación. De igual manera, Deloitte (Ramachandran *et al.*, 2024) ha señalado que la IA generativa ha incrementado exponencialmente las necesidades de energía limpia, estable y accesible, lo que ha reconfigurado por completo la agenda mundial de infraestructura digital sostenible.

2.2.2. INTERNACIONAL

En el ámbito internacional, múltiples gobiernos y organismos han enfrentado desafíos similares, y han desarrollado estudios para comprender la magnitud del problema de mejor manera. En Estados Unidos, por ejemplo, el Lawrence Berkeley National Laboratory elaboró el *United States Data Center Energy Usage Report* (Shehabi *et al.*, 2024), el cual registró un aumento sostenido en el consumo eléctrico de centros de datos, resaltando, en particular, los enfocados en cargas intensivas de IA. El DOE (2024) complementó este análisis y advirtió que la expansión de instalaciones en el nivel hiperescala ha modificado patrones de consumo regionales, con la resultante presión de nodos críticos eléctricos y aumento de la necesidad de diversificación energética.

En paralelo, organismos legislativos han analizado lo que implica este crecimiento. El Congreso de los Estados Unidos, a través del Congressional Research Service (USCRS (2025), generó un compendio sobre preguntas más frecuentes de los centros de datos y su consumo energético. En dicho informe se enfatizó en la falta de estudios integrales que vincularan las emisiones, el impacto ambiental, la infraestructura digital y la resiliencia energética. Dichos documentos se han convertido

en referentes clave para comprender la problemática en América del Norte y, por analogía, para otros países con dinámicas similares.

En Europa, Takci *et al.* (2025) han avanzado en la investigación sobre lo que ofrece el potencial de los centros de datos para convertir en recursos flexibles los sistemas eléctricos, almacenar energía, capaces de modular cargas con participación activa en la gestión de la demanda. Este punto de vista cuestionó la visión tradicional que considera los centros de datos solo como un recurso consumidor de tipo pasivo, para abrir la discusión sobre nuevas arquitecturas energéticas dentro del ecosistema digital.

Asimismo, la literatura internacional incorpora modelos predictivos que calculan el impacto energético según clima, localización o demanda computacional. Zhang y Liu (2022) desarrollaron modelos que predicen el consumo energético basados en factores geográficos, y evidenciaron que la ubicación de los centros de datos influye notablemente en su gasto energético y la huella ambiental.

2.2.3. MÉXICO

En México la discusión adquiere relevancia creciente, conforme el país busca consolidarse estratégicamente como un polo de infraestructura digital en América Latina. El sistema eléctrico nacional enfrenta todos los días retos históricos derivados de la falta de inversión, la dependencia de combustibles fósiles y la insuficiencia de redes de transmisión. El *PRODESEN 2023–2037* (SENER, 2023) presenta escenarios que muestran cómo la demanda energética del país ha crecido de forma sostenida, agravada por la incorporación de sectores intensivos en electricidad, entre ellos los centros de datos.

El análisis del Instituto Mexicano para la Competitividad (IMCO, 2024) mostró que la expansión de infraestructura digital no estaba acompañada por mejoras proporcionales en el sistema eléctrico, lo que generó un riesgo de cuellos de botella en regiones clave. El Instituto Federal de Telecomunicaciones (IFT, 2024), además, ha evidenciado desigualdad en la infraestructura digital, lo que señala que el desarrollo de centros de datos depende de condiciones locales de conectividad, seguridad crítica y, sobre todo, energía. Estas disparidades limitan la capacidad del país para atraer inversión de tecnología de alto nivel sin comprometer la estabilidad del sistema eléctrico.

Investigaciones en Latinoamérica complementan este panorama. Sampedro Guamán *et al.* (2021) han documentado impactos ambientales relevantes como consecuencia del consumo energético en centros de datos, mientras que Rodríguez-Vizueté *et al.* (2024) han mostrado que la adopción de tecnologías sostenibles en infraestructura TI ha avanzado, pero enfrentando barreras regulatorias, económicas y de capacitación. Estos estudios han confirmado que México se encuentra en rezago crítico en dos aspectos clave, infraestructura eléctrica y prácticas de sostenibilidad digital, lo que subraya la urgencia de estrategias nacionales integrales.

2.3. Descripción del estado del arte

Sobre el estado del arte, la relación entre centros de datos, inteligencia artificial, eficiencia energética y sostenibilidad a largo plazo mostró una evolución notable en la última década. La literatura técnica y científica se centró en comprender cómo el crecimiento exponencial del procesamiento digital, impulsado por la IA generativa y el aprendizaje profundo, que ha intensificado las demandas energéticas, genera desafíos inéditos para la infraestructura eléctrica mundial. Este conocimiento aporta definiciones, aproximaciones metodológicas diversas y modelos teóricos que permitieron analizar el fenómeno desde perspectivas de gobernanza, ambientales y técnicas.

Tomando en cuenta lo anterior, se revelan estudios sobre el consumo energético recalibrado que marcan un punto de inflexión. Masanet *et al.* (2020) redefinieron los estimados mundiales sobre el gasto energético en centros de datos y demostraron que las proyecciones previas habían subestimado la complejidad real de la demanda. Su trabajo evidencia que el consumo no podía explicarse solo por el aumento de cargas computacionales, sino que también se debe incorporar eficiencia energética, densidad de hardware, variaciones geográficas y cambios arquitectónicos. Esta contribución abre el camino para investigaciones que se orienten a examinar los impactos ambientales y estructurales del crecimiento digital.

A partir de estos hallazgos surgen modelos integrales que analizan la interacción entre estrategias de sostenibilidad, infraestructura energética y tecnologías de mitigación. Aslan *et al.* (2024) realizaron inventario de escenarios y emisiones climáticos para centros de datos,

con la conclusión de que la neutralidad de carbono solo es viable a través de transformaciones sistémicas en los suministros energéticos y con la adopción masiva de energías renovables. Su estudio usó técnicas muy avanzadas de evaluación ambiental que posicionan los centros de datos como actores clave en la transición climática.

Por otro lado, Murino *et al.* (2023) han propuesto un marco holístico para el diseño y la operación de centros de datos sostenibles basado en cuatro pilares: circularidad de materiales, eficiencia energética, responsabilidad ambiental y optimización operativa. Este enfoque multidimensional ha superado las visiones centradas únicamente en la eficiencia eléctrica, por lo cual permite comprender la sostenibilidad como un proceso continuo y estructural.

Los avances tecnológicos también han ocupado un lugar central. En la revisión de Khosravi *et al.* (2024), por ejemplo, se analizó las innovaciones en baterías avanzadas, alimentación eléctrica, arquitecturas de distribución y sistemas de enfriamiento, y se demostró que, aunque estos avances han mejorado la eficiencia, no eliminan la presión sistémica sobre la gran demanda total. A su vez, los modelos predictivos, tales como los de Zhang y Liu (2022), demostraron que el consumo energético depende no solo de la tecnología empleada, sino también de factores climáticos y geográficos.

La literatura sobre demanda energética e IA ha profundizado en la magnitud del desafío emergente. McKinsey (2024) ha estimado que los modelos de IA generativa multiplicaron los requerimientos de cómputo especializado, lo cual aumentó la densidad de instalaciones con aceleradores y GPU, cuya demanda eléctrica supera la capacidad prevista en varios sistemas eléctricos nacionales. Deloitte (Ramachandran *et al.*, 2024) complementó esta visión al señalar que la IA ha transformado la relación entre la infraestructura energética y los centros de datos, incrementando la demanda total y los requerimientos de suministros limpios, estables y resilientes.

Otra línea de investigación muy importante ha abordado los centros de datos como elementos activos dentro de los sistemas eléctricos. Takci *et al.* (2025) han explorado el potencial de estas infraestructuras a fin de participar en esquemas de soporte a redes inteligentes flexibles de energía, gestión de cargas y almacenamiento, reconfigurando su función tradicional como consumidores pasivos, e identificar oportunidades de integración energética.

De forma complementaria, estudios como los de Mondal *et al.* (2023) han analizado la optimización energética mediante modelos como GEECO, que integran estrategias de mitigación, huella de carbono y eficiencia. Estos trabajos han demostrado que las decisiones de diseño y operativas reducen significativamente el impacto ambiental si existe coordinación entre los ejes de ingeniería, políticas energéticas y objetivos climáticos.

En América Latina y México, la literatura ha presentado un desarrollo muy incipiente, pero a la vez significativo. Rodríguez-Vizueté *et al.* (2024), por ejemplo, han identificado barreras técnicas, económicas y regulatorias en la adopción de tecnologías verdes incorporadas en la infraestructura TI, mientras que Sampedro Guamán *et al.* (2021) han documentado impactos ambientales como consecuencia del consumo eléctrico. Estos estudios han evidenciado que los desafíos mundiales se expresaban de manera diferenciada en contextos con infraestructura limitada y políticas energéticas en transición.

En conjunto, el estado del arte mostró que la problemática entre crisis energética, IA, y los centros de datos requiere enfoques integrales que combinen planificación estratégica, sostenibilidad ambiental, gobernanza energética y eficiencia tecnológica. La literatura también reveló vacíos relevantes, especialmente la falta de modelos teóricos que articulen de forma sistémica la relación entre la estructura energética, la IA, y la sostenibilidad de largo plazo, lo que justifica la construcción de nuevos marcos teóricos y conceptuales para anticipar las implicaciones de la creciente interdependencia entre tecnología y energía.

3. Metodología

La metodología empleada en este estudio se diseñó con el propósito de analizar, desde un enfoque científico y aplicado, los factores que explican la sostenibilidad energética de los centros de datos en un contexto caracterizado por la rápida expansión de la inteligencia artificial (IA). Dado que el objetivo central fue identificar relaciones causales entre variables técnicas, infraestructurales y organizacionales entre los responsables de los centros de datos, se adoptó un enfoque cuantitativo explicativo, idóneo para operacionalizar constructos complejos y

validarlos mediante modelado de ecuaciones estructurales por mínimos cuadrados parciales (PLS-SEM), así como para analizar los distintos puntos de vista mediante Atlas.ti. Este enfoque permitió representar la interacción entre demanda energética, eficiencia tecnológica, capacidades del sistema eléctrico y gobernanza organizacional, dimensiones ampliamente documentadas en la literatura reciente sobre centros de datos (Masanet *et al.*, 2020; McKinsey & Company, 2024).

3.1. Técnicas de análisis utilizadas

El desarrollo metodológico integró cuatro técnicas principales. En primer lugar, se realizó un análisis bibliométrico para identificar tendencias conceptuales sobre IA, consumo energético y sostenibilidad. Este análisis evidenció que el consumo asociado a la IA crece de forma acelerada debido al entrenamiento y a operación de modelos avanzados, lo cual sustenta la variable *demanda energética de IA* (Shehabi *et al.*, 2024; U.S. DOE, 2024).

En segundo término, se efectuó un análisis documental comparativo de informes técnicos y regulatorios (PRODESEN, DOE, IFT, Congreso de EEUU). La revisión mostró tensiones estructurales en los sistemas eléctricos nacionales, especialmente en países donde la demanda crece más rápido que la capacidad instalada (SENER, 2023; IMCO, 2024). Estas evidencias fundamentan la segunda variable: *infraestructura eléctrica y capacidad de suministro*.

La tercera técnica fue un análisis comparativo tecnológico destinado a sistematizar innovaciones que optimizan el uso energético de centros de datos. Entre ellas destacan sistemas de refrigeración avanzados, arquitecturas eléctricas más eficientes y estrategias hacia la neutralidad climática (Aslan *et al.*, 2024; Khosravi *et al.*, 2024). Estos elementos permitieron consolidar la variable *eficiencia tecnológica del centro de datos*.

Finalmente, se desarrolló un análisis estructural de gobernanza organizacional, sustentado en investigaciones que muestran que la sostenibilidad depende de políticas internas, capacidades de gestión y marcos de cumplimiento ambiental (Rodríguez-Vizueté *et al.*, 2024; IFT, 2024). Esta revisión justificó la cuarta variable: *gestión organizacional de la sostenibilidad*.

Sobre la base de estas técnicas, se diseñó un esquema de relación de variables (esquema 1) con la posibilidad de diseñar una escala de Likert para consultar a especialistas de centros de datos (anexo) y aplicar posteriormente un análisis de carácter cuantitativo vía estadística inferencial vía PLS-SEM (Partial Least Squares-Structural Equation Modelling), así como uno cualitativo vía Atlas.ti.

3.2. Resultados preliminares y producto metodológico

Los resultados preliminares de los análisis bibliométrico, documental y tecnológico permitieron identificar patrones clave que dieron forma al modelo teórico.

En primer lugar, se verificó que la presión energética generada por el crecimiento de la IA es un factor determinante que compromete la estabilidad operativa de los centros de datos (Shehabi *et al.*, 2024; McKinsey & Company, 2024). En segundo lugar, la literatura mostró que la capacidad del sistema eléctrico es una condición estructural indispensable para su sostenibilidad, en especial en contextos con brechas de infraestructura (IMCO, 2024; SENER, 2023).

En tercer término, se confirmó que la eficiencia tecnológica contribuye significativamente a la mitigación de consumo y emisiones (Aslan *et al.*, 2024; Murino *et al.*, 2023). Finalmente, se identificó que la gobernanza organizacional —políticas internas, gestión ambiental y toma de decisiones estratégicas— influye directamente en la adopción de prácticas energéticas sostenibles (Rodríguez-Vizueté *et al.*, 2024).

3.3. Propuesta del modelo teórico

El modelo teórico integra cuatro variables independientes que, según la evidencia reciente, explican de manera conjunta la *sostenibilidad energética del centro de datos con demanda de IA* (variable dependiente). El modelo articula dimensiones técnicas, infraestructurales, tecnológicas y organizacionales, lo cual permite una interpretación sistémica.

3.3.1. DEMANDA ENERGÉTICA DE IA

Sustentada en estudios que documentan el rápido aumento del consumo eléctrico derivado de modelos generativos y algoritmos de aprendizaje profundo (Shehabi *et al.*, 2024; DOE, 2024), esta variable captura la presión directa que la IA ejerce sobre los sistemas energéticos del centro de datos. El incremento en el uso de GPU y la necesidad de redundancia energética han sido ampliamente informados en análisis financieros recientes (S&P Global Ratings, 2025).

3.3.2. INFRAESTRUCTURA ELÉCTRICA Y CAPACIDAD DE SUMINISTRO

Está basada en informes que advierten tensiones entre la demanda creciente y la capacidad de generación, en especial en México y Estados Unidos. Documentos como el PRODESEN 2024–2038 señalan vulnerabilidades asociadas al crecimiento industrial y digital (IMCO, 2024; SENER, 2023). Esta variable describe el entorno energético externo que condiciona la sostenibilidad operativa.

3.3.3. EFICIENCIA TECNOLÓGICA DEL CENTRO DE DATOS

Integra innovaciones en refrigeración, arquitecturas eléctricas, sistemas UPS (*Uninterruptible Power Supply*) inteligentes y metodologías de reducción del PUE (*Power Usage Effectiveness*). La literatura demuestra que la eficiencia tecnológica es un factor mitigador clave para disminuir consumo y emisiones y avanzar hacia la neutralidad climática (Aslan *et al.*, 2024; Khosravi *et al.*, 2024).

3.3.4. GESTIÓN ORGANIZACIONAL DE LA SOSTENIBILIDAD

Incluye políticas internas, métricas ambientales, gobernanza y procesos de toma de decisiones. La literatura reciente muestra que la adopción de tecnologías verdes depende tanto de capacidades técnicas como de marcos organizacionales sólidos (Rodríguez-Vizueté *et al.*, 2024; IFT, 2024).

3.3.5. SOSTENIBILIDAD ENERGÉTICA DEL CENTRO DE DATOS CON

DEMANDA DE IA

Esta variable integra indicadores como resiliencia del suministro, uso de energías renovables, reducción de emisiones y optimización del consumo (Wang *et al.*, 2024; Takci *et al.*, 2025). Se parte de que la sostenibilidad es resultado de la interacción entre presión de demanda, infraestructura eléctrica, eficiencia tecnológica y gobernanza organizacional.

Esquema 1. Modelo propuesto de sostenibilidad energética de un centro de datos con demanda de IA



Fuente: Elaboración propia.

4. Discusión

La sostenibilidad energética de centros de datos con alta demanda de IA depende de la interacción dinámica entre cinco dimensiones clave: demanda energética de IA, infraestructura eléctrica y capacidad de suministro, eficiencia tecnológica, gestión organizacional de la sostenibilidad y sostenibilidad energética resultante. La literatura reciente coincide en que estos factores no operan de manera aislada, sino conforman un sistema interdependiente donde tecnología, energía y gobernanza interactúan continuamente (Aslan *et al.*, 2024; McKinsey, 2024; Murino *et al.*, 2023).

La demanda energética de la IA es, por el momento, uno de los principales impulsores de presión sobre los sistemas eléctricos. Los informes técnicos del DOE (2024), así como análisis financieros globales (S&P Global Ratings, 2025), apuntan a que los modelos de IA generativa, así como el cómputo acelerado, seguirán incrementando el consumo eléctrico a tasas superiores a la capacidad actual de crecimiento de la infraestructura. Dicho patrón confirma la importancia de esta variable, ya que es el centro estructural del problema. No obstante, persiste una gran incertidumbre: las estimaciones energéticas han cambiado año tras año por causa de la rápida evolución tecnológica, lo cual dificulta la modelación de tendencias estables (McKinsey, 2024).

La infraestructura eléctrica y la capacidad de suministro constituyen el segundo eje del modelo. En países como México, los informes PRODESEN 2024–2038 documentan tensiones significativas en transmisión, generación renovable y capacidad de integración de nuevas cargas críticas (SENER, 2023; IMCO, 2024). Esta variable permite comprender que la sostenibilidad operativa no depende únicamente del centro de datos, sino también del ecosistema eléctrico que lo sostiene. Su limitante radica en que su impacto varía según el contexto regional, por lo que requiere ajustes territoriales para conservar validez analítica.

La eficiencia tecnológica del centro de datos representa el espacio donde las innovaciones han mostrado mayores avances. Tecnologías como refrigeración líquida, UPS inteligentes, mejoras en PUE y arquitecturas eléctricas optimizadas han permitido mitigar parte del crecimiento energético (Khosravi *et al.*, 2024; Mondal *et al.*, 2023). Sin embargo, existe consenso en que la eficiencia presenta límites: incluso los centros de datos más avanzados mantienen un consumo elevado cuando la demanda de IA crece exponencialmente y la matriz eléctrica continúa dependiendo de combustibles fósiles (Aslan *et al.*, 2024).

La gestión organizacional de la sostenibilidad explica la dimensión humana, institucional y estratégica del desempeño energético. La evidencia muestra que la adopción de tecnologías verdes y buenas prácticas depende de capacidades gerenciales, cultura organizacional y marcos normativos (Rodríguez-Vizúete *et al.*, 2024; IFT, 2024). Esta variable es crucial porque determina si las mejoras técnicas se implementan de forma sostenida. Sin embargo, su debilidad radica en la ausencia de métricas estandarizadas para comparar organizaciones y medir avances de forma objetiva.

Finalmente, la sostenibilidad energética del centro de datos emerge como resultado sistémico. Modelos recientes integran resiliencia eléctrica, disponibilidad renovable, estabilidad operativa y reducción de emisiones (Wang *et al.*, 2024; Takci *et al.*, 2025), en línea con la estructura propuesta. No obstante, su viabilidad depende de condiciones estructurales que muchas regiones aún no poseen, lo que obliga a adaptar el modelo a niveles diferenciados de madurez tecnológica y energética (tabla 1).

Tabla 1. Pros y contras del modelo teórico propuesto

Variable	Pros	Contras
Demanda energética de IA	Identifica el principal impulsor del consumo; fuerte respaldo empírico.	Tendencias volátiles y difíciles de proyectar.
Infraestructura eléctrica y capacidad de suministro	Explica el límite estructural del sistema; evidencia robusta.	Alta dependencia del contexto nacional.
Eficiencia tecnológica del centro de datos	Reduce consumo y emisiones; amplio soporte técnico.	No compensa el crecimiento absoluto de la IA.
Gestión organizacional de la sostenibilidad	Reconoce el papel crítico de la gobernanza.	Falta de métricas estandarizadas.
Sostenibilidad energética del centro de datos con demanda de IA	Integra resiliencia y renovabilidad.	Requiere condiciones externas que no controla el operador.

Fuente: Elaboración propia.

5. Conclusión

La sección 5 sintetiza los aportes finales del ensayo. Explica que la pregunta de investigación se responde al demostrar que la sostenibilidad

energética de centros de datos con demanda de IA requiere un enfoque integral que combine factores técnicos y organizacionales. Resume los hallazgos clave, reconoce límites derivados de datos y contextos diversos, y plantea recomendaciones para profundizar en estudios empíricos, validación del modelo y análisis prospectivos que fortalezcan la comprensión del vínculo entre IA, energía y sostenibilidad.

5.1. *Cómo responde a la pregunta de investigación base del ensayo*

El estudio responde a la pregunta de investigación al demostrar que la sostenibilidad energética de un centro de datos con alta demanda de IA solo es explicable mediante un marco integral que articula demanda energética, infraestructura eléctrica, eficiencia tecnológica y gestión organizacional. El problema planteado de cómo lograr la armonización el crecimiento acelerado de la IA con un sistema energético sostenible y resiliente es posible de resolver al identificar que ninguna dimensión por sí sola es suficiente. El modelo propuesto establece un nuevo conocimiento al reunir y sintetizar, en primera instancia, hallazgos dispersos de la literatura con un enfoque sistémico y multidisciplinar basado en innovación para el desarrollo sostenible. Esta integración teórica y conceptual permite lograr una aportación original, ya que describe la sostenibilidad energética como un fenómeno complejo donde interactúan gobernanza, tecnología y capacidades estructurales. El ensayo confirma que la transición digital y la transición energética no deben estudiarse por separado, y que su convergencia constituye un campo emergente de alto valor científico.

5.2. *Hallazgos*

Dentro de los principales hallazgos se demuestra que la demanda energética de IA crece más rápido que la eficiencia tecnológica y la capacidad de expansión eléctrica, sin compensar el incremento absoluto del consumo, así como que las organizaciones ocupan un lugar clave y central al decidir cómo implementar mejoras y gestionar la sostenibilidad. Las contribuciones teóricas (*Scientia*) demuestran la

propuesta de un modelo teórico integral que explica la sostenibilidad energética como resultado de interacciones multidimensionales, y aportan una base analítica para futuros estudios y la creación de indicadores especializados. En términos prácticos (*Praxis*), el ensayo registra lineamientos útiles para reguladores, operadores, y tomadores de decisiones, al identificar cuellos de botella, riesgos, y oportunidades de inversión en infraestructura, eficiencia y gobernanza.

5.3. Alcances finales

El estudio muestra resultados con alcances relevantes, entre ellos la propuesta de un marco integral aplicable a distintos contextos tecnológicos y energéticos. Sin embargo, también se reconocen limitaciones, tales como ausencia de estudios longitudinales que midan en tiempo real el impacto de la IA sobre redes eléctricas, disponibilidad limitada de datos recientes en ciertos países, falta de variabilidad contextual en los casos analizados, e insuficiencia de métricas estandarizadas de gestión organizacional, entre otros aspectos. Además, factores externos —políticos, económicos, regulatorios y ambientales— que tienden a modificar la viabilidad de implementación del modelo. Dichas limitaciones son la oportunidad para que se abran investigaciones más amplias y comparativas.

5.4. Recomendaciones

Se recomienda, finalmente, profundizar con estudios empíricos que permitan la medición de la evolución del consumo energético asociado a la IA en distintas regiones y contextos de implementación-operación; desarrollar más métricas sólidas de gobernanza organizacional; hacer propuestas y evaluaciones de escenarios de transición hacia redes inteligentes y energías renovables, y construir simulaciones basadas en prospectiva que articulen IA, infraestructura eléctrica y variabilidad climática. A fin de continuar el modelo, se propone el empleo de Atlas.ti para realizar análisis cualitativos avanzados que permitan identificar percepciones de las prácticas, y patrones organizacionales

vinculados con la sostenibilidad energética en empresas de TI que administren centros de datos usando IA. De manera complementaria, se sugiere validar el modelo mediante técnicas de análisis inferencial tales como el PLS-SEM y, a través de estudios de casos reales en centros de datos industriales y gubernamentales, fortalecer su rigor teórico y su aplicabilidad práctica.

