ANALISIS DE RIESGOS Y MITIGACION EN LA CADENA DE SUMINISTRO GLOBAL

RISK ANALYSIS AND MITIGATION IN THE GLOBAL SUPPLY CHAIN

Alfredo Rufino Del Rio Villamayor
Universidad de la Integración de las Américas
Facultad de Educación a Distancia y Semipresencial
adelrionicole@gmail.com

Rubén Juan José Benítez Aquino
Universidad de la Integración de las Américas
Facultad de Educación a Distancia y Semipresencial
rubenbenitez11@gmail.com

Alicia Beatriz Morales de Irala
Universidad de la Integración de las Américas
Facultad de Educación a Distancia y Semipresencial
pichimorales@gmail.com

RESUMEN

El análisis de riesgos en la cadena de suministro global y la ciberseguridad desde el punto de las innovaciones tecnológicas ha impulsado una modernización profunda en los distintos sectores productivos, pero a su vez la falta de visibilidad y supervisión de los niveles de seguridad, expone a las organizaciones a riesgos informáticos, que comprometen la continuidad operativa e integridad de los datos, la ciberseguridad pasa a ser un mecanismo esencial para garantizar bases confiables, resilientes y acorde con los objetivos del desarrollo sostenible. El presente artículo analiza la relación existente entre el objetivo de desarrollo sostenible 9, que promueve la innovación, el desarrollo industrial y la construcción de infraestructuras seguras y sostenibles. La metodología que se utiliza está basada en revisiones documentales de investigaciones académicas, informes anuales de riegos globales y guías técnicas de organismos de ciberseguridad, con el propósito de identificar amenazas, vulnerabilidades, filtraciones de datos, manipulación de programas informáticos e interrupciones operativas. Los resultados denotan un incremento sostenido de ataques dirigidos principalmente a instituciones gubernamentales, telecomunicaciones, salud y finanzas, que evidencian la necesidad de adoptar medidas preventivas más seguras. Se observa además la utilización de herramientas avanzadas, como ser la inteligencia artificial, análisis de comportamiento, automatización de respuestas y sistemas basados en

tecnologías de registro digital descentralizado e inmutable. Finalmente, al adoptar políticas públicas eficaces, inversiones en tecnología, capacitación continua, mejorar la capacidad regional y cooperación institucional, serán necesarias para fortalecer la resiliencia digital y contribuir de manera directa al cumplimiento de los objetivos de desarrollo sostenible 9.
PALABRAS CLAVES: Análisis de riesgos, ciberseguridad, infraestructura digital, resiliencia, sostenibilidad.

ABSTRACT

Risk analysis in the global supply chain and cybersecurity, from the perspective of technological innovations, has driven profound modernization across various productive sectors. However, the lack of visibility and oversight of security levels exposes organizations to cyber risks that compromise operational continuity and data integrity. Cybersecurity has become an essential mechanism for ensuring reliable and resilient foundations aligned with the Sustainable Development Goals. This article analyzes the relationship between Sustainable Development Goal 9, which promotes innovation, industrial development, and the construction of secure and sustainable infrastructure. The methodology employed is based on reviews of academic research, annual global risk reports, and technical guidelines from cybersecurity organizations, with the aim of identifying threats, vulnerabilities, data breaches, software manipulation, and operational disruptions. The results indicate a sustained increase in attacks primarily targeting government institutions, telecommunications, healthcare, and finance, highlighting the need for more robust preventative measures. The use of advanced tools is also observed, such as artificial intelligence, behavioral analysis, automated responses, and systems based on decentralized and immutable digital record technologies. Finally, adopting effective public policies, investing in technology, providing ongoing training, improving regional capacity, and fostering institutional cooperation will be necessary to strengthen digital resilience and contribute directly to achieving Sustainable Development Goal 9.
KEYWORDS: Cybersecurity, digital infrastructure, resilience, risk analysis, sustainability.

