

Internet de las cosas (IoT) y automatización inteligente en organizaciones modernas

The Internet of Things (IoT) and Smart Automation in Modern Organizations



Erazo-Luzuriaga, Alex Fernando¹

<https://orcid.org/0000-0002-1089-383X>



alex.erazo@esPOCH.edu.ec



Ecuador, Riobamba, Escuela Superior Politécnica De Chimborazo.



Herrera-Ramírez, César Daniel³

<https://orcid.org/0009-0009-7600-8643>



chherrera15@espe.edu.ec



Ecuador, Sangolquí, Universidad de las Fuerzas Armadas - ESPE.



Gruezo-Realpe, Mariela Stephany²

<https://orcid.org/0000-0002-5929-4336>



mariela.gruezo.realpe@utelvt.edu.ec



Ecuador, Esmeraldas, Universidad Técnica Luis Vargas Torres de Esmeraldas.



Borja-Almeida, Luis Gonzalo⁴

<https://orcid.org/0009-0001-1338-1493>



lugobal.espe@gmail.com



México, Cancún, Universidad Americana de Europa.

Autor de correspondencia¹



DOI / URL: <https://doi.org/10.55813/gaea/revistacec/v3/n1/51>

Resumen: El Internet de las cosas y la automatización inteligente están reconfigurando el desempeño de las organizaciones al convertir datos operativos en decisiones oportunas, aunque sus efectos dependen de capacidades tecnológicas, humanas e institucionales. Este estudio tuvo como propósito analizar sus aplicaciones, beneficios, riesgos y condiciones de adopción, con énfasis en América Latina. Se desarrolló una revisión bibliográfica cualitativa, documental, no experimental y de alcance exploratorio-descriptivo, mediante la consulta de publicaciones difundidas entre 2015 y 2025 en Scopus, Web of Science, ScienceDirect, IEEE Xplore y SciELO, complementadas con estudios seminales e informes regionales. Los hallazgos evidenciaron mejoras potenciales en monitoreo continuo, mantenimiento predictivo, trazabilidad, calidad, productividad, integración logística, agilidad e innovación; sin embargo, estos beneficios no derivan automáticamente de la conectividad, sino de la interoperabilidad, la gobernanza de datos, la convergencia tecnológica y las competencias del personal. También se identificaron barreras económicas, sistemas heredados, dependencia de proveedores, resistencia organizacional y riesgos de ciberseguridad, privacidad y automatización sustentada en datos deficientes. Se concluye que estas tecnologías fortalecen el desempeño cuando se implementan gradualmente, responden a problemas verificables y se articulan con la estrategia, los procesos y la madurez digital institucional.

Palabras clave: Internet de las cosas; automatización inteligente; desempeño organizacional; transformación digital; gobernanza de datos.



Check for updates

Recibido: 26/Feb/2026
Aceptado: 25/Mar/2026
Publicado: 24/Abr/2026

Cita: Erazo-Luzuriaga, A. F., Gruezo-Realpe, M. S., Herrera-Ramírez, C. D., & Borja-Almeida, L. G. (2026). Internet de las cosas (IoT) y automatización inteligente en organizaciones modernas. *Revista Científica Enfoques Del Conocimiento*, 3(1), 90-113. <https://doi.org/10.55813/gaea/revistacec/v3/n1/51>

Revista Científica Enfoques del Conocimiento (RCEC)
<https://www.blez.edu.ec>
<https://revistacec.blez.edu.ec>
revistacec@blez.edu.ec

© 2026. Este artículo es un documento de acceso abierto distribuido bajo los términos y condiciones de la **Licencia Creative Commons, Atribución-NoComercial 4.0 Internacional**.



Abstract:

The Internet of Things and intelligent automation are reshaping organizational performance by transforming operational data into timely decisions, although their effects depend on technological, human, and institutional capabilities. This study aimed to analyze their applications, benefits, risks, and adoption conditions, with particular emphasis on Latin America. A qualitative, documentary, non-experimental, and exploratory-descriptive literature review was conducted using publications issued between 2015 and 2025 and retrieved from Scopus, Web of Science, ScienceDirect, IEEE Xplore, and SciELO, complemented by seminal studies and regional reports. The findings revealed potential improvements in continuous monitoring, predictive maintenance, traceability, quality, productivity, supply chain integration, agility, and innovation. However, these benefits do not arise automatically from connectivity; rather, they depend on interoperability, data governance, technological convergence, and workforce competencies. Economic constraints, legacy systems, vendor dependence, organizational resistance, and risks related to cybersecurity, privacy, and automation based on deficient data were also identified. It is concluded that these technologies strengthen organizational performance when they are implemented gradually, address verifiable problems, and are aligned with institutional strategy, processes, and digital maturity.

Keywords: Internet of Things; intelligent automation; organizational performance; digital transformation; data governance.

1. Introducción

En las organizaciones modernas, la convergencia entre el Internet de las cosas (IoT), la inteligencia artificial, la computación en la nube y la analítica avanzada está desplazando la automatización basada en reglas hacia sistemas capaces de captar datos, reconocer patrones y ejecutar acciones en tiempo real. El IoT articula objetos físicos, sensores, redes y plataformas de procesamiento, mientras que la automatización inteligente convierte los datos obtenidos en decisiones operativas y respuestas autónomas. En América Latina y el Caribe, esta convergencia forma parte de una transformación que modifica procesos, modelos de negocio y cadenas de valor, aunque su incorporación permanece desigual entre países, sectores y tamaños empresariales (Atzori et al., 2010; CEPAL, 2022; Gubbi et al., 2013).

El problema central no radica únicamente en disponer de dispositivos conectados, sino en integrarlos de manera estratégica con los procesos, las personas y los objetivos institucionales. Una evaluación realizada mediante la herramienta Chequeo Digital en más de 19.800 micro, pequeñas y medianas empresas latinoamericanas — muestra autoseleccionada y, por tanto, no representativa de todas las firmas regionales— encontró que el 47 % se encontraba en el nivel inicial de madurez digital.

Asimismo, el 63 % estaba en etapas iniciales en la dimensión de personas y organización, mientras que el 72 % presentaba esa condición en datos y analítica, evidenciando que la principal limitación trasciende la adquisición tecnológica y alcanza las capacidades organizacionales (Cathles et al., 2022).

No obstante, cuando su implementación responde a necesidades organizacionales verificables, el IoT posibilita supervisar activos, automatizar operaciones, anticipar fallas, optimizar inventarios y mejorar la trazabilidad de las cadenas de suministro. Su integración con algoritmos de aprendizaje automático también favorece el mantenimiento predictivo, el control de calidad y la adaptación de los procesos según variaciones de demanda o condiciones ambientales. En contraste, las organizaciones que mantienen procedimientos fragmentados y exclusivamente reactivos pueden experimentar mayores tiempos de inactividad, desperdicio de recursos, decisiones tardías y menor capacidad para competir en mercados digitalizados, especialmente cuando sus rivales utilizan información operacional en tiempo real (Lee & Lee, 2015; Rahman & Ghosh, 2023; Solis Pino et al., 2025).

A pesar de estas oportunidades, la adopción plantea afectaciones económicas, técnicas, laborales e institucionales que no deben reducirse a problemas de conectividad. Los costos de infraestructura, la incompatibilidad con sistemas heredados, la ausencia de estándares, la limitada calidad de los datos y la escasez de personal especializado pueden impedir que los proyectos piloto alcancen una implementación sostenible. A ello se añaden riesgos de ciberseguridad, vigilancia indebida, pérdida de privacidad, dependencia de proveedores y redefinición de funciones laborales. En consecuencia, una automatización carente de gobernanza puede trasladar errores a gran escala, profundizar resistencias internas y producir transformaciones organizacionales no previstas junto con los beneficios esperados (Ahmetoglu et al., 2022; Brous et al., 2020).

En este sentido, la literatura ha avanzado ampliamente en arquitecturas, sensores, protocolos y aplicaciones industriales, pero todavía presenta una fragmentación considerable al explicar cómo interactúan la preparación tecnológica, el liderazgo, las competencias laborales, la gobernanza de datos y el desempeño organizacional. Las investigaciones suelen concentrarse en manufactura o en casos tecnológicos específicos, mientras son menos frecuentes los estudios longitudinales, las comparaciones entre países latinoamericanos y los análisis aplicados a pequeñas organizaciones o servicios públicos. Además, persiste una separación entre los trabajos centrados en beneficios operacionales y aquellos orientados a riesgos sociales y organizativos, lo que dificulta construir explicaciones integrales sobre la adopción efectiva del IoT (Ahmetoglu et al., 2022; Lee & Lee, 2015; Solis Pino et al., 2025).

