La cadena de suministro digital

DOI: 10.29236/sistemas.n164a6

Perspectivas y reflexiones desde el riesgo cibernético.

Resumen
En medio de las tensiones internacionales y la dinámica de los negocios actuales, la cadena de suministro se convierte en un factor determinante para mantener las economías globales y la entrega de productos y servicios a los ciudadanos de los diferentes países. La emergencia sanitaria internacional llevó a los participantes de esta cadena a reconocer y acelerar sus procesos de transformación digital con el fin de mejorar su agilidad y la gestión de sus costos. En este sentido, una cadena de suministro digital (CSD) no sólo genera nuevas oportunidades para sus diferentes actores, sino una ampliación de la superficie de ataque que revela una mayor exposición y retos para concretar su operación a nivel global. En consecuencia, este artículo desarrolla una breve reflexión sobre el riesgo cibernético en la CSD y sus diferentes escenarios de operación para alcanzar una postura resiliente frente a la materialización de eventos cibernéticos.

Palabras clave
Cadena de suministro, resiliencia, reductores, amplificadores, riesgo cibernético

Introducción

Hoy en medio de las tensiones internacionales y las inestabilidades geopolíticas las cadenas de suministro se han hecho más visibles y sensibles, comoquiera que la interrupción que se genere en ellas termina afectando la dinámica comercial y global de todas las naciones con repercusiones que comprometen la vida de sus ciudadanos. Basta con mirar las diferentes fortalezas y centros de poder internacional basado en productos agrícolas como los cereales, los hidrocarburos, la fabricación de semiconductores, la producción de bienes de uso en el hogar, para observar cómo cambian las posturas de los gobiernos para proteger sus economías y la estabilidad de sus naciones (Shih, 2022).

La pandemia del Covid-19 hizo evidente que la cadena de suministro global y sus representaciones locales, se convierten en articuladores del bienestar de los países. Sin una adecuada coordinación y automatización de procesos, queda expuesta la entrega de los productos o servicios comprometidos. Las vacunas, los tapabocas, los respiradores y el material quirúrgico y de asistencia médica se vieron envueltos en los enredos internacionales y prioridades que los productores (centros de poder) pusieron sobre la mesa, creando inestabilidad global, generando inequidad y un circuito de demanda y oferta acelerada e inestable que la cadena de suministro tuvo que sortear (Alicke et al., 2020b).

En este contexto, la cadena de suministro tuvo que avanzar rápidamente en su transformación digital con el fin de hacer más fácil y ágil su desarrollo, para generar menores costos y cargos para sus usuarios. Sin embargo, un estudio de Mckinsey confirma los retos y debilidades que las cadenas de suministro identificaron frente a esta realidad del trabajo remoto y sin contacto en medio del Covid-19: (Alicke et al., 2020b)

- 73 por ciento experimentó problemas con su base de proveedores.
- 75 por ciento dificultades asociadas a la producción y la distribución.
- En las industrias de alimentos y bienes de consumo, el 100 por ciento de los participantes tuvieron problemas de producción y distribución, y el 91 por ciento con sus proveedores.
- 85 por ciento de los entrevistados debió lidiar con tecnologías digitales ineficientes en sus cadenas de suministro.

Lo anterior muestra un panorama de inercia y comodidad que permanecía latente y acostumbrado a los tiempos y movimientos de un sector, que tuvo que cambiar y renovarse de forma acelerada para

pasar de una postura de continuidad de las operaciones, a una basada en resiliencia y digitalización. En este sentido, la cadena de suministro empezó a entender la realidad sistémica que ella representa en sí misma, y cómo se encuentra interconectada con los retos y expectativas a nivel global.

En consecuencia, este breve artículo presenta la convergencia entre lo físico y lo lógico que implica la transformación digital de la cadena de suministro, y cómo el riesgo cibernético y los ciberataques se abren paso en medio de una acelerada incorporación de tecnologías para crear inestabilidades y tensiones geopolíticas que deben ser atendidas desde la cadena misma y sus participantes para identificar y privilegiar amplificadores de resiliencia e identificar y disminuir sus reductores, con el fin de mantener la dinámica de sus operaciones ahora y en el futuro.