INTRODUCCIÓN

La digitalización de los procesos productivos y la incorporación de tecnologías emergentes han transformado profundamente la actividad industrial, generando mayores niveles de eficiencia, innovación y competitividad. Este cambio ha impulsado nuevas formas de producción y gestión, mejorando la capacidad de respuesta de las empresas frente a los retos del mercado global.

Sin embargo, este avance también ha incrementado la vulnerabilidad frente a amenazas cibernéticas que afectan la estabilidad, confiabilidad y continuidad de infraestructuras críticas. Diversos estudios y reportes internacionales señalan un crecimiento sostenido de los ataques dirigidos a sectores estratégicos como energía, transporte, salud, comunicaciones y finanzas, lo que evidencia la necesidad de fortalecer las capacidades de protección digital a nivel institucional y regional.

En este escenario, la ciberseguridad se posiciona como un componente esencial para el cumplimiento del Objetivo de Desarrollo Sostenible 9 (ODS 9), orientado a promover el desarrollo industrial, la innovación y la consolidación de infraestructuras resilientes. Por este motivo, el presente estudio tiene como objetivo analizar el papel de la ciberseguridad en el marco del ODS 9, identificando las amenazas predominantes, las metodologías aplicadas y las soluciones tecnológicas emergentes que contribuyen a mejorar la resiliencia digital.

La revisión de antecedentes científicos y técnicos evidencia que la investigación en ciberseguridad ha experimentado un crecimiento significativo en los últimos años, destacando enfoques basados en inteligencia artificial, automatización y análisis de comportamiento. Estos avances permiten anticipar ataques, mejorar la detección de vulnerabilidad y optimizar la respuesta ante incidentes cibernéticos.

En coherencia con este estado de la investigación, el presente trabajo tiene como objetivo analizar el papel de la ciberseguridad en el marco del ODS 9, identificando las amenazas predominantes, las metodologías aplicadas y las soluciones tecnológicas emergentes que contribuyen a mejorar la resiliencia digital. Se busca aportar una reflexión integral sobre la importancia de la ciberseguridad para garantizar infraestructuras seguras, sostenibles y adaptadas a los desafíos actuales de la transformación digital.

MATERIALES Y METODOLOGÍA

La presente investigación adopta un enfoque cualitativo, adecuado para analizar fenómenos complejos como los riesgos inherentes a la cadena de suministro global y las amenazas asociadas a la ciberseguridad. Este enfoque permite interpretar información proveniente de documentos técnicos, estudios científicos, informes internacionales y marcos normativos relacionados con el ODS 9, que promueve el desarrollo de infraestructuras resilientes, la industrialización sostenible y la innovación.

El análisis cualitativo ayuda a identificar patrones, relaciones causa y efecto, así como vulnerabilidades y estrategias de mitigación que se aplican en diferentes contextos. Para ello, se revisan diversas fuentes confiables, lo que nos permite construir una visión clara de los desafíos y soluciones en la ciberseguridad aplicada a la industria y la cadena de suministro global.

El estudio se desarrolla bajo una investigación documental, basada en la recolección, revisión, análisis e interpretación de información existente en diversas fuentes. Cada paso se realizó de forma ordenada para garantizar que los hallazgos fueran claros y confiables, sin perder la perspectiva del objetivo principal de la investigación.

Este tipo de diseño es pertinente dado que el fenómeno estudiado riesgos en cadenas de suministro globales y ciberseguridad cuenta con extensa evidencia técnica y científica presente en varias en publicaciones especializadas y documentos de organismos internacionales. La delimitación, se centra en el periodo comprendido del 2015 – 2025, considerando los avances recientes en digitalización y ciberseguridad.

Fuentes primarias documentales

- Informes del Programa de las Naciones Unidas para el Desarrollo (PNUD) y del sistema ONU sobre el avance del ODS 9.
- Informes del World Economic Forum sobre riesgos globales y vulnerabilidades en cadenas de suministro.
- Normas internacionales en gestión de riesgos y seguridad de la información (ISO 31000, ISO 28000, ISO 27001, NIST Cybersecurity Framework).
- Estudios y reportes de consultoras especializadas en logística, transporte y resiliencia (Gartner, DHL Insights).