Por consiguiente, revisar críticamente esta producción científica resulta conveniente para distinguir entre la incorporación superficial de dispositivos y la creación de capacidades de automatización inteligente. Su relevancia social reside en orientar

transformaciones que protejan los datos, fortalezcan las competencias de los trabajadores y eviten ampliar las brechas entre organizaciones con diferentes recursos. En el plano económico e institucional, la revisión puede apoyar decisiones sobre inversión, interoperabilidad, formación y evaluación de resultados; teóricamente, permitirá relacionar dimensiones tecnológicas, humanas y organizacionales; y, metodológicamente, facilitará ordenar indicadores de madurez, beneficios, riesgos y condiciones de adopción pertinentes para América Latina (Cathles et al., 2022; CEPAL, 2022).

La investigación es viable mediante una revisión bibliográfica de artículos disponibles en bases como Web of Science, Scopus, IEEE Xplore y ScienceDirect, complementada con SciELO y documentos de organismos regionales. Este corpus permite contrastar revisiones, estudios empíricos, modelos de madurez y evidencia institucional sin intervenir directamente sobre personas o infraestructuras organizacionales. En términos éticos, el estudio deberá mantener criterios explícitos de búsqueda y selección, representación fiel de los hallazgos, reconocimiento de limitaciones y trazabilidad de las referencias, evitando presentar estimaciones comerciales o resultados de muestras particulares como evidencia generalizable para toda la región (Ahmetoglu et al., 2022; Cathles et al., 2022).

En consecuencia, el objetivo general de este artículo es analizar la contribución del IoT y la automatización inteligente a la transformación de las organizaciones modernas, considerando sus aplicaciones, beneficios, riesgos y condiciones de adopción, con énfasis en América Latina. Específicamente, se propone identificar las aplicaciones organizacionales predominantes; comparar los beneficios operacionales y estratégicos con los riesgos técnicos, sociales y éticos; y sintetizar los factores tecnológicos, humanos e institucionales que facilitan o restringen su implementación. La contribución esperada consiste en ofrecer una perspectiva integradora que conecte automatización, madurez digital y gobernanza, superando el análisis exclusivamente técnico y proporcionando una base para investigaciones comparativas y decisiones organizacionales contextualizadas en la realidad latinoamericana (Ahmetoglu et al., 2022; Brous et al., 2020; Solis Pino et al., 2025).

2. Materiales y métodos

La investigación se desarrolló mediante un enfoque cualitativo, con diseño no experimental y carácter documental, debido a que la unidad de análisis estuvo constituida por publicaciones científicas y documentos institucionales relacionados con el Internet de las cosas y la automatización inteligente en las organizaciones modernas. El estudio presentó un alcance exploratorio-descriptivo, orientado a reconocer las principales aplicaciones, beneficios, riesgos, barreras y condiciones organizacionales vinculadas con la adopción de estas tecnologías. Asimismo, se emplearon los métodos analítico y sintético: el primero permitió descomponer la evidencia según sus dimensiones tecnológicas, humanas, operativas e institucionales,

mientras que el segundo facilitó integrar los hallazgos en categorías interpretativas coherentes. Este diseño resultó pertinente para examinar un campo interdisciplinario cuyos conceptos, aplicaciones y resultados todavía aparecen dispersos entre la ingeniería, la administración y los estudios organizacionales (Santander-Salmon et al., 2023).

La búsqueda bibliográfica comprendió artículos publicados entre enero de 2015 y diciembre de 2025, sin excluir trabajos anteriores cuando fueron considerados fundamentales para la conceptualización del IoT o la automatización organizacional. Se consultaron las bases de datos Scopus, Web of Science, IEEE Xplore, ScienceDirect y SciELO, debido a su cobertura de literatura tecnológica, administrativa y multidisciplinaria. De manera complementaria, se examinaron informes elaborados por organismos internacionales y regionales, como la Comisión Económica para América Latina y el Caribe y el Banco Interamericano de Desarrollo, cuando aportaron datos sobre transformación digital, madurez tecnológica o condiciones de adopción en América Latina. La combinación de fuentes científicas e institucionales permitió ampliar la comprensión del fenómeno sin equiparar los informes técnicos con la evidencia revisada por pares (Chamorro-Quiñónez & Navarrete-Zambrano, 2025).

Para recuperar los documentos se utilizaron descriptores en español e inglés, combinados mediante operadores booleanos. La ecuación general incluyó los términos “Internet of Things”, “IoT”, “Industrial Internet of Things”, “IIoT”, “Internet de las cosas”, “intelligent automation”, “smart automation”, “artificial intelligence”, “machine learning”, “automatización inteligente”, “organizations”, “enterprises”, “firms”, “business” y “organizaciones”. También se incorporaron términos como “Latin America”, “América Latina”, “digital maturity”, “madurez digital”, “organizational performance”, “cybersecurity”, “governance” y “adoption barriers”, con el propósito de identificar evidencia contextualizada. Las combinaciones fueron aplicadas en títulos, resúmenes y palabras clave, ajustándose a las opciones de búsqueda disponibles en cada base de datos para conservar la mayor equivalencia posible entre las consultas.

Se incluyeron artículos originales, revisiones de literatura y trabajos académicos evaluados por pares que analizaran aplicaciones del IoT, automatización inteligente, inteligencia artificial o analítica avanzada dentro de empresas, instituciones públicas u otras organizaciones. También fueron considerados estudios que abordaran desempeño operativo, mantenimiento predictivo, gestión de activos, cadenas de suministro, gobernanza de datos, competencias laborales, ciberseguridad, interoperabilidad o madurez digital. En contraste, se excluyeron documentos duplicados, publicaciones sin acceso al texto completo, materiales publicitarios, entradas de blogs, opiniones sin respaldo metodológico y estudios centrados exclusivamente en el diseño técnico de sensores o protocolos sin relación con procesos organizacionales. Los informes institucionales se admitieron únicamente cuando presentaron autoría identificable, metodología explícita y datos relevantes para el contexto latinoamericano (Chamorro-Quiñónez & Navarrete-Zambrano, 2025).

La selección se realizó mediante un proceso secuencial de identificación, depuración, revisión y elegibilidad. En primer lugar, se eliminaron los registros duplicados; posteriormente, se examinaron los títulos y resúmenes para descartar publicaciones ajenas al objetivo del estudio. En una etapa posterior se revisaron los textos completos, verificando su correspondencia con los criterios de inclusión, la claridad de sus objetivos y la relación de sus resultados con la adopción organizacional del IoT y la automatización inteligente. Las decisiones de inclusión y exclusión se registraron en una matriz de control para garantizar la trazabilidad del procedimiento. Aunque el trabajo correspondió a una revisión exploratoria y no a una revisión sistemática, el proceso de selección se organizó tomando como referencia los principios de transparencia y documentación establecidos por PRISMA 2020 (Casanova-Villalba & Casanova-Villalba, 2024).

La información de los documentos seleccionados se organizó en una matriz que incluyó autoría, año de publicación, país o región, sector económico, propósito del estudio, diseño metodológico, tecnologías analizadas, aplicaciones organizacionales, beneficios reportados, barreras de implementación, riesgos y principales conclusiones. Posteriormente, se aplicó un análisis temático para identificar patrones recurrentes, diferencias sectoriales, relaciones conceptuales y vacíos de conocimiento. La codificación se desarrolló mediante categorías iniciales derivadas de los objetivos del artículo, las cuales fueron ajustadas conforme emergieron nuevos temas durante la lectura comparativa. Finalmente, los resultados se integraron mediante una síntesis narrativa, sin realizar metaanálisis, debido a la diversidad de diseños, variables, sectores, indicadores y unidades de análisis presentes en la literatura examinada.

La calidad y pertinencia de las fuentes se valoraron considerando la claridad del objetivo, la coherencia entre metodología y resultados, la identificación de la población o contexto estudiado, la transparencia del procedimiento analítico y la correspondencia de las conclusiones con la evidencia presentada. También se compararon estudios provenientes de diferentes sectores y regiones para evitar que los resultados de casos particulares fueran generalizados sin sustento. Debido a que la investigación utilizó documentos públicos y no involucró intervención con personas, recopilación de datos personales ni experimentación directa, no se requirió consentimiento informado; sin embargo, se mantuvieron los principios de integridad académica, reconocimiento de autoría, fidelidad interpretativa y correcta atribución de las ideas. Estas decisiones favorecieron una revisión reproducible, crítica y metodológicamente coherente con su alcance exploratorio (Maldonado-Nova, 2022).

