

Análisis de la resiliencia en la cadena de suministro ante ataques cibernéticos en empresas del sector logístico y de transporte

Nombres y apellidos

Ximena Patricia Mercado Manotas
Yimmy Armando Santos Rosales

Código estudiantil:

201911611101
201921417745

Trabajo de Investigación presentado como requisito para optar el título de:
Especialista en Logística de Operaciones

Tutor(es):

Leidy Pérez Coronell
David Martínez Sierra

RESUMEN

La digitalización de los procesos logísticos ha mejorado la eficiencia de las cadenas de suministro, pero también ha incrementado su exposición a amenazas cibernéticas. Este artículo analiza la resiliencia operativa de las organizaciones del sector logístico y de transporte frente a ciberataques, con el objetivo de identificar herramientas tecnológicas efectivas para mitigar estos riesgos. A través de un estudio cuantitativo basado en escenarios simulados, se evaluaron variables clave como la frecuencia de ataques, el tiempo medio de recuperación y el porcentaje de afectación operativa, estableciendo su relación con el índice de resiliencia. Los resultados muestran que, si bien las herramientas tradicionales (firewalls, antivirus, SIEM, VPN) ofrecen cierto nivel de protección, su enfoque es mayoritariamente reactivo. En contraste, la adopción de soluciones basadas en Inteligencia Artificial y Blockchain permite anticiparse a las amenazas, reducir tiempos de respuesta y garantizar una mayor integridad en la gestión de datos. Se concluye que una estrategia de ciberseguridad integral, que combine tecnología avanzada, protocolos de respuesta, formación continua y colaboración con proveedores, es fundamental para fortalecer la resiliencia de la cadena de suministro en un entorno digital cada vez más complejo y vulnerable.

Palabras clave: Ciberseguridad, cadena de suministro, resiliencia operativa, inteligencia artificial, blockchain, logística.

ABSTRACT

The digitalization of logistics processes has improved supply chain efficiency but has also increased exposure to cyber threats. This article analyzes the operational resilience of logistics and transportation organizations facing cyberattacks, aiming to identify effective technological tools to mitigate these risks. Through a quantitative study based on simulated scenarios, key variables such as attack frequency, mean recovery time, and operational disruption percentage were evaluated to determine their relationship with the resilience index. The results indicate that, although traditional tools (firewalls, antivirus, SIEM, VPN) provide a basic level of protection, their approach is mainly reactive. In contrast, the implementation of Artificial Intelligence and Blockchain-based solutions enables threat anticipation, faster response times, and greater data integrity. The study concludes that a comprehensive cybersecurity strategy—integrating advanced technology, incident response protocols, continuous training, and supplier collaboration—is essential to strengthen supply chain resilience in an increasingly complex and vulnerable digital environment.

Key Words: Cybersecurity, supply chain, operational resilience, artificial intelligence, blockchain, logistics.

