

Cadena de suministro digital

DOI: 10.29236/sistemas.n164a1



La nueva frontera de la resiliencia de las empresas

Jeimy J. Cano M.

En un contexto acelerado de cambios e inestabilidades globales, la cadena de suministro entra en un proceso de transformación digital expuesta a diferentes tensiones internacionales que pueden ocasionar eventos inusuales e inespera-

dos. Por tanto, es necesario desarrollar capacidades para asumir los retos de un nuevo entorno digital que exige una postura de resiliencia de la cadena de suministro digital entre las empresas y sus terceros de confianza.

La incorporación de las tecnologías emergentes y disruptivas en el escenario de la cadena de suministro, establece un nuevo avance de las empresas de logística y transporte global, como quiera que hoy forman parte del nuevo ecosistema digital global, para articular a todos los actores claves, de manera que los productos y servicios se entreguen al cliente final en tiempo y forma adecuados.

En este contexto, la Cadena de Suministro Digital (CSD) como nuevo jugador visible y relevante para la dinámica de las empresas y naciones en el contexto digital juega un papel fundamental como habilitador de posibilidades, servicios o productos que terminan apalancando nuevas oportunidades para las organizaciones y sus negocios, cambiando la forma tradicional de las operaciones logísticas globales.

Como indica un informe de McKinsey (Alicke et al., 2016) sobre la cadena de suministro 4.0, “La digitalización de la cadena de suministro habilita a las empresas a hacer frente a las nuevas exigencias de los clientes, a los retos del lado de la oferta y a las expectativas de mejora de la eficiencia”.

Así las cosas, ya no es suficiente mantenerse informado y consciente de las volatilidades económicas y geopolíticas globales, es necesario cambiar los normales de la cadena de suministro global sa-

biendo que con la incorporación de nuevas tecnologías emergentes y disruptivas las exigencias estarán marcadas por:

- *Más rapidez* basada en enfoques avanzados de pronóstico, como el análisis predictivo de datos internos (por ejemplo, la demanda) y externos (por ejemplo, las tendencias del mercado, el tiempo, las vacaciones escolares, los índices de construcción), lo que proporciona una previsión mucho más precisa de la demanda de los clientes.
- *Más flexibilidad* a través de la planificación ad hoc y en tiempo real para reaccionar con elasticidad a los cambios en la demanda o en la oferta.
- *Más granularidad* para la generación de productos cada vez más individualizados, lo que da fuerte impulso a la microsegmentación y las ideas de personalización masiva en la práctica.
- *Más precisión* en términos de transparencia de las operaciones en tiempo real de principio a fin en toda la cadena.
- *Más eficiencia* basada en la automatización de las tareas físicas como de planificación de las operaciones (Alicke et al., 2016).

Es por esto que las cadenas de suministro digital, como nuevo agente

disruptivo de la logística internacional, se consolida como el horizonte y reto global, que exige a las naciones, empresas e individuos reconocer y comprender las interdependencias e interacciones en este nuevo escenario, así como sus riesgos inherentes entre los cuales están: (Roar Nygård & Katsikas, 2022)

- Infección por malware
- Ingeniería social
- Ataques de fuerza bruta
- Explotación de vulnerabilidad de software
- Explotación de deficientes configuraciones
- Ataques o modificaciones físicas
- Inteligencia de fuentes abiertas
- Falsificación de documentos o dispositivos tecnológicos

De ahí que esta edición de la revista *Sistemas*, de la Asociación Colombiana de Ingenieros de Sistemas –ACIS–, apunte a revisar, explorar y analizar los retos y oportunidades de la cadena de suministro digital, con el fin de traer al escenario actual diferentes posturas sobre el tema, como insumo para plantear alternativas y opciones en un entorno inestable como el actual. Con ese propósito fueron convo-

cados profesionales especialistas, quienes desde su experiencia proponen reflexiones para seguirle la pista al desarrollo de las tendencias y prácticas vigentes de esta temática, capitalizando lecciones aprendidas, repensando las dinámicas de los negocios y retos actuales, así como al futuro que se avizora en el horizonte.

Juan Mario Posada, columnista invitado, señala varios asuntos relacionados con la protección e indica que, para gestionar las crecientes amenazas inherentes al entorno de negocios, las organizaciones necesitan integrar los principios de seguridad en toda la red de la cadena de suministro.