3. Resultados

3.1. Impacto del IoT y la automatización inteligente en el desempeño organizacional

El impacto del Internet de las cosas y de la automatización inteligente no debe interpretarse como una consecuencia automática de instalar sensores, conectar máquinas o adquirir plataformas analíticas. Su incidencia en el desempeño surge de una cadena de transformación mediante la cual los datos del entorno físico son capturados, transmitidos, depurados, analizados y convertidos en decisiones operativas. En este proceso, el IoT proporciona la infraestructura de observación y conectividad, mientras que la automatización inteligente incorpora algoritmos, reglas y capacidades predictivas para intervenir sobre los procesos. Por consiguiente, la tecnología solo produce valor cuando la información obtenida modifica decisiones, reduce incertidumbre o mejora la coordinación organizacional; de lo contrario, puede limitarse a generar mayores volúmenes de datos sin utilidad estratégica verificable (Brous et al., 2020; Lee & Lee, 2015).

Desde esta perspectiva, conviene distinguir entre adopción, integración y asimilación tecnológica. La adopción representa la decisión de incorporar el IoT; la integración supone conectarlo con sistemas empresariales, equipos industriales y procesos de trabajo; y la asimilación implica convertir su uso en una práctica institucional capaz de mejorar sistemáticamente el desempeño. Esta diferenciación explica por qué organizaciones con inversiones tecnológicas semejantes pueden obtener resultados divergentes. La evidencia recopilada en 239 empresas manufactureras estadounidenses muestra que la adopción efectiva está condicionada por la convergencia entre tecnologías de información y tecnologías operacionales, la interoperabilidad, la infraestructura y la gobernanza tecnológica, lo que confirma que el desempeño no depende del dispositivo aislado, sino del entramado organizacional en el que se incorpora (Ehie & Chilton, 2020).

Asimismo, el desempeño organizacional constituye una categoría multidimensional y no debe reducirse exclusivamente a la disminución de costos. Comprende resultados operativos, como productividad, calidad, utilización de activos y tiempos de respuesta; resultados estratégicos, como innovación, flexibilidad y diferenciación; y resultados organizacionales, como aprendizaje, coordinación y capacidad de adaptación. La revisión de 221 artículos sobre 11 tecnologías centrales de la Industria 4.0 confirma que los efectos sobre las cadenas de suministro son heterogéneos y dependen tanto de la tecnología utilizada como de los factores críticos que favorecen o restringen su implementación. En consecuencia, afirmar que el IoT “mejora el desempeño” sin precisar la dimensión evaluada, el mecanismo causal y el contexto de aplicación conduce a generalizaciones conceptualmente insuficientes (Rad et al., 2022).

3.1.1. Beneficios operativos y estratégicos

En el plano operativo, el primer beneficio atribuible al IoT consiste en ampliar la visibilidad de procesos que anteriormente eran observados mediante inspecciones periódicas, registros manuales o informes retrospectivos. Los sensores conectados permiten recopilar continuamente datos sobre ubicación, velocidad, temperatura, vibración, presión, humedad, consumo energético, estado de inventarios y funcionamiento de equipos. Esta observabilidad reduce los intervalos entre la ocurrencia de un evento y su detección, lo que facilita responder a desviaciones antes de que se conviertan en fallas críticas. Sin embargo, la visibilidad no constituye por sí misma un resultado de desempeño: adquiere valor cuando se combina con procedimientos de alerta, asignación de responsabilidades y capacidad efectiva de intervención organizacional (Ahmetoglu et al., 2022; Lee & Lee, 2015).

En este sentido, el mantenimiento predictivo representa una de las aplicaciones más relevantes. A diferencia del mantenimiento correctivo, que interviene después de la falla, y del preventivo, que opera según calendarios preestablecidos, el mantenimiento sustentado en IoT utiliza información sobre la condición real de los activos para estimar anomalías y programar acciones. Su importancia organizacional radica en que transforma el mantenimiento desde una función reactiva hacia una capacidad de anticipación. No obstante, para que este beneficio se materialice, la organización debe disponer de datos históricos confiables, umbrales técnicamente validados, personal capacitado y mecanismos que traduzcan las predicciones en órdenes de trabajo; por ello, el rendimiento no proviene únicamente del algoritmo, sino de la coordinación entre datos, tecnología y gestión de activos (Brous et al., 2020; Rad et al., 2022).

La automatización inteligente también puede mejorar la productividad al disminuir tareas repetitivas, reducir errores de registro y acelerar actividades de inspección, clasificación o control. Cuando los datos capturados por sensores se conectan con sistemas de ejecución, la organización puede ajustar automáticamente parámetros de producción, activar reposiciones, modificar rutas logísticas o suspender procesos ante condiciones anómalas. Esta capacidad reduce la dependencia de decisiones exclusivamente manuales y libera tiempo para actividades de mayor complejidad. Sin embargo, el beneficio no debe confundirse con la eliminación indiscriminada de la intervención humana, pues los sistemas automáticos requieren supervisión, mantenimiento y criterios de escalamiento para responder a eventos que no fueron contemplados durante su configuración (Ahmetoglu et al., 2022; Brous et al., 2020).

Otro efecto operativo se relaciona con la calidad. El monitoreo continuo permite identificar variaciones de proceso que podrían afectar las características del producto o del servicio antes de que las unidades defectuosas lleguen al cliente. En industrias manufactureras, alimentarias, farmacéuticas o logísticas, la integración de sensores con mecanismos de trazabilidad facilita reconstruir el recorrido de materiales y determinar en qué etapa se originó una desviación. De este modo, el IoT puede reducir la dependencia de inspecciones finales y favorecer un control preventivo de la calidad.

No obstante, esta capacidad requiere calibración de dispositivos, validación de mediciones y reglas claras para diferenciar una variación normal de una anomalía relevante, porque los datos inexactos pueden generar decisiones automáticas igualmente erróneas (Aamer et al., 2021; Ahmetoglu et al., 2022).

En la gestión de inventarios y cadenas de suministro, la conectividad permite conocer con mayor precisión la ubicación y el estado de insumos, productos y activos móviles. Esta trazabilidad contribuye a reducir discrepancias entre los inventarios físicos y los registros informáticos, anticipar faltantes, controlar condiciones de almacenamiento y coordinar la reposición. El beneficio estratégico aparece cuando dicha información es compartida entre proveedores, distribuidores y unidades internas, dado que la visibilidad común puede disminuir la incertidumbre y mejorar la sincronización de decisiones. Por el contrario, si cada actor conserva sistemas aislados o utiliza estándares incompatibles, el IoT puede aumentar la cantidad de información disponible sin resolver la fragmentación de la cadena (Birkel & Hartmann, 2019; Rad et al., 2022).

La evidencia empírica respalda este carácter mediado del impacto tecnológico. Argyropoulou et al. (2024) analizaron información proporcionada por ejecutivos de 66 empresas minoristas grandes, medianas y pequeñas del Reino Unido mediante modelación de ecuaciones estructurales. Los resultados mostraron que la capacidad de IoT influía positivamente en el desempeño empresarial a través de la integración y de las capacidades de la cadena de suministro. En términos interpretativos, este hallazgo indica que la conectividad no genera ventajas competitivas de manera directa: primero debe mejorar el intercambio de información, la articulación de procesos y la capacidad de responder a las condiciones del mercado. Por tanto, la integración opera como el mecanismo que convierte la información tecnológica en un resultado organizacional mensurable (Argyropoulou et al., 2024).

De manera convergente, el estudio de Ehie y Chilton (2020) muestra que la infraestructura tecnológica, la gobernanza y la interoperabilidad favorecen la convergencia entre las tecnologías de información y las tecnologías operacionales, la cual influye sobre la adopción del IoT en manufactura. Este resultado es particularmente significativo porque evidencia que el valor del IoT depende de la posibilidad de conectar los datos de las máquinas con los sistemas de planificación, inventarios, mantenimiento y control empresarial. Una organización puede disponer de sensores técnicamente sofisticados, pero si sus datos no se integran con las decisiones presupuestarias, logísticas o productivas, la utilidad se mantiene localizada y no se traduce en desempeño sistémico (Ehie & Chilton, 2020).

A partir de estos hallazgos, puede sostenerse que el principal beneficio inmediato del IoT no es la automatización total, sino la disminución de la incertidumbre operacional. La información en tiempo real permite conocer con mayor precisión qué ocurre, dónde ocurre y en qué condiciones se presenta un evento. Posteriormente, la analítica y la automatización pueden establecer qué respuesta resulta más conveniente. En

consecuencia, el valor se incrementa conforme la organización avanza desde la descripción hacia el diagnóstico, la predicción y la intervención automática. Esta progresión exige niveles crecientes de calidad de datos, capacidad analítica y gobernanza, por lo que no todas las organizaciones pueden transitar simultáneamente hacia formas avanzadas de automatización inteligente (Lee & Lee, 2015; Brous et al., 2020).