Fundamentos básicos de la cadena de suministro

Si bien existen múltiples definiciones alrededor de este tema, se advierten algunos acuerdos que definen la cadena de suministro como "una red de compañías autónomas, o semiautónomas, responsables de la obtención, producción y entrega de un determinado producto y/o servicio al cliente final" (Valles, s.f.). Una definición que reconoce el carácter sistémico del concepto y el reto que implica comprender no sólo sus diferentes componentes, sino las relaciones que hacen realidad del producto o servicio en el cliente final.

En la cadena de suministro se advierten al menos cinco temas clave a tener en cuenta que definen su capacidad de resiliencia, los cuales deben ser atendidos por todo el sistema, para efectos de hacer evidentes las vulnerabilidades inherentes a su dinámica y cómo rebotar y responder de forma ágil frente a la inevitabilidad de la falla. Los temas son: (Alicke et al., 2020)

- Planeación y red de proveedores
  - ¿Cuán predecible es la planeación de la demanda?
  - ¿Qué tan compleja o concentrada está la red de abastecimiento, y cuan resiliente es a la disrupción?
  - ¿Qué tan expuesta está la red a derechos de aduana y otras inestabilidades comerciales?
- Transporte y logística
  - ¿Qué tan resiliente son los flujos físicos y la red logística?
- Resiliencia financiera
  - ¿Qué grado de flexibilidad financiera posee la compañía para hacer frente a mayores costos de la cadena de suministro o a inestabilidades sostenidas?
- Complejidad de productos
  - ¿Los componentes de los productos son reemplazables?
  - ¿Qué grado de flexibilidad posee el diseño si los componentes originales ya no estuvieran disponibles?

- ¿Qué tan vulnerable es el producto a cambios regulatorios?
• Madurez organizacional
- ¿Qué tan proactivas o reactiva es la organización para identificar y mitigar disrupciones en la cadena de abastecimiento?

Las respuestas a estos interrogantes establecen el nivel de preparación y respuesta que tiene la cadena de suministro para enfrentar inestabilidades que puedan afectar su promesa de valor con el cliente. En este sentido, los temas asociados con el factor humano, la incorporación de tecnologías y los posibles escenarios geopolíticos, deberán estar en la agenda estratégica de los ejecutivos de las empresas que articulan esta cadena, de tal forma, que cada volatilidad e incierto a nivel global se traduzca en una respuesta concreta y clara que permitan fortalecer los esfuerzos logísticos globales, y no en un excusa que termine con el compromiso de los productos y servicios requeridos a nivel global.

Por tanto, "para mejorar la planeación de contingencias bajo circunstancias en constante evolución, la visibilidad en tiempo real dependerá no solo de medir la puntualidad del transporte en tránsito, sino también de monitorear cambios más amplios, como congestión de aeropuertos o cierres de fronteras. Mantener un abordaje ágil para la gestión logística será imperativo para adaptarse con rapidez a cualquier cambio de situación o de contexto" (Alicke et al., 2020).

Transformación digital de la cadena de suministro: Mayor superficie de ataque

Si bien "digitalizar la gestión de la cadena de abastecimiento mejora la velocidad, la precisión y la flexibilidad de la gestión del riesgo" (Alicke et al., 2020), no es la optimización de las operaciones lo que termina por concretar el valor de la transformación, sino el ecosistema que se construye alrededor de los diferentes actores, lo que define la manera como se hace más rentable y resiliente la cadena de suministro. En esta medida, cuando los diferentes proveedores pueden compartir sus capacidades y reconocerse entre ellos, es posible hablar de una transformación exitosa del sector.

