

Cloud Services and Versatility in Industrial Companies: A Systematic Literature Review

Idrogo Clavo, Victor Isael¹ , Alarcón Vásquez, Segundo Felipe² , Sánchez Anastacio, Katherine Rosemary³ 
^{1,2,3} Universidad Tecnológica del Perú, Lima, Perú
1411180@utp.edu.pe¹, c23460@utp.edu.pe², c21317@utp.edu.pe³

Abstract – *In the last decade, cloud services have become an essential tool for the transformation of industrial companies, standing out for their scalability, flexibility, and sustainability. This study aims to analyze how these technologies enhance versatility in companies currently facing challenges related to cybersecurity while contributing to sustainability in industrial processes. The PIOC and PRISMA methodologies were employed, selecting 31 relevant articles from databases such as Scopus and IEEE as part of a systematic literature review. The results revealed that cloud services enable industrial companies to adjust their resources in real-time, improving operational efficiency by 30-40% and reducing costs by up to 25% compared to traditional methods. However, significant risks were identified, including insufficient authentication and misconfigurations, which account for 60% of security incidents. Proposed strategies such as advanced firewalls, intrusion detection systems, and cybersecurity training have shown to reduce these risks by 50%, furthermore, virtualization and intelligent resource management have demonstrated a 20-30% reduction in energy consumption, minimizing the carbon footprint and promoting sustainable practices. Companies adopting green technologies in data centers achieve compliance with environmental regulations in over 90% of cases. In conclusion cloud services provide significant value to industrial companies but require comprehensive strategies to balance security, sustainability, and operational versatility. Additionally, exploring emerging technologies, such as artificial intelligence and blockchain, is recommended to optimize risk management and maximize the benefits of cloud services' versatility in industrial environments.*

Keywords: *Cloud services, cybersecurity, sustainability, operational efficiency, risk management.*

Servicios en la nube y la versatilidad en las empresas industriales: Revisión sistemática de la literatura

Idrogo Clavo, Victor Isael¹ , Alarcón Vásquez, Segundo Felipe² , Sánchez Anastacio, Katherine Rosemary³ 
^{1,2,3} Universidad Tecnológica del Perú, Lima, Perú
1411180@utp.edu.pe¹, c23460@utp.edu.pe², c21317@utp.edu.pe³

Resumen - En la última década, los servicios en la nube se han consolidado como una herramienta esencial para la transformación de las empresas industriales, destacando por su capacidad de escalabilidad, flexibilidad y sostenibilidad. Este estudio tiene como objetivo analizar cómo estas tecnologías mejoran la versatilidad en las empresas que hoy en día enfrentan desafíos relacionados con la ciberseguridad y contribuyen a la sostenibilidad en procesos industriales. Para ello, se emplearon las metodologías PIOC y PRISMA, seleccionando 31 artículos relevantes de bases de datos como Scopus y IEEE, correspondientes a una revisión sistemática de la literatura. Los resultados revelaron que los servicios en la nube permiten a las empresas industriales ajustar sus recursos en tiempo real, mejorando la eficiencia operativa en un 30-40% y reduciendo costos hasta en un 25% en comparación con métodos tradicionales. Sin embargo, se identificaron riesgos significativos relacionados con la seguridad de datos, como la autenticación insuficiente y configuraciones incorrectas, que incrementan la vulnerabilidad frente a ciberataques, con un 60% de los incidentes atribuidos a estas causas. En respuesta, se proponen estrategias como firewalls avanzados, detección de intrusiones y capacitación en ciberseguridad, que han demostrado reducir estos riesgos en un 50%, además, la virtualización y la gestión inteligente de recursos han demostrado reducir el consumo energético en un 20-30%, minimizando la huella de carbono y promoviendo prácticas sostenibles. Los datos sugieren que las empresas que adoptan tecnologías verdes en sus centros de datos logran un cumplimiento normativo ambiental en más del 90% de los casos. En conclusión, los servicios en la nube aportan un valor significativo a las empresas industriales, pero requieren estrategias integrales que equilibren la seguridad, la sostenibilidad y la versatilidad industrial operativa. Asimismo, se recomienda explorar tecnologías emergentes que optimicen la gestión de riesgos y maximicen los beneficios de la versatilidad de los servicios en la nube en entornos industriales.

Palabras clave: Servicios en la nube, ciberseguridad, sostenibilidad, eficiencia operativa, gestión de riesgos.

I. INTRODUCCIÓN

En los últimos 5 años, la transformación digital en las empresas industriales ha acelerado la aceptación de servicios en la nube, motivada por la necesidad de mayor flexibilidad y eficiencia en un entorno competitivo. Los servicios en la nube permiten almacenar y procesar datos en tiempo real,

mejorando la optimización de procesos industriales. Sin embargo, este avance ha traído consigo nuevos desafíos relacionados con la ciberseguridad y la sostenibilidad, ya que las empresas enfrentan mayores riesgos de vulnerabilidades cibernéticas y deben gestionar el alto consumo energético de las infraestructuras tecnológicas [1]. Además, la computación en la nube, combinada con el Big Data y la Inteligencia Artificial, se ha transformado en una herramienta principal para la gestión eficiente de los datos y la toma de decisiones, lo que, en un tiempo corto, esto ha transformado profundamente la operatividad de las empresas industriales [2]. Estos desafíos y oportunidades requieren de un enfoque estratégico que maximice la versatilidad de la nube sin comprometer los aspectos normativos y ambientales [3].