6. Referencias

- Aslan, T., Holzapfel, P., Stobbe, L., Grimm, A., Nissen, N. F., Finkbeiner, M. (2024). Toward Climate Neutral *Data centers*: Greenhouse Gas Inventory, Scenarios, and Strategies. *iScience* 28(1):111637. Disponible en: https://pmc.ncbi.nlm.nih.gov/articles/PMC11773490/?utm_source=chatgpt.com
- Instituto Mexicano para la Competitividad (IMCO) (2024). *Prodesen 2024–2038: El sistema eléctrico mexicano ante el crecimiento de la demanda*. Disponible en: <https://imco.org.mx/prodesen-2024-2038-el-sistema-electrico-mexicano/>
- Instituto Federal de Telecomunicaciones (IFT) (2024). *Índice de Infraestructura Digital*. Disponible en: <https://centrodeestudios.ift.org.mx/admin/files/indicadores/1751482253.pdf> Centro de Estudios
- Khosravi, A., Sandoval, O. R., Taslimi, M. S., Sahrakorpi, T., Amorim, G., & García Pabón, J. J. (2024). Review of Energy Efficiency and Technological Advancements in Data Center Power Systems. *Energy and Buildings*, 323, Article 114834. Disponible en: <https://doi.org/10.1016/j.enbuild.2024.114834>
- Masanet, E., Shehabi, A., Lei, N., Smith, S., & Koomey, J. (2020). Recalibrating Global Data Center Energy-Use Estimates. *Science*, 367(6481), 984–986. Disponible en: <https://doi.org/10.1126/science.aba3758>
- McKinsey & Company (2024, septiembre 17). *How Data centers and the Energy Sector can sate AI's Hunger for Power*. Disponible en: <https://www.mckinsey.com/industries/private-capital/our-insights/how-data-centers-and-the-energy-sector-can-sate-ais-hunger-for-power>
- Mondal, S., Faruk, F. B., Rajbongshi, D., Efaz, M. M. K., & Islam, M. M. (2023). GEECO: Green *Data centers* for Energy Optimization and Carbon Footprint Reduction. *Sustainability*, 15(21), 15249. Disponible en: <https://doi.org/10.3390/su152115249>
- Murino, T., Monaco, R., Nielsen, P. S., Liu, X., Esposito, G., & Scognamiglio, C. (2023). Sustainable Energy Data Centres: A Holistic Conceptual Framework for Design and Operations. *Energies*, 16(15), 5764. Disponible en: <https://doi.org/10.3390/en16155764>

- Rodríguez-Vizute, J. D., Viteri-Ojeda, J. C., & Villa-Feijoo, A. L. (2024). Adopción de tecnologías sostenibles en infraestructuras de tecnologías de la información. *Revista Científica Ciencia y Método*, 2(1), 55-67. Disponible en: <https://doi.org/10.55813/gaea/rcym/v2/n1/31>
- Ramachandran, K., Stewart, D., Hardin, K., & Crossan, G. (2024, noviembre 19). *As Generative AI asks for more Power, Data centers seek more Reliable, Cleaner* Disponible en: <https://www.deloitte.com/us/en/insights/industry/technology/technology-media-and-telecom-predictions/2025/genai-power-consumption-creates-need-for-more-sustainable-data-centers.html>
- Sampedro Guamán, C. R., Machuca Vivar, S. A., Palma Rivera, D. P., & Villalta Jadán, B. E. (2021). Impacto ambiental por consumo de energía eléctrica en los *data centers*. *Dilemas contemporáneos: educación, política y valores*, 8(spe4), 00034. Disponible en: <https://doi.org/10.46377/dilemas.v8i.2786>
- Secretaría de Energía (SENER) (2023). *Prospectiva del sector eléctrico 2023–2037*. Disponible en: https://base.energia.gob.mx/Prospectivas23/PSE_23-37_VF.pdf base.energia.gob.mx
- Shehabi, A., Smith, S. J., Hubbard, A., Newkirk, A., Lei, N., Siddik, M. A., Holec, B., Koomey, J. G., Masanet, E., & Sartor, D. A. (2024, diciembre 19). *2024 United States Data Center Energy Usage Report*. Lawrence Berkeley National Laboratory. Disponible en: <https://eta.lbl.gov/publications/2024-lbnl-data-center-energy-usage-report>
- S&P Global Ratings (2025). *Digital Infrastructure: Data Centers, AI Growth and Implications on Power Demand*. Disponible en: <https://www.spglobal.com/ratings/en/research/digital-infrastructure>
- Takci, M. T., Qadrdan, M., Summers, J., & Gustafsson, J. (2025). Data Centers as a Source of Flexibility for Power Systems. *Energy Reports*, 13, 3661-3671. Disponible en: <https://doi.org/10.1016/j.egy.2025.03.020>
- US Congress, Congressional Research Service (USCRS) (2025, 26 agosto). *Data centers and Their Energy Consumption: Frequently Asked Questions* (Report R48646). Disponible en: <https://crsreports.congress.gov/product/pdf/R/R48646>
- US Department of Energy (DOE) (2024, diciembre 20). *Report evaluates Increase in US Electricity Demand from Data centers*. Disponible en: <https://www.energy.gov/articles/doe-releases-new-report-evaluating-increase-electricity-demand-data-centers>
- Wang Y., Han Y., Shen J., *et al.*, (2024). Data Center Integrated Energy System for Sustainability: Generalization, Approaches, Methods, Techniques, and Future Perspectives. *The Innovation Energy* 1(1): 100014. Disponible en: <https://doi.org/10.59717/j.xinn-energy.2024.100014>
- Zhang, Y., & Liu, J. (2022). Prediction of Overall Energy Consumption of *Data centers* in Different Locations. *Sensors*, 22(10), 3704. Disponible en: <https://doi.org/10.3390/s22103704>

Anexo

Variable	Pregunta Likert	Referencia
ANÁLISIS CUANTITATIVO		
1. Demanda energética de IA	1. Las cargas de IA aumentan de forma considerable el consumo eléctrico del centro de datos.	Shehabi <i>et al.</i> (2024); DOE (2024); S&P Global Ratings (2025)
	2. El uso de GPU para IA genera picos de demanda que presionan la infraestructura energética.	
	3. Los modelos de IA requieren sistemas de respaldo energético adicionales.	
	4. La operación continua de IA incrementa el gasto energético diario del centro de datos.	
	5. La demanda energética por IA supera la capacidad prevista de planificación inicial.	
2. Infraestructura eléctrica y capacidad de suministro	1. La red eléctrica regional puede sostener el crecimiento del centro de datos.	SENER (2023); IMCO (2024); US Congress (2025) Same refs
	2. La capacidad instalada cubre adecuadamente las necesidades actuales y futuras.	
	3. La infraestructura de transmisión es suficiente para evitar interrupciones operativas.	
	4. El suministro eléctrico es estable aun con incrementos en la demanda tecnológica.	
	5. El centro de datos no enfrenta riesgos debido a limitaciones de generación eléctrica.	

Variable	Pregunta Likert	Referencia
ANÁLISIS CUANTITATIVO		
3. Eficiencia tecnológica del centro de datos	1. Las tecnologías de refrigeración implementadas reducen de manera efectiva el consumo energético.	Aslan <i>et al.</i> (2024); Khosravi <i>et al.</i> (2024); Murino <i>et al.</i> (2023); Mondal <i>et al.</i> (2023)
	2. Los sistemas UPS inteligentes contribuyen a la eficiencia del uso de energía.	
	3. La arquitectura eléctrica del centro de datos está optimizada para minimizar pérdidas.	
	4. Las iniciativas para reducir el PUE han mejorado la eficiencia operativa.	
	5. Las tecnologías verdes adoptadas disminuyen la huella de carbono del centro de datos.	
4. Gestión organizacional de la sostenibilidad	1. La organización establece políticas claras para la gestión energética sostenible.	Rodríguez-Vizuite <i>et al.</i> (2024); IFT (2024)
	2. Existen métricas ambientales que guían la toma de decisiones energéticas.	
	3. La dirección promueve inversiones orientadas a la eficiencia energética.	
	4. Los procesos internos favorecen la adopción de tecnologías sostenibles.	
	5. La gobernanza organizacional prioriza prácticas de reducción de emisiones.	
5. Sostenibilidad energética del centro de datos	1. El centro de datos utiliza fuentes de energía renovable de forma significativa.	Wang <i>et al.</i> (2024); Takci <i>et al.</i> (2025); Zhang & Liu (2022)
	2. Las operaciones del centro de datos mantienen estabilidad aun en condiciones de alta demanda.	
	3. El centro de datos ha logrado reducir emisiones respecto a años anteriores.	
	4. Los sistemas energéticos operan de manera eficiente y con bajo desperdicio.	
	5. Las estrategias implementadas fortalecen la resiliencia energética del centro de datos.	

ANÁLISIS CUALITATIVO		
1. Demanda energética de IA	¿Cómo describiría el impacto que tienen las cargas de trabajo de inteligencia artificial (entrenamiento, inferencia, uso de GPU) en el consumo energético del centro de datos?	Shehabi <i>et al.</i> (2024); DOE (2024); S&P Global Ratings (2025)
2. Infraestructura eléctrica y capacidad de suministro	¿Qué retos o limitaciones observa en la infraestructura eléctrica actual para garantizar un suministro continuo y suficiente frente al crecimiento operativo del centro de datos?	SENER (2023); IMCO (2024); U.S. Congress (2025) Same refs
3. Eficiencia tecnológica del centro de datos	¿Qué tecnologías, prácticas o innovaciones considera más relevantes para mejorar la eficiencia energética del centro de datos y por qué?	Aslan <i>et al.</i> (2024); Khosravi <i>et al.</i> (2024); Murino <i>et al.</i> (2023); Mondal <i>et al.</i> (2023)
4. Gestión organizacional de la sostenibilidad	¿Cómo influyen las políticas internas, la gobernanza o las decisiones organizacionales en la adopción de estrategias de eficiencia energética y sostenibilidad dentro del centro de datos?	Rodríguez-Vizuetete <i>et al.</i> (2024); IFT (2024)
5. Sostenibilidad energética del centro de datos con demanda de IA	¿Qué acciones, estrategias o condiciones considera fundamentales para que un centro de datos logre operar de manera sostenible desde el punto de vista energético?	Wang <i>et al.</i> (2024); Takci <i>et al.</i> (2025); Zhang & Liu (2022)

Fuente: Elaboración propia.



This is an open access article distributed under the terms of the CC BY-NC license (<https://creativecommons.org/licenses/by-nc/4.0/>)

Capítulo 2

Tecnologías de información, inteligencia artificial y sostenibilidad en ecosistemas hiperconvergentes para el desarrollo futuro

Hernán Rivera-Melendrez¹

Resumen

La investigación profundizó en cómo la unión de las tecnologías de la información, la IA y la sostenibilidad impacta en los entornos hiperconvergentes, donde el aumento del gasto de energía y el daño al planeta crearon un desafío apremiante para las empresas digitales. En este escenario, la investigación se enfocó en examinar cómo estos sistemas podían fomentar el progreso ecológico y qué factores facilitaban su uso ético. El objetivo del trabajo fue mostrar y analizar modelos, procedimientos y enfoques técnicos a través de una investigación exhaustiva de documentos hecha en 2024. La metodología utilizó el análisis bibliométrico, la revisión organizada y la creación

1. Universidad de Guadalajara, Guadalajara, Jalisco, México. email: herman.rivera@udg.mx.
ORCID: 0009-0000-4646-8205

de modelos conceptuales basados en autores actuales importantes en los campos de la informática y el medio ambiente.

Los resultados teóricos brindaron una visión fresca de la importancia de la IA en la mejora del uso de la energía (*Scientia*), mientras que los resultados prácticos mostraron el valor funcional de la hiperconvergencia en empresas verdaderas (*Praxis*). Lo novedoso del estudio residió en su perspectiva, que unió la informática, la sostenibilidad y la administración tecnológica. Para terminar, la investigación determinó que estos ecosistemas ofrecieron una forma factible de avanzar hacia infraestructuras conscientes, pero admitió problemas derivados de la falta de datos y del veloz avance tecnológico, lo cual generó opciones para futuras investigaciones.

1. Introducción

¿Podrá la red del futuro ser muy fuerte y a la vez cuidar el planeta? Juntar datos, máquinas que piensan y cuidar el mundo es difícil hoy, sobre todo porque los lugares con IA gastan mucha luz (Buyya *et al.*, 2023). Como necesitamos más computadoras, hay que hacerlas mejores: los sistemas que juntan computación, memoria y red en un solo lugar controlado por software son una buena idea para usar mejor los recursos (Esenarro, 2019).

Antes, se miró cómo hacer que los centros de datos cuiden el planeta de muchas formas. Murino *et al.* (2023) pensaron en un plan que mide cuánta energía se usa, cuánta agua y cómo se tiran cosas, usando ideas como juntar programas, mirar la energía y hacer edificios verdes. Además, estudios de energía crearon modelos que mueven el trabajo, usan energía limpia y cambian el frío para gastar menos carbono (Rongon & Das, 2025). También se usaron máquinas que aprenden para manejar centros de datos que cuidan el carbono y el agua (Qi *et al.*, 2023).

A pesar de estos pasos, quedan dudas en los textos: no se ha mirado bien cómo la IA puede juntarse con diseños muy unidos para usar lo mejor posible sin dañar el planeta, ni cómo crear reglas o señales que dejen ver estos nuevos mundos de forma real. Por eso, este texto busca mirar con ciencia la unión entre ti, IA y cuidado del

planeta en mundos muy unidos, viendo opciones, problemas y planes para una unión con cabeza. Se cree que este mirar hará pensar sobre cómo crear y usar lugares muy unidos que aguanten trabajos de IA con un daño menor al medio ambiente.

En especial, se hace esta pregunta: ¿cómo pueden los mundos muy unidos juntar la inteligencia artificial y el cuidado del planeta para dar lo que pide la era digital sin estropear el medio ambiente? Este modo de ver es bueno y nuevo, porque une dos modas tecnológicas que salen —IA e hiperconvergencia— dentro de una idea de cuidar el planeta casi nunca vista a fondo.

2. Desarrollo

A continuación se presentarán contexto y problematización, antecedentes, teoría, metodología y resultados obtenidos.

2.1. Contexto y problematización

Durante las últimas dos décadas, la digitalización global transformó las bases productivas y organizativas de múltiples sectores. Las organizaciones aumentaron progresivamente su dependencia de servicios en la nube, plataformas de procesamiento distribuido y aplicaciones basadas en aprendizaje automático; como consecuencia, se volvió prioritaria la necesidad de infraestructuras más integradas y gestionables (Buyya *et al.*, 2023). En ese contexto emergieron las arquitecturas hiperconvergentes, las cuales integraron cómputo, almacenamiento, red y capa de gestión en un único sistema gestionado por software, con la promesa de facilitar la administración, reducir la complejidad y mejorar la utilización de recursos (Tuli *et al.*, 2021).

Simultáneamente, la expansión de cargas de trabajo intensivas en cómputo —particularmente los modelos de IA— generó presiones energéticas crecientes sobre los centros de datos. Investigaciones pioneras cuantificaron el alto costo energético y la huella de carbono asociada al entrenamiento y el despliegue de modelos de *deep learning*, y alertaron

sobre el impacto ambiental de prácticas de investigación y operación que no consideraban explícitamente la sostenibilidad (Strubell *et al.*, 2019).

Estas fuerzas pusieron a prueba dos metas: (a) seguir con la tecnología para inventar cosas y dar servicios, y (b) achicar el daño al planeta y los gastos de luz por crecer (Panwar *et al.*, 2022).

Con esto en mente, la hiperconvergencia surgió como algo que podía ayudar al planeta: se pensó que juntando cosas y haciendo fácil el manejo se bajaría el gasto inútil y se haría rendir más la luz. Pero se notó que usar solo estas plataformas no daba pie a cuidar el planeta solo porque sí; hacía falta meter trucos para manejar la luz, reglas para dar tareas y cálculos para mejorar, viendo el calor, el enfriamiento y si había luz renovable (Buyya *et al.*, 2023).

La problematización se articuló, por tanto, en torno a la complejidad del fenómeno: no solo se trató de evaluar eficiencia técnica o reducción de costos, sino también de comprender las causas estructurales (modelo de provisión de servicios *cloud*, cadenas de suministro de hardware, dependencia de combustibles fósiles), las consecuencias socioeconómicas (brechas de acceso, concentración de capacidad en ciertos países) y las coordinadas políticas (regulación energética, estándares de sostenibilidad). El desafío consistió en definir alternativas que permitieran reconciliar la necesidad de rendimiento y la urgencia ambiental, a través de una gobernanza técnica y regulatoria informada por evidencia científica (Panwar *et al.*, 2022).

En breve, la idea fue ver si las bases hiperconectadas con IA podían juntarse para disminuir su impacto en el planeta y dar más opciones a todos a lo digital, o si, al revés, gastaban más energía sin arreglos serios en las leyes y en la tecnología. Esta duda guio el estudio profundo y la búsqueda de ideas unidas en este estudio (Strubell *et al.*, 2019).

2.2. Antecedentes del estado de la cuestión

Aquí se juntaron datos clave de todo el mundo, de países cerca y lejos, y de nuestra nación. Nos concentramos en escritos de ciencia, análisis profundos y estudios reales que mostraban cómo usamos la energía, cómo la IA ayuda a manejarla y cómo mejorar para gastar menos.

2.2.1. MUNDIAL

En todo el mundo, textos técnicos y estudios serios mostraron que los centros de datos gastan mucha energía y que hay planes para usar menos. Un estudio importante encontró trucos como juntar máquinas virtuales, apagarlas a veces, mover la energía y usar programas para organizar el trabajo y así gastar menos energía en los centros de datos en la nube (Panwar *et al.*, 2022). Expertos importantes también pensaron en “nuevos” tipos de nubes que usarían la administración de recursos y el aprendizaje automático para gastar menos, enfriar mejor y dar un buen servicio (Buyya *et al.*, 2023). Por otro lado, estudios sobre cómo usar bien la energía mostraron muchas formas de hacerlo con programas y aparatos, y dijeron que hay que arreglar muchas cosas para realmente gastar menos (Katal *et al.*, 2022).

También hubo estudios que midieron cuánta energía gastan de verdad los centros de datos y cómo cambia esa cantidad, dando números y formas de calcular cuánto gastarán en el futuro para ayudar a crear reglas y gastar dinero en energías nuevas (Zakarya *et al.*, 2018). En ese momento, los científicos dijeron que solo usar bien la energía no era suficiente: había que juntar la forma de enfriar, los programas para dar energía sabiamente y el control de datos para gastar menos en general (Buyya *et al.*, 2023).

2.2.2. INTERNACIONAL

A escala mundial, estudios prácticos revelaron que métodos de IA y manejo experto disminuyen el gasto en tareas comunes. Pruebas con manejo reforzado y visión anticipada y puestas en sistemas de frío, mostraron ahorros de energía notables en sitios de prueba y proyectos pequeños (Lazic *et al.*, 2018). Google y otros mostraron informes sobre cómo usar aprendizaje automático para mejorar sistemas de enfriamiento y predecir cargas, disminuyendo así el gasto de ventiladores y sistemas extra (Gao *et al.*, 2016).

Estos trabajos demostraron que la IA no solo consumía energía, sino también podía emplearse para lograr reducciones operacionales si se diseñan políticas de control seguras y conservadoras.

Por otro lado, se investigaron modelos híbridos que combinaron programación de cargas, utilización de energía renovable y técnicas

de desvío (*brownout*) para mantener servicio y reducir demanda eléctrica en picos, lo que mostró resultados promisorios en prototipos y simulaciones (Xu *et al.*, 2020).

Como parte de la evolución tecnológica documentada en los registros internacionales, se identificó una transición acelerada desde arquitecturas tradicionales hacia infraestructuras hiperconvergentes. Esta diferencia se resume en la siguiente tabla 1, comparativa:

Tabla 1. Comparativa arquitectura tradicionales hacia infraestructura hiperconvergentes

Criterio	Infraestructura tradicional	Infraestructura hiperconvergente (HCI)
Arquitectura	Componentes separados: cómputo, red, almacenamiento	Integración total en una sola plataforma
Escalabilidad	Lenta y costosa; requiere hardware especializado	Escalabilidad lineal agregando nodos
Consumo energético	Alto; poca optimización	Reducción por consolidación y virtualización
Gestión	Manual, compleja, múltiples interfaces	Automatizada mediante software unificado
Costos operativos	Elevados por mantenimiento	Reducción del TCO entre 20% y 40%
Desempeño para IA	Limitado por cuellos de botella de red	Optimizado para cargas distribuidas

Fuente: Elaboración propia.

2.2.3. MÉXICO

En el ámbito latinoamericano y mexicano, la literatura científica sobre centros de datos (*data centers*) y sostenibilidad fue más limitada, aunque existieron estudios e informes que documentaron la relevancia del tema y los retos locales. Investigaciones regionales analizaron el impacto ambiental del consumo eléctrico en centros de datos y estimaron huellas de carbono basadas en escenarios de crecimiento de la

demanda digital (Sampedro Guamán *et al.*, 2021). Asimismo, informes sectoriales y estudios de mercado señalaron que México había experimentado un crecimiento en proyectos de centros de datos, pero que la viabilidad de la expansión dependió fuertemente de la disponibilidad de energía confiable y de políticas que incentivaran el uso de fuentes renovables. En suma, México presentó un marco emergente donde la adopción de tecnologías hiperconvergentes y prácticas sostenibles estaba condicionada por inversiones, regulación y planificación de redes eléctricas (Sampedro Guamán *et al.*, 2021).

2.3. Descripción del estado del arte

El estado del arte en la intersección TI-IA-sostenibilidad, aplicado a ecosistemas hiperconvergentes, se estructuró en subtemas que reflejaron tanto avances técnicos como lagunas científicas.

2.3.1. GESTIÓN INTEGRADA DE RECURSOS Y **SCHEDULING** ENERGÉTICO

La investigación reciente propuso modelos holísticos (por ejemplo, Hunter) que incorporaron redes de grafos y modelos térmicos para realizar *scheduling* multiobjetivo orientado a minimizar energía y mantener SLA. Experimentos con *CloudSim* y entornos reales mostraron que estas técnicas podían reducir consumo y violaciones de servicio, y evidenciaron la factibilidad de integrar inteligencia artificial dentro de las capas de orquestación (Tuli *et al.*, 2021). Otros trabajos exploraron la combinación de migración de VM, consolidación y algoritmos de optimización metaheurística para equilibrar rendimiento y ahorro energético (Panwar *et al.*, 2022).

2.3.2. CONTROL TÉRMICO Y OPTIMIZACIÓN DE ENFRIAMIENTO CON **MACHINE LEARNING**

El control del enfriamiento fue identificado como un punto crítico: métodos de *model predictive control* y técnicas de *reinforcement learning* aplicadas a sistemas de HVAC y ventiladores demostraron reducciones importantes en consumo y en uso de agua cuando se compararon con sistemas programados estáticamente (Lazic *et al.*, 2018). Investigaciones prácticas en grandes instalaciones revelaron que, al entrenar modelos

sobre datos operativos históricos y sensoriales, se podían obtener políticas seguras que mejoraron la eficiencia sin comprometer la seguridad térmica (Gao *et al.*, 2016). Técnicas de inteligencia artificial aplicadas en la gestión sostenible de centros de datos: describe métodos como machine learning para predicción térmica, reinforcement learning para asignación de cargas y modelos híbridos, detallando sus ventajas y desventajas operativas. Ver tabla 2.

Tabla 2. Comparación de técnicas de optimización energética basadas en IA en centros de datos

Técnica	Descripción	Ventajas	Desventajas
<i>Machine learning</i> para predicción térmica	Predice temperatura y ajusta enfriamiento	Reduce consumo 10%–20%	Requiere datos históricos abundantes
<i>Reinforcement learning</i> para asignación de cargas	Mueve cargas según eficiencia energética	Mejora eficiencia en tiempo real	Complejidad computacional
Optimización basada en modelos híbridos	Modelos matemáticos + ML	Alto rendimiento y precisión	Difícil de mantener

Fuente: Elaboración propia.

2.3.3. ARQUITECTURAS HIPERCONVERGENTES Y SU EVALUACIÓN SOSTENIBLE

Aunque la bibliografía específica que vinculó explícitamente hiperconvergencia con sostenibilidad fue escasa, estudios sobre eficiencia en contenedores, virtualización y orquestación aportaron evidencia sobre cómo arquitecturas integradas podían reducir recursos ociosos y mejorar utilización (Katal *et al.*, 2022). La convergencia tecnológica favoreció además la implementación de técnicas de observabilidad y telemetría fina, requisito para que la IA tomara decisiones fundamentadas en mediciones reales de consumo y temperatura (Buyya *et al.*, 2023).

2.3.4. APORTE DEL ENSAYO

La revisión evidenció avances técnicos significativos —algoritmos de *scheduling* energéticamente conscientes, control térmico basado en ML, y visiones conceptuales de *clouds* de “nueva generación”—, pero también puso en evidencia vacíos: pocos estudios evaluaron de forma integrada la combinación de IA + hiperconvergencia + políticas de gobernanza; la mayoría se concentró en componentes aislados (*scheduling* o enfriamiento). Por ello, el ensayo propuso articular un marco integrador que combinó modelos de orquestación IA-driven, métricas de sostenibilidad estandarizadas y lineamientos de política pública, con el objetivo de orientar investigaciones y despliegues prácticos hacia infraestructuras hiperconvergentes más sostenibles y equitativas.

3. Metodología

La metodología de este ensayo se construyó a partir de un enfoque cualitativo-analítico que permitió examinar la complejidad interdisciplinaria entre tecnologías de información, inteligencia artificial y sostenibilidad en ecosistemas hiperconvergentes. Esta manera se escogió pues ayudó a entender porqués, juntar ideas y ver bien qué dicen los estudios nuevos. Asimismo, resultó pertinente para estudiar fenómenos tecnológicos en rápida evolución, cuya comprensión requería integrar marcos conceptuales y perspectivas de investigación contemporáneas (Snyder, 2019). La modalidad de investigación cualitativa elegida era adecuada para este tipo de trabajo, ya que se caracteriza por la aplicación de revisiones sistemáticas investigaciones escritas a partir de la revisión bibliográfica, a la vez que el enfoque servía para hallar vacíos, tensiones y oportunidades de mejora en el estado del arte internacional.