Sin perjuicio de lo anterior, cuando se articulan en un ecosistema estratégico tecnologías como el internet de las cosas, los grandes datos y la analítica, la automatización industrial, los vehículos no tripulados y drones, la computación en la nube y el blockchain (ALC, 2020), no sólo se establece un nuevo referente de cambio y evolución de la cadena de suministro para todos los participantes, sino una superficie de ataque extendida que se traduce en relaciones e interconexiones visibles e invisibles que pueden y serán aprovechadas por los adversarios.

En este sentido, se hace imperativo incluir dentro de los retos de la cadena de suministro comprender la dinámica del riesgo cibernético, para lo cual se hace necesario reconocer quiénes son los adversarios más relevantes y sus capacidades, para identificar las vulnerabilidades propias del ecosistema de proveedores, las complejidades de las interacciones con el mundo físico y su convergencia con la realidad, y sobremanera establecer los nuevos referentes de controles y prácticas de ciberseguridad que se requieren para hacer más resistente la cadena frente a los planes de los atacantes ahora y en el futuro (WEF, 2021).

Si bien, existe una idea errónea, reiterada por la cobertura mediática de los incidentes cibernéticos, de que la ciberseguridad consiste únicamente en la tecnología, la cadena de suministro revela el carácter sistémico de las interacciones y los efectos cascada que se pueden tener en cada uno de sus componentes. El concepto de "contagio del riesgo" es una característica concreta que advierte en la cadena de suministro la necesidad de estar alienados y vigilantes en el ecosistema frente al nivel de acoplamiento e interacción de los componentes, y así saber, cómo una inestabilidad o falla puede causar y propagar un daño específico (Boyes, 2015).

Por tanto, una ciberseguridad en la cadena de suministro se basa en un enfoque holístico que abarca aspectos humanos, de proceso, físicos y tecnológicos que permita aumentar la confianza no sólo en los participantes del ecosistemas digital requerido para cumplir con la promesa de valor, sino en los clientes finales que terminan por obtener el producto y/o servicio por el cual han pagado (Alicke et al., 2016). Sin una perspectiva holística de la cadena de suministro, y sin una comprensión ecosistémica de sus interacciones, las capacidades de defensa que se establezcan no tendrán la fuerza y la sostenibilidad para hacerse más resistente frente a la agenda oculta de los agentes estatales o no estatales para desestabilizar organizaciones, sectores o naciones.

Cadena de suministro digital: amplificadores y reductores de la resiliencia

Un ciberataque exitoso en la cadena de suministro digital puede tener un gran impacto en la continuidad de las operaciones, incluida la seguridad del personal y los activos (es decir, la disponibilidad, la seguridad operacional y la resiliencia). Por ejemplo, una grave afectación de los controles de acceso a los sistemas de control industrial de una planta, puede provocar su mal funcionamiento y provocar daños físicos e interrupciones operativas, que comprometan la infraestructura y a los diferentes aliados estratégicos articulados para lograr sus productos y servicios (Boyes, 2015).

En este sentido, se hace necesario reconocer en una vista holística de la cadena de suministro cuáles son los amplificadores de la resiliencia y cuáles sus reductores con el fin de reconocer en su diseño aquellas áreas que son vulnerables, volátiles, sensitivas o resilientes. De esta forma, los participantes de este sistema logístico y abastecimiento puede advertir las debilidades y tomar las decisiones correspondientes para incorporar más amplificadores de resiliencia que permitan una mayor capacidad de absorción de eventos inesperados y así mejorar la capacidad de rebote y recuperación de las operaciones (Blackhurst et al., 2011).

Un *amplificador de resiliencia* es todo aquel factor o actividad que reduce el impacto de una disrupción o perturbación en la cadena, aumentando su capacidad resiliente, mientras un reductor de resiliencia hace referencia todos aquellos factores que amplifican el impacto de una interrupción y, por tanto, restan resiliencia a la cadena de suministro (Blackhurst et al., 2011). En este sentido, en la medida que se identifiquen y privilegien amplificadores de resiliencia en la cadena, ahora articulada y transformada con tecnología, habrá mayor oportunidad para una absorción de la inestabilidad y recuperación ágil de la cadena.