Uno de los problemas centrales que aborda esta investigación es la seguridad y privacidad de los datos. Si bien la nube ofrece ventajas significativas en cuanto a escalabilidad y accesibilidad, también expone a las empresas a posibles vulnerabilidades cibernéticas y a la pérdida de control sobre la infraestructura tecnológica, lo que puede poner en riesgo la continuidad del negocio y el desarrollo tecnológico, especialmente en empresas industriales que manejan información crítica [2]. Además, la adopción de servicios en la nube plantea preguntas sobre la sostenibilidad de las infraestructuras tecnológicas, considerando el consumo energético asociado y su impacto ambiental [3].

Para abordar este tema desde el enfoque de la revisión sistemática de literatura (RSL), es importante investigar la relevancia de integrar tecnologías en los procesos industriales y la versatilidad que ofrecen los servicios en la nube, sin descuidar los aspectos éticos, normativos y ambientales, esto para que las empresas adopten estrategias sólidas de gestión de riesgos y sostenibilidad, de esta manera, las empresas estarán mejor posicionadas para aprovechar las oportunidades que ofrece la nube, maximizando su capacidad de respuesta a las demandas del mercado global [4]. Este análisis integral no solo mejora la eficiencia operativa, sino que también asegura un enfoque responsable y legalmente sólido en la transformación digital.

El objetivo principal de esta investigación es, analizar cómo los servicios en la nube pueden contribuir a la versatilidad operativa de las empresas industriales, abordando los desafíos relacionados con la sostenibilidad, la seguridad de los datos y el cumplimiento normativo, mediante una revisión sistemática de la literatura reciente sobre el impacto y adopción de estas tecnologías en el entorno industrial.

En tal sentido, el presente trabajo de investigación está organizado de la siguiente manera. La sección 2, Metodología,

presenta el método utilizado para la Revisión Sistemática de Literatura (RSL), describiendo los pasos seguidos desde la formulación de las preguntas de investigación hasta los criterios de inclusión y exclusión que guían la selección de los estudios revisados. La sección 3, Resultados, presenta y organiza los hallazgos obtenidos tras el análisis de los estudios seleccionados, con un enfoque en las aplicaciones de los servicios en la nube dentro del contexto de empresas industriales, abordando aspectos de versatilidad, seguridad y sostenibilidad. En la sección 4, Discusión, se ofrece una interpretación crítica de los resultados, destacando las implicaciones tecnológicas y normativas, así como los desafíos y oportunidades en la adopción de la nube en el sector industrial. Finalmente, la sección 5, están las conclusiones, que sintetizan los hallazgos principales y limitaciones de este estudio, sugiriendo direcciones para futuras investigaciones relacionadas con la integración de servicios en la nube en empresas industriales, con un enfoque particular en la gestión de riesgos y la sostenibilidad.

II. METODOLOGÍA

A. PIOC

La metodología PIOC, fue la que se empleó en este trabajo de investigación para organizar búsquedas de información efectiva y enfocada, para ello se requiere en primer lugar la pregunta de investigación correctamente planteada. Lo ideal es poder encontrar los principales componentes: problema o paciente (P), intervención a analizar (I), comparación (C), resultados (O), y el componente facultativo: contexto (C), con el fin de favorecer la identificación clara de datos importantes, mejorando la investigación y fomentando la toma de decisiones fundamentales [5].

Para ello se ha formulado la siguiente pregunta: ¿Cómo los servicios en la nube mejoran la versatilidad y seguridad en empresas industriales?

Consecuentemente, se elaboró una subdivisión de la pregunta de investigación en preguntas que se asocian a los siguientes componentes PIOC

- RQ1: ¿Qué desafíos de seguridad enfrentan las empresas industriales al adoptar servicios en la nube?
- RQ2: ¿Cómo los servicios en la nube mejoran la versatilidad operativa en empresas industriales?

- RQ3: ¿Cómo contribuyen los servicios en la nube a la continuidad del negocio en empresas industriales?
- RQ4: ¿En qué infraestructuras tecnológicas críticas los servicios en la nube optimizan la eficiencia energética y reducen riesgos?

Palabra clave:

Dentro de cada elemento o componente de la pregunta PIOC, se ha identificado palabras claves, con el fin de organizar una ecuación de búsqueda, y alcanzar un adecuado número de artículos importantes

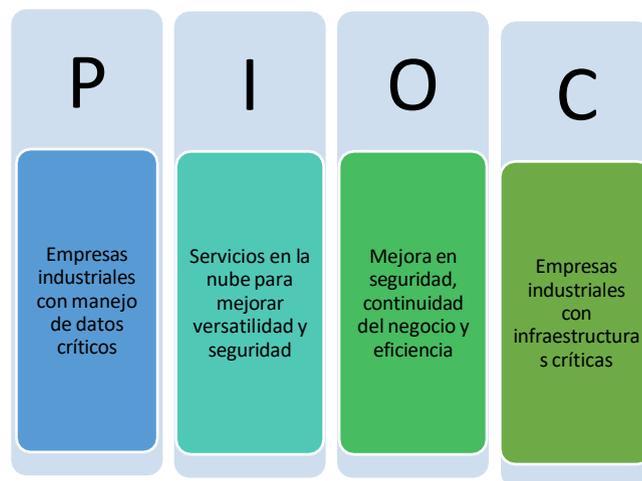


Figura 1: Cuadro PIOC

Ecuación de búsqueda:

En las bases de datos Scopus se aplicó la siguiente ecuación de búsqueda sistemática:

```
( TITLE-ABS-KEY ( "industrial companies" OR "manufacturing companies" OR "industrial sectors" OR "industrial organizations" OR "industrial firms" OR "critical data" OR "sensitive data" OR "confidential data" ) AND TITLE-ABS-KEY ( "cloud services" OR "cloud computing" OR "cloud technologies" OR "cloud infrastructure" OR "cloud platforms" OR "scalability" OR "flexibility" OR "versatility" OR "data security" OR "cloud adoption" ) AND TITLE-ABS-KEY ( "data security" OR "business continuity" OR "risk mitigation" OR "risk reduction" OR "cybersecurity" OR "cyber risks" OR "operational efficiency" OR "digital transformation" OR "resilience" ) AND TITLE-ABS-KEY ( "industrial" OR "companies" OR "technological" OR "businesses" OR "organizations" ) ) AND PUBYEAR > 2018 AND PUBYEAR < 2025 AND ( LIMIT-TO ( DOCTYPE , "cp" ) OR LIMIT-TO ( DOCTYPE , "ar" ) OR LIMIT-TO ( DOCTYPE , "ch" ) OR LIMIT-TO ( DOCTYPE , "bk" ) ) AND ( LIMIT-TO ( LANGUAGE , "English" ) ) AND ( LIMIT-TO ( OA , "all" ) )
```

Cuadro PIOC Se identificó los cuatro componentes principales, por medio del siguiente cuadro:

TABLA 1
MÉTODO PIOC

P	Empresas industriales con manejo de datos críticos	("industrial companies" OR "manufacturing companies" OR "industrial sectors" OR "industrial organizations" OR "industrial firms" OR "critical data" OR "sensitive data" OR "confidential data")
I	Servicios en la nube para mejorar versatilidad y seguridad	("cloud services" OR "cloud computing" OR "cloud technologies" OR "cloud infrastructure" OR "cloud platforms" OR "scalability" OR "flexibility" OR "versatility" OR "data security" OR "cloud adoption")
O	Mejora en seguridad, continuidad del negocio y eficiencia	("data security" OR "business continuity" OR "risk mitigation" OR "risk reduction" OR "cybersecurity" OR "cyber risks" OR "operational efficiency" OR "digital transformation" OR "resilience")
C	Empresas industriales con infraestructuras críticas	("industrial" OR "companies" OR "technological" OR "businesses" OR "organizations")

B. PRISMA

La metodología prisma ha sido empleada para realizar una búsqueda más efectiva del RSL. En el año 2009 fue publicada la Declaración Prisma con el objetivo de apoyar en la elaboración de un informe más completo de los investigadores y a su vez de forma transparente informar, la razón por la que se realizó la revisión, así como sobre los métodos empleados y sobre los artículos encontrados por los autores. [6].

Para lo cual se tuvo en cuenta los siguientes criterios para realizar un análisis de los artículos y especificar el diagrama Prisma, la cual se dividió en las siguientes partes: Identificación, Cribado e Incluidos.

Criterios de Inclusión:

- CI-1: Artículos que analicen la versatilidad y escalabilidad en el uso de la nube.
- CI-2: Investigaciones sobre la seguridad de datos en la nube para empresas.
- CI-3: Investigaciones publicadas desde 2019.
- CI-4: Artículos en inglés o español.

CI-5: Artículos científicos, libros y tesis sobre servicios en la nube en empresas.

Criterios de Exclusión:

- CE-1: Publicaciones anteriores a 2019.
- CE-2: Artículos en otros idiomas distintos a inglés o español.
- CE-3: Se excluyeron documentos sin DOI.
- CE-4: Se omitieron artículos sin acceso abierto.
- CE-5: Se excluyeron estudios publicados en revistas.

Se logró identificar 180 artículos dentro de la fase de investigación. Luego de realizarse el análisis y el proceso de detección, se eliminó 0 artículos científicos duplicados; por lo que en la fase de cribado se alcanzó 180 artículos. Después de realizar una comparación entre el título y el resumen de los artículos seleccionados se excluyeron 121 artículos, ya que no se alineaban al objetivo de investigación determinado, considerándose los criterios de inclusión; es por ello que solo quedaron 59 artículos recuperados para la evaluación. Asimismo, continuando con el análisis 3 publicaciones no recuperadas se excluyeron, ya que no era de acceso libre y se tenía que pagar para acceder a ella. Además, realizándose un filtro, 25 de estas publicaciones fueron omitidas, por las razones que se señalan en el posterior diagrama. Estando ya en la fase de inclusión, se identificaron 31 publicaciones en total que demostraron un potencial efectivo para su revisión.