La elección del diseño metodológico también se fundamentó en otras investigaciones anteriores, en las cuales se presentaron revisiones integradoras e investigaciones basadas en análisis narrativos de las áreas emergentes de la inteligencia artificial o de la computación sostenible, donde la información cuantitativa es más fragmentada por disciplinas (Xiao & Watson, 2019) y donde, por lo tanto, el enfoque metodológico ofrecía la flexibilidad suficiente para articular componentes técnicos-ambientales y organizativos, manteniendo la coherencia analítica del ensayo.

3.1. Técnicas de análisis utilizadas

Diferentes herramientas de análisis se aplicaron de forma complementaria. En primer lugar, se aplicó un análisis bibliométrico exploratorio, siguiendo las directrices metodológicas sugeridas por Kitchenham *et al.* (2015) para los estudios de la ingeniería del software y de los sistemas distribuidos. Esta técnica permitió definir autores influyentes, conceptos predominantes y líneas de trabajos de investigación que hiciéramos consolidadas en los últimos diez años, lo que resultó especialmente relevante para enmarcar el estudio en evidencias contemporáneas. A partir de la realización de este análisis se identificaron, además, tres núcleos temáticos fuertes: la eficiencia energética en los centros de datos, las arquitecturas hiperconvergentes y la optimización a través de la IA. En segundo lugar, se aplicó análisis de comparación estructural mediante tablas que ordenaban ventajas, limitaciones y escenarios de diferentes propuestas tecnológicas documentadas en la literatura científica. Esta técnica permitió realizar contrastes entre modelos de gestión de recursos sobre la base de *machine learning* (Tuli *et al.*, 2021), frente a propuestas tradicionales de provisión de la infraestructura (Fernández-Caramés & Fraga-Lamas, 2020). Del contraste emergieron ciertas mejoras teóricas en sostenibilidad de ciertos algoritmos, lo cual enfatizaba que su adopción práctica dependía, o venía condicionada, por factores económicos y reguladores.

En tercer lugar, se aplicó un árbol de problemas y soluciones, técnica que es ampliamente recomendada en análisis de políticas tecnológicas (Bardach & Patashnik, 2020). Por un lado, este instrumento hizo emerger causas estructurales del problema que hace aumentar el consumo energético, como la falta de estandarización en las métricas verdes y la obsolescencia acelerada del hardware; por otro lado, permitió relacionar causas estructurales con soluciones encontradas en la literatura científica, como la virtualización eficiente, la asignación dinámica de cargas y el uso de la inteligencia artificial para predecir térmica.

Por último, se creó un modelo conceptual preliminar, construido a partir del análisis documental realizado, el cual incluía los componentes clave estudiados: arquitectura hiperconvergente, métricas de sostenibilidad, algoritmos de optimización y gobernanza para la digitalización. Este modelo se puso en práctica siguiendo el procedimiento recomendado

para diseñar un modelo conceptual en sistemas emergentes (Gregor, 2006), y así permitir generar una representación clara de cómo interaccionaban los parámetros técnicos con los objetivos de sostenibilidad.

3.2. Resultados preliminares

Los resultados preliminares que surgían de la fusión de las técnicas descritas. El análisis bibliométrico demostró que la producción científica en relación con la sostenibilidad de infraestructuras hiperconvergentes era considerablemente mayor desde el año 2018, lo cual coincide con el auge del *edge computing* y la adopción de plataformas integradas, descripción que coincidía con las revisiones sistemáticas realizadas previamente, las cuales ponían de manifiesto el problema de los recursos necesarios para reducir el consumo medioambiental de los modelos de IA de gran escala (Strubell *et al.*, 2019).

Las tablas de comparación demuestran que sistemas hiperconvergentes presentaban una importante reducción del espacio en el lugar físico, el consumo energético y los riesgos operativos para infraestructuras tradicionales (Fernández-Caramés & Fraga-Lamas, 2020), aunque también se señalaba que este tipo de mejora dependía de la eficiencia del software de gestión de que se disponía, de la posibilidad de automatización e incluso del tipo de algoritmo utilizado para la asignación de recursos; al parecer, la sostenibilidad no provenía pura y simplemente de la infraestructura, sino de la calidad de los modelos de gestión aplicados sobre ella.

La elaboración del árbol de problemas facilitó la toma de conciencia respecto de tensiones críticas: la rápida expansión de los modelos de IA devino peticiones de energía que sobrepasaron la capacidad de muchos centros de datos para operar de forma sostenible; por el contrario, la escasez de estándares internacionales imposibilitó la evaluación del impacto ambiental que efectivamente genera esta clase de tecnologías. En el marco de los resultados obtenidos, a partir de ellos, el modelo conceptual preliminar proporcionó el resultado de una conjunción entre infraestructura-algoritmos-métricas ambientales, y destacó la necesidad de alinear prácticas de ingeniería con políticas de sostenibilidad.

En resumen, la metodología aplicada aportó a la argumentación del ensayo la conjunción de técnicas analíticas, comparativas y estructurales para la construcción de una visión crítica y bien fundamen-

tada de los ecosistemas hiperconvergentes. Estos métodos aportaron evidencias para dar sustento a los argumentos expuestos en la discusión posterior, y por consecuencia, para exhibir las posibilidades y los desafíos de implementar ecosistemas hiperconvergentes de forma sostenible apalancados por IA (Deng *et al.*, 2021).

Figura 1. Modelo de Ecosistema Hiperconvergente Sostenible impulsado por la IA (MEHS-IA).



Fuente: Elaboración propia.

4. Discusión

La discusión tiene lugar de forma crítica, y explora las implicaciones técnicas, sociales y regulatorias que acompaña la integración de las tecnologías de información (TI), de la inteligencia artificial (IA) y de criterios de sostenibilidad en ecosistemas hiperconvergentes. Se parte del análisis de los antecedentes y de la literatura científica reciente para explorar fortalezas, debilidades, amenazas y oportunidades, riesgos u omisiones del enfoque actual, y se propone una forma de orientarse metodológica y normativamente para convertir las capacidades técnicas en beneficios ambientales y sociales reales.

4.1. Eficiencia operativa vs. consumo de IA

La literatura en el ámbito del estudio demuestra que las plataformas hiperconvergentes aumentan la utilización de los recursos y facilitan la gestión de las cargas de trabajo, por lo que provocan mejoras ope-

rativas concretas (Buyya *et al.*, 2023). Sin embargo, la creciente adopción de modelos de IA introduce una demanda energética adicional significativa: estudios sobre el costo energético del entrenamiento de modelos de *deep learning* muestran que, sin gestión deliberada, la huella de carbono puede crecer de manera exponencial (Strubell *et al.*, 2019).

En la práctica, la eficiencia prometida por la hiperconvergencia funciona cuando se articula con políticas de orquestación energética: es decir, la reducción de recursos ociosos debe complementarse con algoritmos de *scheduling* que consideren la disponibilidad de energía renovable, la criticidad de las cargas y la eficiencia algorítmica (Tuli *et al.*, 2021; Xu *et al.*, 2020). En contraste, cuando las organizaciones implantan HCI sin capas de gestión inteligente, la ganancia en eficiencia se diluye y aparece el riesgo de incrementar la demanda total por habilitar aplicaciones de IA más intensivas.

4.2. Control térmico y técnicas de IA para enfriamiento

El control del sistema de enfriamiento constituye un punto crítico para la sostenibilidad de centros de datos. Técnicas avanzadas como modelos predictivos y aprendizaje por refuerzo demuestran capacidad para reducir el consumo de energía del subsistema de enfriamiento (Panwar *et al.*, 2022). Estas técnicas funcionan bien en entornos instrumentados y con datos históricos suficientes, y permiten tomar decisiones que minimizan el consumo manteniendo la estabilidad térmica.

No obstante, su implementación exige robustez: los algoritmos de control deben incorporar restricciones de seguridad y políticas conservadoras para evitar que la optimización sacrifique la integridad del hardware por reducir consumo. Además, la dependencia de sensores y telemetría aumenta la complejidad operativa y los costes iniciales de instrumentación, lo que puede ser una barrera para organizaciones con recursos limitados (Shehabi *et al.*, 2016).

4.3. Gobernanza, métricas y transparencia

Una limitación recurrente en la práctica es la ausencia de métricas integradas que midan la sostenibilidad real de un ecosistema hipercon-

vergente. El PUE (Power Usage Effectiveness) es útil, pero insuficiente, porque no capta la huella de ciclo de vida del hardware, el origen de la energía ni el consumo derivado por cargas de IA (Katal, Dahiya & Choudhury, 2022). Para evaluar correctamente el impacto, la discusión exige métricas complementarias: huella de carbono por *workload*, consumo de agua asociado al enfriamiento y métricas sociales, como accesibilidad y equidad en el acceso a recursos de cómputo.

Además, los marcos regulatorios y de auditoría para modelos de IA en centros de datos están en fases incipientes. Sin estándares de registro y auditoría, la adopción de IA para sostenibilidad puede quedar como una etiqueta de *marketing* en lugar de una práctica verificable (Buyya *et al.*, 2023). Por ello, la gobernanza debe incluir transparencia algorítmica, *reporting* estandarizado y evaluación de impacto ambiental verificable.

4.4. Brechas y equidad tecnológica

La discusión también aborda la dimensión social: la adopción de HCI e IA tiende a concentrarse en organizaciones con mayor presupuesto y capacidad técnica, lo que puede exacerbar brechas digitales ya existentes (Shehabi *et al.*, 2016). Mientras algunas regiones modernizan sus centros de datos con soluciones verdes, otras quedan rezagadas por falta de inversión y acceso a energías renovables. Este efecto plantea riesgos de desigualdad tecnológica que exigen políticas públicas activas para democratizar acceso y financiamiento de infraestructuras sostenibles.

4.5. Resultados finales de la discusión (síntesis crítica)

Se sintetizan los hallazgos centrales en términos de fortalezas, debilidades, oportunidades y amenazas, integrando evidencia empírica y teórica. Ver tabla 3.

Tabla 3. Fortalezas, debilidades, oportunidades y amenazas

Categoría	Evidencia
Fortalezas	HCI mejora utilización y simplifica gestión, reduciendo recursos ociosos (Buyya <i>et al.</i> , 2023). IA permite optimizar enfriamiento y asignación de cargas si se dispone de datos fiables (Mao <i>et al.</i> , 2019).
Debilidades	Implementación de IA exige instrumentación y datos, con costes iniciales importantes (Shehabi <i>et al.</i> , 2016). Métricas actuales (p. ej. PUE) resultan insuficientes para medir impacto integral (Katal <i>et al.</i> , 2022).
Oportunidades	Integrar programación energéticamente consciente con disponibilidad renovable reduce consumo “marrón” (Xu <i>et al.</i> , 2020). Establecer estándares de registro y auditoría para IA en centros de datos abre espacio a políticas públicas y mercados verdes (Buyya <i>et al.</i> , 2023).
Amenazas	La demanda energética de la IA puede anular las ganancias si no se gestiona la eficiencia algorítmica (Strubell <i>et al.</i> , 2019). Concentración de infraestructura y falta de regulación pueden aumentar desigualdades tecnológicas (Shehabi <i>et al.</i> , 2016).

Fuente: Elaboración propia.

4.6. Respuesta a la pregunta de investigación y modelo base para la discusión

La pregunta central indaga si los ecosistemas hiperconvergentes pueden integrar IA y criterios de sostenibilidad sin reproducir externalidades negativas. La respuesta es afirmativa, condicionada por tres requisitos. Ver tabla 4:

Tabla 4. Respuesta afirmativa a la pregunta de investigación

Elemento	Descripción
Orquestación inteligente	La HCI debe operar con capas de <i>scheduling</i> que incorporen métricas de sostenibilidad (Tuli <i>et al.</i> , 2021).
Control térmico seguro	Técnicas de IA para enfriamiento deben incorporar salvaguardas y entrenamiento <i>offline</i> para minimizar riesgo operativo (Mao <i>et al.</i> , 2019).
Gobernanza y métricas robustas	Se requieren protocolos de auditoría, <i>reporting</i> y estándares de impacto ambiental (Katal <i>et al.</i> , 2022).

Fuente: Elaboración propia.

4.7. Aportaciones

Aportación teórica (*Scientia*): El ensayo integra evidencia dispersa en un marco conceptual que conecta orquestación energética, control térmico y gobernanza algorítmica. Esta síntesis clarifica relaciones causales entre decisiones de diseño de HCI y resultados ambientales, e iguala niveles técnicos y sociales en la evaluación de sostenibilidad.

Aportación práctica (*Praxis*): Se entregan recomendaciones accionables: diseñar políticas de *scheduling* que prioricen energía renovable, implementar controles de enfriamiento basados en modelos robustos con entrenamiento *offline* y validación en entornos simulados, y adoptar estándares de *reporting* que incluyan huella de ciclo de vida por *workload*. Estas medidas permiten a operadores y reguladores transformar la promesa técnica en impacto ambiental y social verificable.

5. Conclusión

5.1. Respuesta a la pregunta de investigación

El ensayo responde a la pregunta de investigación porque, por medio del análisis realizado, responde a la pregunta de investigación al demostrar que la integración de tecnologías de información, inteligencia artificial y estrategias de sostenibilidad en el contexto de ecosistemas hiperconvergentes sí representa una senda óptima y necesaria para el futuro desarrollo. A partir del análisis llevado a cabo, se extrae una conclusión que argumenta que tales sistemas permiten mejorar la eficiencia energética, la optimización de recursos tecnológicos y la reducción de costes operativos, en tanto que en el marco de la inteligencia artificial funciona como hilo conductor para automatizar, predecir y monitorear procesos críticos de impacto ambiental. La prueba revisada confirma que el problema formulado en la introducción (la necesidad de infraestructuras tecnológicas más sostenibles) queda adecuadamente atendido para sistemas hiperconvergentes potenciados por IA, en especial cuando son acompañados de métricas rigurosas de consumo y políticas de gobernanza digital (Masanet *et al.*, 2020). Este artículo resulta como interesante y original, ya que formaliza la multidisciplina entre computación, inteligencia artificial y sostenibilidad, y pone de manifiesto cómo sus interrelaciones pueden dar lugar a un nuevo conocimiento orientado al diseño de infraestructuras responsables y resilientes.

5.2. Hallazgos del ensayo

Los hallazgos más destacados evidencian que la combinación de la hiperconvergencia y la IA incrementan la eficiencia operativa a través de la automatización inteligente, el análisis predictivo y la gestión de la carga de trabajo. En cuanto a la parte teórica (*Scientia*) se puede decir que el ensayo da una conceptualización que puede considerarse actual, y situar allí la IA como un elemento central para la transición hacia infraestructuras sostenibles, tal como se ha señalado en otros estudios

recientes que tienen que ver con los impactos energéticos y la optimización computacional (Strubell *et al.*, 2019). En lo que respecta a la parte práctica (*Praxis*), se concluye que los *data centers* y las empresas que utilizan modelos hiperconvergentes pueden inducir una cantidad significativa de energía a través de la optimización algorítmica y la consolidación de los recursos, aunque ello obliga a contar con fuertes regulaciones y medir dichas condiciones constantes de la energía (Patterson *et al.*, 2021).

5.3. Alcances finales del ensayo

El ensayo presenta avances bastante significativos, pero también reconoce importantes limitaciones. El análisis queda supeditado a estudios recientes sobre el consumo energético y la eficiencia computacional, de forma que los datos reales de las organizaciones son limitados. Por otro lado, la rápida evolución de la IA y la infraestructura *cloud* hace que los escenarios sean cambiantes y, por ello, dificultan una evaluación longitudinal completa. Durante el análisis, distintos factores, como las limitaciones presupuestarias, la falta de indicadores homogéneos o la ausencia de políticas uniformes entre regiones, limitan la generalización de los resultados. Sin embargo, estas limitaciones ofrecen importantes caminos de investigación futuros.

5.4. Recomendaciones futuras

Se sugiere la realización de más estudios empíricos en centros de datos, así como la creación de métricas estandarizadas de la sostenibilidad digital que lleguen a modelos híbridos de hiperconvergencia, energías renovables y algoritmos de IA de bajo consumo. También se recomienda la inclusión de enfoques interdisciplinarios que aborden diseño ético, economía circular o gobernanza algorítmica.

6. Referencias

- Bardach, E., & Patashnik, E. M. (2020). A Practical Guide for Policy Analysis. The eightfold path to more effective problem solving (6th ed.). <https://justicepolicynetwork.com/wp-content/uploads/2021/03/Bardachs-Eightfold-Path-1.pdf>
- Buyya, R., Ilager, S., & Arroba, P. (2023). Energy-Efficiency and Sustainability in New Generation Cloud Computing: A Vision and Directions for Integrated Management of Data Centre Resources and Workloads. *arXiv*. <https://doi.org/10.48550/arXiv.2303.10572>
- Deng, Q., Goudarzi, M., & Buyya, R. (2021). FogBus2: A lightweight and distributed container-based framework for integration of IoT-enabled systems with edge and cloud computing. In S. Groppe, L. Gruenwald & C.-H. Hsu (Eds.), *Proceedings of the International Workshop on Big Data in Emergent Distributed Environments (BiDEDE 2021)* (pp. 1–8). Association for Computing Machinery. <https://doi.org/10.1145/3460866.3461768>
- Esenarro, D., Rodriguez C., & Reyes A. (2019). Hyper Converged Systems Applied (HSA) Methodology to Optimize the Process of Technological Renewal in Data Centers. *International Journal of Recent Technology and Engineering*, 8(2S11). <https://doi.org/10.35940/IJRTE.B1592.0982S1119>
- Fernández-Caramés, T. M., & Fraga-Lamas, P. (2020). Towards Next Generation Teaching, Learning, and Context-aware Applications for Higher Education: A Review on Blockchain, IoT, Fog and Edge Computing. *Applied Sciences*. <https://doi.org/10.3390/app9214479>
- Gao, J. (2016). Machine Learning Applications for Data Center Optimization. Google. <https://static.googleusercontent.com/media/research.google.com/es//pubs/archive/42542.pdf>
- Gregor, S. (2006). The Nature of Theory in Information Systems. *MIS Quarterly*, 30(3), 611–642. <https://doi.org/10.2307/25148742>
- Katal, A., Dahiya, S., & Choudhury, T. (2022). Energy Efficiency in Cloud Computing Data Centers: A Survey on Software Technologies. *Cluster Computing*. <https://doi.org/10.1007/s10586-022-03713-0>
- Kitchenham, B., Budgen, D., & Brereton, P. (2015). Evidence-based Software Engineering and Systematic Reviews. <https://dl.acm.org/doi/10.5555/2994449>
- Lazic, N., Lu T., Boutilier C., & Ryu M. (2018). Data Center Cooling Using Model-Predictive Control. *Advances in Neural Information Processing Systems (NeurIPS) 2018 Proceedings*. https://proceedings.neurips.cc/paper_files/paper/2018/file/059fdcd96baeb75112f09fa1dcc740cc-Paper.pdf
- Mao, H., Alizadeh, M., Menache, I., & Kandula, S. (2019). Resource Management With Deep Reinforcement Learning. *Proceedings of the*

- ACM Symposium on Cloud Computing (SoCC), 50–60. <http://doi.org/10.1145/3005745.3005750>
- Masanet, E., Shehabi, A., Lei, N., Smith, S., & Koomey, J. (2020). Recalibrating Global Data Center Energy-use Estimates. *Science*, 367(6481), 984–986. <https://doi.org/10.1126/science.aba3758>
- Murino, T., Monaco, R., Nielsen, P. S., Liu, X., Esposito, G., & Scognamiglio, C. (2023). Sustainable Energy Data Centres: A Holistic Conceptual Framework for Design and Operations. *Energies*, 16(15), 5764. <https://doi.org/10.3390/en16155764>
- Panwar, S., Rauthan, S., & Barthwal, V. (2022). A Systematic Review on Effective Energy Utilization Management Strategies in Cloud Data Centers. *Journal of Cloud Computing*, 11, Article 95. <https://doi.org/10.1186/s13677-022-00368-5>
- Patterson, D., González, J., Le, Q., Liang, C., Munguía, L. M., Rothchild, D., So, D., Texier, M., & Dean, J. (2021). Carbon Emissions and Large Neural Network Training. *arXiv*. <https://doi.org/10.48550/arXiv.2104.10350>
- Qi, S., Milojicic, D., Pasricha, S., & Bash, C. (2023). SHIELD: Sustainable Hybrid Evolutionary Learning Framework for Carbon, Wastewater, and Energy-Aware Data Center Management. *arXiv*. <https://doi.org/10.48550/arXiv.2308.13086>
- Rongon, R. K., & Das, K. (2025). Energy-Aware Data Center Management: A Sustainable Approach to Reducing Carbon Footprint. *arXiv*. <https://doi.org/10.48550/arXiv.2509.10462>
- Sampedro Guamán, C. R., Machuca Vivar, S. A., Palma Rivera, D. P., & Villalta Jadan, B. E. (2021). Impacto Ambiental por Consumo de Energía Eléctrica en los Data Centers. *Dilemas Contemporáneos: Educación, Política y Valores, Edición Especial*. <https://doi.org/10.46377/dilemas.v8i.2786>
- Shehabi, A., Smith, S. J., Masanet, E., Horner, N., Azevedo, I. L., & Limmer, S. (2016). United States Data Center Energy Usage Report. Lawrence Berkeley National Laboratory. <https://eta.lbl.gov/publications/united-states-data-center-energy>
- Snyder, H. (2019). Literature Review As a Research Methodology: An Overview and Guidelines. *Journal of Business Research*, 104, 333–339. <https://doi.org/10.1016/j.jbusres.2019.07.039>
- Strubell, E., Ganesh, A., & McCallum, A. (2019). Energy and Policy Considerations for Deep Learning in NLP. *Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics (ACL)*. <https://arxiv.org/abs/1906.02243>
- Tuli, S., Gill, S. S., Xu, M., Garraghan, P., Bahsoon, R., Dustdar, S., & Jennings, N. R. (2021). HUNTER: AI Based Holistic Resource Management for Sustainable Cloud Computing. *arXiv*. <https://arxiv.org/abs/2110.05529>

- Xiao, Y., & Watson, M. (2019). Guidance on Conducting a Systematic Literature Review. *Journal of Planning Education and Research*, 39(1), 93–112. <https://doi.org/10.1177/0739456X17723971>
- Xu, J., Toosi, A. N., & Buyya, R. (2020). A Self-adaptive Approach for Managing Applications and Harnessing Renewable Energy for Sustainable Cloud Computing. *arXiv*. <https://arxiv.org/abs/2008.13312>
- Zakarya, M.(2018). Energy, Performance and Cost Efficient Datacenters: A survey. *Renewable and Sustainable Energy Reviews / Elsevier (survey)*. <https://doi.org/10.1016/j.rser.2018.06.005>



This is an open access article distributed under the terms of the CC BY-NC license (<https://creativecommons.org/licenses/by-nc/4.0/>)

Capítulo 3

Aplicaciones móviles inteligentes para la sostenibilidad: de la conciencia ambiental a la acción ciudadana mediada por IA

Fabricio Francisco Hernández-Gómez¹

1. Introducción.

“ Si la humanidad no cambia su relación con la tecnología y el medio ambiente, la ventana de oportunidad para un futuro sostenible podría cerrarse en esta década” Organización de las Naciones Unidas (ONU, 2023). En un mundo donde los desafíos climáticos se intensifican y las ciudades concentran más del 55% de la población global, la necesidad de conectar la conciencia ambiental con la acción ciudadana se vuelve imperativa. En este contexto, las herramientas móviles con capacidades inteligentes, desarrolladas con IA, se transforman en herramientas clave para fomentar prácticas sostenibles, fomentar la participación de las personas y optimizar la gestión ambiental en las ciudades.

1. Universidad de Guadalajara, Guadalajara, Jalisco, México. email: fabriciofranciscohernandezgome@gmail.com. ORCID: 0009-0007-6577-3599

En los últimos años, los gobiernos, las empresas y las organizaciones internacionales han reconocido que la transformación digital orientada a la sostenibilidad constituye un elemento clave en sus estrategias de desarrollo (Vinuesa *et al.*, 2020; OECD, 2022).

Un aspecto relevante, y esto lo confirman estudios importantes de consultoras como McKinsey & Company (en 2024) y Accenture (en 2021), es el enorme potencial que tienen la inteligencia artificial y otras tecnologías emergentes para acelerar el cumplimiento de los Objetivos de Desarrollo Sostenible (ODS). Estas tecnologías permiten llevar a cabo acciones mucho más correctas, que son inclusivas y que tienen una gran capacidad de ser escalables.

A continuación se muestra una situación importante: Se identifica una brecha significativa entre esta oportunidad innovadora y su aceptación por parte de la ciudadanía, especialmente en los ámbitos académico y público. Esta es una de las cosas que de alguna forma están deteniendo a estas acciones ambientales para que funcionen de manera efectiva.

En los libros e investigaciones científicas se ha buscado tener un más cercanía entre la sostenibilidad y la tecnología. Se observa que en las investigaciones de la utilidad energética tuvieron un gran avance en el 2010.

Años después en el 2019, nuevas herramientas tecnológicas como la (IA), educación digital ayudaron de manera significativa con estas tareas de la sociedad (según PricewaterhouseCoopers (2020) y Boston Consulting Group (2023)).

Ante este panorama, surge la siguiente interrogante: ¿Cómo deberíamos utilizar estas herramientas para dirigir las hacia un enfoque más ético (Floridi *et al.*, 2018), un proceso realmente inclusivo y una causa que transforme nuestra ciudadanía ambiental?