En el plano estratégico, el IoT puede contribuir a transformar la propuesta de valor de las organizaciones. Los datos obtenidos de productos conectados permiten comprender patrones de utilización, anticipar necesidades y ofrecer servicios posteriores a la venta. De esta manera, una empresa puede evolucionar desde la venta de un activo hacia servicios de monitoreo, mantenimiento remoto, disponibilidad garantizada o cobro según uso. Este desplazamiento hacia la servitización digital modifica la relación con el cliente porque el valor deja de concentrarse únicamente en la transacción inicial y se extiende durante el ciclo de vida del producto. Sin embargo, esta transformación requiere redefinir ingresos, responsabilidades, estructuras comerciales y capacidades de soporte, por lo que no constituye una simple extensión tecnológica del modelo tradicional (Lee & Lee, 2015; Brous et al., 2020).

Del mismo modo, la automatización inteligente fortalece la agilidad organizacional cuando permite interpretar rápidamente cambios en la demanda, el estado de los activos o las condiciones del entorno. Una organización ágil no es aquella que acumula más datos, sino la que puede convertirlos en respuestas oportunas sin comprometer la calidad ni la seguridad. En este sentido, los sistemas conectados pueden facilitar la reasignación de recursos, la modificación de programas de producción y la priorización de pedidos. No obstante, cuando la toma de decisiones permanece centralizada, los procedimientos son rígidos o las áreas no comparten información, la velocidad tecnológica puede superar la capacidad institucional de respuesta, reduciendo el beneficio potencial de la automatización (Rad et al., 2022; Argyropoulou et al., 2024).

La sostenibilidad representa otra dimensión potencial del desempeño. Los dispositivos conectados pueden registrar consumos energéticos, pérdidas de materiales, emisiones o condiciones de transporte, lo que ofrece información para identificar inefficiencias y orientar medidas correctivas. Sin embargo, la relación entre IoT y sostenibilidad no es intrínsecamente positiva, porque los sistemas también consumen energía, requieren infraestructura de almacenamiento y generan residuos electrónicos. Por consiguiente, las evaluaciones deben considerar tanto los ahorros derivados de la optimización como los costos ambientales de fabricar, operar, reemplazar y desechar dispositivos. El beneficio sostenible dependerá del balance del ciclo de vida y no únicamente de la reducción observada en una actividad específica (Rad et al., 2022; Ahmetoglu et al., 2022).

En América Latina y el Caribe, la materialización de estos beneficios está condicionada por una madurez digital todavía desigual. El instrumento Chequeo

Digital había sido aplicado, hasta abril de 2022, a más de 14.800 mipymes chilenas y a más de 5.000 empresas de otros 12 países de la región. Entre las organizaciones participantes, el 47 % se ubicó en la categoría principiante; además, el 63 % se encontraba en una etapa inicial en personas y organización y el 72 % en datos y analítica. Estas cifras no constituyen una muestra probabilística de todas las empresas latinoamericanas, pues corresponden a organizaciones que utilizaron voluntariamente el autodiagnóstico; aun así, muestran que la principal restricción no consiste solo en acceder a tecnologías, sino en desarrollar las capacidades necesarias para utilizarlas de forma productiva (Cathles et al., 2022).

Tabla 1
Relación entre capacidades de IoT, mecanismos organizacionales y desempeño

Capacidad tecnológica u organizacional	Mecanismo mediante el cual genera valor	Resultado esperado	Condición o limitación
Sensores y monitoreo continuo	Incrementan la visibilidad sobre activos y procesos	la Detección temprana de anomalías y menor tiempo de respuesta	Requiere datos confiables y protocolos de actuación (Brous et al., 2020).
Analítica y automatización	Transforman datos en alertas, predicciones o acciones	Mantenimiento predictivo, control de calidad y optimización	Depende de modelos validados y supervisión humana (Ahmetoglu et al., 2022).
Integración de cadena suministro	Facilita el intercambio de y la coordinación entre actores	Mayor sincronización, trazabilidad y capacidad de respuesta	El efecto está mediado por integración y capacidades organizacionales (Argyropoulou et al., 2024).
Convergencia IT/OT	Conecta sistemas empresariales con equipos operacionales	Gestión coordinada de producción, activos e inventarios	Exige infraestructura, gobernanza e interoperabilidad (Ehie & Chilton, 2020).
Productos y servicios conectados	Generan información durante el uso del producto	Personalización, servicios posventa y nuevos modelos de ingresos	Requiere rediseñar procesos, responsabilidades y propuesta de valor (Lee & Lee, 2015).
Gobernanza de datos	Define calidad, acceso, seguridad y responsabilidad	Decisiones confiables y aprovechamiento institucional	más Su ausencia incrementa y errores, riesgos y usos no autorizados (Brous et al., 2020).

Nota: La síntesis muestra que los resultados se producen mediante capacidades complementarias; por ello, la adquisición de dispositivos no equivale a una mejora automática del desempeño organizacional (Argyropoulou et al., 2024; Brous et al., 2020; Ehie & Chilton, 2020) (Autores, 2026).

En conjunto, la evidencia permite inferir una secuencia de generación de valor compuesta por cuatro niveles. El primero corresponde a la conectividad y la captura de datos; el segundo, a la integración de dichos datos con los procesos; el tercero, a su conversión en decisiones; y el cuarto, a la obtención de resultados operativos o estratégicos. Una interrupción en cualquiera de estos niveles reduce el beneficio final. Por ejemplo, datos abundantes sin interoperabilidad permanecen aislados; información integrada sin capacidad analítica no produce conocimiento; y predicciones técnicamente precisas sin autoridad para actuar no modifican el desempeño. Esta secuencia explica por qué los efectos positivos del IoT suelen encontrarse mediados

por capacidades organizacionales y no por la tecnología considerada aisladamente (Argyropoulou et al., 2024; Ehie & Chilton, 2020).

3.1.2. Barreras y riesgos de implementación

La primera barrera corresponde a la complejidad arquitectónica. Los entornos organizacionales suelen combinar maquinaria de distintas generaciones, sistemas heredados, aplicaciones empresariales, plataformas en la nube y dispositivos desarrollados por múltiples proveedores. La integración de estos componentes exige protocolos compatibles, interfaces estables y modelos comunes de datos. Cuando estas condiciones no se cumplen, aparecen silos tecnológicos, duplicación de registros y dificultades para escalar los proyectos. La revisión sistemática de Ahmetoglu et al. (2022) identifica entre los desafíos recurrentes la compatibilidad, complejidad, escalabilidad, costos de implementación y disponibilidad de conocimientos técnicos, lo que demuestra que el éxito depende de una arquitectura coherente y no únicamente de la funcionalidad individual de los dispositivos (Ahmetoglu et al., 2022).

La interoperabilidad representa una barrera tanto técnica como organizacional. Desde el punto de vista técnico, implica que los sistemas puedan intercambiar datos y comprender su significado; desde el punto de vista organizacional, supone que las áreas acuerden definiciones, responsabilidades y procedimientos comunes. Una empresa puede integrar tecnológicamente dos plataformas y, aun así, mantener conflictos sobre quién valida los datos, quién responde ante una alerta o qué unidad financia el mantenimiento. Por ello, la interoperabilidad real comprende dispositivos, información, procesos y estructuras de decisión. La evidencia de manufactura confirma que su presencia favorece la convergencia IT/OT, mientras que su ausencia limita la adopción efectiva del IoT (Ehie & Chilton, 2020).

La segunda barrera es económica. El costo de adopción no se limita a sensores o licencias, sino que comprende conectividad, almacenamiento, integración, mantenimiento, ciberseguridad, capacitación, actualización y sustitución de dispositivos. También existen costos indirectos asociados con interrupciones durante la instalación, rediseño de procesos y dependencia de consultores o proveedores especializados. En consecuencia, evaluar el proyecto únicamente mediante el precio inicial puede producir una estimación incompleta. Lee y Lee (2015) señalan que la valoración de inversiones de IoT debe considerar la incertidumbre y la evolución de los beneficios, debido a que estos proyectos pueden generar opciones estratégicas cuyo valor no se manifiesta inmediatamente en los flujos financieros convencionales (Lee & Lee, 2015).