Los amplificadores de resiliencia están relacionados con las personas, las capacidades y planes internos de la organización, así como sus relaciones con aliados estratégicos, y con activos físicos y la tecnologías de soporte al monitoreo y gestión de los riesgos (Blackhurst et al., 2011). En esta línea, algunos ejemplos de estos amplificadores son:

- Educación y entrenamiento
- Protocolos de comunicación
- Planes de contingencia
- Monitorización de nodos
- Equipos interdisciplinares de riesgo

Por otra parte, los *reductores de resiliencia* están relacionados con el flujo de las actividades en la cadena, el número de nodos que producen los flujos y la volatilidad del contexto donde se originan o sitúan los nodos (Blackhurst et al., 2011). En la medida que haya mayores flujos de operación y más nodos intervengan en esas interacciones, habrá menos capacidad de respuesta resiliente, pues los efectos de la propagación de un evento inesperado serán directamente proporcional a su interacción y acoplamiento en toda la cadena. Algunos ejemplos de reductores de resiliencia son:

- Mayor número de nodos
- Regulaciones estrictas
- Productos complejos
- Volatilidad de la ubicación del proveedor

- Capacidad del proveedor

Así las cosas, en el siguiente cuadro se concreta el análisis de la resiliencia de la cadena de suministro en el contexto digital, donde se ubican los cuadrantes claves que revelan el diagnóstico particular para cada uno de los componentes de la cadena frente a su sensibilidad en la materialización de un ataque cibernético (Figura 1).

Desde el punto de vista digital, una cadena de suministro será *vulnerable* en la medida que existan mayor cantidad de nodos presentes, cuyo acoplamiento e interacción son altas (reductores), y existen pocos o nulos amplificadores que permitan capacidad de rebote o reacción frente a un evento cibernético adverso. Esto se traduce en pocos controles o prácticas básicas de seguridad y control aplicadas y debidamente aseguradas, así como bajos niveles de ejercicios o simulaciones para enfrentar posibles ataques cibernéticos en el desarrollo de sus actividades.

La cadena será *volátil* cuando existan una cantidad importante de reductores disponibles y activos en el componente analizado y así mismo, múltiples amplificadores disponibles y funcionales en la cadena de suministro analizada. En el contexto digital de la cadena, esto se explica en un escenario incierto e impredecible, pues podrá haber controles y prácticas disponibles de seguridad y control, que posiblemente no estén articuladas con los

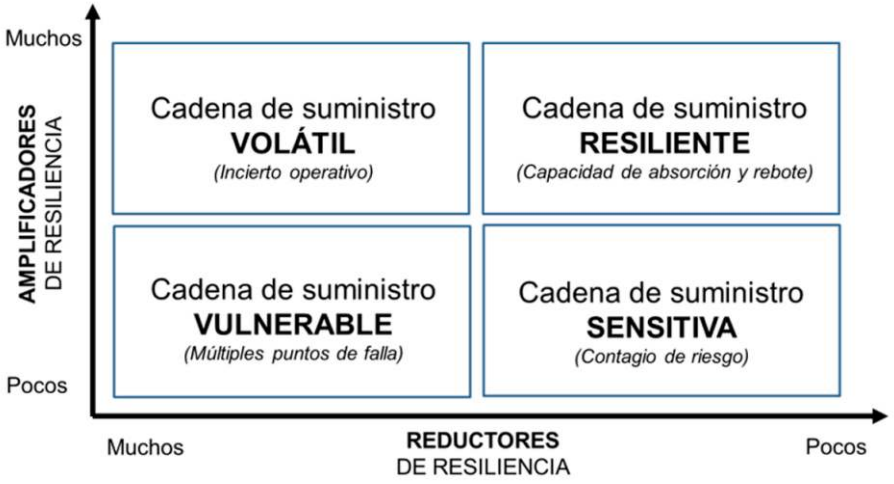

Figura 1. Matriz de resiliencia de la cadena de suministro digital
(Traducción libre de: Blackhurst et al., 2011)

reductores detectados, creando una zona de incertidumbre de efectos de un ataque cibernético, donde no es viable identificar con claridad dónde se concentrarán los esfuerzos de aseguramiento de los procesos digitalmente transformados.