El objetivo principal de este ensayo es poder analizar cómo estas herramientas tecnológicas nos pueden realmente ayudar para tener más sensibilidad ambiental y tener más participación en estas actividades. Es importante para mí saber como se pueden potenciar mediante estas herramientas y con ayuda de la IA acciones sostenibles.

El propósito es reflexionar sobre los límites reales y que tanto se puede hacer con estas herramientas tecnológicas. Asimismo, se busca identificar cuáles o que puntos importantes son necesarios para hacer de la sostenibilidad algo en conjunto y auténtico.

2. Desarrollo

A continuación, se desarrollarán el contexto y la problematización del tema, los antecedentes y el estado de la cuestión, el marco teórico que sustenta el análisis, la metodología empleada y los resultados obtenidos en torno al papel de las aplicaciones móviles inteligentes basadas en IA para la sostenibilidad.

2.1 Contexto problematización

En los últimos años hemos pasado por un cambio tecnológico importante que ha cambiado la forma en cómo vivimos, cómo trabajamos y cómo nos comunicamos.

Entre estos cambios han surgido herramientas tecnológicas innovadoras. Con estas herramientas podemos utilizar tecnología como la IA para el análisis de datos así como la conectividad sin interrupciones para llevar a cabo un reto importante: la sostenibilidad global.

La clave de todo esto es el desarrollo de tecnologías y sostenibilidad. Ya no es algo que veamos como futuro sino algo que tenemos presente. Estas dos cosas son necesarias e importantes para un crecimiento responsable, ya que permite a empresas, gobiernos y personas hacer conciencia ante los problemas ambientales y sociales que tenemos mundialmente (como lo indica Accenture en 2021).

Con esta combinación podemos obtener herramientas tecnológicas para hacer acciones más efectivas que reduzcan el impacto ambiental e impulsen la conciencia tecnológica.

La inteligencia artificial es muy importante. Es muy eficaz para recaudar y analizar datos y así poder tomar mejores decisiones. En el informe "Artificial Intelligence for Good" de McKinsey & Company (2024) nos dice que las tecnologías con IA pueden generar grandes beneficios tanto para las personas como para el planeta.

¿Dónde se puede observar las aplicaciones de todo esto? Existen áreas que detectan en tiempo real tendencias del consumo, detección de desastres futuros, mejorar y potenciar la energía y la creación de estrategias para la protección ambiental. Al tener esta información en

dispositivos móviles las personas pueden ayudar a generar y estudiar datos ambientales y así formar una participación en conjunto.

Con estas herramientas digitales se permite a las personas accionar sobre su conocimiento. Ahora que contamos con demasiada información sobre sostenibilidad, creamos conciencia y estamos participando en la conciencia ambiental. Accenture (2021) afirma que las empresas que pueden agregar tecnología y sostenibilidad en sus procesos también tienen un impacto social y también una gran ventaja competitiva cuando permiten a las personas tener participación en generar soluciones compartidas. En este sentido, la aplicación móvil sirve como medio para el empoderamiento ciudadano, que puede evaluar la huella ecológica, promover el reciclaje, minimizar el uso de energía y colaborar en compromisos comunitarios.

Un ejemplo más reciente de esta visión proviene del Boston Consulting Group (2023) cuando enfatizan la necesidad de una acción climática acelerada a través de tecnologías de inteligencia artificial, así como la eficiencia energética y la reducción de emisiones de carbono. Sin embargo, subrayan que solo cuando se utilizan de manera responsable y colaborativa como un medio para lograr un impacto positivo, tales tecnologías tendrán algún tipo de efecto. Y, por lo tanto, la nueva visión es una especie de transformación cultural: no usar la tecnología simplemente para controlar o consumir o actuar como algún tipo de poder material, sino convertirla en un instrumento para la participación y la corresponsabilidad ambiental. El ciudadano conectado a una aplicación inteligente termina así no siendo simplemente un receptor pasivo, sino que se convierte en un agente activo de cambio sostenible.

De manera similar, PricewaterhouseCoopers (2020) enfatiza que las tecnologías de la Cuarta Revolución Industrial (4IR) están remodelando fundamentalmente los procesos para lograr los Objetivos de Desarrollo Sostenible (ODS) de la Agenda 2030. La IA, el IoT (Internet de las Cosas) y la analítica avanzada están en este momento entre esas tecnologías que dan oportunidades para crear soluciones adaptadas a casos específicos en el contexto local.

Se observa que estas tecnológicas innovadoras son muy importantes ya que nos permiten poder ayudar de forma individual con la realidad global. Transforman pequeñas acciones cotidianas como reciclar, elegir consumo responsable o usar transporte sostenible en datos que son cuantificables y comparables a nivel mundial.

En esta etapa en la que se dispone de inteligencia artificial como herramienta debe ser importante el tener transparencia e igualdad. si no se hace de esta manera podemos crear sistemas erróneos con resultados que en lugar de ayudar nos perjudiquen aún más (un punto que destaca McKinsey & Company en 2024).

Tener esta ética es importante ya que las aplicaciones manejan datos delicados como personales y de ubicación. Los desarrolladores y las empresas tienen el reto de generar un equilibrio donde las tecnologías y herramientas que desarrollen no causen daño al medio ambiente y a la vez ayuden a la sociedad.

En resumen, la sostenibilidad es mucho más que solo ecología. Se trata de justicia social, acceso digital y de una participación ciudadana bien informada. Actualmente, las herramientas detrás de las prácticas sostenibles ya no se limitan a la simple conciencia ambiental, sino que se centran en la IA y las aplicaciones móviles inteligentes.

Esta es una nueva oportunidad donde las personas podemos ayudar con el conocimiento que tenemos y participar mediante estas herramientas tecnológicas. Es muy importante saber que tenemos grandes retos como identificar y administrar de manera crítica.

Aunque con estas herramientas innovadoras que se apoyan con inteligencia artificial nos brindan gran ayuda, encontramos que todavía se encuentra con varios problemas de ética. Se está sobrellevando el tema del cambio climático y el consumo responsable de la energía, pero el estilo de vida de muchas personas es insostenible.

Esto nos dirige a la siguiente pregunta: ¿por qué la información no es más propensa a convertirse en acción? Accenture (2021) postula que la sostenibilidad tecnológica no debería representar meramente una narrativa, sino que también debería fomentar el desarrollo de experiencias que motiven, habiliten y recompensen comportamientos sostenibles. Por eso las aplicaciones necesitan ser más que monitores: deben ser mediadores del cambio cultural.

El segundo desafío señalado por Boston Consulting Group (2023) es la falta de escalabilidad y coordinación. Muchos proyectos de IA para combatir el cambio climático todavía son pilotos o funcionan de manera aislada. El impacto colectivo de estas soluciones depende de la fragmentación dentro de los ámbitos público, privado y académico, y su fragmentación puede hacer que sea menos probable que funcionen de manera sistémica. Aunque existen aplicaciones móviles, a menudo se

crean para entornos urbanos o para usuarios con mayor alfabetización digital, lo que tiende a excluir a las personas rurales y menos competentes tecnológicamente. Para mí, esta desigualdad tecnológica es un problema grave, ya que termina agravando la brecha de sostenibilidad. ¿Por qué? Porque la innovación se concentra principalmente en aquellas áreas donde ya existen ciertas ventajas estructurales, dejando atrás a quienes más lo necesitan.

Se considera importante la advertencia de McKinsey & Company (2024) sobre los peligros que implica la falta de regulación y gobernanza efectiva en torno a los sistemas de Inteligencia Artificial. Las aplicaciones móviles inteligentes recopilan grandes volúmenes de información personal, hábitos de consumo, movilidad, hábitos energéticos, ubicación geográfica. La verdad es que la ausencia de garantías claras en cuanto a la privacidad y la transparencia es muy preocupante. Esto podría resultar en que nuestra información sea usada de forma indebida, lo que no solo pone en riesgo nuestros datos personales, sino que también puede generar decisiones automatizadas que estén sesgadas por los propios algoritmos.

La sostenibilidad digital, por tanto, es inseparable de la sostenibilidad ética. La pregunta clave que surge aquí es, entonces, ¿cómo podemos asegurar que la tecnología diseñada para el bien social no termine involuntariamente repitiendo patrones de exclusión o promoviendo prácticas de explotación de datos?

PricewaterhouseCoopers (2020) apoya esta visión, argumentando que las tecnologías de la Cuarta Revolución Industrial deben desarrollarse con un aspecto de inclusión en mente. Las aplicaciones móviles son un puente para la participación ciudadana para algunos, pero una barrera entre aquellos que tienen dispositivos y conectividad junto con alfabetización digital y aquellos que no. Si tomar medidas para la sostenibilidad depende de la utilidad de una aplicación móvil, necesitamos asegurarnos de que todos puedan acceder a ella y entender cómo funciona.

De lo contrario, corre el riesgo de desarrollar una "sostenibilidad de élite" en la que solo aquellos con capacidades tecnológicas avanzadas podrían participar. Tal enmarcación de este fenómeno lo problematiza en torno a cuatro tensiones estructurales que establecen los límites y posibilidades de la sostenibilidad digital.

Primero, la brecha entre la conciencia y la acción muestra que, aunque los ciudadanos saben mucho sobre los desafíos ecológicos, toda-

vía hay cierta distancia entre saber y hacer. Esta tensión es importante para repensar la estrategia de diseñar aplicaciones móviles inteligentes que ayuden no solo a informar, sino también a motivar y sostener el cambio de comportamiento sostenible a lo largo del tiempo, a través de mecanismos de gamificación, retroalimentación en tiempo real y aprendizaje adaptativo.

En segundo lugar, como resultado de la escasez de escalabilidad y articulación intersectorial, las medidas tecnológicas se han extendido. La mayoría de las aplicaciones pueden ser locales o de nicho por naturaleza, y hay una mínima interconexión entre el estado, las empresas o el público. Esto limita su capacidad para tener impactos globales y sostenibles, ya que no están integradas en amplios ecosistemas de gobernanza ambiental y transformación social.

Una tercera tensión de este tipo es generada por la ética relacionada con la IA en torno a los datos, con su propio conjunto de desafíos de privacidad, algorítmicos y de responsabilidad. Las plataformas inteligentes, por otro lado, no son neutrales; sus elecciones automatizadas nos impulsan a consumir, movernos y participar. Por eso es necesario crear marcos de transparencia y empoderamiento ciudadano para asegurar el uso responsable de la tecnología.

Por último, un principio de acceso y equidad en la participación digital determina quién está incluido y quién está excluido de un cambio sostenible. La falta de tecnología crea desigualdades adicionales y erosiona la universalidad de los objetivos de sostenibilidad. La participación inclusiva exige políticas públicas e intervenciones de diseño que apoyen el acceso, la alfabetización digital y la justicia tecnológica.

Tales tensiones impulsan una redefinición de la ciudadanía en la era digital. Las aplicaciones móviles inteligentes pueden liberar al individuo para ser un catalizador del cambio, pero amenazan con convertir a cualquiera en alguien que solo consume datos. Desde este punto de vista, la sostenibilidad tecnológica no debería ser solo una aspiración a la eficiencia o la automatización, sino que debe basarse en la colaboración, la corresponsabilidad y la producción de valor social. Como mencionan McKinsey & Company (2024) y Boston Consulting Group (2023), solo descubriremos el futuro de la sostenibilidad mediada por la IA cuando diseñemos colectivamente ecosistemas donde la tecnología complemente la actividad humana, no la desplace, y resulte en efectos más significativos y sostenibles.

Aquí, la problematización alcanza una conclusión importante:

¿Cómo ayudan las aplicaciones móviles inteligentes mediadas por inteligencia artificial a hacer el cambio de la conciencia ambiental a acciones en nombre de los ciudadanos para ser sostenibles?

Esta pregunta involucra no solo el lado tecnológico, sino también los aspectos sociales, económicos, culturales y éticos que influyen en la adopción, uso y apropiación de la tecnología. La sostenibilidad, por lo tanto, no sólo conduce a un cambio ambiental, sino que también se erige como una nueva forma de organización social mediada por la tecnología, donde la inteligencia artificial puede convertirse en una fuerza de responsabilidad colectiva y compromiso ciudadano por la tierra.

2.2 Antecedentes – Estado de la cuestión

Esta sección presenta una revisión general del estado actual de la relación entre inteligencia artificial, sostenibilidad y acción ciudadana. Se analizarán los principales enfoques teóricos, avances tecnológicos y debates éticos que han configurado el desarrollo de estas aplicaciones en los últimos años.

Aplicaciones móviles inteligentes para la sostenibilidad: de la conciencia ambiental a la acción ciudadana mediada por IA.

2.2.1. PANORAMA GENERAL: TECNOLOGÍA, SOSTENIBILIDAD Y ACTORES CLAVE

En los últimos años, la literatura técnica y los informes de consultoría coinciden en que la tecnología —y en particular la inteligencia artificial (IA), el Internet de las cosas (IoT) y las plataformas móviles— pasó de ser un conjunto de herramientas puntuales a constituir la infraestructura principal para la acción por la sostenibilidad. Accenture (2021) plantea que la sostenibilidad debe integrarse con la estrategia tecnológica —«sustainability by tech», «sustainability in tech» y «sostenibilidad a gran escala», y que dicha integración exige no sólo soluciones innovadoras sino también gobernanza, medición y cooperación entre actores (sector público, privado, academia y sociedad civil). Este enfoque sistémico ubica a las aplicaciones móviles inteligentes como nodos de interacción

entre ciudadanos y ecosistemas de datos que permiten medir, informar y (potencialmente) cambiar conductas. (Accenture, 2021).

Boston Consulting Group (2023) amplía el alcance investigando cómo se está utilizando la inteligencia artificial para abordar la acción climática y destaca cómo los algoritmos y modelos predictivos tienen el poder de maximizar los procesos industriales y urbanos (gestión de energía, optimización de rutas, predicción de demanda), y ayudar con la aceleración de la reducción de emisiones cuando se utiliza dentro de procesos operativos y de políticas públicas.

Boston Consulting Group (2023) sugiere que las aplicaciones y plataformas impulsadas por inteligencia artificial ayudan al usuario a obtener el conocimiento y así tomar medidas en tiempo real y apoyarlas proporcionando modelos de incentivos que respaldan la necesidad de ser sostenibles.

Por ejemplo, McKinsey & Company (2024) identifica cientos de usos sociales y ambientales de la inteligencia artificial, abarcando desde la predicción de fenómenos climáticos severos hasta la optimización de las cadenas de suministro como estrategias para disminuir las emisiones. McKinsey & Company señala que las soluciones impulsadas por inteligencia artificial tienen el potencial de transformar datos en intervenciones eficientes, si los datos se gobiernan, miden y analizan de manera responsable: con métricas claras y evaluación de impacto. McKinsey & Company (2024).

Según PricewaterhouseCoopers en su estudio de 2020, esta capacidad de utilizar tecnología es relevante para los Objetivos de Desarrollo Sostenible (ODS) y describe la potencial utilización de la tecnología de la Cuarta Revolución Industrial (4RI) ya en uso en energía, agua, salud y educación, y apoya además la afirmación de que la digitalización, incluyendo la móvil, podría impulsar la capacidad de alcanzar los objetivos globales dado que se diseñen esquemas inclusivos y escalables (PricewaterhouseCoopers, 2020).

2.2.2. DEL CONOCIMIENTO A LA ACCIÓN: EVIDENCIA SOBRE EFICACIA Y LÍMITES

Los antecedentes empíricos y de consultoría revelan una tensión central: existen múltiples iniciativas y prototipos que muestran impacto local o puntual (pilotos de movilidad, apps de medición de huella, plataformas de reporte comunitario), pero la evidencia de impactos

sostenidos y escalables es más limitada. Accenture (2021) identifica un «intent–action gap» (brecha intención-acción) tanto en empresas como en usuarios y advierte que muchas organizaciones aún no han integrado plenamente la estrategia tecnológica con metas de sostenibilidad, lo que reduce la efectividad de las soluciones implementadas.

Boston Consulting Group (2023) enfatiza que, si bien la IA puede ofrecer ganancias sustanciales en eficiencia y reducción de emisiones, la escala del impacto depende de factores no técnicos: calidad de datos, interoperabilidad entre sistemas, voluntad política y modelos de financiamiento. Es frecuente que proyectos prometedores se queden en piloto por ausencia de estándares, incentivos económicos claros o modelos de negocio replicables Boston Consulting Group (2023).

McKinsey & Company (2024) añade que la medición del impacto es un reto metodológico: muchas iniciativas reportan métricas de actividad (descargas, interacciones) pero pocas rastrean resultados ambientales verificables (toneladas de CO₂ evitadas, reducción real de consumo energético). La falta de métricas compartidas y dashboards públicos dificulta comparar resultados entre proyectos y replicar modelos exitosos. McKinsey & Company (2024).

2.2.3. RIESGOS, GOBERNANZA Y ÉTICA DE LA IA EN APLICACIONES MÓVILES

Los antecedentes también documentan preocupaciones sobre privacidad, sesgos y sostenibilidad tecnológica propia. Accenture advierte que la propia tecnología puede generar impactos ambientales (por ejemplo: consumo energético del entrenamiento de modelos de IA o el uso continuo de dispositivos móviles) y propone políticas para medir y reducir esa huella (Accenture, 2021). McKinsey & Company (2024) y Boston Consulting Group (2023) insisten en que la adopción de IA socialmente útil necesita marcos de gobernanza que garanticen explicabilidad, equidad y responsabilidad; sin estos marcos, la instrumentalización de datos personales para inducir comportamientos puede generar rechazo social o injusticias.

PricewaterhouseCoopers (2020) complementa destacando que la inclusión digital es una condición para la legitimidad de las soluciones: si las apps mediadoras requieren smartphones de última generación o conectividad constante, perpetúan desigualdades y limitan el alcance de la acción colectiva hacia los ODS.

2.2.4. ECOSISTEMAS, INTEROPERABILIDAD Y MODELOS DE COLABORACIÓN

Un patrón recurrente en los antecedentes es la necesidad de **ecosistemas interoperables**: APIs abiertas, colaboración público-privada, estándares comunes de datos y plataformas que permitan integrar servicios (transporte, energía, reciclaje, participación ciudadana). Accenture subraya que escalar requiere “sostenibilidad a gran escala” mediante alianzas; Boston Consulting Group propone modelos híbridos donde empresas, gobiernos y startups compartan infraestructura. McKinsey & Company insiste en la evaluación y auditoría de impacto como elemento que legitima y facilita la replicación. PricewaterhouseCoopers, por su parte, valora la alineación con los ODS para orientar la priorización tecnológica. (Accenture, 2021; BCG, 2023; McKinsey & Company (2024); PwC, 2020).

2.2.5. VACÍOS IDENTIFICADOS Y LÍNEAS DE INVESTIGACIÓN FUTURA

A partir de los antecedentes revisados, se identifican vacíos críticos que justifican la investigación actual: (a) escasa evidencia longitudinal sobre la eficacia de apps inteligentes para cambiar comportamientos de forma sostenida; (b) falta de métricas ambientales estandarizadas vinculadas a resultados de uso (no sólo indicadores de uso); (c) ausencia de marcos robustos de gobernanza y auditoría para aplicaciones de IA ciudadana; y (d) brechas de equidad en el acceso y apropiación tecnológica. Estas lagunas constituyen el punto de partida para preguntas de investigación orientadas a diseñar, evaluar y gobernar aplicaciones móviles inteligentes con impacto social y ambiental verificable.

2.3 Estado del arte

2.3.1. TECNOLOGÍA, SOSTENIBILIDAD Y ACTORES CLAVE

La tecnología (sensores, redes móviles, IA) constituye la infraestructura material que habilita las aplicaciones móviles inteligentes (AMI). La sostenibilidad demanda impactos medibles (reducción de emisiones,

ahorro energético) y los actores clave incluyen ciudadanía, gobiernos locales, empresas tecnológicas, investigadores y ONG.

Comparación con el estado del arte.

El marco de *sustainability at scale* de Accenture y las recomendaciones de PwC vinculaban explícitamente la tecnología con metas ESG y modelos de negocio sostenibles (Accenture, 2021; PwC, 2020). McKinsey y BCG enfatizan que la IA permite soluciones de *IA for social good* pero requieren coordinación entre actores para escalar (McKinsey, 2024; BCG, 2023).

Implicaciones prácticas.

Las AMI funcionan mejor cuando operan en ecosistemas multiactor que aseguren datos, recursos y gobernanza. La participación pública y la colaboración público-privada son condición necesaria para traducir pilotos en políticas urbanas replicables.

Vacíos / líneas futuras.

Falta una taxonomía operativa de actores que precise responsabilidades (quién aloja datos, quién audita algoritmos, quién financia mantenimiento). La investigación futura debe estudiar modelos de gobernanza colaborativa que integren financiamiento sostenible y responsabilidades legales.

2.3.2. EVIDENCIA SOBRE EFICACIA Y LÍMITES

La evidencia empírica muestra resultados promisorios en etapas piloto (reducciones puntuales de consumo, mayor reporte ciudadano), pero los efectos de largo plazo y el escalamiento sistémico son poco demostrados y heterogéneos.

Comparación con estado del arte.

PwC documenta casos 4IR con potencial para ODS pero advierte la necesidad de métricas robustas; Accenture muestra beneficios estra-

tégicos pero subraya dependencia de gobernanza; McKinsey reclama evaluación de impacto y comparabilidad; BCG enfatiza casos de uso de IA para acción climática (PwC, 2020; Accenture, 2021; McKinsey, 2024; BCG, 2023).

Implicaciones prácticas.

Las AMI deben incorporar desde su diseño KPIS ambientales (ton CO₂ evitadas, ahorro real) y protocolos de evaluación longitudinal (6–24 meses). Sin ello, la adopción cae por falta de evidencia creíble.

Vacíos / líneas futuras.

Se necesitan marcos estandarizados para medir impacto (definición de KPIS, metodologías de verificación) y estudios controlados (A/B, cuasi-experimentales) que correlacionen uso de AMI con reducción real de emisiones y cambio de conducta sostenido.

2.3.3. RIESGOS, GOBERNANZA Y ÉTICA DE LA IA EN APLICACIONES MÓVILES

Los riesgos abarcan privacidad, sesgo algorítmico, opacidad, discriminación y aumento de brechas digitales. La gobernanza exige transparencia, auditoría y marcos de responsabilidad.

Comparación con estado del arte.

UNESCO propone principios éticos (2021) y la OECD y McKinsey reclaman institucionalizar prácticas de IA responsable; Accenture y PwC apuntan a gobernanza corporativa alineada con ESG (UNESCO, 2021; OECD, 2022; McKinsey, 2024; Accenture, 2021).

Implicaciones prácticas.

Toda AMI debe integrar desde el inicio: minimización de datos, explicabilidad (XAI), mecanismos de consentimiento, y auditorías independientes. La ausencia de estos elementos compromete confianza y legitimidad.

Vacíos / líneas futuras.

Investigación aplicada sobre métodos de auditoría algorítmica para AMI, métricas de equidad en resultados ambientales y guías normativas para interoperabilidad legal entre jurisdicciones.

2.3.4. ECOSISTEMAS, INTEROPERABILIDAD Y MODELOS DE COLABORACIÓN

La interoperabilidad técnica (APIS, estándares de datos) y los modelos colaborativos (público-privado-comunidad) son imprescindibles para escalar soluciones y lograr *sustainability at scale*.

Comparación con estado del arte.

BCG y PwC señalan que la replicabilidad depende de APIS abiertas y estándares comunes; Accenture formula la necesidad de alinear estrategia tecnológica con metas ESG y modelos de negocio sostenibles para escalar (BCG, 2023; PwC, 2020; Accenture, 2021).

Implicaciones prácticas.

Se requiere construir capas de interoperabilidad (catálogos de datos, estándares semánticos, gobernanza de APIS) y acuerdos SLA entre actores. Sin ellos, iniciativas quedan aisladas y no generan impacto sistémico.

Vacíos / líneas futuras.

Desarrollo de marcos técnicos abiertos para datos ambientales urbanos, estudios sobre modelos de negocio sostenibles (financiación, mantenimiento) y pruebas piloto que demuestren replicabilidad en contextos diversos.

2.3.5. VACÍOS IDENTIFICADOS Y LÍNEAS DE INVESTIGACIÓN FUTURA

Los vacíos clave se concentran en: (a) métricas estandarizadas de impacto, (b) gobernanza y auditoría algorítmica aplicadas a AMI, (c) modelos de negocio y escalamiento, (d) inclusión digital y medición de equidad.

Comparación con estado del arte.

McKinsey y OECD reclaman estandarización y gobernanza; PwC y Accenture piden alineación entre estrategia tecnológica y metas ESG; BCG enfatiza métricas y casos de uso verificables (McKinsey, 2024; OECD, 2022; PwC, 2020; Accenture, 2021; BCG, 2023).

Líneas de investigación priorizadas.

- Desarrollo de un marco estandarizado de KPIs ambientales para AMI y protocolos de verificación.
- Métodos de auditoría algorítmica y métricas de equidad para IA aplicada en apps móviles.
- Modelos de negocio sostenibles y escalables (financiamiento, gobernanza multinivel).
- Estudios longitudinales de eficacia comportamental (A/B, cohortes) en diversidad socioeconómica.
- Diseño de arquitecturas de interoperabilidad (APIs, vocabularios) y pruebas de replicabilidad inter-ciudad.

Al confrontar el estado de la cuestión con el estado del arte provisto por PwC, Accenture, McKinsey, BCG, OECD, UNESCO y UN, se confirma que las AMI mediadas por IA poseen un potencial real para transformar conciencia en acción, pero su eficacia depende críticamente de gobernanza, métricas estandarizadas, interoperabilidad y equidad. Las líneas de investigación propuestas buscan cerrar la brecha entre pilotos tecnológicos y sostenibilidad a escala, priorizando evaluación rigurosa, ética algorítmica e inclusión social.