La incertidumbre del retorno de la inversión se intensifica cuando los objetivos se expresan de forma genérica, como “digitalizar la empresa” o “mejorar la eficiencia”. Sin una línea base y sin indicadores específicos, resulta difícil atribuir los cambios observados a la tecnología. Para evaluar el desempeño deberían establecerse métricas relacionadas con tiempos de ciclo, utilización de activos, frecuencia de fallas,

desperdicio, exactitud de inventarios, calidad, consumo energético o velocidad de respuesta. Además, los beneficios deben compararse con el costo total durante el ciclo de vida. Este razonamiento es particularmente importante para las mipymes, cuyos recursos limitados reducen su capacidad para absorber proyectos fallidos o periodos prolongados de aprendizaje tecnológico (Ahmetoglu et al., 2022; Cathles et al., 2022).

La ciberseguridad constituye uno de los riesgos más críticos porque cada dispositivo conectado puede convertirse en un punto potencial de acceso. A diferencia de los sistemas informáticos convencionales, algunos sensores y controladores poseen capacidades limitadas para ejecutar mecanismos avanzados de cifrado, autenticación o actualización. En ambientes industriales, además, la aplicación de parches puede posponerse para evitar interrupciones en equipos esenciales. Esta situación amplía la superficie de ataque y puede comprometer la confidencialidad, integridad y disponibilidad de la información. Cuando el IoT controla procesos físicos, un incidente puede trascender la pérdida de datos y afectar operaciones, activos, trabajadores o usuarios (Ahmetoglu et al., 2022; Birkel & Hartmann, 2019).

La seguridad debe concebirse, por tanto, como una propiedad del ciclo de vida completo. Esto implica evaluar proveedores, configurar adecuadamente dispositivos, gestionar identidades, segmentar redes, actualizar firmware, monitorear eventos y establecer procedimientos de respuesta. Una organización que concentra su atención en la fase de instalación, pero omite el mantenimiento de seguridad, acumula vulnerabilidades conforme los dispositivos envejecen. Asimismo, la responsabilidad puede diluirse cuando intervienen fabricantes, operadores, integradores y proveedores de servicios en la nube. La literatura sostiene que los beneficios del IoT están acompañados por riesgos inesperados y transformaciones institucionales, por lo que la gobernanza de seguridad debe desarrollarse paralelamente a la expansión tecnológica (Brous et al., 2020; Birkel & Hartmann, 2019).

La privacidad plantea un riesgo adicional, especialmente cuando los dispositivos recopilan información sobre comportamiento, ubicación, productividad o patrones de uso. En el entorno laboral, el monitoreo puede contribuir a la seguridad y optimización de tareas, pero también puede convertirse en vigilancia excesiva si no existen límites sobre la finalidad y el tratamiento de los datos. En relación con los clientes, los productos conectados pueden generar información útil para personalizar servicios, aunque su utilización secundaria sin transparencia puede deteriorar la confianza. Por consiguiente, la organización debe definir qué datos son necesarios, quién puede acceder a ellos, cuánto tiempo serán conservados y con qué propósito podrán reutilizarse (Brous et al., 2020; Ahmetoglu et al., 2022).

La calidad de los datos constituye otra barrera estructural. La automatización inteligente reproduce las características de la información que recibe: sensores mal calibrados, registros incompletos o datos desactualizados pueden generar alertas incorrectas y decisiones ineficientes. El riesgo se intensifica cuando la organización

atribuye objetividad absoluta a los resultados algorítmicos y reduce la revisión humana. En consecuencia, el desempeño depende de procedimientos de validación, limpieza, trazabilidad y monitoreo de los datos. La ausencia de estas prácticas puede convertir la rapidez de la automatización en un factor de amplificación del error, porque una decisión equivocada puede ejecutarse repetidamente y extenderse a múltiples procesos antes de ser detectada (Brous et al., 2020; Ahmetoglu et al., 2022).

En el ámbito humano, la resistencia al cambio no debe entenderse como una oposición irracional a la tecnología, sino como una respuesta ante transformaciones que alteran funciones, autonomía, conocimientos requeridos y seguridad laboral. Los trabajadores pueden percibir el monitoreo como un mecanismo de control o interpretar la automatización como una amenaza de sustitución. Estas percepciones se intensifican cuando la implementación se comunica exclusivamente en términos de reducción de costos y no se explica cómo cambiarán las tareas. Por ello, la participación de los empleados, la capacitación y la redefinición transparente de responsabilidades constituyen condiciones para la apropiación tecnológica y no actividades accesorias posteriores a la instalación (Ahmetoglu et al., 2022; Brous et al., 2020).

La escasez de competencias digitales también limita la capacidad de obtener beneficios. Operar ecosistemas de IoT requiere conocimientos sobre redes, análisis de datos, ciberseguridad, mantenimiento, integración y gestión del cambio. No obstante, disponer de especialistas técnicos tampoco garantiza la transformación si los directivos carecen de criterios para relacionar la tecnología con los objetivos estratégicos. Se necesita, por tanto, una combinación de competencias técnicas, analíticas y gerenciales. Los resultados de Chequeo Digital, según los cuales el 63 % de las mipymes participantes se encontraba en una etapa inicial en personas y organización y el 72 % en datos y analítica, muestran que estas capacidades representan una restricción particularmente relevante en América Latina y el Caribe (Cathles et al., 2022).

La dependencia de proveedores constituye igualmente un riesgo estratégico. Las organizaciones pueden adoptar plataformas que utilizan formatos propietarios, arquitecturas cerradas o servicios difíciles de sustituir. Esta situación eleva los costos de migración, reduce el poder de negociación y puede condicionar futuras decisiones tecnológicas. Además, la discontinuidad de un producto, la desaparición del proveedor o el cierre de una plataforma puede dejar dispositivos sin soporte. Por consiguiente, las decisiones de adquisición deben considerar portabilidad de datos, compatibilidad, condiciones contractuales, disponibilidad de actualizaciones y posibilidad de integración con soluciones alternativas. La literatura ubica las relaciones con proveedores y colaboradores entre los factores que influyen sobre la adopción organizacional del IoT (Ahmetoglu et al., 2022; Birkel & Hartmann, 2019).

Los riesgos tampoco se distribuyen de manera uniforme entre organizaciones. Las grandes empresas poseen mayores probabilidades de financiar infraestructura,

contratar especialistas y absorber procesos prolongados de experimentación, mientras que las pequeñas empresas enfrentan restricciones de capital, personal y capacidad de negociación. Esta asimetría puede ampliar las brechas de productividad entre organizaciones digitalmente maduras y aquellas que permanecen en fases iniciales. El diagnóstico regional resulta significativo: el 47 % de las mipymes que utilizaron Chequeo Digital fue clasificado en el nivel principiante, frente a solo el 5 % ubicado en la categoría experta. Aunque estos resultados no son representativos de todas las empresas latinoamericanas, reflejan una marcada heterogeneidad en las condiciones de preparación tecnológica (Cathles et al., 2022).

La distancia entre expectativas y resultados también aparece en la evidencia empírica. Kisanjara (2023) estudió el desempeño de bancos tanzanos mediante un cuestionario aplicado a 342 participantes, con una tasa de respuesta del 82,16 %. Aunque la mayoría de las relaciones evaluadas resultó estadísticamente significativa, no se encontró un efecto significativo de la expectativa de desempeño sobre la reducción de los costos operativos ni de la disponibilidad del IoT sobre la mejora de la calidad del servicio. Estos resultados cuestionan una interpretación determinista: disponer de tecnología o esperar beneficios no garantiza que estos se materialicen, porque intervienen factores como integración, calidad de implementación, competencias y rediseño de procesos (Kisanjara, 2023).

La brecha regional también se manifiesta en los niveles avanzados de producción inteligente. La evidencia recopilada por el Banco Interamericano de Desarrollo a partir de datos de la Organización de las Naciones Unidas para el Desarrollo Industrial señala que poco más del 1 % de las empresas manufactureras latinoamericanas incluidas en la encuesta utilizaba tecnologías clasificadas como producción inteligente de cuarta generación. En contraste, cerca del 30 % empleaba conjuntamente tecnologías de producción ajustada e integración digital. Los tamaños muestrales por país eran reducidos, por lo que estos porcentajes deben interpretarse con cautela; aun así, evidencian que el tránsito desde la digitalización básica hacia sistemas inteligentes plenamente integrados continúa siendo limitado (Cathles et al., 2022).