REFERENCIAS BIBLIOGRÁFICAS

1. Aguilar-Antonio, J. M. (2019). Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad. *URVIO Revista Latinoamericana de Estudios de Seguridad*, 24-40.
2. Ahmed, A., & Abdullah, A. (2024). arXiv. Obtenido de <http://arxiv.org/abs/2407.13785><https://arxiv.org/abs/2407.13785>
3. Arias-Vargas, M., Sanchís, R., & Poler, R. (2023). Potenciación de la resiliencia en empresas y cadenas de suministro a través de la inteligencia artificial: una revisión de la literatura reciente. *Dirección y organización*, 13-29.
4. Betul, G., Leonardo, A., & Basel, H. (2023). Software supply chain: review of attacks, risk assessment strategies and security controls. Obtenido de <http://arxiv.org/abs/2305.14157><https://arxiv.org/abs/2305.14157>
5. Bytemaster. (02 de 2025). Ciberseguridad en logística. Obtenido de Ciberseguridad en logística.: <https://www.bytemaster.es/en/servicios-cloud/ciberseguridad-logistica-2/>
6. Cano, F. (2022). The role of cybersecurity in logistics operations. *Journal of Supply Chain Security*, 45-58.
7. Cano, J. (2022). La cadena de suministro digital. *Revista Sistemas*, 53-63.
8. Cheung, K. F. (2021). Cybersecurity in logistics and supply chain management: An overview and future research directions. *Transportation Research Part E: Logistics and Transportation Review*. 146.
9. Cheung, M. L. (2021). Cybersecurity resilience in supply chain management: Challenges and strategies. *International Journal of Logistics Management*, 103-120.
10. Fortinet. (2024). State of Operational Technology and Cybersecurity Report.
11. Globaltranz. (01 de 2025). Obtenido de Globaltranz: <https://www.globaltranz.com/company/>
12. Jhanjhi, N. Z. (2024). AI and machine learning for cybersecurity in supply chains. *Journal of Advanced Technology in Logistics*, 77-91.
13. Jhanjhi, N. Z. (2024). Cybersecurity Measures for Logistics Industry Framework. Igi Global.
14. Kevin Hu, R. L. (2022). Supply Chain Characteristics as Predictors of Cyber Risk: A Machine-Learning Assessment. Obtenido de arXiv: arXiv [q-fin.RM]. <http://arxiv.org/abs/2210.15785>
15. Kumar, S. &. (2024). Cybersecurity frameworks for supply chain resilience. *Journal of Cybersecurity Policy*, 150-163.
16. Ludvigsen, K. R., Nagaraja, S., & Daly, A. (2022). Preventing or mitigating adversarial supply chain attacks: A legal analysis. *ACM*.
17. Mohamed, A. S., Lee, S., & Kundur, D. (2023). Reinforcement learning for supply chain attacks against frequency and voltage control. (págs. 369-375). *IEEE*.
18. Moveris. (09 de 12 de 2024). ¿Qué es la ciberseguridad y cómo se aplica en la logística? Obtenido de ¿Qué es la ciberseguridad y cómo se aplica en la logística?: <https://www.moveris.com/blog/que-es-la-ciberseguridad-y-como-se-aplica-en-la-logistica>

19. Odimarha, A. C. (2024). Securing the digital supply chain: Cybersecurity best practices for logistics and shipping companies. *World Journal of Advanced Science and Technology*, 5(1).
20. Odimarha, F. O. (2024). Logistics, supply chain cybersecurity, and operational resilience. *International Journal of Cybersecurity*, 44-59.
21. Radanliev, P., De Roure, D., Page, K., Nurse, J. R., Mantilla Montalvo, R., Santos, O., . . . Burnap, P. (2020). Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains. *Cybersecurity*.
22. Silva, J. D. (2017). Gestión de la cadena de suministro: una revisión desde la logística y el medio ambiente. *Entre Ciencia e Ingeniería*, 51-59.
23. Smith, R. &. (2023). The importance of cybersecurity collaboration in logistics supply chains. *Journal of Transport and Logistics*, 202-212.
24. Treiblmaier, H., & Rejeb, A. (2023). Exploring blockchain for disaster prevention and relief: A comprehensive framework based on industry case studies. *Journal of business logistics*, 550-582.
25. Urciuoli, L. (20 de 10 de 2022). La ciberseguridad en la cadena de suministro, una tendencia al alza. Obtenido de La ciberseguridad en la cadena de suministro, una tendencia al alza.: <https://www.mecalux.com.mx/articulos-de-logistica/luca-urciuoli-ciberseguridad-cadena-suministro>
26. Urrea, D. I. (3 de 12 de 2024). "El error humano sigue siendo la principal puerta de entrada de los ciberataques" ¿Cuántos recibió Colombia en 2024? "El error humano sigue siendo la principal puerta de entrada de los ciberataques" ¿Cuántos recibió Colombia en 2024? Obtenido de Enter.co: <https://www.enter.co/empresas/seguridad/el-error-humano-sigue-siendo-la-principal-puerta-de-entrada-de-los-ciberataques-cuantos-recibio-colombia-en-2024/>
27. Vargas, J. (05 de 12 de 2024). Ciberataques en Colombia: 36 mil millones de intentos registrados en el 2024. Obtenido de Xataka: <https://www.xataka.com.co/seguridad/ciberataques-colombia-36-mil-millones-intentos-registrados-2024>