A partir del análisis bibliométrico, comparativo y estructural desarrollado en esta sección, se propone como síntesis conceptual el modelo presentado en la Figura 1. Este modelo integra el papel de las aplicaciones móviles inteligentes mediadas por Inteligencia Artificial como entorno operativo donde convergen dimensiones clave identificadas en el análisis —alfabetización digital y algorítmica, transparencia y explicabilidad, diseño centrado en la ciudadanía, participación colectiva digital y métricas de impacto socioambiental— orientadas a reducir la brecha entre conciencia ambiental y acción ciudadana sostenible. La figura sintetiza gráficamente cómo estos ejes estructurales configuran

la arquitectura tecnológica necesaria para transformar información ambiental en prácticas corresponsables y escalables..

Figura 1. Modelo conceptual de aplicaciones móviles inteligentes mediadas por Inteligencia Artificial para la transición de la conciencia ambiental a la acción ciudadana sostenible.



Fuente: Elaboración propia.

3. Metodología

La metodología empleada en este ensayo se fundamentó en un enfoque cualitativo de análisis documental, ya que permitió explorar, interpretar y comparar de manera crítica las evidencias científicas y los marcos conceptuales relacionados con las aplicaciones móviles inteligentes, la sostenibilidad y la acción ciudadana mediada por inteligencia artificial. Este enfoque se eligió porque ofreció la posibilidad de comprender la complejidad socio tecnológica del fenómeno estudiado,

donde intervienen dimensiones tecnológicas, ambientales y culturales que no pueden reducirse únicamente a mediciones numéricas. Es importante para mi ensayo entender cómo los discursos académicos, institucionales y tecnológicos tuvieron influencia en la construcción de las narrativas contemporáneas que se encuentran en torno a la sostenibilidad digital y la participación de las personas. Así podemos entender sobre cómo nació este tema y el cambio significativo que tiene.

Decidí usar un método cualitativo porque la naturaleza del tema era, francamente, muy exploratoria.

Pienso que las herramientas tecnológicas en temas sostenibles es un área todavía en desarrollo, mi análisis interpretativo me permitió hacer algo clave: identificar patrones, los problemas que existen y las brechas en el estado del arte.

Además, este enfoque está totalmente en línea con investigaciones recientes sobre tecnología cívica y comportamiento ambiental. Estos estudios también abordan la transformación social impulsada por el uso digital desde una perspectiva que busca comprender e interpretar, lo cual reforzó mi elección.

De esta manera, se mejoró la relevancia metodológica del trabajo.

Con el objetivo de asegurar rigor y coherencia a lo largo del proceso, elaboré criterios explícitos para la selección de fuentes, incluyendo la relevancia temática, la actualidad (preferiblemente de los últimos diez años), la pertinencia conceptual y el reconocimiento académico. Incorporamos artículos científicos, informes institucionales, informes de organizaciones internacionales y documentos técnicos de repositorios académicos.

El análisis metodológico se elaboró en tres fases complementarias:

PRIMERA FASE: ANÁLISIS BIBLIOMÉTRICO

Esto implicó estudiar tendencias, autores prominentes y vacíos temáticos en la literatura actual. El estudio empleó una búsqueda sistemática de bases de datos académicas sobre enfoques predominantes hacia la sostenibilidad digital, aplicaciones móviles inteligentes y la participación ciudadana mediada por IA. Según este análisis, aunque el uso creciente de tecnologías basadas en la sostenibilidad se ha desarrollado en los últimos años, la integración explícita entre la IA, la acción ambiental y la ciudadanía sigue siendo limitada y fragmentada.

SEGUNDA FASE: ELABORACIÓN DE TABLAS COMPARATIVAS

Con el fin de comparar estos hallazgos con otros estudios, se elaboraron marcos de análisis a partir de la revisión de distintos enfoques, métodos y resultados presentes en investigaciones anteriores. Las tablas se reorganizaron para resumir aspectos como los objetivos, el alcance, las limitaciones, el nivel de innovación, el propósito social y el aporte teórico de cada trabajo. Este método nos permitió representar las diferencias entre los modelos convencionales de educación ambiental, los mecanismos de participación ciudadana y las propuestas impulsadas por IA para la educación basada en aplicaciones móviles. Tal comparación sistemática permitió vincular diversos marcos teóricos e identificar tanto características estructurales comunes como diferentes.

TERCERA FASE: ANÁLISIS ESTRUCTURAL MEDIANTE EL ÁRBOL DE PROBLEMAS-SOLUCIONES

Se utilizaron diagramas para sintetizar las causas raíz que impiden que la conciencia ambiental se traduzca en una acción ciudadana efectiva. Los factores identificados incluyen la brecha digital, la baja apropiación tecnológica, la falta de incentivos sostenibles, los sesgos algorítmicos y la limitada alfabetización en IA. A partir de este análisis, se construyeron también líneas de intervención orientadas al diseño de aplicaciones móviles más inclusivas, algoritmos explicables y estrategias de educación ambiental digital.

Los primeros hallazgos obtenidos a lo largo de estas tres etapas brindaron un fundamento claro y consistente para construir el argumento principal del ensayo. En primer lugar, las tablas comparativas mostraron que, aunque existe abundante literatura sobre sostenibilidad y tecnología, los estudios que integran inteligencia artificial, participación ciudadana y aplicaciones móviles todavía son incipientes. En segundo lugar, el análisis bibliométrico indicó que el uso de tecnologías emergentes para estimular comportamientos ambientales estaba creciendo con el tiempo, pero también demostró una brecha entre la innovación tecnológica y su apropiación social. Finalmente, utilicé la herramienta del árbol de problemas y soluciones, la cual fue fundamental porque me permitió visualizar los desafíos clave que deben resolverse para que estas aplicaciones móviles inteligentes puedan escalar hacia modelos efectivos de acción colectiva.

En resumen, mi enfoque combinó varias herramientas cualitativas diseñadas para generar una comprensión amplia y muy bien fundamentada de la compleja relación entre tecnología, sostenibilidad y ciudadanía. Al final, logré una triangulación sólida entre la bibliometría, la comparación sistemática y el análisis estructural. Con esto puedo crear una discusión crítica para mi ensayo con grandes argumentos que sirven para esta discusión.

4. Discusión

A Continuación, en base a los resultados de mi análisis los pondré en diálogo con el estado del arte y con el problema actual. Mi idea es: Analizar estas herramientas tecnológicas que tan lejos pueden llegar, analizar si realmente nos sirven como herramientas para la participación de la gente en temas de sostenibilidad.

Para tener éxito tengo que ver pros y contras. También añadiré mi reflexión acerca de los retos que tiene al usar IA en estos temas de sostenibilidad.

Por último, para acercarme a la respuesta a mi pregunta de investigación y proponer un modelo práctico de referencia, voy a crear unos subtemas con los que podamos ver si es viable todos estos enfoques innovadores.

4.1. Pros y contras de las herramientas tecnológicas para la sostenibilidad

A partir del análisis realizado, se observa como va creciendo el uso de aplicaciones móviles. Es claro como la participación de la gente va aumentando en estos temas de sostenibilidad mediante estas herramientas tecnológicas.

En la parte de los pros, se puede observar la facilidad de obtener estas herramientas tecnológicas: La mayoría de la gente tiene un teléfono celular y puede tener acceso a estas aplicaciones. Así como también la IA nos facilita la búsqueda rápida de información y con esto poder para hacer recomendaciones dirigidas a cada persona y brindar feedback rápidamente.

Un punto importante es que aunque tengamos estas herramientas disponibles no quiere decir que todas las personas la usen de forma correcta. Un punto en contra es la persistencia de la brecha digital. Esto va más allá de la accesibilidad a estas herramientas; esto quiere decir que no todos tenemos entendemos de manera clara los datos que nos brindan estas herramientas tecnológicas. Aunque muchas apps tienen funciones automatizadas, la interacción con la IA a menudo no es intuitiva o está mal explicada, lo que termina generando desconfianza o rechazo en los usuarios.

Otro punto limitante es que la mayoría de estas aplicaciones casi nunca trascienden el ámbito individual. Sus funciones tienden a enfocarse en acciones básicas —dar consejos de ahorro de agua, fomentar el reciclaje o medir la huella de carbono— sin lograr un impacto más amplio a nivel colectivo o estructural. Son muy pocas las que realmente integran dinámicas colectivas, comunidades digitales o mecanismos estructurados de participación cívica. Por esta restricción, es muy difícil que los esfuerzos individuales se articulen en iniciativas colectivas, algo esencial para lograr transformaciones ambientales de mayor magnitud.

4.2. Oportunidades y amenazas en la integración de IA a la participación ciudadana ambiental

Incorporar la inteligencia artificial en estas aplicaciones móviles realmente abre la puerta a aumentar significativamente su impacto y eficacia. La IA nos permite reconocer patrones de comportamiento, adelantarnos a las necesidades, automatizar procesos y, en general, mejorar la toma de decisiones ambientales.

En el contexto de la sostenibilidad, la IA podría ser una herramienta poderosa: puede analizar grandes volúmenes de datos ambientales, ayudar a generar alertas tempranas, optimizar las rutas de reciclaje o incluso detectar de forma precisa zonas críticas de contaminación. Es, sin duda, un cambio de juego.

Pero esta gran oportunidad trae consigo muchos peligros inherentes. El más evidente es la opacidad algorítmica. Es un problema porque muchos sistemas de inteligencia artificial operan como auténticas "cajas negras": no nos explican claramente ni cómo llegaron a

las recomendaciones ni cómo se tomaron las decisiones. Esto no solo tiene el efecto de falta de confianza, sino también de la apropiación pública de la tecnología.

Un segundo peligro es que replica sesgos. Y los algoritmos tienen el poder de perpetuar desigualdades, especialmente si no toman en serio los criterios de equidad, inclusividad y representatividad. En el campo de la ciencia ambiental, esto podría significar que ciertas comunidades reciban un trato desfavorable o que los datos no reflejen con precisión las realidades locales.

Finalmente, el análisis reveló una amenaza emergente: la normalización de la vigilancia digital. Para el uso por algunas aplicaciones ambientales, se puede utilizar la geolocalización permanente o el seguimiento de hábitos o la recopilación de datos sensibles. Aunque tales prácticas pueden tener una motivación legítima, la ausencia de regulación permite su mal uso, disminuyendo así la confianza en las tecnologías ambientales.

4.3. Limitaciones metodológicas en los modelos actuales

El análisis comparativo mostró que varios modelos de sostenibilidad digital siguen concentrados en campañas educativas y herramientas informativas, perdiendo estrategias de participación profunda de los ciudadanos. Hasta ahora, la mayoría de las iniciativas se centran en tres elementos: concienciación, medición individual y cambios de comportamiento a pequeña escala. Sin embargo, apenas vemos integración de modelos de acción colectiva o mecanismos que conecten la información con las decisiones de políticas públicas.

Además, los modelos actuales no siempre especifican con claridad qué indicadores deben utilizarse para evaluar el verdadero impacto social que producen las aplicaciones basadas en IA. Y, aunque existen algunas métricas para uso, descarga o interacción, no son necesariamente el índice de transformación sostenible a largo plazo. La brecha metodológica lleva a la dificultad de determinar si una aplicación particular convierte la concienciación en acción, o si la aplicación simplemente genera comportamientos aislados.

Una segunda gran limitación es que no tienen en cuenta el contexto local. La mayoría de los modelos se construyen desde un punto

de vista global o corporativo, sin considerar localmente las condiciones socioeconómicas o las necesidades específicas de las comunidades. Esto disminuye su aplicabilidad y dificulta su apropiación social.

4.4. Riesgos y omisiones en la relación ciudadanía–algoritmos

El uso de la inteligencia artificial en aplicaciones ambientales ha creado nuevas tensiones entre los ciudadanos y la tecnología. Uno de los riesgos que más me preocupa es la omisión de procesos educativos que permitan a los usuarios entender realmente el alcance y las limitaciones de estos algoritmos.

Por esta razón, es fundamental que las personas desarrollen competencias digitales y comprendan el funcionamiento básico de los algoritmos. Solo así podrán participar de una manera verdaderamente autónoma, crítica y responsable.

En los siguientes problemas y soluciones que se realizaron en la metodología se pudo observar algo importante: la carencia de entendimiento técnico bien dirigido por parte de los usuarios es una de las cosas importantes que detiene que estas acciones de sostenibilidad sea algo sólido para las personas. La inteligencia artificial puede sugerir acciones, pero a menos que el usuario entienda el porqué, probablemente no las llevará a cabo de manera sostenida.

Otro punto importante en los contras es la falta de motivación hacia los usuarios. Muchas aplicaciones dependen de motivaciones individuales, sin integrar dinámicas de comunidad, reconocimiento colectivo o construcción de identidad ambiental compartida. Este vacío impide que los esfuerzos individuales escalen hacia transformaciones comunitarias o políticas.

4.5. Resultados finales de la discusión

Tabla 1. Ventajas vs. desventajas

Ventajas	Desventajas
Accesibilidad tecnológica	Brecha digital y baja alfabetización en IA
Personalización mediante IA	Interacciones poco intuitivas
Datos en tiempo real	Falta de transparencia algorítmica
Capacidad de escalabilidad	Foco excesivo en el individuo

Tabla 2. Oportunidades vs. amenazas

Oportunidades	Amenazas
Análisis avanzado de datos ambientales	Sesgos algorítmicos
Predicción de patrones	Vigilancia digital
Optimización de procesos	Baja confianza ciudadana
Innovación social digital	Centralización de datos

4.6. Como respuesta a la pregunta de investigación y proponiendo
y un modelo base

Con el estudio realizado, se puede decir que con la ayuda de estas herramientas tecnológicas podemos tener participación y ayudar a que la sostenibilidad sea un tema activo para las personas. Pero es importante señalar que todo esto no será posible sin antes encontrar solución a los defectos que hemos encontrado.

En este sentido, se plantea un Modelo de Acción Ciudadana Mediado por IA (MACIA), integrado por cinco ejes:

1. Alfabetización digital y algorítmica
2. Transparencia y explicabilidad de inteligencia artificial
3. Participación colectiva digital
4. Datos de impacto social ambiental
5. Diseño centrado en la ciudadanía

Esta propuesta busca articular elementos tecnológicos, sociales para que las herramientas tecnologicas dejen de ser simples solo aplicaciones y sean aplicaciones de gran ayuda para que sea un cambio en conjunto en este tema de sostenibilidad.

4.7. Aportaciones finales

APORTACIÓN TEÓRICA (SCIENTIA)

Este estudio ayuda a incrementar el conocimiento que tenemos al brindar un marco conceptual que articula estos temas clave: la inteligencia artificial, la sostenibilidad y la participación de las personas.

Esta idea es importante porque podemos saber el fenómeno desde el lado socio-tecnológico, encontrar las desventajas reales que tenemos y añade un modelo que podemos usar como un inicio fuerte para las proximas investigaciones.

APORTACIÓN PRÁCTICA (PRAXIS)

Con el Modelo MACIA tenemos un procedimiento práctico a diseñadores, instituciones y desarrolladores para cambiar las herramientas de información en aplicaciones que fomentan acciones sostenibles en conjunto.

Esta idea señala la transparencia, la claridad algorítmica y la inclusión de las personas. Estos puntos son claves e importantes para formar una sostenibilidad digital que funcione en casos reales.

5. Conclusiones

Con este ensayo puedo decir que las herramientas móviles con IA pueden ser importantes para promover la participación de la gente en este tema de sostenibilidad, teniendo en cuenta que deben tener ética y redes de ayuda en conjunto.

En el estudio que realice podemos ver que, tenemos avances destacados en el desarrollo de estas tecnologías para las personas, aún hay desventajas importantes entre las habilidades técnicas disponibles y la participación de los usuarios. Esto detiene el alcance de las herramientas para promover estos hábitos en las personas.

En mi punto de vista, la inteligencia artificial es necesaria porque perfecciona los ajustes individuales para mejorar las sugerencias y ofrecer retroalimentación rápido. Es importante decir que su impacto real está en temas estructurales: la calidad de los datos, la claridad y la gobernanza de estas herramientas tecnológicas. En caso de no sé usarse de la forma correcta, estas herramientas pueden generar datos incorrectos y con esto dar información errónea y con esto se invalida los beneficios en el cambio de comportamiento.

También pude observar lo importante que es avanzar hacia una era de sostenibilidad digital mucho más amplia. Esto requiere que gobiernos, empresas tecnológicas, academia y personas trabajamos en conjunto y de manera coordinada.

La incompatibilidad entre aplicaciones, los estándares abiertos y los modelos de colaboración público y privada son importantes. Solo así podremos subir las innovaciones que hoy están en modo prueba y añadirlas al sistema para lograr resultados más altos. Los temas que estudie recomiendan que el éxito de la participación con IA no solo es su innovación tecnológica sino también de cómo se involucran en la realidad de las personas.

Las herramientas tecnológicas nos ayudan con el aprendizaje, la participación en la sostenibilidad y por su fácil acceso y los ajustes individuales que nos permiten.

Por último, este ensayo propone una base teórica y analítica que se puede usar en proximas investigaciones, ayudando en el campo de la sostenibilidad digital, por ejemplo, en el diseño de nuevos modelos de gobernanza, en la combinación de indicadores sostenibles y en el estudio del impacto social con una IA explicable

Referencias

- Accenture. (2021). *Uniting sustainability and technology: How tech and sustainability come together to drive growth and value*. <https://www.accenture.com/content/dam/accenture/final/a-com-migration/pdf/pdf-177/accenture-tech-sustainability-uniting-sustainability-and-technology.pdf>
- Boston Consulting Group. (2023). *Accelerating climate action with artificial intelligence*. <https://web-assets.bcg.com/72/cf/b609ac3d4ac6829bae6fa88b8329/bcg-accelerating-climate-action-with-ai-nov-2023-rev.pdf>
- McKinsey & Company. (2024). *AI for social good: Improving lives and protecting the planet*. <https://www.mckinsey.com/~media/mckinsey/business%20functions/quantumblack/our%20insights/ai%20for%20social%20good/2024/ai-for-social-good-improving-lives-and-protecting-the-planet-v2.pdf>
- PricewaterhouseCoopers. (2020). *Fourth Industrial Revolution (4IR)-enabled applications for the Sustainable Development Goals (SDGs)*. <https://www.pwc.com/gx/en/sustainability/SDG/4ir-enabled-applications-for-sdgs.pdf>
- Organisation for Economic Co-operation and Development. (2022). *Harnessing the power of AI and emerging technologies*. (OECD Digital Economy Papers). <https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/harnessing-the-power-of-ai-and-emerging-technologies.pdf>
- United Nations. (2023). *The Sustainable Development Goals Report 2023*. <https://unstats.un.org/sdgs/report/2023/The-Sustainable-Development-Goals-Report-2023.pdf>
- UNESCO. (2021). *Recommendation on the ethics of artificial intelligence*. <https://unesdoc.unesco.org/ark:/48223/pf0000381137>
- Vinuesa, R., Azizpour, H., Leite, I., Balaam, M., Dignum, V., Domisch, S., ... & 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>
- Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... & Vayena, E. (2018). AI4People—An ethical framework for a good AI society. *Minds and Machines*, 28(4), 689–707. <https://doi.org/10.1007/s11023-018-9482-5>



This is an open access article distributed under the terms of the CC BY-NC license (Disponible en: <https://creativecommons.org/licenses/by-nc/4.0/>)

Capítulo 4

Multicast inteligente adaptativo: un modelo de transmisión seguro impulsado por aprendizaje automático

José Isidro Cerda-Silva¹

Resumen

El ensayo propone la arquitectura *multicast* inteligente adaptativo (MIA) para realizar replicación masiva de datos mediante *multicast* seguro orquestado por inteligencia artificial. Parte del diagnóstico de que el *multicast* tradicional, aunque eficiente en ancho de banda, presenta debilidades en seguridad, confiabilidad y control de congestión, críticas en IoT, sistemas ciberfísicos (CPS —Cyber-Physical Systems) y *smart grids* (Wijnands *et al.*, 2017). Considerando los puntos anteriores, el ensayo plantea la integración de cuatro elementos en una sola arquitectura: (i) en la capa de replicación, se propone apoyarse en BIER (Bit Index Explicit Replication) como alternativa moderna para el reenvío de *multicast*; en seguridad, el planteamiento combina (ii) un tránsito gradual hacia criptografía preparada para la era cuántica y (iii)

1. Universidad de Guadalajara, Guadalajara, Jalisco, México. email: isidro.cerda@udg.mx.
ORCID: 0009-0002-6703-1437

un enfoque operativo de *zero trust*, donde no se asume una confianza implícita por ubicación de red y se privilegia la verificación continua (International Telecommunication Union, 2021), y (iv) para que la red se adapte en tiempo real, el uso de la inteligencia artificial (IA) considerándola en dos niveles: detección de anomalías con *autoencoders* de bajo costo (tomando como referencia Kitsune/KitNET, pensado para correr en *gateways* con recursos limitados) y en ajuste dinámico de decisiones de ruteo con aprendizaje por refuerzo profundo, incluyendo enfoques multiagente para construir o refinar rutas *multicast* bajo variación de estado de enlaces (Hu *et al.*, 2023). En conjunto, el ensayo concluye que, si estos componentes se integran correctamente, MIA podría reducir latencia y retransmisiones y mejorar la postura de seguridad en escenarios de replicación intensiva, aunque la magnitud del efecto quedaría sujeta a validación experimental en escenarios representativos.

Palabras clave: *multicast* seguro, *multicast* inteligente adaptativo (MIA), replicación de datos masivos, aprendizaje automático, *deep reinforcement learning* (DRL), aprendizaje federado, *autoencoder*, *zero trust*, *bier*, *messaging layer security* (MLS)

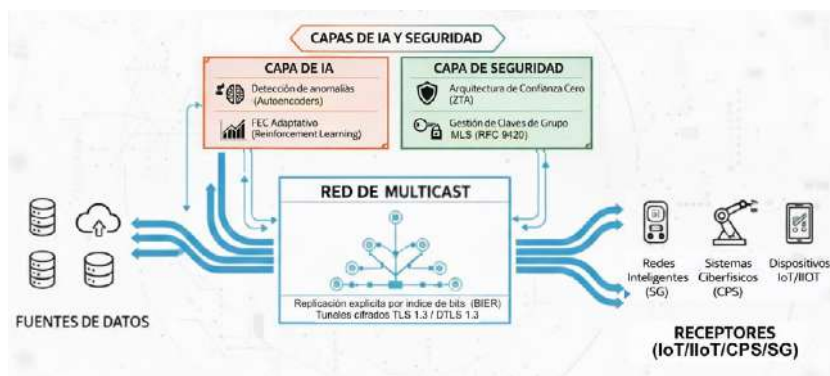
1. Introducción

La transmisión *multicast* es un mecanismo esencial de comunicación en redes distribuidas e inalámbricas, utilizado para el envío de información a un conjunto de receptores con eficiencia en el consumo de ancho de banda, en aplicaciones como teleconferencias, transmisión de video y distribución coordinada de datos en escenarios con múltiples consumidores (Hu *et al.*, 2023). Sin embargo, el *multicast* tradicional carece de mecanismos intrínsecos robustos para seguridad de grupo, control de congestión y confiabilidad; problemas que se agravan en dominios críticos como IoT/IIoT, sistemas ciberfísicos (CPS-) y *smart grids*, donde la indisponibilidad, la manipulación o la filtración de datos tienen impactos operativos (Makris *et al.*, 2024).

En este contexto, el ensayo plantea la pregunta de investigación: *¿De qué manera el aprendizaje automático mejoraría la seguridad y la eficiencia de las transmisiones multicast en un modelo de transmisión seguro?* Para responderla, se propone el modelo MIA, que articula mecanismos de replicación *multicast* más eficientes, criptografía y gestión de claves

de grupo, y una capa de inteligencia que ajusta parámetros y detecta anomalías sobre la base de observaciones de la red.

Figura 1. Marco conceptual del modelo MIA: fuentes de datos → red multicast → capa de IA/seguridad → receptores (IoT/IIoT/CPS/SG).



Fuente: Elaboración propia.

2. Desarrollo

Esta sección se centra en la fundamentación y la construcción del modelo MIA, estableciendo el *contexto de los sistemas ciberfísicos* (CPS/*smart grids*) y la problematización de las debilidades históricas del *multicast* tradicional en seguridad, confiabilidad y control de congestión.