Fuentes secundarias

- Artículos científicos de bases de datos como Scopus, Scielo, IEEE Xplore y Google Scholar.
- Libros académicos sobre logística internacional, continuidad operativa y seguridad informática.
- Documentos institucionales y reportes de centros de investigación en innovación e infraestructura.

La búsqueda sistemática de información, se enfocó en la selección de palabras claves como riesgo de la cadena de suministro global, ciberseguridad, resiliencia, infraestructura crítica, ODS 9, Industria 4.0, mitigación de riesgos. Se aplicaron criterios de inclusión de actualidad, relevancia temática, base científica, confiabilidad institucional y la depuración de documentos irrelevantes o redundantes.

Para realizar la organización y clasificación, los documentos se agruparon según tres ejes analíticos: riesgos en la cadena de suministro global, amenazas de ciberseguridad, su impacto en la infraestructura y el Objetivo de Desarrollo Sostenible 9 (ODS 9) enfocado en industria, innovación e infraestructura resiliente. Este proceso implicó la elaboración de fichas de contenido y la categorización conceptual.

Para la síntesis y elaboración de resultados, se llevaron a cabo varias acciones clave: se sistematizaron los hallazgos principales; se construyeron tablas descriptivas de riesgos y estrategias de mitigación; y se elaboraron conclusiones orientadas al fortalecimiento de infraestructuras resilientes conforme al ODS 9.

Al tratarse de una investigación de tipo documental, no se interactúa directamente con personas. No obstante, se adoptó un compromiso con la ética académica, lo que garantiza la correcta citación de todos los autores, el uso de fuentes confiables, la prevención del plagio y el respeto a los derechos de propiedad intelectual.

RESULTADOS

Los resultados obtenidos a partir del análisis documental cualitativo permiten identificar tendencias globales, vulnerabilidades recurrentes y estrategias emergentes de mitigación frente a los riesgos que afectan a la cadena de suministro. La evidencia revisada revela una creciente interdependencia entre los riesgos logísticos tradicionales y los riesgos cibernéticos, así como la necesidad de fortalecer infraestructuras resilientes conforme a los

principios del ODS 9.

Del análisis de informes internacionales, artículos científicos y marcos normativos, emergieron cinco categorías principales de riesgos identificados en la cadena de suministro global: riesgos disruptivos y geopolíticos, riesgos operativos, riesgos tecnológicos, riesgos de ciberseguridad y riesgos de sostenibilidad e infraestructura. Estos factores, que se han vuelto más frecuentes e intensos, subrayan la fragilidad inherente a las cadenas de suministro modernas y la necesidad de una gestión proactiva.

Riesgos disruptivos y geopolíticos: Se identificaron eventos como conflictos geopolíticos, restricciones comerciales, crisis sanitarias y fenómenos climáticos extremos, que generan interrupciones críticas en las cadenas de suministro. Estos riesgos muestran un aumento en frecuencia e intensidad, afectando la disponibilidad de materias primas, el transporte y la logística internacional.

Riesgos operativos: Esta categoría incluye las fallas en procesos internos, el incumplimiento por parte de los proveedores, problemas de transporte, baja visibilidad logística y deficiencias en la gestión de inventarios. Los estudios revisados evidencian que la dependencia de múltiples actores globales incrementa significativamente el impacto de fallas que, en un sistema menos interconectado, serían aisladas.

Riesgos tecnológicos: La digitalización acelerada introduce riesgos inherentes a las fallas de sistemas, la excesiva dependencia de plataformas de gestión de terceros y los errores en los procesos de automatización. Además, surgen vulnerabilidades específicas en la implementación de tecnologías de Internet de las Cosas (IoT) y la Industria 4.0, lo cual requiere una gestión de riesgos de ciberseguridad más robusta.