En consecuencia, el riesgo principal no consiste únicamente en que un proyecto tecnológico falle, sino en que funcione técnicamente sin generar valor organizacional. Un sistema puede transmitir datos correctamente y, pese a ello, no mejorar el desempeño si carece de indicadores, responsables, integración o capacidad decisoria. Esta forma de fracaso resulta menos visible que una avería, porque la infraestructura permanece operativa mientras los beneficios esperados no se materializan. Por consiguiente, la evaluación debe distinguir entre éxito técnico —conectividad, disponibilidad y funcionamiento—, éxito de utilización —uso regular por las áreas— y éxito organizacional —mejora comprobable de resultados— (Brous et al., 2020; Argyropoulou et al., 2024).

En síntesis, el IoT y la automatización inteligente presentan una dualidad estructural: las mismas capacidades que incrementan visibilidad, velocidad y control también

pueden ampliar vulnerabilidades, dependencia y vigilancia. Cuanto mayor sea la conectividad, mayor será la información disponible, pero también aumentarán los puntos de exposición y la complejidad de gobernanza. Por ello, el desempeño positivo debe entenderse como un resultado contingente de la alineación entre estrategia, arquitectura, procesos, personas y seguridad. La evidencia examinada permite concluir que las organizaciones obtienen mayores beneficios cuando conciben el IoT como una capacidad sociotécnica y no como una colección de dispositivos; es decir, cuando vinculan la inversión con necesidades verificables, indicadores de desempeño, gobernanza de datos, interoperabilidad y aprendizaje organizacional (Ahmetoglu et al., 2022; Brous et al., 2020; Rad et al., 2022).

4. Discusión

Los hallazgos examinados permiten sostener que el impacto del Internet de las cosas y de la automatización inteligente sobre el desempeño organizacional es favorable, aunque no lineal ni tecnológicamente determinista. La disponibilidad de sensores, conectividad y algoritmos no produce por sí sola mejoras sostenidas, pues el valor emerge cuando los datos capturados se integran con los procesos, las decisiones y los objetivos estratégicos. En consecuencia, el IoT debe comprenderse como una capacidad sociotécnica mediante la cual la infraestructura digital interactúa con las competencias humanas, la estructura organizacional y los mecanismos de gobernanza. Esta interpretación coincide con Brous et al. (2020), quienes advierten que la adopción organizacional del IoT genera simultáneamente beneficios y riesgos, y con Ahmetoglu et al. (2022), cuya revisión identifica factores tecnológicos, organizacionales y ambientales que condicionan sus resultados.

En términos operativos, la revisión evidenció que la principal contribución del IoT radica en reducir la incertidumbre acerca del estado de los activos, los inventarios y los procesos. El monitoreo continuo permite sustituir parcialmente la supervisión episódica por una observación sistemática y, cuando se combina con automatización inteligente, facilita detectar anomalías, anticipar fallas y ejecutar respuestas oportunas. Sin embargo, la mejora no proviene exclusivamente de recopilar información, sino de disminuir el intervalo entre la identificación de una desviación y la intervención correctiva. En esta lógica, el mantenimiento predictivo, el control preventivo de la calidad y la trazabilidad constituyen expresiones de una misma capacidad: transformar datos físicos en decisiones operativas. Esta interpretación concuerda con Lee y Lee (2015), quienes señalan que el valor empresarial del IoT depende de la comunicación entre dispositivos y de su articulación con aplicaciones capaces de mejorar procesos y servicios.

No obstante, los resultados también revelan que una mayor visibilidad no equivale automáticamente a un mejor desempeño. Una organización puede disponer de información en tiempo real y, aun así, mantener respuestas tardías cuando las responsabilidades no están delimitadas, los procedimientos son rígidos o los datos

permanecen fragmentados entre departamentos. Por esta razón, la interoperabilidad debe analizarse más allá de su dimensión técnica: supone que los sistemas intercambien información, pero también que las unidades organizacionales compartan definiciones, criterios y protocolos de actuación. El estudio de Ehie y Chilton (2020), realizado con datos de 239 empresas manufactureras estadounidenses, respalda esta interpretación al demostrar que la infraestructura tecnológica, la gobernanza y la interoperabilidad favorecen la convergencia entre las tecnologías de información y las tecnologías operacionales, condición relevante para una adopción efectiva del IoT.

En el ámbito de las cadenas de suministro, el impacto positivo parece estar mediado por capacidades organizacionales complementarias. La conectividad facilita conocer la ubicación y las condiciones de materiales, productos y activos, pero la mejora del desempeño se produce cuando esa información incrementa la integración con proveedores, distribuidores y unidades internas. Argyropoulou et al. (2024) encontraron que la capacidad de IoT influye en el desempeño empresarial mediante la integración y las capacidades de la cadena de suministro, lo que refuerza la idea de que la tecnología opera como un habilitador y no como una causa autosuficiente. De manera convergente, Rad et al. (2022), tras sintetizar 221 artículos sobre 11 tecnologías de la Industria 4.0, concluyeron que sus beneficios dependen de factores críticos de éxito y de las interacciones existentes entre tecnologías, procesos y actores organizacionales.

Desde una perspectiva estratégica, los hallazgos sugieren que el IoT puede trascender la optimización incremental y favorecer transformaciones en la propuesta de valor. Los productos conectados generan información durante su utilización, lo que permite ofrecer mantenimiento remoto, personalización, monitoreo posventa o servicios basados en disponibilidad y consumo. No obstante, convertir estos datos en nuevos modelos de ingresos exige modificar estructuras comerciales, responsabilidades contractuales y mecanismos de relación con los clientes. Por consiguiente, la servitización digital no constituye una consecuencia automática de conectar productos, sino una reconfiguración organizacional sustentada en información. Lee y Lee (2015) ya advertían que las inversiones en IoT debían evaluarse considerando tanto sus beneficios operativos como las opciones estratégicas que generan, mientras que Rad et al. (2022) subrayan que las tecnologías de la Industria 4.0 pueden modificar simultáneamente eficiencia, flexibilidad, innovación y capacidad de respuesta.

Esta capacidad transformadora convive, sin embargo, con una estructura de riesgos que se expande conforme aumenta la conectividad. Cada dispositivo incorporado amplía potencialmente la superficie de ataque, mientras que la heterogeneidad de equipos y la coexistencia con sistemas heredados dificultan aplicar estándares uniformes de autenticación, cifrado y actualización. En entornos industriales, una vulnerabilidad puede trascender la exposición de información y afectar la continuidad de procesos físicos, la disponibilidad de activos o la seguridad operacional. Por ello, la ciberseguridad no debe considerarse una fase posterior a la implementación, sino

un atributo transversal del ciclo de vida tecnológico. La dualidad descrita por Brous et al. (2020) resulta especialmente pertinente: los mismos mecanismos que incrementan visibilidad, automatización y control también pueden intensificar vulnerabilidades, dependencia tecnológica y complejidad institucional.

La privacidad y la gobernanza de los datos introducen una segunda tensión. El monitoreo continuo puede fortalecer la trazabilidad y la prevención de riesgos, pero también posibilitar formas desproporcionadas de vigilancia sobre trabajadores y clientes. Esta ambivalencia obliga a delimitar finalidades, permisos de acceso, periodos de conservación y responsabilidades frente a decisiones automatizadas. Además, los algoritmos no neutralizan las deficiencias de los datos: una medición inexacta, incompleta o sesgada puede convertirse en una decisión automática reiterada, amplificando el error con mayor rapidez que un procedimiento manual. En consecuencia, la calidad de los datos debe considerarse una dimensión del desempeño y no únicamente un problema técnico. Birkel y Hartmann (2019) identifican precisamente la seguridad, la privacidad, la integración y la incertidumbre como riesgos interrelacionados en las cadenas de suministro habilitadas por IoT.

Las barreras humanas y organizacionales adquieren una relevancia particular en esta discusión, porque la automatización inteligente modifica tareas, jerarquías y criterios de evaluación. La resistencia del personal no debe interpretarse exclusivamente como falta de disposición tecnológica, sino como una respuesta comprensible ante cambios que pueden alterar autonomía, identidad profesional y estabilidad laboral. En este sentido, la capacitación es necesaria, pero insuficiente cuando no se acompaña de participación, comunicación y rediseño transparente de las funciones. Ahmetoglu et al. (2022) incluyen el conocimiento técnico, el apoyo directivo, la cultura organizacional y la resistencia al cambio entre los factores críticos de adopción, lo que confirma que la apropiación del IoT requiere una política de transformación organizacional y no una intervención exclusivamente informática.