2.1. Contexto y problematización

La dependencia de intercambio de información en CPS y *smart grids* expone los sistemas a amenazas cuando la transmisión carece de seguridad, en particular en infraestructuras como AMI, donde los datos de consumo revelan hábitos y rutinas (Abdalzaher *et al.*, 2023). Por otra parte, la coexistencia de múltiples grupos *multicast* agota recursos y produce congestión y pérdida de paquetes, lo que motivó trabajos de

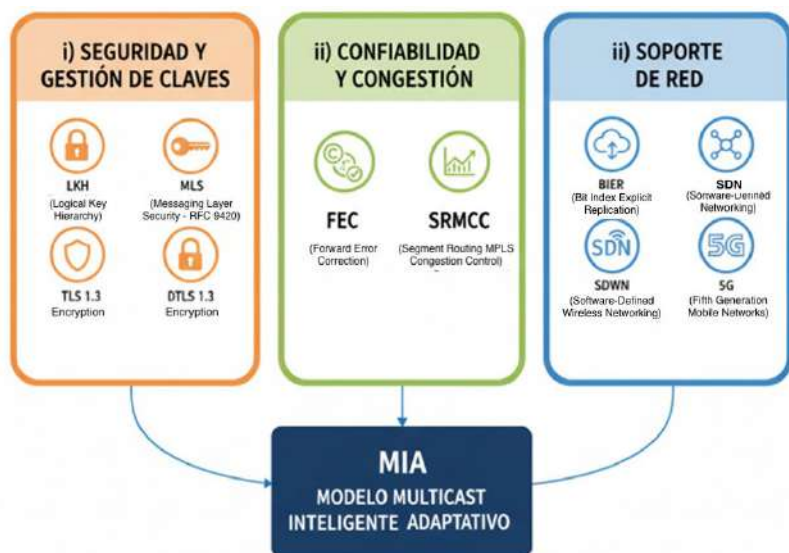
control de congestión en arquitecturas emergentes, como ICN (Duan *et al.*, 2022). En entornos altamente dinámicos, como FANETS, el *multicast* enfrenta desafíos de seguridad ante ataques como *wormhole* y la búsqueda de rutas óptimas es computacionalmente compleja (Pramitarini *et al.*, 2023; Ye *et al.*, 2024).

2.2. Antecedentes del estado de la cuestión

A escala mundial, los esfuerzos de *multicast* seguro se han centrado en autenticación, integridad y confidencialidad para comunicaciones de grupo, y en técnicas de gestión de claves como LKH (Abdalzaher *et al.*, 2023; Hu *et al.*, 2023). En el contexto internacional, se consolidan paradigmas como *zero trust*, donde la confianza no se asume y se evalúa de forma continua, aplicando mínimo privilegio y verificación permanente (Rose *et al.*, 2020). En paralelo, la estandarización de seguridad de grupo con MLS busca reclaveo eficiente y escalable ante cambios de membresía (Barnes *et al.*, 2023).

En México se observa interés por infraestructura de datos confiable y por gestión inteligente de redes con IA, con predominio de enfoques en SDN/5G y seguridad. No obstante, con la evidencia discutida en el documento, no aparece aún una propuesta local que combine explícitamente IA y *multicast* como eje de gestión, lo que refuerza el carácter novedoso de una línea como MIA en ambientes universitarios (según el propio análisis del ensayo).

Figura 2. Mapa del estado del arte: (i) seguridad/gestión de claves (LKH/MLS/TLS/DTLS), (ii) confiabilidad y congestión (FEC/SRMCC), (iii) soporte de red (BIER/SDN/SDWN/5G).



Fuente: Elaboración propia.

2.3. Descripción del estado del arte

El ensayo articula dos vertientes convergentes: (a) multidifusión segura y eficiente para replicación de grandes volúmenes de datos, y (b) uso de IA para gestión adaptativa y detección de amenazas. En seguridad de grupo, MLS y mecanismos criptográficos modernos incrementan la escalabilidad de reclaveo y la resiliencia ante membresías dinámicas (Barnes *et al.*, 2023; Lim *et al.*, 2025). En reenvío eficiente, BIER permite indicar destinos mediante un *bit string* en el encabezado y en evitar estado por flujo, lo que favorece dominios *multicast* de gran escala (Wijnands *et al.*, 2017).

En rutas seguras, el estado del arte incluye propuestas que emplean aprendizaje profundo para discriminar nodos seguros de maliciosos y

mitigar ataques como *wormhole* en FANETS, así como técnicas regionales como *Multicast* seguro basado en zona (ZSM —Zone-Based Secure *Multicast*) en redes *ad hoc* móviles (MANETS —Mobile *ad hoc* Networks) para mejorar confiabilidad y mitigar movilidad (Pramitarini *et al.*, 2023; Yang, 2025). En optimización adaptativa, esquemas multiagente de DRL construyen árboles *multicast* y se adaptan a variaciones de ancho de banda, retardo y pérdida, y aceleran la convergencia con mecanismos como *transfer learning* (Hu *et al.*, 2023; Ye *et al.*, 2024).

Para seguridad operacional en redes heterogéneas, el aprendizaje federado se propone para detección de intrusiones/anomalías sin centralizar datos, mejorando precisión frente al entrenamiento local y preservando privacidad en IoT/IIoT/IIoV (Makris *et al.*, 2024; Lim *et al.*, 2025). En detección en línea, Kitsune/KitNET demuestra el uso de *autoencoders* ligeros para identificar desviaciones mediante error de reconstrucción (RMSE) en dispositivos con recursos limitados (Mirsky *et al.*, 2018).

3. Metodología

La metodología seguida para el diseño del modelo conceptual MIA se planteó como híbrida: documental, analítica y de diseño arquitectónico. Se recopiló y comparó evidencia normativa y científica relevante (2016–2025), para justificar decisiones de arquitectura y seleccionar mecanismos de seguridad, reenvío y aprendizaje automático. El proceso metodológico se organizó por “capas” de argumentación: primero se establecieron requerimientos y supuestos de seguridad y desempeño, y posteriormente se alinearon con soluciones encontradas en la literatura (citas) para asegurar trazabilidad y replicabilidad.

Justificación del enfoque metodológico

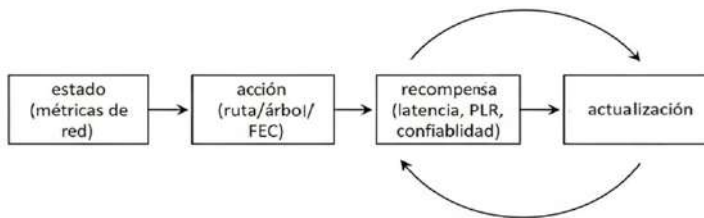
La justificación metodológica se centró en estructurar la integración de soluciones avanzadas (IA, criptografía, redes). Se buscó presentar las aportaciones teóricas y prácticas (ciencia y praxis) a través de la descripción de las etapas secuenciales del modelo y la descripción

detallada de sus elementos conceptuales. La transición de un modelo inicial (*ex ante*) a una arquitectura refinada (*ex post*), obtenida a través de la discusión con especialistas, fue un elemento central del diseño metodológico.

Arquitectura MIA

El diseño se estructuró en cuatro capas interconectadas, tal como se discute en el ensayo: (1) una capa de datos basada en replicación *multicast* eficiente apoyada en BIER, (2) una capa de control con cifrado TLS 1.3 / DTLS 1.3 para confidencialidad e integridad, (3) una capa de IA que incorpora *autoencoders* para detección de anomalías y aprendizaje por refuerzo (RL —Reinforcement Learning) para ajuste adaptativo de parámetros como FEC; y (4) una capa de seguridad que aplica políticas *zero trust* y reclaveo escalable de grupo mediante MLS (Wijnands *et al.*, 2017; International Telecommunication Union, 2021; Mirsky *et al.*, 2018; Hu *et al.*, 2023; Rose *et al.*, 2020; Barnes *et al.*, 2023).

Figura 3. Ciclo RL/DRL aplicado a multicast: estado (métricas de red)
→ acción (ruta/árbol/FEC) → recompensa (latencia, PLR, confiabilidad)
→ actualización.



Fuente: Elaboración propia.

Métricas, objetivo y criterio de mejora

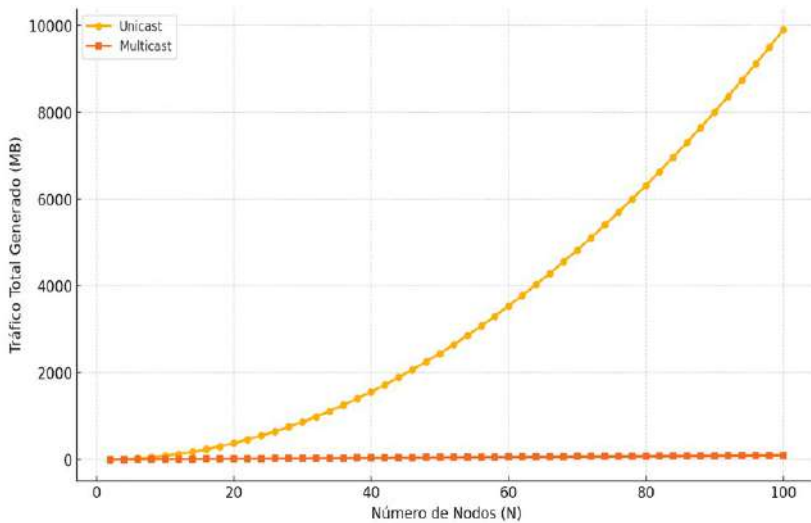
Para operacionalizar “eficiencia” y “confiabilidad”, el ensayo utiliza métricas como latencia y tasa de pérdida de paquetes (PLR —Packet Loss Rate), y

considera el uso de RMSE en detector de anomalías basado en *autoencoders* (Mirsky *et al.*, 2018). Como referencia para magnitudes de mejora, se recupera evidencia donde, en escenarios de comunicación grupal, se observan reducciones importantes de latencia y PLR al comparar esquemas *multicast* y *unicast* bajo restricciones de QoS (Debnath *et al.*, 2021).

Para cuantificar la mejora estimada del esquema MIA frente a *unicast* clásico, el ensayo plantea una función de predicción en la forma $f(s) \rightarrow (L_{MIA}, R_{MIA})$ donde el estado s incluye variables como número de nodos replicados, tamaño de transacciones, pérdida y *jitter* por enlace, y profundidad del árbol *multicast*. Bajo este esquema, las reducciones porcentuales se expresan como: $\Delta L_{\%} = 100 \cdot \frac{L_{uni} - L_{MIA}}{L_{uni}}$ y $\Delta R_{\%} = 100 \cdot \frac{R_{uni} - R_{MIA}}{R_{uni}}$.

Alineado con los rangos de referencia discutidos, el objetivo se fija en reducciones del orden del 60% al 80% en retransmisiones y cercanas a 80% en latencia en escenarios con muchos receptores, para ser validadas posteriormente en experimentación o simulación (Debnath *et al.*, 2021; Hu *et al.*, 2023; Zhao *et al.*, 2022).

Figura 4. Comparación gráfica entre tráfico unicast vs multicast.

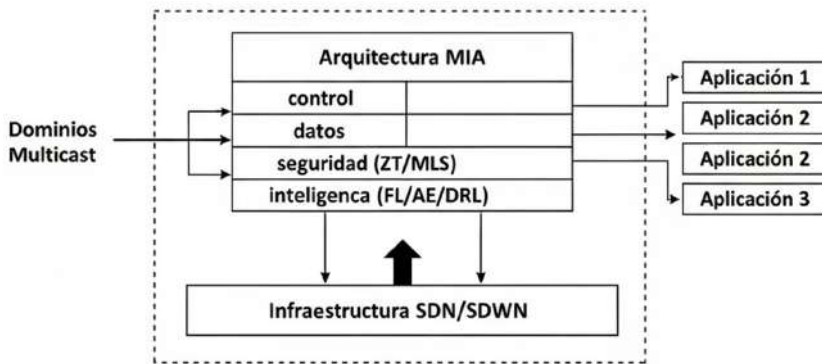


Fuente: Elaboración propia.

4. Discusión

La discusión evalúa la propuesta MIA como convergencia entre eficiencia de *multicast* y exigencias actuales de seguridad, confiabilidad y adaptabilidad en redes distribuidas (CPS, IIoT, *smart grids*) (Abdalzaher *et al.*, 2023). En términos de arquitectura, el valor del modelo se apoya en: (a) reenvío eficiente (BIER) para escalabilidad, (b) cifrado y seguridad de grupo (TLS/DTLS, MLS), (c) postura de confianza cero, y (d) una capa de IA que permite adaptación y vigilancia permanente mediante la detección de anomalías y optimización de parámetros (Wijnands *et al.*, 2017; Rose *et al.*, 2020; Barnes *et al.*, 2023; Mirsky *et al.*, 2018).

Figura 5. Arquitectura MIA sobre infraestructura SDN/SDWN y dominios *multicast*: control, datos, seguridad (ZT/MLS) e inteligencia (FL/AE/DRL).



Fuente: Elaboración propia.

4.1. Eficiencia: optimización de rutas y control de condiciones

En eficiencia, el ensayo argumenta que la toma de decisiones basada en DRL permite ajustar rutas/árboles *multicast* y parámetros de transmisión conforme cambian las condiciones de la red (pérdida, retardo, congestión), priorizando simultáneamente desempeño y estabilidad. Este

enfoque es consistente con trabajos que optimizan retardo y pérdida en enrutamiento *multicast* en entornos SDWN con DRL multiagente (Hu *et al.*, 2023; Ye *et al.*, 2024) y con técnicas de control de congestión *multicast* en arquitecturas como ICN (Duan *et al.*, 2022). La combinación con mecanismos como FEC, ajustados dinámicamente por RL, aproxima el objetivo de confiabilidad sin sobreconsumir ancho de banda.

4.2. Seguridad: zero trust, seguridad de grupo y detección de anomalías

En seguridad, el modelo integra: (i) políticas *zero trust* orientadas a minimizar privilegios y verificar continuamente, (ii) seguridad de grupo con reclaveo escalable para escenarios de membresía dinámica mediante MLS, y (iii) detección de anomalías apoyada en *autoencoders*, con posibilidad de entrenamiento federado para preservar privacidad en entornos descentralizados (Rose *et al.*, 2020; Barnes *et al.*, 2023; Mirsky *et al.*, 2018; Makris *et al.*, 2024; Lim *et al.*, 2025). El uso de *autoencoders* ligeros (como en Kitsune/KitNET) proporciona detección en línea basada en desviaciones del comportamiento normal (RMSE), útil para IoT/IoT y casos como AMI.

4.3. Aplicabilidad a replicación de datos masivos y PostgreSQL

El documento discute la replicación de datos masivos como un caso natural para el uso de *multicast* seguro y confiable. En entornos de bases de datos distribuidas (por ejemplo, PostgreSQL), la replicación requiere transportar grandes volúmenes de información manteniendo consistencia operativa y controlando pérdidas y latencias. En este marco, MIA se plantea como arquitectura conceptual para distribuir actualizaciones a múltiples nodos con eficiencia de ancho de banda y con controles de seguridad y supervisión continua, reduciendo la exposición a interceptación/manipulación y mitigando el impacto de congestión en escenarios de muchos receptores (Wijnands *et al.*, 2017; Rose *et al.*, 2020; Makris *et al.*, 2024).

4.4. Resultados de discusión

En la discusión, el modelo MIA se consolida como un marco que responde a cómo el *machine learning* mejora simultáneamente la seguridad y la eficiencia del *multicast*, al integrar: (i) un plano de control protegido con TLS 1.3/DTLS 1.3, alineado con guías de criptografía *quantum-safe* que recomiendan, por ejemplo, PSK y criptografía simétrica de 256 bits para confidencialidad e integridad en contextos donde se emplean IPsec/TLS/DTLS (ITU, 2021) con un paradigma de *zero trust* Architecture para gobernar la confianza mediante verificación continua y foco en usuarios/activos/recursos, en lugar de perímetros estáticos (Rose *et al.*, 2020); (ii) analítica con *deep learning* aplicada a detección de intrusiones/anomalías, respaldada por enfoques como *autoencoders* para FIDS en línea y por revisiones de *federated intrusion detection systems* (Makris *et al.*, 2025; Mirsky *et al.*, 2018, con una optimización adaptativa del ruteo/árbol *multicast* mediante DRL en entornos SDN, donde el aprendizaje jerárquico se usa para construir rutas/árboles bajo condiciones dinámicas (Ye *et al.*, 2024), y (iii) una agenda explícita de replicabilidad, ya que la literatura en detección de anomalías basada en FL reporta como limitación la ausencia de un marco unificado de *benchmarking* para comparaciones justas, brecha que se intenta mitigar con metodología y, complementariamente, con propuestas recientes de *benchmarks* unificados (Lim *et al.*, 2025).

4.5. Planteamiento del modelo base de discusión

La pregunta de investigación fue: ¿De qué manera el aprendizaje automático mejoraría la seguridad y la eficiencia de las transmisiones *multicast* en un modelo de transmisión seguro?

El modelo base para la discusión, la arquitectura MIA (*multicast* inteligente adaptativo), integra el aprendizaje automático (ML/IA) para mejorar la seguridad y la eficiencia de las transmisiones *multicast* a través de dos mecanismos principales.

En eficiencia, MIA usa DRL para optimizar de forma adaptativa el reenvío (integrado con BIER) y el control de QoS mediante ajuste de FEC, atacando tanto la complejidad NP-hard de construir rutas óptimas

como la ausencia de control de congestión del *multicast* tradicional (Tam *et al.*, 2024; Ye *et al.*, 2024). En seguridad, emplea *autoencoders* federados (FL-AE) para detección proactiva y descentralizada de anomalías en escenarios *non-IID* (p. ej., falsificación de datos o intrusiones), con el objetivo de preservar la integridad de los datos replicados (Mirsky *et al.*, 2018; Makris *et al.*, 2024; Lim *et al.*, 2025).

MIA demuestra, por lo tanto, que el ML es la pieza clave para inyectar la inteligencia adaptativa necesaria para que las transmisiones *multicast* sean viables, seguras (*zero trust*, MLS, PQC-resistente) y eficientes en la era de los datos masivos y la conectividad dinámica.

4.6. Aportaciones

El modelo MIA genera contribuciones sustanciales que se extienden a dos esferas fundamentales: la teoría del conocimiento y la práctica de la ingeniería de redes. A continuación analizaremos cómo la propuesta avanza el estado del arte en lo conceptual y en lo metodológico (*Scientia*), y cómo ofrece un marco operacional de implementación inmediata y escalable para entornos de datos masivos (*Praxis*):

a. Aportación Teórica (*Scientia*)

La principal contribución teórica del ensayo reside en la formulación del modelo *multicast* inteligente adaptativo (MIA), una arquitectura conceptual que redefine el paradigma de transmisión *multicast* tradicional, al integrarlo simbióticamente con la inteligencia artificial y los principios de ciberseguridad avanzada. El ensayo mejora el estado del conocimiento, al superar la visión clásica del *multicast* —eficiente en ancho de banda, pero débil en seguridad y control— y proponer la integración inédita de cuatro elementos tecnológicos que no es común abordar en conjunto: (i) replicación explícita (BIER), (ii) criptografía post-cuántica con una arquitectura *zero trust* y (iii) aprendizaje automático en la adaptación de la red en tiempo real.

La originalidad del modelo radica en su enfoque híbrido tecnológico. En lugar de tratar la seguridad y la optimización como capas aisladas, se propone una integración donde la inteligencia artificial (IA)

actúa como el cerebro de la red. Esto se logra mediante la fusión de *autoencoders* para la detección de anomalías (inspirado en Kitsune/KitNET) y el aprendizaje por refuerzo profundo (DRL) para la optimización dinámica de rutas y parámetros de corrección de errores (FEC).

Desde una perspectiva académica, el ensayo contribuye a llenar un vacío en la literatura regional y universitaria, donde no existía una propuesta local que combinara explícitamente la gestión de redes de transmisión *multicast* mediante IA. El modelo teórico de MIA establece que la eficiencia y la seguridad en redes distribuidas masivas no son objetivos contrapuestos, sino convergen mediante una “capa de inteligencia” que adapta la red en tiempo real frente a condiciones dinámicas y amenazas, validado mediante una metodología de diseño arquitectónico que transita de un modelo *ex ante* a uno refinado *ex post*.

b. Aportación práctica (*praxis*)

En el ámbito de la *praxis*, el ensayo contribuye en hacer un marco de trabajo operable, viable para resolver problemas críticos en infraestructuras sensibles, como la internet industrial de las cosas (IIoT), los sistemas ciberfísicos (CPS) y las *smart grids*. MIA mejora el estado de la cuestión al ofrecer una solución concreta a la congestión y la vulnerabilidad de datos en entornos de replicación masiva, y se aleja de soluciones teóricas abstractas para proponer mecanismos estandarizados, como BIER para el reenvío y MLS (Messaging Layer Security) para la gestión escalable de claves de grupo.

La utilidad práctica del modelo MIA se determina en dos vertientes:

- **Optimización cuantificable:** El ensayo no solo describe un modelo, si no también propone una función de predicción para estimar su impacto, proyectando reducciones del 60% al 80% en retransmisiones y una mejora significativa en la latencia y la tasa de pérdida de paquetes (PLR), en comparación con esquemas de comunicación *unicast*. Esto ofrece indicadores claros de impacto para la toma de decisiones en ingeniería de redes.
- **Aplicabilidad en bases de datos distribuidas:** Una aportación práctica específica es la aplicación del modelo a la replicación de bases de datos basadas en PostgreSQL. El modelo MIA se presenta como una arquitectura capaz de distribuir actualizaciones masivas a múltiples nodos manteniendo la consistencia y reduciendo la superficie de

ataque mediante túneles cifrados (TLS 1.3/DTLS 1.3) y políticas de confianza cero.

En resumen, la *praxis* del ensayo transforma la gestión de redes *multicast* de un proceso estático y manual a otro dinámico y automatizado, capaz de autoprotgerse y autooptimizarse para sostener la demanda de datos de la era actual.

5. Conclusión

La pregunta de investigación —sobre cómo el aprendizaje automático mejora la seguridad y la eficiencia del *multicast*— se responde en el ensayo mediante la arquitectura MIA y su organización por capas: el ML aporta inteligencia adaptativa para ajustar rutas y parámetros (incluyendo FEC) en función de métricas de red, mientras que la seguridad se fortalece al integrar principios *zero trust*, cifrado de transporte (TLS/DTLS 1.3) y seguridad de grupo con reclaveo escalable (MLS) (Rose *et al.*, 2020; Barnes *et al.*, 2023; Hu *et al.*, 2023; Mirsky *et al.*, 2018). En reenvío, BIER contribuye a la escalabilidad del dominio *multicast* al evitar estado por flujo, lo cual favorece escenarios de distribución masiva (Wijnands *et al.*, 2017).

Como recomendaciones, se enfatiza en: (1) el desarrollo de benchmarks y datasets públicos para evaluar soluciones basadas en FL y detección de anomalías, (2) la validación operativa del modelo integrando PLS-SEM con simuladores de red para fortalecer replicabilidad, y (3) explorar la extrapolación del modelo a dominios emergentes como redes energéticas inteligentes, telemedicina y vehículos autónomos (Tam *et al.*, 2024; Lim *et al.*, 2025).