La cadena será *sensitiva* o frágil cuando el análisis de sus componentes esté marcado tanto por pocos reductores como amplificadores de resiliencia, lo que advierte una propagación del "contagio del riesgo" de forma acelerada e incierta. Incluso las pequeñas interrupciones podrían aumentar su gravedad y propagarse tanto en sentido ascendente como descendente dentro de la cadena de suministro, llevando a que un evento pueda terminar siendo catastrófico. Desde el punto de vista digital, este es el escenario de mayor compromiso y daño que puede terminar con la operación y toma de control por parte del adversario.

Finalmente la cadena será *resiliente*, en la medida que cuente con pocos reductores y altos amplificadores de resiliencia, lo que implica un compromiso y balance de la inversión de medidas de seguridad y control, basado en el conocimiento del nivel de acoplamiento e interacción de sus componentes, lo que la habilita para absorber los impactos de eventos cibernéticos adversos y volver a condiciones estables rápidamente, y así, preparar a la organización para actuar en medio de la inestabilidad y concretar una ventaja competitiva única para sus participantes en un ecosistema.

Reflexiones finales

Las naciones y empresas resilientes comparten algunas características claves, que deben ser igualmente atendidas por las cadenas de suministro en el contexto digital.

Dichas características implican la capacidad de articular dos ciclos de acción de forma permanente y articulada: el *feedback* y el *feedforward*, el primero para actuar frente situaciones conocidas y el segundo para preparar a la organización frente a eventos que aún no existen. Las características son: (Fiskel, 2015)

- Anticipan cambios disruptivos
- Reconocen nuevas oportunidades
- Construyen relaciones sólidas
- Adaptación efectiva frente a turbulencias
- Desarrollan posturas disruptivas

En este sentido las cadenas de suministro en el contexto digital deberán incorporar y fortalecer múltiples amplificadores de resiliencia, con el fin de mejorar su capacidad de absorción de los efectos de los eventos cibernéticos adversos, sabiendo todo el tiempo que los reductores estarán presente creando

escenarios agrestes que podrán ser capitalizados en cualquier momento por los adversarios.

La incorporación de tecnologías emergentes y algunas disruptivas en la cadena de suministro actual darán mayores y mejores oportunidades a los participantes para disminuir sus costos y aumentar la eficiencia de sus resultados. Sin perjuicio de lo anterior, igualmente van incorporar nuevos puntos de vulnerabilidad antes desconocidos que deberán ser parte de los análisis de la cadena y sus diferentes participantes (Durbin, 2022), ahora en un ecosistema transformado donde es necesario saber cómo cada uno afecta a los demás y cómo las relaciones definen y marcan dinámicas particulares según el diagnóstico entre reductores y amplificadores de resiliencia.

Al ser el riesgo cibernético un riesgo sistémico, emergente y disruptivo es natural que en una cadena de suministro digital (un sistema complejo y tecnológicamente transformado) sea parte integral de su comprensión y análisis, habida cuenta que en la medida que se conocen sus interacciones, nivel de preparación y capacidad de respuesta, es posible no sólo responder a las inestabilidades del entorno, sino establecer un marco de anticipación y acción que incluya las vulnerabilidades de las tecnologías implicadas, la ubicación física de los elementos críticos para el negocio, la interdependencia de los componentes y los procesos de negocio, así como las habilidades requeridas por el personal involucrado en las operaciones de la cadena de suministro (Boyes, 2015).

Así las cosas, una cadena de suministro digital resiliente es un compromiso de múltiples grupos de interés y participantes por mantener un conjunto de prácticas y comportamientos asociados con una postura vigilante en un ecosistema digital que constantemente desarrolle al menos cuatro capacidades claves como apoyo a los amplificadores de resiliencia revisados. Las capacidades son: (Cano, 2021)

- Defensa – Que responda frente a los eventos conocidos y correlacionados, así como tecnologías que responda y detenga aquellos patrones de ataques ya perfilados y revisados por la industria.