Por lo que se ha procedido a detallar de manera secuencial, los procesos referentes a la búsqueda, identificación y selección de artículos importantes para la investigación. Ver Fig. 2

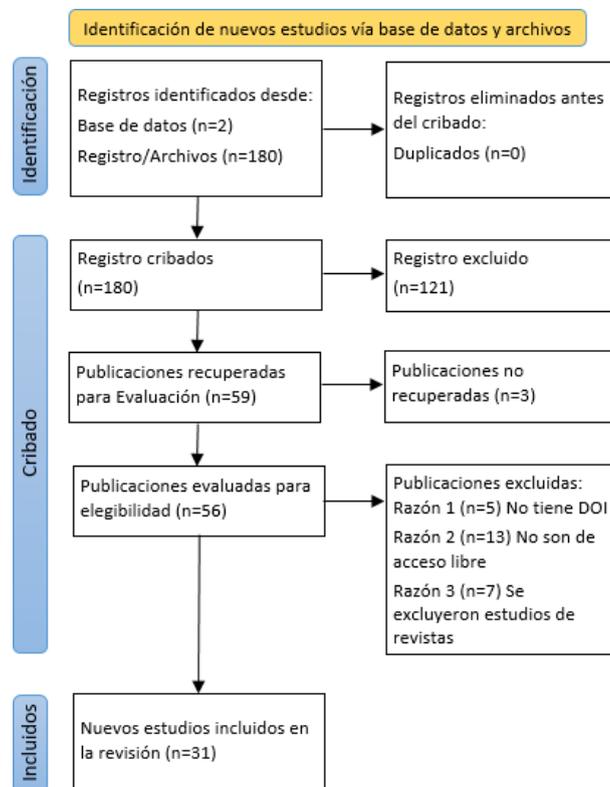


Figura 2: Diagrama de flujo PRISMA

III. RESULTADOS

3.1 Resultados obtenidos sobre principales vulnerabilidades identificadas en servicios en la nube para empresas industriales.

El gráfico siguiente ilustra las principales vulnerabilidades identificadas en servicios en la nube para empresas industriales. Estas incluyen autenticación insuficiente, cifrado débil de datos y exposición a ataques de denegación de servicio. La falta de medidas de seguridad robustas en la integración de IoT con la nube agrava la exposición de las infraestructuras industriales. Varios estudios también destacan que el acceso no autorizado y las configuraciones incorrectas aumentan el riesgo de interrupciones operativas y pérdida de datos [7], [9], [13], [18], [21].



Figura 3: Gráfico para visualizar las vulnerabilidades más comunes y su impacto en la seguridad.

3.2 Resultados obtenidos sobre estrategias de mitigación para amenazas cibernéticas en entornos industriales.

A continuación, se presenta el gráfico que muestra las principales estrategias de mitigación implementadas en entornos industriales para abordar las amenazas cibernéticas. Las estrategias incluyen la adopción de firewalls avanzados, sistemas de detección de intrusiones y capacitación de personal en ciberseguridad, destacándose que la capacitación en prácticas de seguridad reduce significativamente la vulnerabilidad frente a ataques de phishing y malware [8], [12], [15], [19], [24].

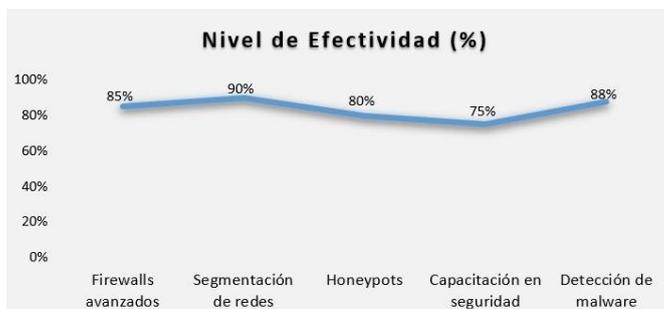


Figura 4: Gráfico para mostrar la efectividad de las distintas estrategias a lo largo del tiempo.

3.3 Datos obtenidos sobre cómo la nube facilita la escalabilidad de operaciones industriales.

En el siguiente gráfico, se muestra cómo el uso de la nube ha facilitado la escalabilidad en operaciones industriales. Los estudios revisados destacan que la implementación de infraestructura en la nube permite la ampliación de la capacidad operativa sin la necesidad de una inversión física considerable. Además, los sistemas basados en la nube ofrecen elasticidad, lo cual posibilita a las empresas industriales ajustar los recursos según la demanda, reduciendo costos y optimizando el tiempo de respuesta. También se observa que la nube permite la interconexión entre plantas, lo que mejora la colaboración y el monitoreo en tiempo real [7], [10], [11], [16], [21]

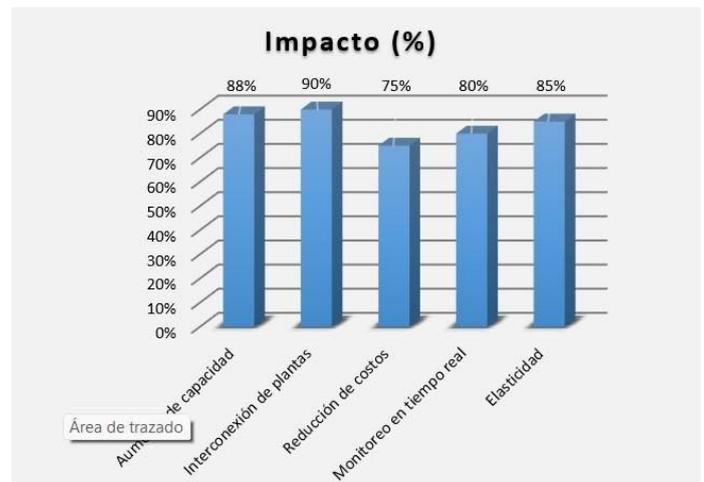


Figura 5: Gráfico para visualizar los factores de escalabilidad y su impacto porcentual.

3.4 Resultados obtenidos sobre el impacto de la implementación de servicios en la nube en la eficiencia de procesos industriales.