Riesgos de ciberseguridad: La información recopilada muestra una tendencia creciente de ataques dirigidos a proveedores, operadores logísticos y plataformas de gestión de la cadena de suministro. Entre los riesgos más frecuentes se identifican: ransomware, intrusiones en sistemas de planificación (ERP, WMS), manipulación de datos, ataques a infraestructuras críticas de transporte. Los ataques a proveedores de programas informáticos o servicios representan un punto débil sistémico, pues su impacto se multiplica en toda la red de suministro.

Riesgos de sostenibilidad e infraestructura: alineado con el Objetivo de Desarrollo

Sostenible 9 (ODS 9), se identificaron vulnerabilidades críticas en las cadenas de suministro. Estas vulnerabilidades están directamente relacionadas con la presencia de infraestructura industrial obsoleta y la persistente baja inversión en innovación tecnológica. Además, representan riesgos significativos la insuficiente resiliencia de las infraestructuras físicas ante desastres naturales y la inestabilidad de las redes digitales que soportan la logística global.

Los descubrimientos sobre ciberseguridad en la cadena de suministro y el análisis cualitativo permitieron sintetizar tres patrones centrales: incremento de ataques dirigidos a proveedores, en los materiales consultados coinciden que los ciberataques ya no apuntan solo a las empresas objetivo, sino a sus proveedores con menor nivel de protección. Esto convierte a la cadena de suministro en un blanco preferencial.

Dada la baja madurez observada en las prácticas de seguridad, se identificó una escasa adopción de estándares reconocidos, como la norma ISO 27001, el marco NIST CSF o la implementación de auditorías de ciberseguridad para proveedores. La mayoría de las organizaciones carecen de un enfoque integral de riesgo cibernético que abarque la totalidad de la red de suministro Interdependencia entre sistemas físicos y digitales

La digitalización de la logística (mediante el uso de IoT, sensores, sistemas de trazabilidad, blockchain y monitoreo en tiempo real) aumenta significativamente las eficiencias operativas, pero simultáneamente amplifica los puntos de vulnerabilidad. Como resultado, las interrupciones cibernéticas pueden desencadenar impactos físicos, financieros y operativos de gran magnitud, afectando la integridad de toda la cadena de suministro.

Estrategias de mitigación documentadas

Del análisis de documentos, surgieron diversas estrategias de mitigación integrales. Para los riesgos logísticos y geopolíticos, las estrategias incluyen la diversificación de proveedores mediante regionalización, el incremento de estratégicos y la planificación basada en escenarios. En cuanto a los riesgos operativos, se propone la integración de tecnologías, auditorías de calidad (ISO 9001, ISO 28000) y evaluación continua del desempeño de proveedores.

Para mitigar riesgos tecnológicos, es fundamental la implementación de estándares

de seguridad (ISO 27001, NIST CSF), la segmentación de redes y la evaluación de ciberseguridad de terceros. Las estrategias vinculadas al ODS 9 se centran en la inversión en infraestructura resiliente, la modernización industrial y programas de sostenibilidad que reduzcan vulnerabilidades estructurales.

Los hallazgos demuestran que la resiliencia de las cadenas de suministro es un pilar fundamental para el logro del ODS 9. Se destacan varios puntos cruciales: la infraestructura logística y digital debe fortalecerse para soportar crisis globales; la innovación tecnológica debe ir siempre acompañada de medidas robustas de seguridad cibernética; y la industrialización sostenible requiere cadenas de suministro que sean estables, transparentes y digitalmente seguras. Además, las interrupciones frecuentes afectan la productividad y la competitividad, poniendo en riesgo las metas de desarrollo industrial. La mitigación proactiva de riesgos logísticos y cibernéticos se convierte en una estrategia para avanzar hacia sistemas industriales más sostenibles y resilientes.