- Radar – Que mantenga una vista exploratoria y proactivas que identifique patrones emergentes y señales débiles relevantes para analizar y actuar en consecuencia.

- Crisis – Que permita actuar de forma coordinada, bien documentada y comunicaciones debidamente preparadas cuando se concreta un evento cibernético adverso.
- Monitorización – Que mantenga un conjunto de alertas definidas en los diferentes puntos sensi-

bles de la cadena, así como las alertas necesarias para actuar cuando un incidente ha ocurrido.

Referencias

ALC (2020). ALC 2030 Construyendo las cadenas de suministro del futuro. Banco Interamericano de desarrollo. Relatoría del evento. https://publications.iadb.org/publications/spanish/document/ALC_2030_Construyendo_las_cadenas_de_suministro_del_futuro_es.pdf

Alicke, K., Azcue, X. & Barriball, E. (2020). La recuperación de la cadena de suministro en tiempos de coronavirus – planificar para el presente y para el futuro. Mckinsey Operations. https://www.mckinsey.com/business-functions/operations/our-insights/supply-chain-recovery-in-coronavirus-times-plan-for-now-and-the-future/es-CL

Alicke, K., Gupta, R. & Trautwein, V. (2020b). Reseteando las cadenas de suministro para la nueva normalidad. Mckinsey Insights. https://www.mckinsey.com/business-functions/operations/our-insights/resetting-supply-chains-for-the-next-normal/es-ES

Alicke, K., Rachor, J. & Seyfert, A. (2016). Supply Chain 4.0 – the next-generation digital supply chain. Mckinsey research. https://www.mckinsey.com/~/media/mckinsey/business%20functions/operations/our%20insights/supply%20chain%2040%20%20the%20next%20generation%20digital%20supply%20chain/08b1ba29ff4595ebea03e9987344dcbc.pdf

Blackhurst, J., Dunn, K. & Craighead, C. (2011). An Empirically Derived Framework of Global Supply Resiliency. Journal of Business Logistics. 32(4). 374–391. Doi: 10.1111/j.0000-0000.2011.01032.x

Boyes, H. (2015). Cybersecurity and Cyber-Resilient Supply Chains. Technology Innovation Management Review, 5(4): 28-34. http://doi.org/10.22215/timreview/888

Cano, J. (2021). Modos de operación de la ciberseguridad empresarial. Capacidades básicas para navegar en el contexto digital. Global Strategy. Global Strategy Report No. 44. https://global-strategy.org/modos-de-operacion-de-la-ciberseguridad-empresarial-capacidades-basicas-para-navegar-en-el-contexto-digital/

Durbin, S. (2022). 5 trends making cybersecurity threats riskier and more expensive. CSO Online. https://www.csoonline.com/article/3667442/5-trends-making-cybersecurity-threats-riskier-and-more-expensive.html

Fiskel, J. (2015). Resilient by design. Creating Businesses That Adapt and Flourish in a Changing World. Washington, D.C., USA: Island Press. https://www.iebschool.com/blog/cadena-gestion-suministro-negocios-internacionales/

Shih, W. (2022). Are the Risks of Global Supply Chains Starting to Outweigh the Rewards? Harvard Busines Review. https://hbr.org/2022/03/are-the-risks-of-global-supply-chains-starting-to-outweigh-the-rewards

Valles, J. (s.f.) Fundamentos de la Cadena de Suministros. Ingeniería en Logística y Transporte. https://www.academia.edu/30079564/Fundamentos_de_la_Cadena_de_Suministros

WEF (2021). Digital Traceability: A Framework for More Sustainable and Resilient Value Chains. White paper.

https://www.weforum.org/whitepapers/digital-traceability-a-framework-for-more-sustainable-and-resilient-value-chains/

***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–.*