En la entrevista, el ingeniero Carlos Bermúdez, director de Ciberseguridad de Servientrega–Centro de Soluciones, comparte sus reflexiones sobre los retos actuales en la cadena de suministro digital y cómo la empresa para la cual trabaja está afrontando estos desafíos fundamentales para la transformación de la compañía y su negocio, visto desde la perspectiva de la resiliencia cibernética para las empresas del sector logístico y transporte.

Por su parte, los ingenieros Andrés Almanza y Jeimy Cano presentan el análisis de diferentes reportes internacionales en materia de la cadena de suministro y su transformación digital, con el fin de establecer las tendencias y retos que se advierten para este sector, particu-

larmente para América Latina, donde las buenas prácticas, el apoyo a las pymes, la automatización de proceso y las políticas públicas se posicionan como temas relevantes y claves para este sector.

El foro de esta revista fue un espacio para compartir visiones desde diferentes ángulos sobre la cadena de suministro digital. La abogada Liliana Patricia Quiñonez García, secretaria general de la Federación Colombiana de Agentes Logísticos en Comercio Internacional, FITAC y los ingenieros Juan Mario Posada Daza, líder de Ciberseguridad de Accenture, Colombia y Emilio Alberto Oropeza Zurita, *Security Engineer Manager* de una empresa en México, desarrollaron un diálogo abierto y nutrido para contrastar y complementar sus posturas desde la vista de un gremio, la práctica de consultoría y un contraste internacional del tema.

Ellos advierten sobre la necesidad de reconocer la cadena de suministro digital como una infraestructura crítica de las naciones, mantener una postura vigilante frente a los cambios e inestabilidades globales que afectan directamente las operaciones de este sector y reconocer la vista sistémica que la cadena de suministro representa para todas las industrias.

Así mismo, nuestros lectores dispondrán de dos artículos para reflexionar sobre la cadena de suministro digital en dos visiones concep-

tuales y prácticas basados en su automatización y operación, así como desde la perspectiva del riesgo cibernético. En un primer documento este servidor, se ocupa del riesgo cibernético en la CSD y sus diferentes escenarios de operación para alcanzar una postura resiliente frente a la materialización de eventos cibernéticos.

En el segundo artículo la ingeniera Fabiola Pinzón Hoyos, Coordinadora Académica y de Investigaciones de la Maestría en Gestión de Redes de Valor y Logística de la Universidad Piloto de Colombia, presenta un resumen de una investigación realizada sobre la gestión de redes de suministro digitales, centrada en el sector comercio, basada en las siguientes categorías: conectividad con clientes, integración interna, conectividad con proveedores, nivel de preparación para iniciar la evolución de las Cadenas de Suministro a Redes de Suministro y de éstas a Redes de Suministro Digitales, sostenibles e inclusivas.

En resumen, se trata de un panorama renovado de nuevas transformaciones, retos y propuestas en la cadena de suministro digital, que tensionan las certezas y prácticas existentes en el comercio exterior y logística nacional e internacional. Su contenido invita a todos los profesionales en las diferentes áreas del saber a explorar las nuevas realidades de un mundo digital, en los que la CSD, revela nuevas incerti-

dumbres y potencia el desarrollo de capacidades de negocio inexistentes, de cara a los riesgos emergentes que aún no aparecen en sus mapas estratégicos.

Referencias

Alicke, K., Rachor, J. & Seyfert, A. (2016). Supply Chain 4.0 – the next-generation digital supply chain. McKinsey Insights.

<https://www.mckinsey.com/capabilities/operations/our-insights/supply-chain-40--the-next-generation-digital-supply-chain>

Roar Nygård, A. & Katsikas, S. (2022). SoK: Combating threats in the digital supply chain. *ARES '22: Proceedings of the 17th International Conference on Availability, Reliability and Security*. 1-8.
<https://doi.org/10.1145/3538969.3544421>

Jeimy J. Cano M., Ph.D, CFE, CICA. Ingeniero y Magíster en Ingeniería de Sistemas y Computación por la Universidad de los Andes. Especialista en Derecho Disciplinario por la Universidad Externado de Colombia. Ph.D en Business Administration por Newport University, CA. USA. y Ph.D en Educación por la Universidad Santo Tomás. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners y Certified Internal Control Auditor (CICA) por The Institute of Internal Controls. Profesor Distinguido de la Facultad de Derecho, Universidad de los Andes. Es director de la Revista SISTEMAS de la Asociación Colombiana de Ingenieros de Sistemas–ACIS–.