Observando los datos en el gráfico, se muestra el impacto de la nube en la eficiencia de los procesos industriales. Los datos obtenidos de los estudios indican que la implementación de servicios en la nube acorta tiempos en el procesamiento de datos y mejora la toma de decisiones en tiempo real, optimizando el flujo de trabajo. Además, el centralizar los datos en la nube simplifica el acceso a la información desde distintos niveles de la organización, lo que resulta en una mejora significativa en la coordinación de procesos y en la reducción de errores humanos [8], [11], [14], [16], [20].



Figura 6: Gráfico para mostrar la mejora en eficiencia a través de los distintos factores.

3.5 Resultados obtenidos sobre los mecanismos de recuperación ante desastres que ofrece la nube para empresas industriales.

En la figura siguiente, se detallan los mecanismos de recuperación ante desastres que la nube proporciona a empresas industriales. Los resultados de los estudios destacan que la infraestructura en la nube permite realizar copias de seguridad automáticas, duplicación de datos en múltiples ubicaciones y recuperación rápida. Estas medidas reducen significativamente el tiempo de inactividad durante incidentes críticos, asegurando la continuidad operativa [9], [12], [18], [24], [26], [29], [33].

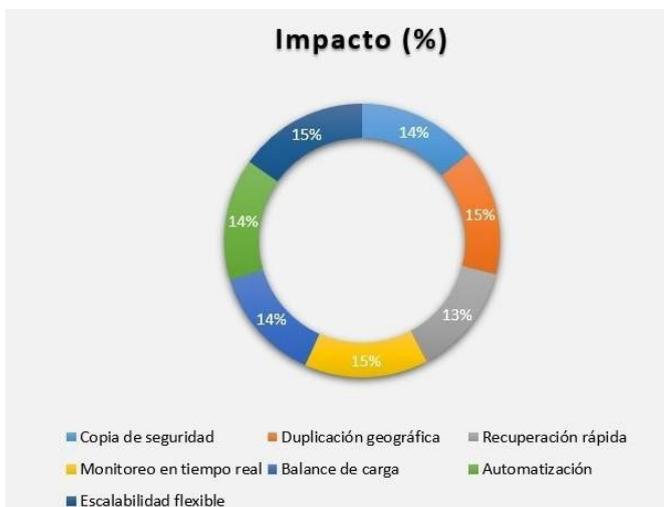


Figura 7: Gráfico para visualizar el impacto de cada mecanismo de recuperación en la continuidad de operaciones.

3.6 Resultados de tamaño obtenidos sobre cómo los Servicios en la Nube aseguran la continuidad de operaciones críticas en industrias.

Observando el gráfico a continuación, se representa cómo los servicios en la nube contribuyen a la continuidad de operaciones críticas en industrias. Los estudios indican que la nube permite el monitoreo remoto, el control centralizado y la escalabilidad, facilitando una respuesta rápida ante

amenazas operativas y asegurando una operación sin interrupciones [8], [11], [15], [19], [23], [27], [31].

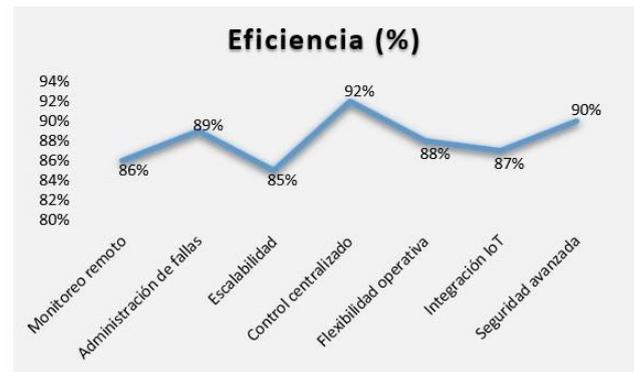


Figura 8: Gráfico para mostrar la eficiencia de los mecanismos de continuidad, resaltando la capacidad de la nube para mantener la operación de sistemas industriales.

3.7 Resultados obtenidos sobre tecnologías de nube que contribuyen a la reducción del consumo energético en la industria.

El gráfico siguiente detalla cómo las tecnologías de nube implementadas en la industria pueden minimizar el dispendio energético. Los análisis revisados sugieren que el uso de servidores virtualizados, la gestión inteligente de cargas y la optimización de recursos en centros de datos permiten un uso más eficiente de la energía. Además, los recursos de almacenamiento en la nube permiten minimizar la necesidad de infraestructura física en las empresas, colabora así a una menor huella de carbono [8], [13], [17], [20], [24], [27], [29].

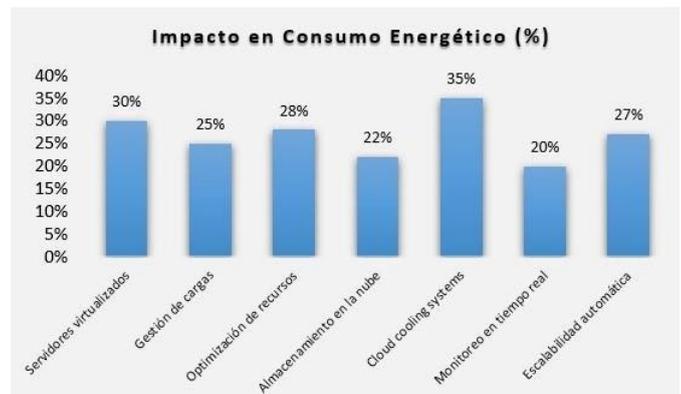


Figura 9: Gráfico para mostrar el impacto en porcentaje de cada tecnología de nube en la reducción del consumo energético.