La realidad latinoamericana profundiza estas restricciones debido a la heterogeneidad de la madurez digital empresarial. El estudio de Cathles et al. (2022), basado en información regional sobre adopción tecnológica, muestra que una proporción considerable de las empresas evaluadas permanece en fases iniciales, especialmente en las dimensiones de personas, organización, datos y analítica. Este resultado permite inferir que la principal brecha regional no consiste únicamente en adquirir sensores o servicios en la nube, sino en construir capacidades para gobernar, interpretar y utilizar la información. Por tanto, la transferencia directa de modelos desarrollados en economías con infraestructura consolidada puede generar resultados limitados cuando no se consideran las restricciones de conectividad, financiamiento, talento especializado y articulación institucional presentes en América Latina y el Caribe.

A partir de esta evidencia, la adopción debería orientarse mediante una lógica gradual y basada en problemas organizacionales verificables. Antes de escalar una iniciativa,

resulta necesario identificar el proceso crítico, establecer una línea base, definir indicadores y determinar cómo los datos producirán una decisión distinta. Esta secuencia evita que el éxito se mida por el número de dispositivos instalados y permite evaluarlo mediante cambios en tiempos de ciclo, frecuencia de fallas, calidad, utilización de activos, desperdicio o capacidad de respuesta. Asimismo, la implementación gradual facilita comprobar interoperabilidad, calidad de datos, aceptación del personal y viabilidad económica antes de extender el sistema. Tal planteamiento coincide con Lee y Lee (2015), quienes destacan la complejidad de justificar las inversiones en IoT, y con Ehie y Chilton (2020), quienes sitúan la convergencia y la preparación organizacional como antecedentes de una adopción eficaz.

En el plano teórico, la revisión respalda una explicación basada en complementariedades: la inversión tecnológica produce resultados cuando se combina con gobernanza, capacidades analíticas, integración de procesos y aprendizaje organizacional. Este razonamiento permite superar la concepción instrumental según la cual el rendimiento depende de las prestaciones técnicas del dispositivo. En cambio, propone comprender el IoT como una capacidad de segundo orden que reorganiza recursos existentes y amplía la posibilidad de observar, decidir y actuar. La evidencia de Argyropoulou et al. (2024) sobre la mediación ejercida por la integración de la cadena, junto con los resultados de Ehie y Chilton (2020) acerca de la convergencia IT/OT, refuerza la necesidad de incorporar variables mediadoras y moderadoras en futuras investigaciones sobre desempeño organizacional.

A pesar de la consistencia general de los resultados, las conclusiones deben interpretarse con cautela. La literatura reúne sectores, países, tecnologías y medidas de desempeño heterogéneas; por ello, no resulta metodológicamente válido asumir que los efectos observados en manufactura o comercio minorista se reproducirán con igual magnitud en servicios públicos, salud o pequeñas empresas latinoamericanas. Además, la presente revisión posee un alcance exploratorio y una síntesis narrativa, por lo que permite identificar tendencias y relaciones conceptuales, pero no estimar un efecto agregado ni establecer causalidad. Snyder (2019) señala que la utilidad de una revisión depende de la correspondencia entre su propósito, su estrategia de búsqueda y su modalidad de síntesis, mientras que Grant y Booth (2009) advierten que los distintos tipos de revisión ofrecen niveles diferentes de exhaustividad, reproducibilidad y análisis.

En definitiva, el IoT y la automatización inteligente pueden fortalecer el desempeño organizacional mediante mayor visibilidad, anticipación, coordinación y capacidad adaptativa; sin embargo, estos beneficios son contingentes a la integración entre tecnología, procesos y personas. La discusión demuestra que el desafío central no reside en conectar más dispositivos, sino en construir una arquitectura organizacional capaz de convertir datos confiables en decisiones legítimas, seguras y económicamente justificables. Cuando esta arquitectura está ausente, la conectividad puede producir sobrecarga informativa, vulnerabilidades y costos sin retorno; cuando

está consolidada, puede sustentar eficiencia operativa, innovación y diferenciación estratégica. En consecuencia, la contribución fundamental de esta revisión consiste en situar el desempeño como resultado de una configuración sociotécnica y contextual, particularmente relevante para organizaciones latinoamericanas con niveles disímiles de madurez digital (Ahmetoglu et al., 2022; Brous et al., 2020; Cathles et al., 2022).

5. Conclusiones

El análisis realizado permite concluir que el Internet de las cosas y la automatización inteligente poseen un potencial significativo para fortalecer el desempeño organizacional, siempre que su adopción trascienda la incorporación aislada de dispositivos y se articule con los procesos, la estrategia y las capacidades institucionales. La generación de valor no depende exclusivamente de la conectividad, sino de la posibilidad de convertir datos confiables en decisiones oportunas, acciones automatizadas y mejoras verificables en productividad, calidad, trazabilidad, mantenimiento y utilización de recursos.

Los beneficios operativos se manifiestan principalmente en la supervisión continua de activos, la detección anticipada de anomalías, el mantenimiento predictivo, el control preventivo de la calidad y la optimización de inventarios y cadenas de suministro. Sin embargo, estos resultados se consolidan únicamente cuando existe interoperabilidad entre los sistemas de información y las tecnologías operacionales, además de una integración efectiva entre las áreas funcionales y los actores externos. Por ello, el IoT debe concebirse como una capacidad organizacional complementaria y no como una solución autónoma capaz de producir resultados por sí misma.

En el plano estratégico, la conectividad y la automatización inteligente pueden favorecer la agilidad, la innovación y la formulación de nuevos servicios basados en datos, especialmente mediante el monitoreo remoto, la personalización y la servitización digital. No obstante, la transformación de la propuesta de valor exige redefinir responsabilidades, modelos de ingresos, relaciones con clientes y mecanismos de gobernanza. En consecuencia, las organizaciones que limitan la adopción del IoT a objetivos exclusivamente técnicos corren el riesgo de obtener beneficios parciales y de no convertir la inversión tecnológica en una ventaja competitiva sostenible.

Asimismo, las barreras identificadas demuestran que la implementación está condicionada por costos de ciclo de vida, incompatibilidad tecnológica, sistemas heredados, escasez de competencias digitales, resistencia al cambio y ausencia de estructuras de gobernanza. A estas restricciones se añaden riesgos de ciberseguridad, privacidad, vigilancia, dependencia de proveedores y decisiones automatizadas sustentadas en datos deficientes. Por consiguiente, una implementación responsable debe incorporar seguridad desde el diseño, gestión de

la calidad de los datos, capacitación continua, participación del personal y criterios transparentes para evaluar el impacto de los sistemas automatizados.

En América Latina y el Caribe, la adopción del IoT enfrenta desafíos adicionales relacionados con la heterogeneidad de la infraestructura, las restricciones financieras y la limitada madurez en personas, organización, datos y analítica. Esta situación evidencia que la prioridad regional no debe concentrarse únicamente en ampliar el acceso a dispositivos o plataformas, sino en desarrollar capacidades institucionales para integrar, interpretar y gobernar la información. En este contexto, las estrategias graduales, orientadas a problemas concretos y acompañadas por indicadores de desempeño, ofrecen una alternativa más viable que la implementación extensiva sin preparación organizacional suficiente.

Finalmente, la principal conclusión de esta revisión es que el impacto positivo del IoT y la automatización inteligente es contingente, multidimensional y dependiente del contexto. La tecnología genera valor cuando existe correspondencia entre infraestructura, procesos, talento humano, gobernanza y objetivos estratégicos; en cambio, su adopción fragmentada puede incrementar los costos, la complejidad y la exposición a riesgos sin producir mejoras sustantivas. Por tanto, futuras investigaciones deberían profundizar en estudios comparativos y longitudinales que permitan determinar cómo las características sectoriales, el tamaño organizacional y la madurez digital moderan la relación entre adopción tecnológica y desempeño, particularmente en el contexto latinoamericano.

CONFLICTO DE INTERESES

“Los autores declaran no tener ningún conflicto de intereses”.