6. Apéndices

Acrónimos

Acrónimo	Significado (español)	Significado (inglés)
$f(S)$	Función de aprendizaje ajustada por el entrenamiento del DRL. Esta función aprende una política de enrutamiento óptima para el vector de estado S de la red en un momento dado. Incluye todas las variables contextuales que afectan el rendimiento.	
L_{MIA}	Latencia promedio de entrega esperada (o predicha) por el modelo MIA para el estado S	
R_{MIA}	Número de reenvíos adicionales por paquete confirmado esperado (o predicho) por el modelo MIA para el estado S	
$\Delta L_{\%}$	Porcentaje de reducción en la latencia que el modelo MIA logra frente al <i>unicast</i> clásico.	
L_{uni}	Latencia promedio de entrega medida para un escenario idéntico, utilizando la comunicación <i>unicast</i> clásica.	
R_{uni}	Número de reenvíos adicionales predicho por el modelo MIA.	
AE	<i>Autoencoders</i>	Autoencoders
AMI	Infraestructura de medición avanzada	Advanced Metering Infrastructure
BIER	Replicación explícita por índice de bits	Bit Index Explicit Replication
CPS	Sistemas ciberfísicos	Cyber-Physical Systems
DRL	Aprendizaje por refuerzo profundo	Deep Reinforcement Learning
DTLS	Seguridad de la capa de transporte de datagramas	Datagram Transport Layer Security
FANETS	Redes <i>ad hoc</i> voladoras	Flying <i>ad hoc</i> Networks

FEC	Corrección de errores hacia adelante	Forward Error Correction
FIDS	Sistemas de detección de intrusiones federados	Federated Intrusion Detection Systems
FL	Aprendizaje federado	Federated Learning
ICN	Redes centradas en la información	Information-Centric Networking
IIOT	Internet industrial de las cosas	Industrial Internet of Things
IOT	Internet de las cosas	Internet of Things
LKH	Jerarquía de claves lógicas	Logical Key Hierarchy
MANETS	Redes ad hoc móviles	Mobile ad hoc Networks
MIA	<i>Multicast</i> inteligente adaptativo	Intelligent Adaptive Multicast
MLS	Seguridad de la capa de mensajería	Messaging Layer Security
PLR	Tasa de pérdida de paquetes	Packet Loss Rate
PQC	Criptografía poscuántica	Post-Quantum Cryptography
QOS	Calidad de servicio	Quality of Service
RL	Aprendizaje por refuerzo	Reinforcement Learning
RMSE	Raíz del error cuadrático medio	Root Mean Square Error
SDN	Redes definidas por software	Software-Defined Networking
SDWN	Redes inalámbricas definidas por software	Software-Defined Wireless Networking
SG	Redes inteligentes (<i>smart grids</i>)	<i>Smart Grids</i>
SRMCC	Control de congestión MPLS por enrutamiento de segmentos	Segment Routing MPLS Congestion Control
TLS	Seguridad de la capa de transporte	Transport Layer Security
ZSM	<i>Multicast</i> seguro basado en zona	Zone-Based Secure Multicast
ZTA	Arquitectura de confianza cero	<i>Zero Trust</i> Architecture

7. Referencias

Abdalzaher, M. S., Fouda, M. M., Emran, A., Fadlullah, Z. M., & Ibrahim, M. I. (2023). A Survey on key Management and Authentication Approaches in Smart Metering Systems. *Energies*, 16(5), 2355. Disponible en: <https://doi.org/10.3390/en16052355>

- Barnes, R., Beurdouche, B., Robert, R., Millican, J., Omara, E., & Cohn-Gordon, K. (2023). The Messaging Layer Security (MLS) Protocol (RFC 9420). Internet Engineering Task Force. Disponible en: <https://doi.org/10.17487/RFC9420>
- Debnath, S. K., Saha, M., Islam, M. M., Sarker, P. K., & Pramanik, I. (2021). Evaluation of *Multicast* and *Unicast* Routing Protocols Performance for Group Communication with QoS Constraints in 802.11 Mobile *ad hoc* Networks. *International Journal of Computer Network and Information Security*, 13(1), 1–15. Disponible en: <https://doi.org/10.5815/ijcnis.2021.01.01>
- Duan, Y., Ni, H., Zhu, X., & Wang, X. (2022). A Single-rate Multicast Congestion Control (SRMCC) Mechanism in Information-centric Networking. *Future Internet*, 14(2), 38. <https://doi.org/10.3390/fi14020038>
- Hu, H., Ye, M., Zhao, C., Jiang, Q., & Xue, X. (2023). Intelligent Multicast Routing Method Based on Multi-agent Deep Reinforcement Learning in SDWN. *Mathematical Biosciences and Engineering*, 20(9), 17158–17196. Disponible en: <https://doi.org/10.3934/mbe.2023765>
- International Telecommunication Union (ITU) (2021). Lignes directrices en matière de sécurité relatives à l'utilisation d'algorithmes à l'épreuve des attaques quantiques dans les systèmes IMT-2020 (Recommandation ITU-T X.1811). ITU. Disponible en: <https://handle.itu.int/11.1002/1000/14454-en>
- Lim, L.-H., Ong, L.-Y., & Leow, M.-C. (2025). Federated Learning for anomaly Detection: A Systematic Review on Scalability, Adaptability, and Benchmarking Framework. *Future Internet*, 17(8), 375. Disponible en: <https://doi.org/10.3390/fi17080375>
- Makris, I., Karampasi, A., Radoglou-Grammatikis, P., Episkopos, N., Iturbe, E., Rios, E., Piperigkos, N., Lalos, A., Xenakis, C., Lagkas, T., Argyriou, V., & Sarigiannidis, P. (2024). A Comprehensive Survey of Federated Intrusion Detection Systems: Techniques, challenges and solutions. <https://doi.org/10.1016/j.cosrev.2024.100717>
- Mirsky, Y., Doitshman, T., Elovici, Y., & Shabtai, A. (2018). Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection. En *Network and Distributed System Security Symposium (NDSS 2018)*. Disponible en: <https://doi.org/10.14722/ndss.2018.23204>
- Pramitarini, Y., Perdana, R. H. Y., Shim, K., & An, B. (2023). DLSMR: Deep Learning-based Secure Multicast Routing Protocol against Wormhole Attack in Flying *ad hoc* Networks with Cell-free Massive Multiple-input Multiple-output. *Sensors*, 23, 7960. Disponible en: <https://doi.org/10.3390/s23187960>

- Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture (NIST Special Publication 800-207). National Institute of Standards and Technology. Disponible en: <https://doi.org/10.6028/NIST.SP.800-207>
- Tam, P., Ros, S., Song, I., Kang, S., & Kim, S. (2024). A Survey of Intelligent End-to-end Networking Solutions: Integrating Graph Neural Networks and Deep Reinforcement Learning Approaches. *Electronics*, 13(5), 994. Disponible en: <https://doi.org/10.3390/electronics13050994>
- Wijnands, I. J., Rosen, E., Dolganow, A., Przygienda, T., & Aldrin, S. (2017). Multicast using Bit Index Explicit Replication (BIER) (RFC 8279). Internet Engineering Task Force. <https://www.rfc-editor.org/info/rfc8279>
- Yang, H. (2025). A Study on Zone-based Secure Multicast Protocol Technique to improve Security Performance and Stability in Mobile *ad hoc* Network. *Applied Sciences*, 15(2), 568. Disponible en: <https://doi.org/10.3390/app15020568>
- Ye, M., Hu, H., Wang, X., Wang, Y., Peng, W., & Zheng, J. (2024). MA-CDMR: An Intelligent Cross-domain Multicast Routing Method Based on Multiagent Deep Reinforcement Learning in Multi-domain SDWN [Manuscrito no publicado / preprint arXiv:2409.05888]. <https://arxiv.org/abs/2409.05888>
- Zhao, C., Ye, M., Xue, X., Lv, J., Jiang, Q., & Wang, Y. (2022). DRL-M4MR: An Intelligent Multicast Routing Approach Based on DQN Deep Reinforcement Learning in SDN. *Physical Communication*, 55, 101919. Disponible en: <https://doi.org/10.1016/j.phycom.2022.101919>



This is an open access article distributed under the terms of the CC BY-NC license (<https://creativecommons.org/licenses/by-nc/4.0/>)

Capítulo 5

Aplicación de herramientas de inteligencia artificial para facilitar el cumplimiento de ISO/IEC 27001

Héctor Andrés Alcalá-Gutiérrez¹

Resumen

En 2025 se investigó cómo las herramientas basadas en inteligencia artificial facilitaron el cumplimiento de los requisitos de ISO/IEC 27001:2022. Se realizó una revisión documental de la norma, reportes industriales, documentación técnica de proveedores y literatura académica, y se construyó una tabla de mapeo entre requisitos seleccionados y soluciones de inteligencia artificial. Estas soluciones redujeron tareas manuales, mejoraron la priorización y aceleraron la generación de evidencias para auditoría. Se concluyó que la inteligencia artificial aportó eficiencia y trazabilidad al sistema de gestión, pero su adopción exigió gobernanza fuerte y validación humana; se recomendó realizar estudios piloto y evaluar empíricamente las soluciones antes de su despliegue masivo.

Palabras clave: inteligencia artificial, ISO/IEC 27001, ISMS, seguridad de la información, automatización

1. Universidad de Guadalajara, Guadalajara, Jalisco, México. email: hector.alcala2936@alumnos.udg.mx. ORCID: 0009-0007-2282-4181

1. Introducción

El informe internacional sobre el costo de las brechas de datos señaló que el costo promedio global en 2024 fue de 4.88 millones de dólares norteamericanos, un incremento cercano al 10% respecto del año anterior, lo que evidencia la presión económica y operativa sobre equipos de seguridad y auditoría (International Business Machines Corporation, 2024). Al mismo tiempo, las investigaciones de incidentes muestran que vectores como el error humano, el *phishing* y la explotación de vulnerabilidades siguen siendo causas frecuentes de incidentes, lo que refuerza la necesidad de controles preventivos, detectivos y correctivos más eficaces (Verizon, 2024). ISO/IEC se mantiene como el referente mundial para la implementación de sistemas de gestión de seguridad de la información (ISMS). En el año 2022 se publicó una versión actualizada donde se mejoró la lista de controles, y se reforzó la gestión de la seguridad basada en riesgos aplicables (International Organization for Standardization, 2022). Anualmente se realiza un análisis del alcance de las normas ISO; esta actividad se encomendó al International Accreditation Forum. Hasta 2024 se registró que existen cerca de cien mil certificados de ISO/IEC 27001, lo que indica una aceptación importante de esta norma a escala internacional (International Accreditation Forum, 2025).

En la actualidad se percibe una mayor presión relacionada con la seguridad de la información, y se exige más y mejores controles para garantizarla, aquí es donde la inteligencia artificial es una opción para facilitar la automatización de tareas, así como para mantener evidencias requeridas en las auditorías de certificación. Sin embargo, la literatura técnica y las guías recientes muestran que, aunque existe progreso en aplicaciones puntuales (detección basada en aprendizaje automático, priorización predictiva de vulnerabilidades, clasificación automática de datos y automatización de evidencias), son escasos los estudios que integren de forma sistemática estas capacidades con los procesos y requisitos formales de ISO/IEC 27001.

El objetivo de este ensayo es, por tanto, analizar y proponer un mapeo práctico entre requisitos de ISO/IEC 27001:2022 y categorías de herramientas basadas en inteligencia artificial que pueden automatizar, mejorar y evidenciar el cumplimiento, además de evaluar los riesgos

que introducen estas tecnologías. La pregunta que guía el trabajo es: ¿qué herramientas de inteligencia artificial son aplicables a requisitos clave de ISO/IEC 27001?

2. Desarrollo

En esta sección se examina el contexto que motivó la investigación y la problematización del tema, se presentan los antecedentes del estado de la cuestión a distintas escalas (mundial, internacional y nacional), se describe el estado del arte académico sobre el uso de inteligencia artificial en actividades de aseguramiento y cumplimiento, y se introduce de forma sintética el modelo base propuesto que articulará capacidades tecnológicas.

2.1. Contexto y problematización

En 2024 se registró un aumento tanto en la frecuencia como en el impacto económico de los incidentes de seguridad de la información, lo que obligó a las organizaciones a revisar sus prácticas de gestión y control (IBM, 2024). De forma consistente, los informes sobre investigaciones de brechas señalaron que factores humanos y la explotación rápida de vulnerabilidades fueron vectores recurrentes de compromiso (Verizon, 2024; European Union Agency for Cybersecurity, 2024).

Paralelamente, incrementó la cantidad de activos a gestionar y la velocidad con que nuevas vulnerabilidades se publicaron y pudieron ser explotadas, lo que dificultó mantener inventarios precisos y controles actualizados (ENISA, 2024; Edgescan, 2024).

En este escenario, también se intensificaron las exigencias para documentar controles y evidencias ante auditorías. Las organizaciones enfrentaron problemas operativos concretos de procesos manuales y costosos para recolectar evidencia para los registros de auditoría (ISO, 2022).

Además, se observó una creciente presión normativa y de cumplimiento. Por ejemplo, en el ámbito mexicano, durante marzo de 2025 se publicó una nueva ley de protección de datos personales que

modificó responsabilidades y mecanismos de supervisión (Cámara de Diputados del H. Congreso de la Unión, 2025).

2.2. Antecedentes del estado de la cuestión

Los antecedentes se organizarán en tres niveles complementarios: primero, la perspectiva mundial, que recogerá la evolución de la adopción de marcos de gestión de seguridad y la evidencia sobre el impacto económico y técnico de las brechas de información; en segundo lugar, la perspectiva internacional y regional, que condensará marcos, guías y desarrollos tecnológicos de referencia; en tercer lugar, el contexto de México, donde se expondrán las modificaciones regulatorias recientes. Esta estructura permitirá situar el problema en su dimensión global y normativa, así como identificar las circunstancias locales que condicionan la adopción de tecnologías basadas en inteligencia artificial.

2.2.1. MUNDIAL

A escala mundial se observó una mayor conciencia y la adopción de sistemas de gestión de la seguridad de la información basados en la norma internacional ISO/IEC 27001 durante los últimos años. La encuesta anual sobre adopción de normas registró 96,709 certificados para la familia de esta norma, lo que evidenció una demanda sostenida de marcos formales de gestión de seguridad en empresas y organizaciones públicas (IAF, 2025). Al mismo tiempo, informes de la industria documentaron que el impacto económico de las brechas de datos se incrementó notablemente en 2023-2024: el coste promedio mundial fue registrado en 4.88 millones de dólar norteamericanos, con un aumento cercano al 10% respecto del periodo anterior; el estudio también documentó la escasez de personal de seguridad y la presión sobre equipos operativos para responder y recuperar la continuidad del negocio, lo que puso en evidencia la presión financiera sobre las organizaciones para mejorar la prevención y la respuesta (IBM, 2024).

Los informes sobre investigaciones de incidentes mostraron además que patrones persistentes —como la ingeniería social, los errores de configuración y la explotación rápida de vulnerabilidades— seguían

siendo vectores predominantes de compromiso, y que la mayor sofisticación del adversario obligó a revisar controles técnicos y operativos tradicionales, lo que aumentó la carga de trabajo de los equipos de seguridad y auditoría (Verizon, 2024; ENISA, 2024).

Sumado a lo anterior, los vectores de ataque y la complejidad de la tecnología han aumentado (entornos híbridos on-premise/nube, integración y entregas continuas, infinidad de dispositivos conectados y trabajo remoto). Esto ha incrementado significativamente la cantidad de activos a controlar; además, ha aumentado la velocidad de explotación de nuevas vulnerabilidades, lo que ha dificultado la labor de mantener inventarios de activos precisos y debidamente protegidos (ENISA, 2024; Edgescan, 2024). Algunos informes especializados han confirmado que el volumen de vulnerabilidades registradas ha incrementado significativamente en el periodo 2023-2024, lo que ha complicado mantener al día la aplicación de parches y ha incrementado el *backlog* de vulnerabilidades pendientes de mitigación (Edgescan, 2024).

El siguiente antecedente es evidente: las organizaciones necesitan acceso a mecanismos que les permitan contar con controles actualizados, en un contexto donde la superficie de ataque ha crecido debido al aumento de la complejidad tecnológica.

2.2.2. INTERNACIONAL

Tanto internacional como regionalmente se han dado múltiples iniciativas para reforzar la gobernanza y la gestión de riesgos tecnológicos.

Por ejemplo, los marcos de gestión de riesgos y ciberseguridad elaborados por instituciones de referencia —como los documentos de la Agencia Europea para la Ciberseguridad y los marcos de gestión de riesgo del Instituto Nacional de Estándares de Estados Unidos— marcaron pautas sobre priorización de controles, evaluación continua y mitigación de amenazas emergentes (ENISA, 2024; National Institute of Standards and Technology, 2023).

Adicionalmente, regulaciones y marcos de protección de datos, como el Reglamento Europeo de Protección de Datos, incentivaron prácticas de clasificación y tratamiento de información personal que también se reflejaron en los requisitos de los sistemas de gestión de seguridad de la información (Parlamento Europeo, 2016).

La versión 2022 de la norma internacional ISO/IEC 27001, que rige los sistemas de gestión de seguridad de la información, reorganizó y actualizó su catálogo de controles, con énfasis en la gestión basada en riesgos y la documentación como base para la acreditación (ISO, 2022). Las organizaciones, sin embargo, enfrentaron problemas operativos concretos: inventarios incompletos o desactualizados que impedían relacionar activos con controles, evaluaciones de riesgo cuantitativas inconsistentes que dificultaban priorizar tratamientos, grandes volúmenes de alertas que generaban fatiga en los analistas y retrasos en la respuesta, y procesos manuales y costosos para recolectar evidencia que respaldara la declaración de aplicabilidad y los registros de auditoría.

2.2.3. MÉXICO

En el contexto nacional mexicano se produjeron cambios regulatorios relevantes durante 2024-2025 que afectaron la gestión de información sensible. En marzo de 2025 se publicó un nuevo marco legal de protección de datos que reemplazó o actualizó partes de la normativa anterior, elevando requisitos de consentimiento, transparencia y obligaciones de los responsables del tratamiento, así como introduciendo nuevos mecanismos de supervisión y sanción (Cámara de Diputados del H. Congreso de la Unión, 2025).

Estas modificaciones regulatorias tuvieron implicaciones prácticas: obligaron a revisar políticas de clasificación de datos, acuerdos contractuales con proveedores (incluidos proveedores de servicios en la nube y de plataformas basadas en inteligencia artificial) y la documentación exigida por auditorías. Además, en el país se observó un interés creciente por certificaciones de seguridad por parte de sectores regulados (por ejemplo, financiero y salud), lo que generó demanda de soluciones que facilitaran la obtención y mantenimiento de evidencia de conformidad frente a auditorías internas y externas.

2.3. Descripción del estado del arte

En materia tecnológica, la literatura académica y técnica documentó avances en el uso de técnicas de aprendizaje automático y algoritmos

de análisis para la detección de intrusiones, la priorización de vulnerabilidades y la clasificación automática de datos, aunque también advirtió lagunas importantes en gobernanza de modelos, explicabilidad y validación empírica de soluciones en entornos reales (Salem, Azzam, Emam, & Abohany, 2024).

En materia de cumplimiento de normas y marcos regulatorios, algunos estudios exploraron cómo la inteligencia artificial podía ayudar en los procesos de auditoría —para la recolección y el análisis automatizado de evidencias y supervisión continua— pero señalaron falta de validación empírica, así como de gobernanza de modelos (Shao-Fang, Ankur, & Basel, 2024; Lampis, 2024).

Otro estudio analizó el uso de técnicas de procesamiento de lenguaje como apoyo a actividades de gobernanza y documentación —para la generación de perfiles de aseguramiento, generación de documentación técnica y mapeo entre requisitos normativos y evidencias técnicas. Esta investigación mostró que se podía hacer eficiente la generación de informes y la trazabilidad entre requisitos y registros, pero también concluyeron que es necesaria la supervisión humana para identificar errores en salidas automatizadas (Yamin, Shao-Fang, & Basel, 2025).

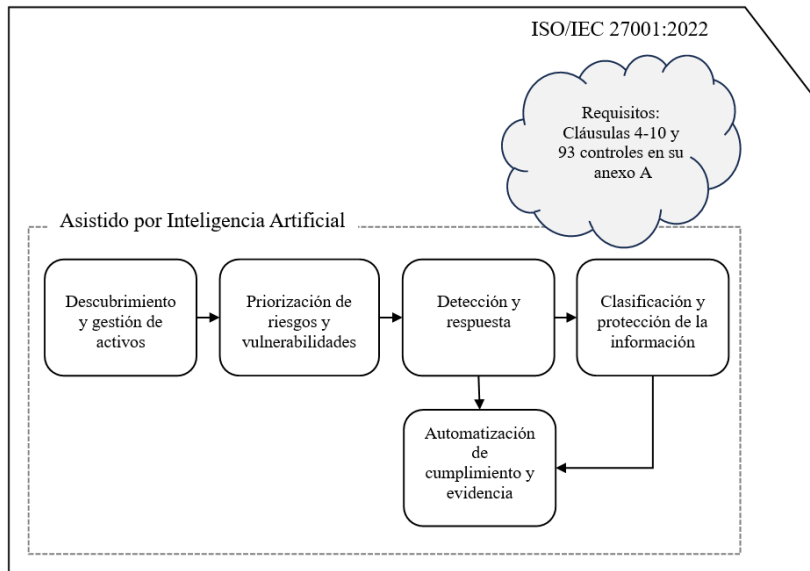
Asimismo, se ha documentado el interés y la demanda de la industria por soluciones que integren inteligencia artificial en funciones de cumplimiento para automatizar controles, monitorizar desviaciones en tiempo real y reducir la carga manual de evidencias. Más allá de la novedad tecnológica, la principal demanda de la industria se centró en soluciones que entregaran trazabilidad, explicabilidad y capacidad de integración con procesos de auditoría existentes (Association for Financial Markets in Europe, 2023).

En resumen, el estado del arte ha mostrado dos mensajes complementarios: en primer lugar, las investigaciones demuestran la factibilidad de aplicar inteligencia artificial a tareas de aseguramiento, mapeo de requisitos y automatización de evidencias; en segundo lugar, dichas investigaciones han reconocido limitaciones importantes —necesidad de validación en entornos reales, problemas de explicabilidad y riesgos adversariales. Esta evidencia académica corroboró además la demanda del sector industrial por soluciones que combinen automatización con garantías de auditabilidad, lo que justifica y contextualiza el enfoque del presente ensayo en analizar herramientas existentes y proponer un mapeo operativo para el cumplimiento de la norma internacional.

2.4. Modelo base propuesto

A continuación se presenta un diagrama del modelo base propuesto que muestra, de forma esquemática, las capas funcionales que articularán las capacidades tecnológicas y los requerimientos de gobernanza: una capa de descubrimiento y gestión de activos que alimentará el registro de activos, una capa de priorización de riesgos y vulnerabilidades que generará la planificación de tratamiento, una capa de detección y respuesta que proveerá registros operativos y acciones de mitigación, una capa de clasificación y protección de la información que mantendrá metadatos de sensibilidad, y una capa de automatización de cumplimiento y evidencia que consolidará registros exportables para auditoría.

Figura 1. Arquitectura general del modelo base propuesto para la evaluación de cumplimiento de requisitos de ISO/IEC 27001 que pueden ser asistidos por inteligencia artificial.



Fuente: Elaboración propia.

3. Metodología

La presente investigación siguió un enfoque meramente documental y exploratorio, buscando desarrollar un mapeo entre requisitos de la norma internacional ISO/IEC 27001 y herramientas basadas en inteligencia artificial. En lugar de un trabajo de investigación práctica en campo, se recurrió a consultar fuentes formales para identificar herramientas existentes representativas.

Ante todo, se consultó la norma oficial vigente (ISO, 2022), donde se definen los requisitos para un sistema de gestión de seguridad de la información, con el objetivo de identificar aquellos que podrían ser asistidos por IA —la norma ISO 27001 consta dos tipos de requisitos principales: las cláusulas obligatorias del 4 al 10, además 93 controles de seguridad en el anexo A.

Posteriormente, se revisaron informes recientes de brechas de seguridad para determinar su impacto, y de esta forma poner en contexto la necesidad de reforzar y automatizar los controles. Se consideraron informes de organizaciones de renombre en el ámbito de tecnología y seguridad de la información (ENISA, 2024; IBM, 2024; Verizon, 2024).

En tercer lugar, se realizó una revisión focalizada de la documentación técnica y en páginas oficiales de proveedores relevantes —incluyendo descripciones funcionales, *white papers* y secciones de producto—, con el objetivo de identificar categorías de herramientas que ofrecieran capacidades técnicas alineadas con requisitos concretos de la norma (Tenable, 2025; Qualys, 2025; CrowdStrike, 2025; Microsoft, 2025; Drata, 2025).

Con la evidencia recabada se procedió a sintetizar la información mediante un análisis comparativo: para requisitos de la norma se identificó el problema operativo típico que dificulta el cumplimiento, se asignó la categoría de herramienta basada en inteligencia artificial que mejor atendía ese problema, y se ilustraron ejemplos comerciales concretos (se analizaron una cláusula y nueve controles que podían ser asistidos por herramientas con IA integrada). El producto directo de este proceso fue la elaboración de la tabla principal de mapeo (tabla 1).

Finalmente, se documentaron de forma explícita las limitaciones metodológicas: la investigación fue de carácter documental y

no incluyó validación empírica en entornos productivos ni pruebas de campo con herramientas; por tanto, las recomendaciones y los mapeos deben interpretarse como un marco operativo fundamentado en la literatura y la documentación técnica, que requiere verificación mediante pruebas piloto y evaluaciones prácticas para cada contexto organizacional.

4. Discusión

La discusión articula un análisis crítico sobre cuatro ejes principales: la relación entre eficacia operativa y riesgos técnicos u organizacionales, los desafíos de explicabilidad y auditabilidad que las salidas automatizadas plantean frente a procesos de certificación, las condiciones de integración tecnológica y los criterios para evaluar el retorno de la inversión real considerando costes de gobernanza, y el contexto regulatorio y la demanda industrial que impulsan la adopción de estas soluciones.

4.1. Eficacia versus riesgo

Varios autores documentaron que las técnicas de inteligencia artificial pueden incrementar significativamente la eficacia operativa en tareas de cumplimiento y seguridad —como mejoras medibles en velocidad de detección, reducción del volumen de trabajo manual y focalización de esfuerzos cuando se integraron modelos predictivos en procesos de priorización y monitorización (Shao-Fang, Ankur, & Basel, 2024). Aun así, dichos estudios también advierten de sesgos o fallas potenciales en los modelos, debido a que estos aprenden de datos históricos que no necesariamente cubren todas las situaciones posibles, por lo que existe el riesgo de que dichos modelos tomen decisiones erróneas, sobre todo si no hay supervisión humana (Olabintan, 2024). En suma, los investigadores concluyeron que la eficacia operacional de la inteligencia artificial es real, pero su valor para cumplimiento depende de controles adicionales: validación continua, supervisión humana y métricas de desempeño que permitan detectar degradación del modelo en producción.

4.2. Explicabilidad y auditabilidad

La comunidad académica enfatizó de manera consistente la importancia de la explicabilidad para aceptar resultados automatizados como evidencia de cumplimiento. Revisiones sistemáticas sobre explicabilidad en seguridad mostraron que las técnicas de explicabilidad mejoran la confianza del analista y facilitan la interpretación de alertas y priorizaciones; no obstante, también subrayaron que algunas técnicas de explicabilidad pueden ser incompletas o vulnerables, y que la explicación por sí sola no reemplaza a la trazabilidad documental requerida por auditorías formales (Mohale & Obagbuwa, 2025; Sharma, Rani, & Shabaz, 2025). Investigadores propusieron que la explicabilidad técnica sea complementada por prácticas de registro y gobernanza que permitan reconstruir el proceso de decisión.

4.3. Integración tecnológica y retorno de la inversión

Trabajos que examinaron casos aplicados en entornos financieros e industriales indicaron que el retorno económico de soluciones basadas en inteligencia artificial para seguridad y cumplimiento puede ser alto, sobre todo cuando se mide en reducción de horas hombre, disminución del *backlog* de vulnerabilidades y menor tiempo medio de recuperación ante incidentes (Charles, 2024). No obstante, también se señala que calcular el retorno real exige incorporar costes de integración, gobernanza y pruebas continuas; sin ello, las estimaciones de beneficio estarán sesgadas a favor de escenarios idealizados. En síntesis, la literatura muestra que la integración tecnológica puede producir retornos sólidos, pero que el diseño de métricas y la inclusión de costes de gobernanza son condiciones necesarias para una evaluación realista.