Las cadenas de suministro enfrentan riesgos cada vez más complejos, interconectados y globales. La ciberseguridad se ha convertido en un componente crítico de la continuidad operativa. Las estrategias de mitigación deben ser integrales, incluir a toda la red de proveedores y alinearse con los estándares internacionales. Los principios del ODS 9 ofrecen un marco adecuado para orientar políticas y decisiones estratégicas que fortalezcan la resiliencia y la innovación.

DISCUSIÓN

La creciente digitalización de los procesos, aporta eficiencia e innovación, pero a su vez incrementa los ataques y expone a las infraestructuras riesgos cibernéticos cada vez más sofisticados. Esto coincide con lo señalado por el World Economic Forum (2024), que posiciona a los incidentes cibernéticos entre las principales amenazas globales debido a su capacidad de generar interrupciones operativas. Investigaciones como las de Anderson et al. (2023) y Kshetri (2022) refuerzan la tendencia observada en este estudio, al destacar que sectores como salud, finanzas y telecomunicaciones enfrentan un incremento en ataques dirigidos, especialmente los basados en inteligencia artificial y técnicas de ingeniería social avanzadas.

La relación entre ciberseguridad y sostenibilidad, particularmente dentro del marco

del ODS 9, ha ganado relevancia en los últimos años. Autores como Alcaraz y Zeadally (2023) sostienen que la resiliencia digital debe ser considerada un componente esencial de las infraestructuras modernas, postura coherente con las conclusiones preliminares de nuestra investigación. Del mismo modo, estudios regionales como los de CEPAL (2023) enfatizan la necesidad de fortalecer capacidades institucionales en América Latina para evitar brechas de seguridad que puedan comprometer el desarrollo industrial sostenible.

En América Latina, la heterogeneidad de marcos normativos y la limitada inversión en ciberseguridad representan desafíos significativos. Estudios de CEPAL (2023) indican que fortalecer las capacidades institucionales es clave para reducir brechas de seguridad que puedan afectar la continuidad de operaciones estratégicas. Asimismo, ENISA (2023) advierte que la escasez de profesionales capacitados y la baja concienciación en sectores críticos dificultan la implementación de políticas de ciberseguridad efectivas.

La metodología utilizada, basada en revisión documental de literatura científica, informes técnicos y reportes anuales de riesgo, se destaca como principal ventaja su capacidad para integrar perspectivas globales y multidisciplinarias. Esta aproximación permitió identificar tendencias, amenazas recurrentes y enfoques tecnológicos emergentes. Sin embargo, también presenta limitaciones: la rápida evolución de los ciberataques puede dejar obsoleta cierta información en un corto periodo de tiempo, y la falta de acceso a datos internos de organizaciones restringe el análisis de incidentes reales. Otros estudios, como los de Bada, Sasse y Nurse (2019), también señalan estas limitaciones cuando se adoptan metodologías similares.

Entre las principales dificultades identificadas se encuentran la heterogeneidad de marcos normativos entre países, la baja inversión en ciberseguridad en economías emergentes y la escasez de profesionales altamente capacitados, lo cual coincide con los desafíos mencionados por ENISA (2023). Para trabajos futuros, se recomienda profundizar en estudios de caso específicos sobre industrias estratégicas, evaluar la implementación de sistemas basados en blockchain para trazabilidad y seguridad, y analizar el impacto económico de los incidentes cibernéticos en la región. También sería pertinente desarrollar modelos predictivos basados en inteligencia artificial para anticipar amenazas y mejorar las estrategias de mitigación.

CONCLUSIONES

El estudio permitió analizar el papel de la ciberseguridad dentro del marco del ODS 9, demostrando que la protección digital es un componente esencial para garantizar infraestructuras industriales seguras, resilientes y sostenibles. Los resultados confirman un incremento sostenido de ataques dirigidos a sectores estratégicos, lo que pone en evidencia la urgente necesidad de adoptar medidas preventivas más robustas, tanto a nivel institucional como regional.