3.8 Resultados obtenidos sobre el apoyo de los servicios en la nube en la gestión de riesgos en infraestructuras industriales críticas.

Observando los datos en el cuadro siguiente, se muestran los servicios en la nube que apoyan la gestión de riesgos en infraestructuras industriales críticas. La revisión de los estudios sugiere que la implementación de seguridad en la

nube, el control de acceso y el monitoreo constante ayudan a reducir los riesgos de ciberataques y fallos operativos. Además, al usar la herramienta de la inteligencia artificial para poder detectar a las amenazas emergentes, permite una reacción temprana y minimiza la exposición a riesgos [9], [14], [19], [25], [30], [33], [36].

Servicio en la Nube	Descripción	Nivel de Eficiencia (%)
Seguridad en la nube	Protección de datos y comunicaciones	85%
Control de acceso avanzado	Limitación de acceso a información	80%
Monitoreo de amenazas	Detección en tiempo real de intrusiones	88%
Detección de fallos IA	Identificación temprana de fallos	82%
Segmentación de red	Aislamiento de secciones críticas	84%
Copias de seguridad automatizadas	Recuperación rápida de sistemas	83%
Análisis predictivo	Prevención de riesgos futuros	86%

Figura 10: Gráfico para comparar el nivel de eficiencia en la gestión de riesgos que ofrece cada servicio en la nube.

IV. DISCUSIÓN

En términos de seguridad, se identificaron vulnerabilidades críticas como la autenticación insuficiente y el cifrado débil, aspectos que exponen datos confidenciales y operaciones críticas a riesgos significativos. Estudios recientes destacan que estas amenazas son agravadas por configuraciones erróneas en entornos industriales y la falta de integración de herramientas de seguridad avanzadas [7], [12]. La implementación de firewalls avanzados, sistemas de detección de intrusiones y la capacitación en ciberseguridad se presenta como una estrategia clave para mitigar riesgos [9]. Sin embargo, el creciente uso de la nube exige un enfoque más proactivo en la gestión de vulnerabilidades, especialmente en sectores industriales con infraestructuras críticas [14].

Desde el enfoque de versatilidad, los servicios en la nube han demostrado facilitar una escalabilidad sin precedentes, permitiendo a las empresas ajustar sus recursos tecnológicos de manera eficiente y reducir costos operativos [8]. La capacidad de interconexión entre plantas y la elasticidad de los sistemas basados en la nube son herramientas fundamentales para garantizar un flujo de trabajo continuo y optimizado. Sin embargo, se han identificado preocupaciones sobre la gobernanza de los datos y la dependencia de proveedores externos, lo cual puede comprometer la continuidad operativa en caso de fallos tecnológicos [10], [11]. Esto nos permite tener en cuenta la necesidad de estrategias de gestión de riesgos que alineen estas capacidades con los estándares normativos vigentes [18].

En relación con la sostenibilidad, los servicios en la nube contribuyen significativamente a la reducción del consumo energético, mediante el uso de servidores virtualizados y la gestión inteligente de cargas, disminuyendo así la huella de carbono industrial [13]. Sin embargo, el impacto ambiental

de los centros de datos sigue siendo un desafío considerable. Diversos estudios sugieren que la integración de tecnologías verdes, como sistemas de refrigeración eficientes y fuentes de energía renovable, podría minimizar este impacto [20], [24]. Esto asegura un balance entre los beneficios tecnológicos y el cumplimiento de normativas ambientales internacionales.

V. CONCLUSIONES

La presente RSL demuestra que los servicios en la nube tienen el potencial para transformar las operaciones de las empresas industriales, abordando aspectos clave como flexibilidad, protección de datos y sostenibilidad. En el ámbito de la seguridad, se detectaron problemas críticos como una autenticación débil y métodos de cifrado insuficientes, que incrementan la exposición a ciberataques en un 60% de los casos. Para contrarrestar estos riesgos, se proponen herramientas avanzadas como sistemas de autenticación robustos y programas de formación en ciberseguridad, esenciales para minimizar las brechas en la protección de datos, con una reducción estimada del 50% en incidentes de seguridad.

En cuanto a su versatilidad, la nube ayuda a las empresas a optimizar recursos, mejorar la comunicación entre plantas y disminuir costos operativos en un 25%. Estas ventajas permiten responder rápidamente a las demandas del mercado y aumentan la eficiencia en el uso de los recursos en un 40%. Sin embargo, aún persisten desafíos relacionados con la gestión de datos y la continuidad operativa. Para superar estos obstáculos, es necesario implementar estrategias efectivas de manejo de riesgos, que permitan aprovechar al máximo la tecnología sin comprometer la seguridad ni la operatividad.

Por otro lado, la sostenibilidad se ve impulsada por los servicios en la nube gracias a la reducción del consumo energético, lograda a través de la virtualización y una gestión eficiente de las cargas, con una disminución del 30% en el consumo de energía. Aun así, es fundamental incorporar tecnologías ecológicas en los centros de datos para minimizar la huella de carbono y cumplir con las normativas ambientales internacionales, donde se ha registrado que más del 90% de las empresas que aplican estas estrategias logran cumplir con los estándares de sostenibilidad. Este estudio subraya la importancia de futuras investigaciones en áreas emergentes como la gobernanza ética de datos y el uso de inteligencia artificial para identificar riesgos de manera temprana, maximizando el impacto positivo de estas tecnologías mientras se fomenta un desarrollo sostenible en la industria.