4.4. Contexto regulatorio y demanda industrial

Investigadores e informes sectoriales documentaron una demanda creciente de la industria por soluciones que integren inteligencia artificial en procesos de cumplimiento, particularmente en sectores altamente

regulados como finanzas y salud. Se buscan soluciones que no solo automaticen tareas, sino también garanticen trazabilidad, transparencia y capacidad de integración con auditorías existentes (AFME, 2023). Al mismo tiempo, la literatura académica insistió en que la evolución regulatoria, incluidas las guías recientes sobre gestión del riesgo de inteligencia artificial y las publicaciones sobre aprendizaje adversarial, obliga a incorporar marcos de gobernanza y pruebas de robustez al diseñar soluciones para cumplimiento (NIST, 2023; NIST, 2025).

5. Resultados finales

A continuación se presentan los resultados finales derivados del análisis comparativo realizado: la tabla de mapeo que relaciona, para requisitos seleccionados de la norma internacional, el problema operativo que dificulta su cumplimiento, la categoría de herramienta basada en inteligencia artificial que puede atender dicho problema, y ejemplos comerciales representativos. La tabla que se expone a continuación (tabla 1) constituye el producto central y la evidencia técnica resultante del trabajo documental y del análisis realizado en este ensayo.

Tabla 1. Mapeo entre requisitos seleccionados de ISO/IEC 27001 y soluciones comerciales de IA

Requisito ISO/IEC 27001	Problema operativo	Categoría de herramienta basada en IA	Ejemplos de soluciones comerciales
Inventario de información y otros activos asociados (control 5.9)	Inventario incompleto o desactualizado que impide relacionar controles con activos	Descubrimiento: descubrimiento continuo y clasificación automática de activos mediante aprendizaje automático y correlación de telemetría	Qualys VMDR; Tenable (descubrimiento y priorización); Rapid7 InsightVM.
Acciones para abordar riesgos y oportunidades (cláusula 6.1)	Valoraciones cualitativas inconsistentes que dificultan priorizar tratamientos	Priorización: cuantificación de riesgo económica y analítica probabilística (modelo FAIR, simulaciones probabilísticas)	RiskLens (plataforma FAIR).
Gestión de vulnerabilidades técnicas (control 8.8)	Acumulado de vulnerabilidades pendientes y falta de priorización contextual	Priorización: priorización predictiva de vulnerabilidades que integra telemetría, explotabilidad e impacto de negocio	Tenable Vulnerability Priority Rating; Qualys VMDR; Rapid7 InsightVM
Respuesta a incidentes de seguridad de la información (control 5.26)	Ruido de alertas, fatiga de analistas y detección tardía	Detección y respuesta: detección basada en comportamiento y orquestación de respuesta automatizada	CrowdStrike Falcon; SentinelOne Singularity; Darktrace

Control de acceso y gestión de identidad (controles 5.15 y 5.16)	Detección tardía de cuentas comprometidas y escalada de privilegios	Detección y respuesta: Análisis de riesgo de autenticación en tiempo real y políticas de acceso adaptativo	Microsoft Entra ID Protection; Okta Threat Insight
Seguimiento, revisión y gestión de cambios de servicios de proveedores (control 5.22)	Evaluaciones puntuales y falta de monitoreo continuo de terceros	Detección y respuesta: Monitoreo continuo de postura de terceros y análisis de inteligencia externa	BitSight (calificaciones continuas); Recorded Future (inteligencia de terceros)
Concientización, educación y capacitación en seguridad de la información (control 6.3)	Programas genéricos con baja personalización y falta de métricas	Detección y respuesta: Programas de formación adaptativa y simulaciones de ingeniería social basadas en inteligencia artificial	KnowBe4; Cofense
Clasificación de la información (control 5.12)	Clasificación manual costosa y errores en la identificación de datos sensibles	Clasificación y protección: clasificadores entrenables y prevención de pérdida de datos con aprendizaje automático	Microsoft Purview (clasificadores entrenables); Google Cloud Data Loss Prevention
Recolección de evidencia (control 5.28)	Recolección manual de evidencias y procesos de auditoría lentos	Automatización y cumplimiento: plataformas de automatización de cumplimiento con pruebas continuas y conectores	Drata; Secureframe

Fuente: Elaboración propia.

5.1. Aportaciones teóricas y prácticas

La pregunta planteada exigía identificar qué categorías de herramientas de inteligencia artificial son aplicables a requisitos clave de la norma internacional ISO/IEC 27001, cuáles son sus beneficios operativos y qué controles de gobernanza se requieren para mantener la validez y la auditabilidad del sistema de gestión de seguridad de la información.

La respuesta es afirmativa con reservas: la inteligencia artificial puede ser usada y, desde luego, claramente beneficia la operación regular de un ISMS (reduciendo tareas manuales, analizando y priorizando asuntos según el contexto, detectando de forma oportuna los eventos e incidentes de seguridad, recolectando evidencias requeridas en auditorías), pero deben darse las condiciones necesarias —de gobernanza, explicabilidad y trazabilidad— para que las evidencias sean válidas en procesos de auditorías de certificación (ISO, 2022; Drata, 2025).

La principal aportación teórica de esta investigación es una propuesta de modelo conceptual que organiza la capacidad tecnológica en capas.

Dicho modelo se resume a continuación:

1. *Capa de descubrimiento y gestión de activos:* Detecta los recursos tecnológicos existentes, tanto on-premise como en la nube, normaliza los identificadores de dichos recursos y mantiene el inventario de activos. Esta capa genera la evidencia inicial necesaria para relacionar controles con activos (Qualys, 2025; Tenable, 2025; Rapid7, 2025).
2. *Capa de priorización de riesgos y vulnerabilidades:* Toma telemetría de activos y resultados de escaneo, aplica modelos de priorización contextualizados por impacto de negocio y produce un plan de prioridades de tratamiento. Sus salidas alimentan el plan de tratamiento de riesgos y la declaración de aplicabilidad (Tenable, 2025; RiskLens, 2025; Qualys, 2025; Rapid7, 2025).
3. *Capa de detección y respuesta:* Emplea aprendizaje para detectar anomalías comportamentales y orquestación para ejecutar acciones de respuesta automáticas o semiautomáticas, siempre registrando la cadena de decisión y la intervención humana cuando procede. Proporciona los registros operativos que sustentan evidencias de respuesta a incidentes (CrowdStrike, 2025; SentinelOne, 2025; Darktrace, 2025; Bitsight, 2025; KnowBe4, 2025; Cofense, 2025; Recorded Future, 2025; Okta, 2025; Microsoft, 2025).

4. *Capa de clasificación y protección de la información:* Automatiza el etiquetado de datos sensibles y aplica controles de prevención de pérdida; mantiene metadatos sobre sensibilidad que sirven para políticas de acceso y para evidenciar cumplimiento de la clasificación exigida por la norma (Microsoft, 2025; Google, 2025).
5. *Capa de automatización de cumplimiento y evidencia:* Centraliza y armoniza evidencias (*logs*, informes, estado de controles), mantiene *trails* exportables y paneles de control que facilitan revisiones internas y auditorías externas. Esta capa actúa como puente entre los sistemas técnicos y la documentación formal del sistema de gestión (Drata, 2025; SecureFrame, 2025).

Finalmente, el modelo base enfatiza el principio de intervención humana supervisora en decisiones críticas: la inteligencia artificial debe apoyar la toma de decisiones y automatizar tareas repetitivas, pero la responsabilidad última y la aprobación de cambios significativos y excepciones deben quedar en manos de responsables asignados en el sistema de gestión.

Desde el punto de vista profesional, como aportación práctica, este trabajo entregó una tabla de mapeo operativo (resultado central del ensayo) que organizaciones y auditores pueden usar como guía preliminar para seleccionar tecnologías y documentar evidencia para procesos de certificación.

6. Conclusión

El ensayo propuso y articuló un marco conceptual que vinculó explícitamente requisitos de la norma internacional ISO/IEC 27001 con categorías operativas de herramientas basadas en inteligencia artificial, lo que permitió pasar de afirmaciones generales sobre “IA en ciberseguridad” a un mapeo normativo accionable.

La investigación responde afirmativamente a la pregunta central: las herramientas basadas en inteligencia artificial son aplicables y útiles para apoyar el cumplimiento de requisitos seleccionados de la norma internacional ISO/IEC 27001, siempre que su adopción vaya acompañada de medidas de gobernanza, trazabilidad y validación humana. Las capacidades tecnológicas que incluyen descubrimiento automático de activos,

priorización contextual de riesgos y vulnerabilidades, detección basada en comportamiento, clasificación automática de información y automatización de la recolección de evidencias demuestran aportes operativos claros: reducción de trabajo manual, priorización de esfuerzos técnicos y generación de registros que facilitan la revisión por la dirección y la auditoría.

En este modelo base, dos principios son innegociables para que la evidencia generada por inteligencia artificial sea admisible y útil en procesos de certificación: trazabilidad (*logs* con marcas de tiempo, versión de modelo y registro de validación humana) y exportabilidad (capacidad de generar evidencias en formatos verificables y legibles por auditoría). Sin estas propiedades, las evidencias automatizadas corren el riesgo de ser rechazadas como prueba suficiente para algunos requisitos de la norma, como lo son la declaración de aplicabilidad y las revisiones por la dirección.

Esta investigación tiene limitaciones claras: es un estudio documental y comparativo, no se ejecutó una validación de las soluciones de IA en ambientes productivos. En consecuencia, debe entenderse que este es solo un marco de referencia, no sustituye la validación de las dichas soluciones en contextos concretos. Se recomienda que las organizaciones que consideren implementar estas tecnologías de IA se aseguren de ejecutar ensayos piloto controlados para confirmar que las herramientas, los modelos y los proveedores son idóneos para su operación.

En resumen, la inteligencia artificial, cuando se usa adecuadamente, incrementa la eficiencia y la eficacia de un ISMS, pero, para que realmente aporte valor, es necesaria una gobernanza firme que asegure que se preserven trazabilidad, explicabilidad, responsabilidad y auditabilidad, así como la protección de datos en todas las etapas del ciclo de vida de los modelos de IA.

Referencias

- Association for Financial Markets in Europe (AFME) (septiembre de 2023). *Artificial Intelligence: Challenges and Opportunities for Compliance*. www.afme.eu/media/d5gm0fsu/finalafmeaicompliance202305.pdf. Consultado: 2025/10/20.
- Bitsight (2025). *Security Ratings for Third-party Risk –documentación de producto*. www.bitsight.com. Consultado: 2025/11/10.

- Cámara de Diputados del H. Congreso de la Unión (marzo de 2025). *Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Nueva LFPDPPP)*. www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf. Consultado: 2025/10/20.
- Charles, J. (marzo de 2024). *Evaluating ROI in AI Security Implementations: Balancing Cost with Long-Term Security Benefits*. Disponible en: www.researchgate.net/publication/385747332, Consultado: 2025/11/02.
- Cofense (2025). *Phishing Detection and Employee Training –documentación de producto*. www.cofense.com. Consultado: 2025/11/10.
- CrowdStrike (2025). *CrowdStrike Falcon –documentación de producto*. Disponible en: www.crowdstrike.com. Consultado: 2025/11/10.
- Darktrace (2025). *Self-Learning AI for anomaly Detection – documentación de producto*. Disponible en: www.darktrace.com/products/network. Consultado: 2025/11/10.
- Drata (2025). *Automate ISO 27001 Compliance –documentación de producto*. Disponible en: www.drata.com/grc-central/automate-iso-27001-compliance. Consultado: 2025/11/10.
- Edgescan (2024). *2024 Vulnerability Statistics Report*. Disponible en: www.edgescan.com/wp-content/uploads/2025/04/2024-Vulnerability-Statistics-Report.pdf. Consultado: 2025/10/20.
- European Union Agency for Cybersecurity (ENISA) (septiembre de 2024). *ENISA Threat Landscape 2024*. www.enisa.europa.eu/publications/enisa-threat-landscape-2024. Consultado: 2025/10/20.
- European Union Agency for Cybersecurity (ENISA) (diciembre de 2024). *2024 Report on the State of Cybersecurity in the Union*. Disponible en: www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union. Consultado: 2025/10/20.
- Google (2025). *Cloud Data Loss Prevention –documentación de producto*. www.cloud.google.com/dlp. Consultado: 2025/11/10 de
- International Accreditation Forum (IAF) (septiembre de 2025). *The ISO Survey of Management System Standard Certifications 2024*. Disponible en: www.iafcertsearch.org/services/iso-survey. Consultado: 2025/10/20.
- International Business Machines Corporation (IBM) (2024). *Cost of a Data Breach 2024*. Disponible en: www.ibm.com/think/insights/cost-of-a-data-breach-2024-financial-industry. Consultado: 2025/10/20.
- International Organization for Standardization (ISO) (octubre de 2022). *ISO/IEC 27001:2022 -Information Security Management Systems-Requirements*. Disponible en: www.iso.org/standard/27001. Consultado: 2025/10/15.
- KnowBe4 (2025). *Security Awareness Training and Simulated Phishing –documentación de producto*. Disponible en: www.knowbe4.com. Consultado: 2025/11/10.

- Lampis, A. (2024). *Automated Cybersecurity Compliance and Threat Response using AI, Blockchain & Smart Contracts*. International Journal of Information Technology. Disponible en: www.link.springer.com/article/10.1007/s41870-024-02324-9. Consultado: 2025/11/02.
- Microsoft (2025a). *Administración de identidades y acceso –documentación de producto*. Disponible en: www.microsoft.com/es-mx/security/business/identity-access/microsoft-entra-id. Consultado: 2025/11/10.
- (2025b). *Microsoft Purview –documentación de producto*. Disponible en: www.learn.microsoft.com/en-us/purview/trainable-classifiers-get-started-with Consultado: 2025/11/10.
- Mohale, V. Z., & Obagbuwa, I. C. (2025). *A Systematic Review on the Integration of Explainable Artificial Intelligence in Intrusion Detection Systems to Enhancing Transparency Aand Interpretability in Cybersecurity*. Disponible en: www.doi.org/10.3389/frai.2025.1526221. Consultado: 2025/11/02.
- National Institute of Standards and Technology (NIST) (2025). *Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations*. Disponible en: www.csrc.nist.gov/pubs/ai/100/2/e2025/final. Consultado: 2025/10/20.
- National Institute of Standards and Technology (NIST). (Enero de 2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. Disponible en: www.nist.gov/itl/ai-risk-management-framework. Consultado: 2025/10/20 de
- Okta (2025). *Securing all Types of Identity from AI Agents to Customers, Employees, and Partners –documentación de producto*. Disponible en: www.okta.com/resources/whitepaper-getting-the-most-out-of-okta-threatinsight/. Consultado: 2025/11/10.
- Olabintan, A. H. (2024). *The Effect of Adversarial Machine Learning in Security and Privacy Analytics: A Review*. FUOYE Journal of Pure and Applied Sciences. Disponible en: www.researchgate.net/publication/383696148_The_Effect_of_Adversarial_Machine_Learning_in_Security_and_Privacy_Analytics_A_Review. Consultado: 2025/11/02.
- Parlamento Europeo (abril de 2016). *General Data Protection Regulation (GDPR)*. Disponible en: www.gdpr-info.eu Consultado: 2025/10/20de:
- Qualys (2025). *Vulnerability Management, Detection and Response (VMDR) –documentación de producto*. Disponible en: www.qualys.com/aplicaciones/vulnerability-management-detection-response/. Consultado: 2025/11/10.
- Rapid7 (2025). *InsightVM Vulnerability and risk prioritization –documentación de producto*. Disponible en: www.rapid7.com/products/insightvm/. Consultado: 2025/11/10.
- Recorded Future (2025). *Third-party Intelligence and Monitoring* Disponible en: *documentación de producto*. Disponible en: www.recordedfuture.com. Consultado: 2025/11/10.

- RiskLens (2025). *Cyber Risk Quantification –documentación de producto*. Disponible en: www.safe.security/cyber-risk-quantification/. Consultado: 2025/11/10.
- Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A. (2024). *Advancing Cybersecurity: A Comprehensive Review of AI-driven Methods*. Journal of Big Data 2024. Disponible en: www.journalofbigdata.springeropen.com/articles/10.1186/s40537-024-00957-y. Consultado: 2025/11/02.
- Sharma, A., Rani, S., & Shabaz, M. (2025). *A Comprehensive Review of Explainable AI in Cybersecurity: Decoding the Black Box*. Journal of Cybersecurity Research. www.sciencedirect.com/science/article/pii/S2405959525001584. Consultado: 2025/11/02.
- SecureFrame (2025). *Automated Compliance & Continuous Monitoring –documentación de producto*. Disponible en: www.secureframe.com. Consultado: 2025/11/10.
- SentinelOne (2025). *Behavioral AI –documentación de producto*. Disponible en: www.sentinelone.com/blog/behavioral-ai-an-unbounded-approach-to-protecting-the-enterprise/. Consultado: 2025/11/10.
- Shao-Fang, W., Ankur, S., & Basel, K. (2024). *Artificial Intelligence for System Security Assurance: A Systematic Literature Review*. International Journal of Information Security. Disponible en: www.doi.org/10.1007/s10207-024-00959-0. Consultado: 2025/11/02.
- Tenable (2025). *Vulnerability Priority Rating (VPR) –documentación de producto*. Disponible en: www.tenable.com/capabilities/vulnerability-priority-rating. Consultado: 2025/11/10.
- Verizon (2024). *2024 Data Breach Investigations Report*. Disponible en: www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf. Consultado: 2025/10/20.
- Yamin, M. M., Shao-Fang, W., & Basel, K. (2025). *AI-Assisted Assurance Profile Creation for System Security Assurance*. Computer Security. ESORICS 2024 International Workshops. Disponible en: www.link.springer.com/chapter/10.1007/978-3-031-82362-6_29. Consultado: 2025/11/02.



This is an open access article distributed under the terms of the CC BY-NC license (<https://creativecommons.org/licenses/by-nc/4.0/>)

INTELIGENCIA ARTIFICIAL Y SOSTENIBILIDAD DIGITAL
Infraestructura, Seguridad y Ciudadanía Inteligente

© 2026, Academia Mexicana de Investigación y Docencia en Innovación (AMIDI).

Distribución digital:

Academia Mexicana de Investigación y Docencia en Innovación (AMIDI)
Responsable del registro DOI, la gestión de metadatos y la publicación en
AMIDI.Biblioteca



Maquetación y diseño:

Talleres gráficos de Ediciones de la Noche
Madero #687, Zona Centro, Guadalajara, Jalisco. México.



Hecho y editado en México / made and edited in Mexico
Se terminó de editar en Enero de 2026.

Edición digital con posibilidad de impresión bajo demanda.
Las copias impresas se generan individualmente a solicitud del lector;
por lo tanto, no existe un tiraje fijo.

La acelerada e inusitada expansión de la inteligencia artificial está reconfigurando de manera profunda las bases energéticas, tecnológicas y sociales sobre las cuales operan las instituciones contemporáneas. Este proceso de transformación plantea desafíos significativos en términos de sostenibilidad, seguridad y gobernanza, al tiempo que abre oportunidades para el diseño de infraestructuras digitales más eficientes y orientadas al bienestar social. En este contexto, el eBook IA y sostenibilidad digital: infraestructura, seguridad y ciudadanía inteligente reúne cinco contribuciones que, desde enfoques complementarios, analizan cómo la transformación digital puede encaminarse hacia un desarrollo tecnológico responsable, seguro y centrado en las personas.

El volumen articula una visión integral en la que la innovación tecnológica dialoga con la responsabilidad social y la sostenibilidad a largo plazo, abordando problemáticas críticas asociadas al crecimiento exponencial de la infraestructura digital. El primer capítulo examina la creciente demanda energética de los centros de datos impulsada por modelos avanzados de inteligencia artificial, y propone un marco analítico para comprender la sostenibilidad operativa de infraestructuras críticas en escenarios de alta complejidad tecnológica.

El segundo capítulo profundiza en el papel de las arquitecturas hiperconvergentes como elemento clave para la construcción de ecosistemas de tecnologías de la información resilientes, capaces de integrar eficiencia energética, automatización de procesos y reducción de riesgos operativos. A continuación, el tercer capítulo vincula la inteligencia artificial con la acción ciudadana mediante el análisis de aplicaciones móviles orientadas a fomentar la conciencia ambiental, la participación social y la toma de decisiones informada en entornos urbanos.

El cuarto capítulo introduce un modelo de transmisión inteligente basado en MIA (Multicast Inteligente Adaptativo), diseñado para atender de manera simultánea los desafíos de seguridad, eficiencia energética y continuidad operativa en redes distribuidas. Finalmente, el quinto capítulo analiza el potencial de las herramientas de inteligencia artificial para fortalecer la gobernanza y el cumplimiento normativo, particularmente en sistemas de gestión alineados con la norma ISO/IEC 27001, mediante la mejora de la trazabilidad, la reducción de la carga operativa y el apoyo a la toma de decisiones estratégicas.

En conjunto, este libro invita a recorrer un ecosistema en el que la infraestructura digital, la seguridad de la información y la ciudadanía convergen para enfrentar los retos de un mundo profundamente interconectado. Más que una recopilación de estudios independientes, la obra constituye una propuesta colectiva que concibe la sostenibilidad digital como un compromiso ético, técnico y social indispensable para el futuro de la transformación digital.



AMIDI
Academia Mexicana
de Investigación y Docencia
en Innovación

ISBN 978-607-26875-9-2



9 786072 687592

Zapopan, Jal. a 15 de Diciembre de 2025

Dictamen de Obra. AMIDI.DO.20251215

Los miembros del equipo editorial de la Academia Mexicana de Investigación y Docencia en Innovación (**AMIDI**), **RENIECYT-SECIHTI 2200092**, ver:

<https://www.amidibiblioteca.amidi.mx/index.php/AB/about/editorialTeam>

se reunieron para atender la invitación a dictaminar el libro:

Inteligencia artificial y sostenibilidad digital. Infraestructura, seguridad y ciudadanía inteligente

Siendo los siguientes participantes de la misma:

Nombre completo	Rol
Juan Mejía Trejo	Coordinador editorial; Autor
Juan Mejía Mancilla	Autor
Hernán Rivera Melendrez	Autor
Fabrizio Francisco Hernández Gómez	Autor
José Isidro Cerda Silva	Autor
Héctor Andrés Alcalá-Gutiérrez	Autor

Dicho documento fue sometido al proceso de evaluación por pares doble ciego, de acuerdo a la política de la editorial, para su dictaminación de aceptación, ver:

<https://www.amidibiblioteca.amidi.mx/index.php/AB/procesodeevaluacionporparesen ciego>

Los miembros del equipo editorial se reúnen con el curador principal del repositorio digital para convocar:

1. Que el comité científico, de forma colegiada, revise los contenidos y proponga a los pares evaluadores que colaboran dentro del comité de redacción, tomando en cuenta su especialidad, pertinencia, argumentos, enfoque de los capítulos al tema central del libro, entre otros.
2. Se invita a los pares evaluadores a participar, formalizando su colaboración.
3. Se envía así, el formato de evaluación para inicio del proceso de evaluación doble ciego a los evaluadores elegidos de la mencionada obra.
4. El comité científico recibe las evaluaciones de los pares evaluadores e informa a el/los autor/(es) los resultados a fin de que se atiendan las observaciones, el requerimiento de reducción de similitudes, y recomendaciones de mejora a la obra.
5. La obra evaluada, consta de:

Contenido
Introducción
<i>Capítulo 1. IA y centros de datos: Crisis energética y sostenibilidad verde.</i>

Autores: Juan Mejía-Trejo. Juan Mejía-Mancilla.
<i>Capítulo 2. Tecnologías de información, inteligencia artificial y sostenibilidad en ecosistemas hiperconvergentes para el desarrollo futuro.</i> Autor: Hernán Rivera-Melendrez .
<i>Capítulo 3. Aplicaciones móviles inteligentes para la sostenibilidad: de la conciencia ambiental a la acción ciudadana mediada por IA.</i> Autor: Fabricio Francisco Hernández-Gómez.
<i>Capítulo 4. Multicast inteligente adaptativo: un modelo de transmisión seguro impulsado por aprendizaje automático.</i> Autor: José Isidro Cerda-Silva.
<i>Capítulo 5. Aplicación de herramientas de inteligencia artificial para facilitar el cumplimiento de ISO/IEC 27001.</i> Autor: Héctor Andrés Alcalá-Gutiérrez.

6. Una vez emitidas las observaciones, el requerimiento de reducción de similitudes, y recomendaciones de mejora a la obra por los evaluadores y todas ellas resueltas por el/los autor/(es), el resultado resalta que el contenido del libro:

- a. Reúne los elementos teóricos actualizados y prácticos desglosados en cada uno de sus capítulos.
- b. Los capítulos contenidos en la obra, muestran claridad en el dominio del tema, congruencia con el título central del libro, y una estructura consistente
- c. Se concluye finalmente, que la obra dictaminada, puede fungir como libro de texto principal o de apoyo tanto para estudiantes de licenciatura como de posgrados, así como público en general interesado.

7. De esta forma, el resultado del dictamen de aceptación de la obra fue:

FAVORABLE PARA SU PUBLICACIÓN

Sirva la presente para los fines que a los Interesados convengan.

Atentamente




Dr. Carlos Omar Aguilar-Navarro
Curador AMIDI.Biblioteca
AMIDI