Las tecnologías emergentes, como inteligencia artificial, análisis de comportamiento, automatización de respuestas y sistemas basados en registros digitales descentralizados, se presentan como herramientas clave para fortalecer la resiliencia digital. No obstante, su implementación efectiva requiere inversiones sostenidas, capacitación continua y una articulación sólida entre organismos públicos, privados y académicos.

En relación con los objetivos planteados, se concluye que:

1. La ciberseguridad es indispensable para el desarrollo industrial moderno y para el cumplimiento del ODS 9, ya que los objetivos de desarrollo sustentable 9, se centran en construir infraestructuras resilientes, promover la industrialización sostenible y fomentar la innovación, elementos que requieren de la ciberseguridad para ser viables y seguros.
2. Las amenazas predominantes incluyen filtración de datos, vulnerabilidades en infraestructuras críticas e interrupciones operativas provocadas por ataques, representan los riesgos cibernéticos más significativos en la actualidad, con un enfoque particular en el impacto en sistemas esenciales.
3. Las metodologías y tecnologías emergentes permiten mejorar significativamente la capacidad de respuesta, aunque aún existen desafíos vinculados a la falta de estandarización, recursos limitados y brechas de talento especializado, que resume con precisión la dualidad del panorama actual de la ciberseguridad, donde los avances coexisten con importantes barreras prácticas.
4. El fortalecimiento de la resiliencia digital depende de políticas públicas eficaces, inversiones estratégicas, cooperación internacional y el desarrollo de capacidades técnicas, estos cuatro pilares son universalmente reconocidos como los componentes esenciales para construir una defensa cibernética robusta y sostenible a nivel nacional e internacional.

De manera general, consideramos que la ciberseguridad se configura como un eje transversal y estratégico fundamental para el progreso tecnológico actual, su importancia radica en la necesidad imperante de consolidar infraestructuras seguras y sostenibles que no solo protejan los datos, sino que también garanticen la continuidad operativa. Esto permite a las organizaciones enfrentar con éxito los desafíos y las amenazas constantes que surgen en el contexto de la transformación digital, asegurando un entorno de confianza para la innovación y el desarrollo.

REFERENCIAS

Alcaraz, C., & Zeadally, S. (2023). Critical infrastructure security in the era of digital transformation. Journal of Cybersecurity, 9(2), 115–129.

Anderson, R., Moore, T., & Murdoch, S. (2023). Cybersecurity risks and long- term trends in global threat landscapes. Computers & Security, 134, 103– 124.

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail? IEEE Security & Privacy, 17(2), 32–41.

CEPAL. (2023). Transformación digital y ciberseguridad en América Latina: retos y oportunidades. Naciones Unidas.

ENISA. (2023). Threat Landscape Report 2023. European Union Agency for Cybersecurity.

Kshetri, N. (2022). Cybersecurity for Industry 4.0: Challenges and Emerging Solutions. Journal of Industrial Information Integration, 27, 1–12.

World Economic Forum. (2024). Global Risks Report 2024. WEF.

Masip-Bruin, X., Marín-Tordera, E., Ruiz, J., Jukan, A., Trakadas, P., Cernivec, A., … Kalogiannis, G. (2021). Cybersecurity in ICT Supply Chains: Key Challenges and a Relevant Architecture. Sensors, 21(18), 6057. https://doi.org/10.3390/s21186057 MDPI.

Uribe, S. C., & Salazar Medina, N. F. (2022). Enfoque de riesgos en la gestión de la cadena de suministros en el sector industrial. Ingeniería Industrial, (?), (?)… (el artículo tiene DOI).

Identificación de riesgos en las cadenas de suministro de la industria automotriz: una revisión de literatura. (2023). Entre ciencias: Diálogos en la Sociedad del Conocimiento, 11(25).

Gestión del riesgo cibernético en cadenas de suministro: a través de proveedores.

OECD. (2024). Promoting resilience and preparedness in supply chains. OECD Trade Policy Paper No. 286.