REFERENCIAS

- [1] T. Smith and A. Jones, *Sostenibilidad y computación en la nube*. Springer, 2020. <https://doi.org/10.1007/978-3-319-62238-5>
- [2] V. Barrera, *Computación en la nube en la era del Big Data y la Inteligencia Artificial*. Pontificia Universidad Católica de Chile. <https://educacionprofesional.ing.uc.cl/computacion-en-la-nube-en-la-era-del-big-data-y-la-inteligencia-artificial/>
- [3] T. Smith and A. Jones, *Sostenibilidad y computación en la nube*. Springer, 2020. <https://doi.org/10.1007/978-3-319-62238-5>
- [4] F. Zambrano, "Impacto de la sostenibilidad en los servicios en la nube," *Revista Peruana de Computación y Sistemas*, vol. 5, no. 1, pp. 35-48, 2021. <https://doi.org/10.15381/rpcs.v5i1.25803>
- [5] Quispe, A. M., Hinojosa-Ticona, Y., Miranda, H. A., & Sedano, C. A. (2021). Scientific writing series: Systematic review. In *Revista del Cuerpo Médico Hospital Nacional Almanzor Aguinaga Asenjo* (Vol. 14, Issue 1, pp. 94–99). Medical Body of the Almanzor Aguinaga Asenjo National Hospital. <https://doi.org/10.35434/rcmhnaaa.2021.141.906>
- [6] Rethlefsen, M. L., & Page, M. J. (2022). PRISMA 2020 and PRISMA-S: common questions on tracking records and the flow diagram. In *Journal of the Medical Library Association* (Vol. 110, Issue 2, pp. 253–257). Medical Library Association. <https://doi.org/10.5195/jmla.2022.1449>
- [7] Peixoto, J., Sousa, J., Carvalho, R., Santos, G., & Cardoso, R. (2023). End-to-End Solution for Analog Gauge Monitoring Using Computer Vision in an IoT Platform. *Sensors*, 23(24). <https://doi.org/10.3390/s23249858>
- [8] Bonello, A., Francalanza, E., & Refalo, P. (2024). The realities of achieving a Smart, Sustainable, and Inclusive shopfloor in the age of Industry 5.0. *Procedia Computer Science*, 232. <https://doi.org/10.1016/j.procs.2024.02.059>
- [9] Krasavina, V., Platonovskiy, N., & Ibiev, G. (2023). Agile as a wave of digital transformation. *E3S Web of Conferences*, 389. <https://doi.org/10.1051/e3sconf/202338907018>
- [10] Fan, X., Wang, Y., & Lu, X. (2023). Digital Transformation Drives Sustainable Innovation Capability Improvement in Manufacturing Enterprises: Based on FsQCA and NCA Approaches. *Sustainability* (Switzerland), 15(1). <https://doi.org/10.3390/su15010542>
- [11] Rahman, A., Islam, M., Band, S., Muhammad, G., Hasan, K., & Tiwari, P. (2023). Towards a blockchain-SDN-based secure architecture for cloud computing in smart industrial IoT. *Digital Communications and Networks*, 9(2). <https://doi.org/10.1016/j.dcan.2022.11.003>
- [12] Zhao, M., Shi, C., & Yuan, Y. (2023). Blockchain-Based Lightweight Authentication Mechanisms for Industrial Internet of Things and Information Systems. *International Journal on Semantic Web and Information Systems*, 20(1). <https://doi.org/10.4018/IJSWIS.334704>
- [13] Sreevidya, B., & Supriya, M. (2024). Malicious Nodes Detection and Avoidance Using Trust-based Routing in Critical Data Handling Wireless Sensor Network Applications. *Journal of Internet Services and Information Security*, 14(3). <https://doi.org/10.58346/JISIS.2024.I3.013>
- [14] Wu, Y., Wu, L., & Cai, H. (2023). Cloud-edge data encryption in the internet of vehicles using Zeckendorf representation. *Journal of Cloud Computing*, 12(1). <https://doi.org/10.1186/s13677-023-00417-7>
- [15] Fan, H., Huang, C., & Liu, Y. (2023). Federated Learning-Based Privacy-Preserving Data Aggregation Scheme for IIoT. *IEEE Access*, 11. <https://doi.org/10.1109/ACCESS.2022.3226245>
- [16] Rajendran, T., Thavasimuthu, R., John, J., Maria Arockia Dass, J., Nithya, T., & Thavasimuthu, A. (2024). Design and Implementation of a Car's Black Box System using Arduino. *International Research Journal of Multidisciplinary Technovation*, 6(3). <https://doi.org/10.54392/irjmt24320>
- [17] Hiremath, S., Shetty, E., Prakash, A., Sahoo, S., Patro, K., & Rajesh, K. (2023). A New Approach to Data Analysis Using Machine Learning for Cybersecurity. *Big Data and Cognitive Computing*, 7(4). <https://doi.org/10.3390/bdcc7040176>
- [18] Chirumalla, K., Ali Jalil, H., & Behnam, M. (2024). Navigating Production Automation as a Service: Unveiling Drivers, Benefits, and Challenges in Manufacturing Companies. *Advances in Transdisciplinary Engineering*, 52. <https://doi.org/10.3233/ATDE240166>
- [19] Ilkevich, S. (2024). Sustainable and resilient strategies for entering international markets for Russian manufacturing companies based on digital platform interactions. *E3S Web of Conferences*, 531. <https://doi.org/10.1051/e3sconf/202453105007>
- [20] Li, M., Liu, J., & Yang, Y. (2024). Automated Identification of Sensitive Financial Data Based on the Topic Analysis. *Future Internet*, 16(2). <https://doi.org/10.3390/fi16020055>
- [21] Xue, J. (2024). Application of Hierarchical Protection Security Mechanism in Database to Party Building in Colleges and Universities. *Applied Mathematics and Nonlinear Sciences*, 9(1). <https://doi.org/10.2478/amns-2024-1567>
- [22] Kostakis, V., Pazaitis, A., & Liarokapis, M. (2023). Beyond high-tech versus low-tech: A tentative framework for sustainable urban data governance. *Big Data and Society*, 10(1). <https://doi.org/10.1177/20539517231180583>