Referencias Bibliográficas

- Aamer, A. M., Al-Awlaqi, M. A., Affia, I., Arumsari, S., & Mandahawi, N. (2021). The internet of things in the food supply chain: Adoption challenges. *Benchmarking: An International Journal*, 28(8), 2521–2541. <https://doi.org/10.1108/BIJ-07-2020-0371>
- Ahmetoglu, S., Che Cob, Z., & Ali, N. (2022). A systematic review of Internet of Things adoption in organizations: Taxonomy, benefits, challenges and critical factors. *Applied Sciences*, 12(9), 4117. <https://doi.org/10.3390/app12094117>
- Ahmetoglu, S., Che Cob, Z., & Ali, N. (2022). A systematic review of Internet of Things adoption in organizations: Taxonomy, benefits, challenges and critical factors. *Applied Sciences*, 12(9), Article 4117. <https://doi.org/10.3390/app12094117>
- Argyropoulou, M., Garcia, E., Nemati, S., & Spanaki, K. (2024). The effect of IoT capability on supply chain integration and firm performance: An empirical study in the UK retail industry. *Journal of Enterprise Information Management*, 37(3), 875–902. <https://doi.org/10.1108/JEIM-06-2022-0219>

- Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, 54(15), 2787–2805. <https://doi.org/10.1016/j.comnet.2010.05.010>
- Birkel, H. S., & Hartmann, E. (2019). Impact of IoT challenges and risks for SCM. *Supply Chain Management: An International Journal*, 24(1), 39–61. <https://doi.org/10.1108/SCM-03-2018-0142>
- Bonilla-Fierro, L. F., & Boné-Andrade, M. F. (2025). Desarrollo de plataformas de comunicación inclusivas mediante diseño universal. *Revista Científica Ciencia Y Método*, 3(2), 59-73. <https://doi.org/10.55813/gaea/rcym/v3/n2/5>
- Brous, P., Janssen, M., & Herder, P. (2020). The dual effects of the Internet of Things: A systematic review of the benefits and risks of IoT adoption by organizations. *International Journal of Information Management*, 51, 101952. <https://doi.org/10.1016/j.ijinfomgt.2019.05.008>
- Carpio-Velasco, F. J., & Garcés-Beltrán, G. M. (2025). Comparación de Estrategias de Control de Temperatura: Controlador PID y Redes Neuronales. *Revista Científica Zambos*, 4(2), 185-196. <https://doi.org/10.69484/rcz/v4/n2/113>
- Casanova-Villalba, C. I., & Casanova-Villalba, L. A. (2024). Uso de análisis de datos avanzados para la detección de fraudes financieros. *Revista Científica Ciencia y Método*, 2(3), 1–12. <https://doi.org/10.55813/gaea/rcym/v2/n3/44>
- Castelo-Vinueza, E. M. (2025). Problemas de la investigación tecnológica y su aplicación en la generación de innovación. *Journal of Economic and Social Science Research*, 5(1), 146–160. <https://doi.org/10.55813/gaea/jessr/v5/n1/166>
- Cathles, A., Suaznábar, C., & Vargas, F. (2022). *The 360° on digital transformation in firms in Latin America and the Caribbean*. Inter-American Development Bank. <https://doi.org/10.18235/0004635>
- Chamorro-Quiñónez, J. G., & Navarrete-Zambrano, C. M. (2025). Avances y desafíos en la contabilidad de costos en entornos industriales digitalizados. *Revista Científica Ciencia y Método*, 3(3), 1–13. <https://doi.org/10.55813/gaea/rcym/v3/n3/37>
- Chávez-Rendón, S. D., Pillasagua-Yépez, T. M., Moreira-Noboa, S. M., & Zamora-Mayorga, D. J. (2025). Análisis del funcionamiento tecnológico del ECU 911 de Quevedo en la gestión pública de la seguridad ciudadana. *Revista Científica Ciencia Y Método*, 3(3), 181-193. <https://doi.org/10.55813/gaea/rcym/v3/n3/71>
- Choez-Calderón, C. J. (2024). Realidad aumentada y su aplicación en la educación a distancia. *Revista Científica Ciencia Y Método*, 2(3), 26-38. <https://doi.org/10.55813/gaea/rcym/v2/n3/46>
- Choez-Calderón, C. J., & Aldo-Patricio, M. O. (2025). La ciberseguridad como prioridad empresarial dentro de marcos los regulatorios y normativos internacionales. *Revista Científica Ciencia Y Método*, 3(3), 14-27. <https://doi.org/10.55813/gaea/rcym/v3/n3/38>
- Comisión Económica para América Latina y el Caribe. (2022). *A digital path for sustainable development in Latin America and the Caribbean*. Naciones Unidas.

<https://www.cepal.org/en/publications/48461-digital-path-sustainable-development-latin-america-and-caribbean>

- Ehie, I. C., & Chilton, M. A. (2020). Understanding the influence of IT/OT convergence on the adoption of Internet of Things (IoT) in manufacturing organizations: An empirical investigation. *Computers in Industry*, 115, Article 103166. <https://doi.org/10.1016/j.compind.2019.103166>
- Galarza-Sánchez, P. C. (2023). Adopción de Tecnologías de la Información en las PYMEs Ecuatorianas: Factores y Desafíos. *Revista Científica Zambos*, 2(1), 21-40. <https://doi.org/10.69484/rcz/v2/n1/36>
- Galarza-Sánchez, P. C., Agualongo-Yazuma, J. C., & Jumbo-Martínez, M. N. (2022). Innovación tecnológica en la industria de restaurantes del Cantón Pedro Vicente Maldonado. *Journal of Economic and Social Science Research*, 2(1), 31–43. <https://doi.org/10.55813/gaea/jessr/v2/n1/45>
- Giraldo-Burgos, G. Y., Avilés-Tinitana, V. V., Palacios-Rodríguez, A. M., & Zamora-Mayorga, D. J. (2025). Desafíos de adopción frente a plataformas digitales externas en la biblioteca de la Universidad Técnica Estatal de Quevedo. *Revista Científica Ciencia Y Método*, 3(3), 194-212. <https://doi.org/10.55813/gaea/rcym/v3/n3/67>
- Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things: A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645–1660. <https://doi.org/10.1016/j.future.2013.01.010>
- Kisanjara, S. (2023). Internet of Things and organizational performance in the Tanzanian banks. *Information Discovery and Delivery*, 51(3), 253–266. <https://doi.org/10.1108/IDD-04-2022-0031>
- Lee, I., & Lee, K. (2015). The Internet of Things: Applications, investments, and challenges for enterprises. *Business Horizons*, 58(4), 431–440. <https://doi.org/10.1016/j.bushor.2015.03.008>
- Maldonado-Nova, V. (2022). El rol del talento humano en la transformación digital de las empresas ecuatorianas. *Revista Científica Zambos*, 1(2), 34–50. <https://doi.org/10.69484/rcz/v1/n2/26>
- Rad, F. F., Oghazi, P., Palmié, M., Chirumalla, K., Pashkevich, N., Patel, P. C., & Sattari, S. (2022). Industry 4.0 and supply chain performance: A systematic literature review of the benefits, challenges, and critical success factors of 11 core technologies. *Industrial Marketing Management*, 105, 268–293. <https://doi.org/10.1016/j.indmarman.2022.06.009>
- Rahman, M. S., & Ghosh, T. (2023). Machine learning and Internet of Things in Industry 4.0: A review. *Measurement: Sensors*, 28, 100822. <https://doi.org/10.1016/j.measen.2023.100822>
- Sánchez-Caguana, D. F., Philco-Reinozo, M. A., Salinas-Arroba, J. M., & Pico-Lescano, J. C. (2024). Impacto de la Inteligencia Artificial en la Precisión y Eficiencia de los Sistemas Contables Modernos. *Journal of Economic and*

Social Science Research, 4(3), 1–12.
<https://doi.org/10.55813/gaea/jessr/v4/n3/117>

- Sangacha-Tapia, L., González-Cañizalez, Y., & Rivas-Herrera, J. (2025). Optimización de Criterios de Búsqueda avanzada para Nuevas Tendencias en la Académica mediante Machine Learning. *Revista Científica Zambos*, 4(2), 197-211. <https://doi.org/10.69484/rcz/v4/n2/114>
- Santander-Salmon, E. S., Herrera-Sánchez, M. J., & Bravo-Bravo, I. F. (2023). La importancia de la digitalización en la administración empresarial mediante un análisis bibliográfico actualizado. *Multidisciplinary Collaborative Journal*, 1(2), 39–51. <https://doi.org/10.70881/mcj/v1/n2/15>
- Solano-Gutiérrez, G. A. (2024). La Tecnología en la Educación a Distancia: Revisión de Progresos y Obstáculos a Superar. *Revista Científica Zambos*, 3(2), 48-73. <https://doi.org/10.69484/rcz/v3/n2/17>
- Solis Pino, A. F., Ruiz, P. H., Mon, A., & Collazos, C. A. (2025). ATLANTIS: A multidimensional maturity model for evaluating the adoption of the Internet of Things in industrial SMEs. *Internet of Things*, 29, 101457. <https://doi.org/10.1016/j.iot.2024.101457>
- Villalva-Salguero, T. F., Llanos-Espín, B. M., Pluas-Llano, M. J., & Quimbata-Costa, J. J. (2026). Estado de las políticas públicas sobre TIC y su incidencia en la brecha digital rural. *Revista Científica Ciencia Y Método*, 4(1), 306-319. <https://doi.org/10.55813/gaea/rcym/v4/n1/152>