- [23] Verma, R., Kumari, A., Anand, A., & Yadavalli, V. (2024). Revisiting Shift Cipher Technique for Amplified Data Security. *Journal of Computational and Cognitive Engineering*, 3(1). <https://doi.org/10.47852/bonviewJCCE2202261>
- [24] Liu, L., Ma, Z., Zhou, Y., Fan, M., & Han, M. (2024). Trust in ESG reporting: The intelligent Veri-Green solution for incentivized verification. *Blockchain: Research and Applications*, 5(2). <https://doi.org/10.1016/j.bcra.2024.100189>
- [25] Mathew, N., Svanberg, M., Sjöholm, J., & Johansson, B. (2023). Digitalization for flexible and resilient production planning and scheduling in engineer-to-order manufacturing. *Procedia CIRP*, 120. <https://doi.org/10.1016/j.procir.2023.09.084>
- [26] Pienta, A., Jang, J., & Levenstein, M. (2023). Beyond Legal Frameworks and Security Controls for Accessing Confidential Survey Data in the United States: Engaging Data Users in Data Protection. *Journal of Privacy and Confidentiality*, 13(2). <https://doi.org/10.29012/jpc.845>
- [27] AlShalaan, M., & Fati, S. (2023). Enhancing Organizational Data Security on Employee-Connected Devices Using BYOD Policy. *Information (Switzerland)*, 14(5). <https://doi.org/10.3390/info14050275>
- [28] Tufan, C., Çiğdem, Ş., Kılıç, Y., & Sayar, G. (2024). Agility and Resilience in Supply Chains: Investigating Their Roles in Enhancing Financial Performance. *Sustainability (Switzerland)*, 16(17). <https://doi.org/10.3390/su16177842>
- [29] Oliveira, M., Chauhan, S., Pereira, F., Felgueiras, C., & Carvalho, D. (2023). Blockchain Protocols and Edge Computing Targeting Industry 5.0 Needs. *Sensors*, 23(22). <https://doi.org/10.3390/s23229174>
- [30] Hien, D., Duc, M., & Tuan, T. (2024). Integrating Six Sigma into an Industry 4.0 System for Enhanced Productivity: A Case Study in CNC Processes. *Management and Production Engineering Review*, 15(1). <https://doi.org/10.24425/mper.2024.149989>
- [31] Vidhya, S., Raja, P., & Sumithra, R. (2024). Blockchain-Enabled Decentralized Healthcare Data Exchange: Leveraging Novel Encryption Scheme, Smart Contracts, and Ring Signatures for Enhanced Data Security and Patient Privacy. *International Journal of Network Management*. <https://doi.org/10.1002/nem.2289>
- [32] Zhang, F., Huang, Z., Kou, L., Li, Y., Cao, M., & Ma, F. (2023). Data encryption based on a 9D complex chaotic system with quaternion for smart grid. *Chinese Physics B*, 32(1). <https://doi.org/10.1088/1674-1056/ac76b2>
- [33] Zhao, T., Gasiba, T., Lechner, U., & Pinto-Albuquerque, M. (2024). Thriving in the era of hybrid work: Raising cybersecurity awareness using serious games in industry trainings. *Journal of Systems and Software*, 210. <https://doi.org/10.1016/j.jss.2023.111946>
- [34] Awadh, W., Hashim, M., & Alasady, A. (2024). Implementing the Triple-Data Encryption Standard for Secure and Efficient Healthcare Data Storage in Cloud Computing Environments. *Informatica (Slovenia)*, 48(6). <https://doi.org/10.31449/inf.v48i6.5641>
- [35] Tazi, F., Nandakumar, A., Dykstra, J., Rajivan, P., & Das, S. (2024). SoK: Analyzing Privacy and Security of Healthcare Data from the User Perspective. *ACM Transactions on Computing for Healthcare*, 5(2). <https://doi.org/10.1145/3650116>
- [36] Hetmanczyk, M. (2024). A Method to Evaluate the Maturity Level of Robotization of Production Processes in the Context of Digital Transformation—Polish Case Study. *Applied Sciences (Switzerland)*, 14(13). <https://doi.org/10.3390/app14135401>
- [37] Farid, G., Warraich, N., & Iftikhar, S. (2023). Digital information security management policy in academic libraries: A systematic review (2010–2022). *Journal of Information Science*. <https://doi.org/10.1177/01655515231160026>